

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Ron M. Redlich, et al.

Serial No.:

(Proposed AU 2137)

Filed: Herewith

For: Data Security System and Method

TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a divisional patent application claiming the benefit of Serial No. 09/916,397, filed July 27, 2001, now pending.

I HEREBY CERTIFY that the below listed documents are being electronically filed with the Patent and Trademark Office on August 17, 2006.

- X Patent application (72 pgs.; 145 clms.)
(spec. 46 pgs., pp. 1-46; claims 24 pgs., pp. 47 - 70; abstract 1 pg., p. 71)
- X Five (5) sheets drawings - formal (5 pgs.)
- X Unsigned Declaration and Power of Attorney for Patent Application (2 pgs.)
- X Information Disclosure Statement with PTO Form 1449 (8 pgs) (10 non-patent references)
- X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231.

Respectfully submitted,

By /Robert Kain/
Robert C. Kain, Jr.
Reg. No. 30,648
FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI & BIANCO, P.L.
750 S.E. Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-div2-Transmittal.wpd

DATA SECURITY SYSTEM AND METHOD

[0001] This patent application is a divisional patent application based upon and claiming the benefit of application serial no. 09/916,397, filed July 27, 2001, now pending and is based upon and claims priority of provisional patent application No. 60/260,398, filed June 5, 2001; application No. 60/287,813, filed on May, 2, 2001; application No. 60/267,944, filed February 12, 2001; application No. 60/247,242, filed November 13, 2000 and application No. 60/247,232, filed November 13, 2000.

[0002] The present invention relates to a data security system and method and, more specifically, the extraction and controlled release of data, on a granular basis, utilizing security protocols.

Background of the Invention

[0003] The extensive use of computers and the continued expansion of telecommunications networks, particularly the Internet, enable businesses, governments and individuals to create documents (whether text, characters, icons, images or a combination thereof, sound, video, and data objects in general, sometimes referred to generally herein as “data objects”) and distribute those documents widely to others. Although the production, distribution and publication of documents is generally beneficial to society, there is a need to limit the distribution and publication of security sensitive words, characters or icons. Concerns regarding the privacy of certain data (for example, an individual’s social security number, credit history, medical history, business trade secrets and financial data) is an important issue in society. In another words, individuals and businesses have a greater concern regarding maintaining the secrecy of certain information in view of the increasing ease of distribution of documents through computer networks and the Internet.

[0004] U.S. Patent No. 6,055,544 to DeRose et al. discloses the generation of chunks of a long document for an electronic book system. DeRose ‘544 discloses solutions available to book

publishers to publish books in electronic format on the worldwide web. One of the problems is that the books are published as small document fragments rather than publishing an entire book which, due to the formatting, protocol and command structure on the Internet, downloads an entire book to the user. The problem involved with publishing small documents is that there is no relationship to other portions of the book. See col. 3, lines 51-55 and col. 4, lines 3-5. One methodology to solve the problem involves inserting hypertext links in the book. This places a large burden on the book publisher. Col. 4, lines 19-21. Accordingly, it is an object of DeRose '544 to provide a mechanism for accessing only a portion of a large, electronically published document and automatically determining what portion of the document to download to the user based upon user selections that is, previous portions and subsequent portions of the document are downloaded with the selected portion, without maintaining separate data files for each portion of the document. Col. 4, lines 34-39. In other words, if a person wanted to access chapter 4 of a text, the system in DeRose '544 would display chapter 4, chapter 3 (the preceding chapter) and chapter 5 (the subsequent chapter). This publishing of portions of the document utilizes a subset of marked up elements established as being significant and a second subset of elements being less significant. For example, "Title elements" define a table of contents. A first representation of the document structure defined by all of the marked up elements may be used in combination with a second representation of the document structure defined only by the significant elements to control selection of portions of the documents such that previous and subsequent portions may be selected and rendered in a consistent and intuitive manner." Col. 4, lines 38-55. A computer system stores a first representation of the hierarchy of all elements in the electronic document. As example, this may be each chapter in its entirety. The computer also stores a second representation of the hierarchy of only significant elements in the electronic document. As an example, this may be a listing of each chapter without

the text associated with the chapter. In response to request for a portion of the document, the computer system selects the portion defined by the significant element in the second representation. For example, if the user requested chapter 4, the entirety of chapter 4 would be downloaded from the web server to the client computer. In addition to rendering or publishing the selected chapter, the computer system looks to the relationship of the elements in the first representation of the hierarchy (the list of all chapters) and downloads from the web server the adjacent chapters. In this example, this would involve downloading chapters 3 and chapter 5. In a further embodiment, the computer system selects only a leaf element of the second representation as a significant element during the download. See the Summary of the Invention, col. 4, line 40 through col. 6, line 14.

[0005] U.S. Patent No. 5,832,212 to Cragun et al. discloses a censoring browser method for viewing downloaded and downloading Internet documents. The abstract describes the system as including a user profile including user selected censoring parameters. Data packet contents are received from the Internet and the packets are compared with the user selected censoring parameters. Responsive to the comparison, the received data packet contents are processed and selectively displayed. The user selected censoring parameters include censored words and word fragments, and user selected categories. Compared word and word fragments can be removed and selectively replaced with predefined characters or acceptable substitute words. Tallies of weights for user selected categories are accumulated and compared with user selected threshold values. A predefined message can be displayed responsive to an accumulated tally exceeding a user selected threshold value without displaying the received data packet contents.

[0006] U.S. Patent No. 6,094,483 to Fridrich discloses an encryption methodology hiding data and messages in images. In one application of the system in Fridrich '483, a method is disclosed of embedding a secret digital square image with 256 gray levels within an image carrier.

The secret image is first encrypted using a chaotic Baker map. The resulting image is a random collection of pixels with randomly distributed gray levels without any spatial correlations. The carrier image which is twice the size (height and width or $2n \times 2m$) the secret image with 256 gray levels. The carrier image is modified according to a mathematical formula.

[0007] U.S. Patent No. 5,485,474 to Rabin discloses a scheme for information dispersal and reconstruction. Information to be transmitted or stored is represented as N elements of a field or a computational structure. These N characters of information are grouped into a set of n pieces, each containing m characters. col. 1, lines 37-46. The system is used for fault tolerance storage in a partitioned or distributed memory system. Information is dispersed into n pieces so that any m pieces suffice for reconstruction. The pieces are stored in different parts of the memory storage medium. A fairly complex mathematical algorithm is utilized to provide reconstruction of the information utilizing no fewer than m pieces.

[0008] U.S. Patent No. 6,192,472 B1 to Garay et al. discloses a method and apparatus for the secure distributed storage and retrieval of information. Garay '472 identifies the problem as how to store information in view of random hardware or telecommunications failures. Col. 1, lines 17-20. The initial solution is to replicate the stored data in multiple locations. Col. 1, lines 28-31. Another solution is to disperse the information utilizing in Information Dispersal Algorithm (IDA). The basic approach taking in IDA is to distribute the information F being stored among n active processors in such a way that the retrieval of F is possible even in the presence of up to t failed (inactive) processors. Col. 1, lines 40-44. Another issue is the utilization of cryptographic tools. With the use of tools called distributed fingerprints (hashes), the stored data is distributed using the fingerprints and coding functions to determine errors. In this way, the correct processors are able to reconstruct the fingerprint using the code's decoding function, check whether the pieces of the

file F were correctly returned, and finally reconstruct F from the correct pieces using the IDA algorithm. Col. 2, lines 50-59. Garay '472 also discloses the use of Secure Storage and Retrieval of Information (SSRI) with the added requirement of confidentiality of information. Col. 3, line 56. With this added requirement, any collision of up to t processors (except ones including the rightful owner of the information) should not be able to learn anything about the information. Confidentiality of information is easily achieved by encryption. Col. 3, lines 56-61. The issue involves encryption key management, that is, the safe deposit of cryptographic keys. Garay '472 discloses confidentiality protocol utilizing distributed key management features. This mechanism allows the user to keep his or her decryption key shared among several n servers in such a way that when the user wants to decrypt a given encrypted text, the user would have to interact with a single server (the gateway) to obtain the matching plaintext while none of the servers (including the gateway) gets any information about the plaintext. Col. 4, lines 5-14.

[0009] U.S. Patent No. 5,996,011 to Humes discloses a system and a method for filtering data received over the Internet by a client computer. The system restricts access to objectionable or target data received by a client computer over an Internet by a web server by filtering objectionable data from the data received. The Humes '011 system filters the data "on the fly." Further, the Humes '011 system can be applied to process any type of target data from the data received and displayed to the user. Col. 2, lines 32-44. If the web page requested by the user contains only a minimum amount of objectionable or target data, the user receives only a portion of the filtered web page for viewing. Hume '011 also provides that if the web page contains a large amount of objectionable material, the system blocks the entire display of the web page on the user's computer monitor. Col. 2, lines 56-62. Hume '011 provides three levels of filtering. At the first level, if the domain name contains objectionable words or material, the initial download from the

domain is blocked. At the second level, the text in the download is filtered and objectionable words are replaced with a predetermined icon, for example, “----“. Col. 3, lines 32-35. The filter uses a dictionary. Col. 3, lines 45-48. The filtered out words are counted. If the final score of “filtered out” material exceeds a predetermined threshold, the entire page is blocked from the user’s view. Col. 4, lines 2-4.

[0010] U.S. Patent No. 5,905,980 to Masuichi, et al., discloses a document processing apparatus for processing various types of documents, a word extracting apparatus for extracting a word from a text item including plural words, a word extracting method used in the document processing apparatus, and a storage medium for storing a word extracting program. Extracted words are associated with other words via an algorithm. The extracted words and associated words are used as a search index for the document.

[0011] U.S. Patent No. 5,996,011 to Humes discloses a computer based system and method for filtering data received by a computer system, and in particular, for filtering text data from World Wide Web pages received by a computer connected to the Internet, for purposes of restricting access to objectionable web sites.

[0012] U.S. Patent No. 6,148,342 to Ho discloses a system for managing sensitive data. The system prevents a system administrator from accessing sensitive data by storing data and identifier information on different computer systems. Each query from a user’s terminal is encrypted using two codes, the first code readable only by an identifier database and a second code readable only by a data access database. The data is routed from the user’s source terminal to the identifier database at the first computer. The first computer/identifier database first verifies the user’s ID and the security clearance for the requested information and substitutes a second internal ID to the data

packet/query. The modified query is then presented to the data access database (the second computer) and, subject to a second security clearance, the response to the data query is sent back to the user's source terminal.

[0013] A publication entitled "Element-Wise XML Encryption" by H. Maruyama T. Imamura, published by IBM Research, Tokyo Research Laboratory, April 20, 2000 discloses a protocol or process wherein certain parts of an XML document are encrypted and the balance of the plaintext is not encrypted. The protocol is useful in three party transactions, for example, when a buyer sends an order in an XML document to a merchant which contains the buyer's credit card information. The credit card information is sent to a credit company and the merchant does not need to know the credit number as long as he obtains clearance or authorization from the credit card company. Another instance is an access control policy which requires a certain part of an XML document to be readable only by a privileged user (for example, a manager could access the salary field in an employee records but others could only access name, phone and office fields). The Imamura article discusses encryption protocol, the delivery of keys and the utilization of compression. The article does not discuss separate storage of the critical data apart from the plaintext of the XML document.

[0014] The Ingrain i100 Content Security Appliance product brochure, available in June, 2001, discloses a system coupled to multiple web servers (computers) to accelerate secured transactions between multiple client computers (over the Internet) and prevents Secure Sockets Layer SSL performance bottlenecks by performing high-performance SSL handshakes and encrypting all data sent to back end servers using long-lived SSL session.

[0015] An article entitled “Survivable Information Storage Systems” by J. Wylie M. Bigrigg, J. Strunk, G. Ganger, H. Kiliccote, and P. Khosla, published August, 2000 in COMPUTER, pp. 61-67, discloses a PASIS architecture which combines decentralized storage system technologies, data redundancy and encoding and dynamic self-maintenance to create survivable information storage. The Bigrigg article states that to achieve survivability, storage systems must be decentralized and must spread information among independent storage nodes. The decentralized storage systems partition information among nodes using data distribution and redundancy schemes commonly associated with disc array system such as RAID (redundancy array of independent discs) insuring scalable performance for tolerance. P. 61. Thresholding schemes - also known as secret sharing schemes or information dispersal protocols - offer an alternative to these approaches which provide both information confidentiality and availability. These schemes and codes, replicate, and divide information to multiple pieces or shares that can be stored at different storage nodes. The system can only reconstruct the information when enough shares are available. P. 62. The PASIS architecture combines decentralized storage systems, data redundancy and encoding and dynamic self-maintenance to achieve survivable information storage. The PASIS system uses threshold schemes to spread information across a decentralized collection of storage nodes. Client-side agents communicate with the collection of storage node to read and write information, hiding decentralization from the client system. P. 62. The device maintains unscrutable audit logs --that is, they cannot be erased by client-side intruders -- security personnel can use the logs to partially identify the propagation of intruder-tainted information around the system. P. 63. The article states that, as with any distributed storage system, PASIS requires a mechanism that translates object names -- for example file names -- to storage locations. A directory service maps the names of information objects stored in a PASIS system to the names of the shares that comprised the

information object. A share's name has two parts: the name of the storage node on which the share is located and the local name of the share on the storage node. A PASIS file system can embed the information needed for this translation in directory entries. P.63. To service a read request, the PASIS call client (a) looks up in the directory service the names of the n shares that comprise the object; (b) sends read requests to at least m of the n storage nodes; (c) collects the responses and continues to collect the responses until the client has collected m distinct shares; and (d) performs the appropriate threshold operation on the received shares to reconstruct the original information.

P. 63. The p - m - n general threshold scheme breaks information into n shares so that (a) every shareholder has one of the n shares; (b) any m of the shareholders can reconstruct the information; and (c) a group of fewer than p shareholders gains no information. P. 64. Secret-sharing schemes are p - m - n threshold schemes that trade off information confidentiality and information availability: the higher the confidentiality guaranty, the more shares are required to reconstruct the original information object. Secret sharing schemes can be thought of as a combination of splitting and replication techniques. P. 64. The article discusses the technique of dissemination which divides information objects into n pieces and stores each piece separately. Dissemination decreases information availability because all shares must be available. It offers no information theoretic confidentiality because each share expresses $1/n$ of the original information. P. 64. Short secret sharing encrypts the original information with a random key, stores the encryption key using secret sharing, and stores the encrypted information using information disperse. P. 64. An extension to the threshold schemes is cheater detection. In a threshold scheme that provides cheater detection, shares are constructed in such a fashion that a client reconstructing the original information object can tell, with high probability, whether any shares have been modified. This technique allows strong information integrity guarantees. Cheater detection can also be implemented using cryptographic

techniques such as adding digest to information before storing it. P. 65. For the highest architecture to be effective as possible, it must make the full flexibility of threshold schemes available to clients. The article believes this option requires automated selection of appropriate threshold schemes on a per object basis. This selection would combine object characteristics and observations about the current system environment. For example, a client would use short secret sharing protocol to store an object larger than a particular size and conventional secret sharing protocol to store smaller objects. The size that determines which threshold scheme to use could be a function of object type, current system performance, or both. P. 67.

Objects of the Invention

[0016] It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.

[0017] It is another object of the present invention to provide a method for securing data on a single personal computer (PC), on a plurality of computers linked together through a local area network (LAN) or a wide area network (WAN).

[0018] It is a further object of the present invention to provide a method for securing data utilizing a client-server computer system. The client-server computer system may be implemented over the Internet.

[0019] It is a further object of the present invention to provide a method for securing data which is highly flexible and programmable by a user.

[0020] It is an additional object of the present invention to enable the user to establish (a) the scope of the security sensitive words, characters or icons, (b) the future use (or destruction) of

a filter enabling extraction of security sensitive data, (c) the selection of storage locations for extracted data and remainder or common data and (d) one or multiple levels of security limiting full reconstruction and enabling partial reconstruction of the extracted data and the remainder or common data.

[0021] These steps may be completely automated (after some parameters are set or programmed by a system administrator), may be fully programmable by the user, or may be a combination of automated and manual controls implemented by the systems administrator and/or the user-client.

Summary of the Invention

[0022] The method for securing data in a computer system includes establishing a group of security sensitive words, characters or icons, filtering the data input from a data input device and extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored. In one embodiment on a personal computer (PC) system, the extracted data and the remainder or common data is stored in different, distributed memory segments. In a network implementation, the extracted data may be stored in one computer and the remainder or common data may be stored in another computer. In a client-server implementation, the server may direct storage of the extracted data to a different location than the remainder data, either on the server or on a further memory system (computer) interconnected to the server or on the client computer and in distributed memory segments. A map may be generated by a software module or sub-system indicating the location of the extracted data and the remainder data in the network. The filter may be destroyed (via a deletion routine) or may be retained for future use by the user. The map may be stored on the client computer or the user's PC or may be stored on the server. Copies of the map may be removed (deleted) from the user's PC or the client computer. The extracted data and/or the

remainder data may be removed (deleted or scrubbed) from the originating computer. Encryption can be utilized to further enhance the security levels of the system. All transfers of the filter between the client to the server may be encrypted, and all data (whether extracted data or remainder data) may be encrypted prior to storage in the distributed memory. Any transfer of extracted data or remainder data or maps or filters may include an encryption feature. Reconstruction of the data is permitted only in the presence of a predetermined security clearance. A plurality of security clearances might be required which would enable a corresponding plurality of reconstructing users to view all or portions of the data. Persons with low level security clearance would only be permitted to have access to low level extracted data (low level security sensitive data) and the common data. Persons with high level security clearances would be permitted access to the entire document reconstituted from the extracted data and the remainder data. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

[0023] The present invention can be configured in various forms. The following descriptions discuss various aspects of the invention and further advantages thereof.

[0024] The present invention enables automatic classification and declassification of documents on the fly. The extraction process downgrades and declassifies documents on the fly (in real time) so that they are useless to unauthorized parties. Presentation by a user of a valid security clearance enables substantially instant and seamless reconstitution of the security sensitive content.

[0025] The present invention automatically secures unstructured documents and freeform documents for example, e-mail, instant messaging, or Word documents (input documents).

[0026] The present invention automatically secures structured documents and transactional documents for example, database records or XML documents (input documents).

[0027] The present invention introduces flexibility into security management, risk management of data, data storage, and data flows and enable automatic responsiveness to threats. The innovation enables automatic response to security challenges and threats. The innovation can maintain, upgrade and downgrade the levels of security through implementation of a leveled granular extraction process and a controlled-release mechanism. Attacks or other external events can trigger a response in the form of higher extraction levels, expanding the type of content extracted, and constricting the release of important and critical data control from storage. How much and what to extract depends on the level of threat or perceived risk. In same manner, the amount and type of content released from storage and reconstituted depends on the level of threat or risk perceived by the system. The system delivers a level of security protection specifically matched to meet security needs as dictated by the changing security threats, environment, policy and organizational needs.

[0028] The present invention introduces multiple levels and standards of security. It is common knowledge that the highest security is delivered through total separation. Whereas this concept has only been implemented physically or by isolating computer environments, the invention achieves this concept of total separation within open and networked computer environments. The invention can implement a total physical and logical separation of important and critical data from its context and can preclude access to that information without a needed granular access permission. The invention is also effective for sounds and images (data objects as security words, characters, terms or icons).

[0029] The present invention introduces a new method and apparatus to monitor security sensitive content through a process of analysis and categorization of each word or character, in a document. The invention enables processing of every character, word, number, as they are entered into a document and categorizes each into one of many pre- set categories. Categories can include surnames, locations, currency, defined terminology, and unknown words or phrases.

[0030] The present invention introduces a method and apparatus for plain text extraction and dispersion of security sensitive data. Maximum security with traditional methods encumbers free flow of information and business efficiency. Encryption burdens computer systems with high performance overhead, and its use is limited to the parties who have decryption capabilities. The invention offers a new solution. It enables leveled security in plain-text format, in addition to none, some, or all of pre-existing encryption, decryption, firewalls, and other security infrastructure. The level of security is determined by the extent of the security sensitive items, selection process; the extent of dispersal to various distributed storage locations; the rules for controlled-release from storage; and the access rules governing the reconstitution of extracts into the secured document.

[0031] The extractions are dispersed to distributed storage on a granular level. The rest of the document can be stored at its original location and/or other storage locations. Dispersal of extractions introduces new barriers not existing in current security. In certain situations, an attacker has first to find the (encrypted) map to the locations, then locate and access the distributed storage, get the data released from the controlled-release storage, and finally reintegrate the extracts into the appropriate documents.

[0032] The present invention introduces a method and apparatus for targeted extraction and encryption of security sensitive items. The extraction capabilities of the system enable different

workflow modes. The system enables extraction and encryption of important and critical content. In essence, only the critical content is extracted and/or encrypted, whereas the rest of the document remains as plaintext. This capability enables the following: advantages and flexibility; and the ability to share the document within the organization or transmit it to outsiders while still maintaining security over the most important and critical content of the document. This is an automatic process for controlling the content of outgoing e-mail. The document owner releases the important and critical content by enabling access to it to defined parties at defined times within defined threat modes.

[0033] The present invention introduces a method and apparatus for encrypting document or extractions with multiple encryption types. The invention can deliver the highest level of security by using multiple types of encryption (and/or multiple keys) for one line, paragraph or document. Maximum security is delivered through automatic selection of security sensitive items, and encrypting these extractions with one or more types of encryption. The remainder data can also be encrypted. Multiple encryption types within one document statistically precludes deciphering that document regardless of the available computer power. Common encryption methods are vulnerable through existing technologies, social engineering methods, carelessness, and workflow habits. Furthermore, simple encryption becomes more vulnerable (including triple DES) assuming future mathematical breakthroughs or quantum computing. Existing methods to crack block ciphers are being improved to compromise the future AES Rijndael standard.

[0034] The present invention to introduce a method and apparatus for content dispersion. The innovation enables control over specific important and critical content items within the general contents of documents or digital files in a computer or within a network. The immediate controlled-release of those important content items according to specific identification and access criteria proactively safeguards the security and the value of documents or digital files. The content control enables broad dissemination of the digital files in closed networks, as well as open networks including the Internet, without compromising the security of the important and critical information in the digital file. The dispersal channels can include any of all of the following: networks, Internet, Virtual Private Channel, Telephone lines, Optical lines, Wireless, Fax, Documents, Verbal communication.

[0035] The present invention introduces a method and apparatus for enhancing the survivability capabilities of an organization and its networks. If networks get damaged, the decryption capability, such as PKI, is likely to be compromised, or at a minimum, suspended. In such instances, the invention enables continuation of work on channels, which need not be secure. In addition, the dispersion of information guarantees maximum partial reconstitution to documents and transactions, or total reconstitution to documents and transactions benefiting from backup at distributed storage facilities.

[0036] The present invention introduces a method and apparatus for delivering security for inter-connecting networks. It enables security for closed networks connecting to the Internet and other open networks. The Internet infrastructure and open networks are not secure. Even secured closed networks, such as VPNs, are not secured enough. The critical content of documents is the critical asset of the organization and must be highly secured, with maximum reliability, full

transparency and instant accessibility. To remain competitive, organizations must maximize utility of the critical data within their documents, files, databases and servers. The securing of such documents must not be at the expense of compromising the access or processing speed of such documents. The invention enables work in plain text, as well as with encryption. Working in plain text reduces the computing performance overload.

[0037] The present invention introduces a method and apparatus for delivering information flow control in decentralized environments. Protection of privacy and confidentiality of information represents a long-standing challenge, The challenge has become much bigger with the expansion of the Internet, which has created decentralized networks. Parties, who do not know or trust each other, have to exchange information. The invention enables free flow and sharing of information between parties by removing burdening security restrictions and creating top security with a controlled-release of the security sensitive content in the documents. The technology enables top security through introduction of user and organization's ownership and control of the critical granular data in documents.

[0038] The system introduces an additional layer of access controls at the granular level of the user document. In order to view the reconstructed critical information the user would need to be verified by additional access controls at the data storage level. The user access code or a physical key enables release of data from the storage. Today's access controls do not stop the user from distributing documents to other parties. The inventions fined grained controlled-release mechanism releases the critical information, only under a required set of circumstances and access validation. The invention enables the user ownership of his security sensitive critical data and conditions for its release and dissemination. The user has the option to hide the critical data through

declassification process and release through a reclassification process in which the critical data would be reconstituted in the document.

[0039] The present invention introduces a method and apparatus for delivering compartmentalization of security sensitive content by leveled access to users. The invention creates leveled sharing of information, for example such that persons with level 3 access will have keys for encryption type RSA persons with level access 2 will have access to Blowfish encryption within one document.

[0040] The present invention introduces a method and apparatus for enabling more use of distributed and dispersed storage including ASPs (application service providers). There is a major human tendency to refrain from sending important documents to web storage locations because of potential security breaches. This cultural issue is both driven by psychological issues and well-founded security concerns. The retention of those documents as is in physical proximity or locked security, provides actual security but precludes gaining any utility from those documents in a functional business setting. Instead the invention enables functional distribution of those documents without the security sensitive data, and a controlled-release of some or all of the extractions in a granular way in order to support business activities while retaining security.

[0041] The present invention introduces a method and apparatus for enabling lower storage costs. The extraction process declassifies and downgrades mission critical documents. The downgrading and transformation of a critical document into a non-critical document, enables storage in less secured and lower cost storage. Taking advantage of this security-initiated, extraction process can yield substantial storage cost savings. The invention enables a high return on investment ROI

for system storage cost arbitrage. Splitting the data into critical and non-critical enables 20 to 90% savings on storage cost.

[0042] The present invention delivers an automated security risk management system that creates added in-depth security defenses at the semantic-level as well as creation of controlled-release mechanisms at the storage-level with significantly reduced performance overhead requirements.

[0043] The present invention presents a technology which answers the security demands as required by Committee on Information Systems Trustworthiness of the National Research Council. The Committee's report, Trust in Cyberspace (1999), defines the security paradigms needed for a safe future. The report states: The substantial commercial off-the-shelf (COTS) makeup of a network information systems, the use of extensible components, the expectation of growth by accretion, and the likely absence of centralized control, trust, or authority demand a new approach to security: risk mitigation rather than risk avoidance; technologies to hinder attacks, rather than prevent them outright; add-on technologies and defense in depth; relocation of vulnerabilities rather than their elimination; none of the existing or security technologies addresses these needs in whole. The invention breaks through this barrier by providing a single system which implements each one of those four elements in a unified way. The invention controls information flow in centralized and decentralized environments, through controlled-release of information within distributed systems.

[0044] The present invention implements security measures while accommodating the performance needs of a network. The invention provides a method and apparatus to ease overhead performance on congested computer networks. It can adjust the security defenses based on the performance needs of the network. Many security systems overburden the already burdened

computing environment in terms of computational overhead, labor, and training requirements. The invention enables to ease the overhead performance of a network by transforming from high overhead performance, encryption methods, and other security methods, to the method presented by this invention.

[0045] The present invention minimizes the time of exposure of the important content within a document. The invention enables to separate the important content from the rest of the document for substantial periods of time, thereby minimizing substantially the exposure to risk. It is possible for example to extract the important content from the document and release it for reconstitution only when the user will open the document. In such situations the important content could for example be time and unexposed for over 99% of the time and exposed for less than 1% of the time, which lowers the risk substantially.

[0046] The present invention provides a security risk management method and system to minimize security risks. The invention enables minimization of security risks by: Automatic separation and extraction of granular critical data from the core document. Dispersal of the extracted critical data groups to different secured storage locations. Reconstitution of the critical data in document for limited time, to minimize exposure to risk. Partial reconstitution, of the critical data, in core document, through a controlled release of granular critical data. Granular controlled release of data to specific authorized people only.

[0047] The present invention provides a controlled release security mechanism to enable the release of content and granular content from storage locations in a centralized and decentralized environment. The controlled release mechanism enables release of the appropriate content to the authorized party at the right time under the right circumstances.

[0048] The present invention provides a security solution against damage by insiders. Studies show that insiders cause 70%-85% of the damage. These nine innovations are described in detail as follows: The invention enables insiders and employees to work with documents while managers and owners control the release of the critical prioritized information. The control is granular, thereby enabling continued work with the rest of the content in the document. The objective is to empower the user with the highest security while enabling him maximum sharing and delivery flexibility. This enables free flow of information between closed networks and public networks, such as the Internet, without compromising the security through extraction of important and critical content. The user can transport documents through various networks and e-mail services knowing that the critical information, which is still under control, and is not compromised.

[0049] The present invention provides an automatic security system in order to overcome human flaws that create security vulnerabilities. Human engineering flaws are the cause of 90% of security vulnerabilities. For example, passwords are exposed through human fault enabling reading of plain text before it is encrypted. The invention enables an automatic process of appropriate response to security threats in an objective way and on an ongoing basis.

[0050] The present invention provides an automatic security system in order to reduce human labor, and training costs.

[0051] The present invention provides protection for important granular content within a document. A feature omitted from computer development is the protection and automatic protection of granular important content in a document. In every facet of life, critical assets are immediately protected. For example, credit cards and cash are protected in a wallet, important items at home are placed in closets, wall units, cabinets and safes.

[0052] The present invention provides an alternative method to encryption. Mathematical security and encryption could be broken. Discovery of a mathematical equation for a shortcut of the factoring of prime numbers would be make mathematical security and encryption extremely vulnerable.

[0053] In 1999 a 512-bit RSA key was broken- at that time 95% of keys in e-commerce were 512 bits long. U.S. government 56-bit Data Encryption Standard was cracked in just 22 hours by the Freedom Foundation. 100, 000 PCs were connected with a supercomputer which enabled the testing of 245 billion keys per second.

[0054] The invention provides an automated security risk management system. The system automatically responds to attacks by matching the defenses level to the level of threats The system responds to security threats through the following mechanisms: (1) controlled extraction of sensitive security data: in normal circumstances, extractions will take place according to pre-set rules; in threat situations, additional extractions will take place to deliver higher security; in an attack, additional substantial amounts of critical data will be extracted to deliver the highest security; (2) controlled dispersal to storage locations; in normal circumstances, dispersal to different storage locations according to pre-set rules will take place; in threat and attack situations, more dispersal to more storage locations, via additional communication channels will take place; and (3) controlled release of extracts for reconstitution; controlling amount of extracts released for reconstitution; controlling time of exposure of extracts in reconstitution; limiting access to specific people; and limiting access to specific times.

[0055] The present invention defends against devices like keyboard sniffers and mouse sniffers that can read information keyed into the computer and transmit it to an adversary. The

invention enables to input security sensitive items through data input devices other than the keyboard. For example credit card numbers can be inputted through a hand held wireless device. The inputted data would be transferred to storage for possible reconstitution.

[0056] The present invention defends against as devices that intercept electromagnetic signals from computers, monitors, printers, and keyboards. For example the Van Eck receptors which can read information off the screen the display screen. The invention enables separation contents of document into two or more displays thereby limiting the potential damage of electromagnetic eavesdropping.

Brief Description of the Drawings

[0057] Further objects and advantages of the present invention can be found in the detailed description of the preferred embodiments when taken in conjunction with the accompanying drawings in which:

[0058] FIG. 1A diagrammatically illustrates a basic system diagram showing filtering and storing extracted data and remainder or common data and, in an enhanced embodiment, generating and storing a map.

[0059] FIG. 1B diagrammatically illustrates a system diagram showing reconstruction of the data, various security clearances and both electronic reconstruction and visual reconstruction.

[0060] FIG. 2 diagrammatically illustrates a system showing major components of a single personal computer (PC) system, a networked system with several PCs (a LAN or WAN) and the network coupled to a telecommunications system and the Internet and shows the interconnection with a server and multiple, Internet-connected memory units.

[0061] FIG. 3 diagrammatically illustrates a basic flowchart showing reconstruction for various security levels.

[0062] FIG. 3A diagrammatically illustrates interleaving district data into different memory locations in a video memory.

[0063] FIG. 4 diagrammatically illustrates a flowchart showing one embodiment of the principal portions of the data security program.

[0064] FIG. 5 diagrammatically illustrates a flowchart showing the basic elements of the reconstruction process for the data security program.

Detailed Description of the Preferred Embodiments

[0065] The present invention relates to a data security system, a methodology of securing data on a personal computer (PC) system, on a computer network (LAN or WAN) and over the Internet and computer programs and computer modules and an information processing system to accomplish this security system.

[0066] It is important to know that the embodiments illustrated herein and described herein below are only examples of the many advantageous uses of the innovative teachings set forth herein. In general, statements made in the specification of the present application do not necessarily limit any of the various claimed inventions. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in the plural and vice versa with no loss of generality. In the drawings, like numerals refer to like parts or features throughout the several views.

[0067] The present invention could be produced in hardware or software, or in a combination of hardware and software, and these implementations would be known to one of ordinary skill in the

art. The system, or method, according to the inventive principles as disclosed in connection with the preferred embodiment, may be produced in a single computer system having separate elements or means for performing the individual functions or steps described or claimed or one or more elements or means combining the performance of any of the functions or steps disclosed or claimed, or may be arranged in a distributed computer system, interconnected by any suitable means as would be known by one of ordinary skill in the art.

[0068] According to the inventive principles as disclosed in connection with the preferred embodiment, the invention and the inventive principles are not limited to any particular kind of computer system but may be used with any general purpose computer, as would be known to one of ordinary skill in the art, arranged to perform the functions described and the method steps described. The operations of such a computer, as described above, may be according to a computer program contained on a medium for use in the operation or control of the computer as would be known to one of ordinary skill in the art. The computer medium which may be used to hold or contain the computer program product, may be a fixture of the computer such as an embedded memory or may be on a transportable medium such as a disk, as would be known to one of ordinary skill in the art.

[0069] The invention is not limited to any particular computer program or logic or language, or instruction but may be practiced with any such suitable program, logic or language, or instructions as would be known to one of ordinary skill in the art. Without limiting the principles of the disclosed invention any such computing system can include, inter alia, at least a computer readable medium allowing a computer to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium may include non-volatile memory, such as ROM, flash memory, floppy disk, disk drive

memory, CD-ROM, and other permanent storage. Additionally, a computer readable medium may include, for example, volatile storage such as RAM, buffers, cache memory, and network circuits.

[0070] Furthermore, the computer readable medium may include computer readable information in a transitory state medium such as a network link and/or a network interface, including a wired network or a wireless network, that allow a computer to read such computer readable information.

[0071] In the drawings, and sometimes in the specification, reference is made to certain abbreviations. The following Abbreviations Table provides a correspondence between the abbreviations and the item or feature.

Abbreviations Table

A-com	computer or memory store for common or remainder data
B-ext	computer or memory store for extracted data
bd	board
CD-RW	compact disk drive with read/write feature for CD disk
CPU	central processing unit
doc	document
dr	drive, e.g., computer hard drive
e	encryption
ext-data	extracted data
I/O	input/output
I-com	Internet storage for common or remainder data
I-ext	Internet storage for extracted data
loc	location

mem	memory
recon	reconstruct
rel	release
req	request
sec	security
sys	system
t	time
tele-com	telecommunications system or network

[0072] FIG. 1A diagrammatically illustrates the basic processes for establishing a secure storage of information, generally identified herein as “data.” “Data,” as used herein, includes any data object, e.g., text, images, icons, etc. Sound bites, data objects and video images may also be extracted as “data.” A source document 100, sometimes referred to as a “plaintext,” is passed through a filter 102. Filter 102, in a most basic sense, separates out common text or remainder data 104 from uncommon text, words, characters or icons. The security sensitive words, characters or icons are separated from remainder or common text 104 as extracted text 106. It should be noted that although the word “text” is utilized with respect to remainder text 104 and extracted text 106, the “text” is a data object and includes words, phrases, paragraphs, single characters, portions of words, characters, whole or partial images, or icons or sound or video. In a basic implementation, filter 102 may utilize a dictionary such that words present in the dictionary (common words) are separated from the source plaintext document 100 and placed into remainder document or common data file 104. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106. For example, a business may wish to impose a security system on a contract document such that the names of the contracting

parties (not found in the dictionary) and the street names (not found in the dictionary) would be stored in extracted data text file 106. The common text or remainder data would be stored in remainder data file 104. In the illustrated embodiment, remainder data file 104 also includes place holders which enables the extracted data to be easily inserted or set back into the remainder data file.

[0073] The security sensitive words, characters or icons may be any word, phrase, letter, character, icon (full or partial), image or whatever as pre-defined or as established by the user. The user may specifically design the filter, begin with a dictionary to define common terms, identify any additional security sensitive words, letters, images, icons, partial versions of the foregoing or any other granular aspect of the plaintext. After defining the filter and accepting the data input, the system filters the plaintext and separates extracted data (security sensitive items) from the remainder data.

[0074] In a basic configuration, the common text or the remainder data is stored in common storage memory 108. This common or remainder data store is identified as A-com generally referring to a segmented memory in a PC or a computer A in a network (LAN or WAN). Remainder data storage 108 may include a confirm storage signal function 111 to send back a confirm storage signal to the data input device generating source plaintext document 100. The extracted data file 106 is stored in a different memory computer storage 110 (B-ext). In a preferred embodiment, memory segment 108 (A-com) is at a different location than computer storage memory segment 110 (B-ext). In a PC embodiment, memory A-com is a different memory segment than memory B-ext. In a networked embodiment, computer storage 108 may be on a different computer as compared with computer storage 110. In any event, the remainder text is stored in a memory A-com and the extracted data or high security words, characters or icons are stored in memory B-ext. After storage of the extracted data in memory 110, a confirmation indicator 113 may be generated to the client

computer or the computer handling source plaintext input document 100 (the originating computer system).

[0075] In a further enhancement of the present invention, the computer or data input device handling source plaintext document 100 may also record the location of A-com 108 and B-ext 110. The location data is called herein “map.” A memory mapping function is utilized. The map may be stored in a third memory location 112. Memory location map 112 may be a segment of the memory of the data input computer originating plaintext 100.

[0076] As a further enhancement of the present invention, the user, prior to initiating the security system, may be given a choice of filtering out all the uncommon words or words not found in the dictionary and adding certain security sensitive words, characters or icons to filter 102. The added words or terms are filtered out with the uncommon words. Of course, the user may be required to manually input all security words or download the security word filter from the Internet or another system on the LAN. For security systems having multiple security levels, a plurality of filters would be created, each filter associated with a different security level. Further, multiple security levels would require, in addition to remainder text document or data 104, a plurality of extracted data documents 106. The common or remainder text document or data 104 would still be stored in remainder computer storage A-com 108. However, each extracted data document 106 would be stored in a respective, separate computer memory segment or computer B-ext 110. Separate storage of a plurality of extracted data at multiple, separate locations in B-ext is one of the many important features of the present invention.

[0077] In view of increasing levels of security relating to (a) the storage location A-com; (b) the transfer of remainder text document 104 to memory computer storage A-com 108; (c) the storage

of map 112; (d) the creation, storage or transfer of filter 102; (e) the storage of extracted data at memory storage B-ext (whether singular or plural storage sites); and (f) the transfer of extracted data thereto, the system may include an encryption e feature. The encryption e function 115, 117 and 118 is diagrammatically illustrated in FIG. 1A.

[0078] FIG. 1B generally diagrammatically illustrates the major features of a reconstruction routine or system. The user, typically at a computer terminal, inputs a reconstruction request 120. The system first executes a security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. The security clearance may be thought of as a security clearance control. If multiple users are permitted access to the documents and those multiple users have different security clearances, the security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext. The security code input by the user is checked against a security code database or list 124. Clearance is provided in step 126. The location of the map and, hence, the location of the remainder data A-com 108 and extraction is provided to the user's computer in step 128. This may include obtaining a copy of the map 130 showing the location of memory segments in (a) the local computer; (b) the LAN or WAN; or (c) the Internet storage sites. The storage segments are A-com 108 and B-ext 110. The common or remainder data is downloaded or transferred or made available to the user's computer as shown at the output of map location and data step 128. Typically, the extracted or security sensitive data from B-ext is downloaded. As described hereinafter, the data can be reconstructed as a complete electronic document in function 130 or may be reconstructed only as a visual reconstruction in step 132. Visual reconstruction is discussed later. Function 130 operates as a compiler to gather the extracted data and remainder data into a single plaintext document.

[0079] If remainder data in A-com memory 108 and extracted data in B-ext computer memory 110 is encrypted, the reconstruction process includes a decryption step. Encryptors and decryptors are relatively well known by persons of ordinary skill in the art. Further, the filter 102 (FIG. 1A) may include some encryption routine operating on the data object (plaintext) during the filtering. A simple encryption may include substituting “dummy” text or images for the security words and keeping a pointer to an encryption key document mapping the security words with the dummy words. The filter may be stored or may be destroyed at the option of the user. Storage of the filter impacts the degree of security of the entire data system but storage of the same filter enables the user to reuse the filter at a later time. Encryption of the stored filter increases the security of the data. Creation and storage of map in memory 112 also impacts the degree of security of the system. However, if the filter 102 is destroyed and all copies of the map are destroyed on the user’s computer originating plaintext document data 100, and the map is stored offsite in a third computer memory location 112, this offsite map storage may enhance the degree of security of the data. The originating computer processing plaintext 100 may be scrubbed to remove all reference and copies of the plaintext, remainder text, extracted data, map storage data, etc., i.e., a deletion routine may be employed on the data input computer.

[0080] FIG. 2 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC -3. PCs 140, 142 and PC-3 are connected together via a network 145(LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to a telecommunications system 148 which leads to Internet 150. The Internet is a global computer network. Internet 150 is coupled to a plurality of servers, one of which is server 152. Server 152 may be designated as an application service processor ASP. Internet 150

also includes various computer memory storage devices such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158. Computer storage enabling the store of extracted data includes a security level clearance module 157. Similarly, map computer storage 158 includes security level clearance module 159.

[0081] As stated earlier, the present data security system can be implemented on a single personal computer 140. In this case, different memory segments or hard drive 168 may be used for A-com and B-ext. Typically, PCs include a keyboard or data input device 161, a display 163, a central processing unit CPU 165, a video board 167 having video board memory 169, a fixed disc hard drive 168, a RAM 166, and input/output device 164, a removable memory media or floppy drive 162 and a removable compact disk (CD) read-write (CD-RW) device or drive 160. The system may include other removable disk drives, tape drives, or flash memory units. Internal units CPU 165, video board 167, hard drive 168, RAM 166 input/output device 164, floppy drive 162 and CD-ROM device 160 are all coupled together via an internal bus 171. Bus 171 represents a plurality of buses as is known to persons of ordinary skill in the art.

[0082] One methodology of implementing the present invention utilizes distinct memory segments which may be designated in one or more of the following: hard drive 168, memory in a removable disk in floppy drive 162, memory in a removable CD disc in CD-RW device 160, and, to a very limited extent, RAM 166. In this manner, the user may select, generally at the outset of the process, that the extracted data memory storage B-ext 110 be stored on a floppy (removable memory) via floppy drive 162 or a CD via CD-RW drive 160. The user can then simply remove the floppy or the CD and carry it with him or her. To reconstruct the data, the operative program, generally discussed above would have access to the floppy or the CD and particularly the memory location of the data on the floppy and the CD in order to reconstruct the entire plaintext document

100 (see FIG. 1A). Alternatively, different portions of hard drive 168 may store A-com and B-ext. Of course, the computer system may utilize tape drives and memories or flash card, programmable memory.

[0083] In a local area network or wide area network implementation, PC 142 includes memory similar to memory units described in PC 140 and a memory segment may be set aside in PC 142 separate from the common data or remainder data storage typically placed on hard drive 168 in PC 140. As a further expansion of the present invention, the extracted data (that is, the high security data), may be stored on computer storage I-ext memory unit 156 via Internet 150, telecommunications system 148 and router/server 146. In this manner, the common data or remainder data is stored on hard drive 168 and the highly sensitive data is stored off site in a secured location. Access to that secured location may be limited via security layer 157. If the user implements an encryption system (see encryption e 118 in FIG. 1A), the extracted data is further secured by the encryption during the transfer from computer 140 through network 145, router/server 146, telecommunication system 148, Internet 150 and ultimately to computer storage I-ext 156.

[0084] The present invention may also be embodied utilizing an Application Service Provider (ASP) on server 152 and in a client-server network.

[0085] An implementation of the present invention over Internet 150 most likely includes the use of a uniform research locator or URL for map memory computer 158, computer storage I-ext 156, computer storage I-com 158 and ASP server 152. In a client-server environment, server 152 acts as a server generally commanding the operation of client computer 140. Of course, persons of ordinary skill in the art recognize that the server may be located on the local area network 145 rather

than being interconnected with Internet 150 as shown in FIG. 2. The claims appended hereto are meant to cover the alternative embodiments.

[0086] As an example of a client-server or web-based implementation of the present invention, the user at computer 140 may define the filter 102 as described above, and input data (plaintext) via keyboard 161 or load plaintext data from floppy drive 162 or CD-ROM drive 160 into RAM 166. In any event, whether the plaintext data is input via keyboard 161 or copied or accessed in or from floppy drive 162 or CD-RW drive 160, the plaintext data is filtered as discussed above in connection with FIG. 1A. Prior to filtering, it would be appropriate for the user at computer 140 to identify where the remainder data or common data will be stored and where the extracted or high security data would be stored. The system is sufficiently flexible to enable the user to select local storage on different memory segments of PC 140 (hard drive 168, floppy drive 162, CD-RW drive 160) or be flexible enough to enable user at computer 140 to designate off site storage of the high security data (extracted data) and/or the common or remainder data. The off site data storage process may include activating server 152 and enabling the server to take over the process directly from user 140. In other words, the user at computer 140 could call up the URL of the server 152, the server could request certain user information (user name, password), and would request data from the client computer to establish the filter pursuant to input selected by the user. The client compute may (a) filter the plaintext thereat or (b) send the data to the server for filtering. The server could store data either locally on computer 140 or remotely at computer memories 154, 156. After storage of the data at any of these locations, the server 152 may establish a map and store the map in memory location 158. Of course, remainder data and the map may be stored at ASP 152 or client computer 140. The map, if stored at map storage 158, may be downloaded to the user at computer 140. The filter may be stored at computer 140 or may be stored at a secured location on server 152.

Alternatively, the map could be destroyed on user computer 140. The filter could also be destroyed on user computer 140. Of course, the filter could be stored in a fourth remote location (not shown), different from I-com 154, I-ext 156 and map computer memory 158. Storage of the map and decryption keys is a critical, high security task. Appropriate security measures should be utilized to protect those items. Local removable memory storage on disc in floppy drive 162 or disc in CD-RW 160 may be reasonable. All traces of the map, the filter, the encryption key, the extracted data, and possibly the remainder data may be scrubbed or deleted from all computer memories (by write-over or disc reformat routines) other than the “com” and “ext” storage sites. Deletion of all URLs, links, etc. is also recommended for high security applications. Deletion systems are known to persons of ordinary skill in the art.

[0087] To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security. By implementing different security levels, the system is dynamic enough such that server 152 can easily locate the various extracted data levels based upon various security codes representing different security levels, as those codes are input by the user at computer 140. Multiple security codes, at the inception and during the process, may be utilized. The user may be required to input security codes at multiple times during the reconstruction or compilation process.

[0088] It should be noted that computer storage 154, 156 and 158 may be located on the same computer or may be located on different computers spread throughout the Internet. If the

storage units are different computers spread throughout the Internet, computer storage 154, 156 and 158 would each have their own URL or Uniform Resource Locator. In any event, during reconstruction, the server 152 gathers the information and downloads the information into RAM 166 of computer 140. This download may include a first download of the common or remainder data from I-com 154. At a separate time, which may or may not include a decryption routine, the extracted from I-ext 156 is downloaded. Preferably, other than inputting initial security codes and any required or desired intermediate security codes, the system operates automatically without further input from the operator at client computer 140. The download of both data sets may be simultaneous in that the download is not humanly perceivable. This is especially true if storage in different memory locations in PC 140 is utilized.

[0089] The role of server 152 may be expanded or reduced dependent upon the desires of the user and the degree of security necessary. For example, server 152 may only enable separate storage of extracted data in I-ext 156. In this limited role, server 152 would require the input of a proper security code and clearance prior to identifying and enabling the download of extracted data from I-ext 156.

[0090] In an expanded mode, server 152 may be involved in filtering the data, extracting the security sensitive words, characters or icons or data objects to obtain extracted data and remainder data thereat, separately storing the extracted data from the remainder data (extracted data being placed in computer memory I-ext 156 and remainder data being stored in common remainder data memory I-com 154) and then permitting reconstruction via separate or combined downloads of the remainder data and the extracted data into computer 140.

[0091] FIG. 3 diagrammatically illustrates a system diagram for various reconstruction routines. A complete reconstruction is shown as security level path A. This involves an electronic integration of plaintext in step 202 resulting from the complete electronic reconstruction of document 100. For example, a merge may occur between the extracted data and the remainder data or common text data. The document is completely compiled in this process. Placeholders in the remainder document are utilized to locate and insert the extracted data. Most likely, there will be no process controls imposed on the integrated document as shown in step 204. In other words, if the user at computer 140 has the proper security clearance, he or she could download or recreate the entire original source, plaintext document and the user would be entitled to edit the document or change it in any way or copy it and reproduce it.

[0092] The second level of security, path B, results in storage of the common or remainder data in a different memory location on the hard drive 168 as compared with the extracted data. This is noted in step 206. Another words, in a simple example, hard drive 168 or RAM 166 would hold a copy of a remainder data document and another copy of the extracted data document, that is, two separate documents. Since two documents are available in RAM 166 or hard drive 168, these documents are stored in different locations in the memory. In step 208, a map showing the memory location of the common or remainder document and the extracted data document is provided to computer 140. Step 210 commands the processor CPU 165 in computer 140 to interleave the extracted data with the common or remainder data in the video board memory. In this process, the extracted data would typically have placeholders for the missing remainder data. Otherwise, control codes to locate the extracted data into the remainder data would be executed by CPU 165 to properly place the extracted data into the “visual space” of the placeholders in the remainder data document. The extracted data document may have placeholder for the remainder data. Some type of register

between the two image documents may be necessary. The compiler, in this embodiment, gathers the document elements and visually compiles and presents the plaintext to the user.

[0093] FIG. 3A diagrammatically shows that video board memory 169 is loaded with remainder or common data 1 and a different location of the video memory is loaded with extracted data 1. The next video memory location is loaded with common data 2 and then a different video memory location is loaded with extraction data 2. Since the refresh rate of computer monitor 163 is fast, the display 163 will show the common or the remainder data and then show the extracted data such that the user could not humanly perceive a difference in the document. However, the user could not copy the document from display screen 163 (a “screen shot”) since the document is never electronically integrated into a single document. There is only a visual presentation of the combined document by interleaving the extracted data with the common or remainder in the video memory 169. Step 212 notes that the user may be limited in his or her ability to process, edit and store the reconstructed and presented plaintext document.

[0094] Security level path C recognizes in step 214 that the data is stored in different memory or computer locations. In this situation, two video boards, video board A and video board B are shown as board 216 and 218. Video board 216 drives display monitor 220. Video board 218 drives display monitor 222. Display screens 220, 222 are overlaid atop each other. Video board 216 is fed with common or remainder data from the remainder data store (see I-com store 154 in FIG. 2) and video board 218 is fed with the extracted data from the extracted data store, for example, I-ext store 156. In this manner, as noted in step 224, the user is presented only with a visual presentation or compilation of the plaintext. Since there was physical separation between video monitor 222 and video monitor 220, there is no electronic integration at all of the plaintext document. Hence, the

ability for the user to do any significant editing on the plaintext document is blocked or prohibited because the user only has access to either the data on video board 216 or the video board 218.

[0095] Security level path D shows that the extracted data may be parsed or further separated based on a plurality of security clearances in step 226. Step 228 recognizes that the system can repeat process and security process paths A, B and C only with portions of the extracted data presented to the user based upon the user's security clearance.

[0096] FIG. 4 diagrammatically illustrates the major components of a flowchart for the data security program. It should be noted that this flowchart may be truncated to limit user selection of certain items. The system would be pre-set to contain these features. Step 230 initializes the system. Step 232 enables the user to designate various levels of security for the activity which he or she will soon engage. The system, in step 234, enables the user to define the levels of security parameters. The following Security Table gives some examples of the type of security that may be available to the user.

Security Table

to whom

to where

when (time of day, day of week, month, floating but predetermined time frame)

why (purpose, match purpose to other security parameters or to certain predetermined criteria)

how (through what medium (LAN, WAN, Internet, direct dial link), download to what site or destination)

how long (duration) the reconstruction process will be permitted per
each security clearance level

how much (different security levels enable reconstitution of
documents and data with different amounts of secure data therein)

timing systems may require synchronization for a standard clock (i.e.,
atomic clock)

[0097] As an example of a truncated or pre-set program, a client-server system over the Internet may have URLs designating storage sites and an ASP 152 (FIG. 2) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152.

[0098] The user, in step 326 can designate the location of the filter, the common storage area for the remainder data, the extraction data storage and potentially multiple data storage areas or segments. Step 238 permits the user to engage or disengage encryption and, if engaged, establish the degree of encryption for the system. Step 240 enables the user to define the parameters of the filter. The user can retrieve a preexisting filter or may define a new filter for each data security session. These filters may consist of dictionaries or any type of compilation of words, characters, icons or pixel formation or any indication that can be perceived by the computer system. Granular extraction of data elements in a data object may be permitted. Step 242 recognizes that the user either inputs a preexisting plaintext document or types data into the system. In any event, the plaintext document is fed through the filter. Step 246 extracts the security data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage. Step 250 conducts an error check on the extracted data. This error check is helpful in discerning problems in the storage of the data prior to closing down the data security system. Step 252 stores

the common data or the remainder data. Step 254 conducts an error check on the common or remainder data. The decision step 256 determines whether the user has selected a “destroy filter” command. If not, the filter is stored with or without encryption in step 257. If YES, the filter is destroyed with a deletion routine. Typically, deletion is complete erasure of all traces of the file including, in high security systems multiple write-overs or disc reformatting. Step 258 stores a map. The map may be stored locally or remotely as described earlier. The system ends in step 260. All traces of these data elements or objects may be swiped clean or removed from whatever computer system generated the data objects or processed them, other than the memory storage locations. Deletion of data also includes the concept of deletion of data transmission paths, URLs, storage site locations and all temporary memory stores. Deletion of file location in the root directory of hard drive 168 of computer 140 is preferable in high security systems.

[0099] FIG. 5 diagrammatically illustrates basic flowchart features for the reconstruction process. Step 302 accepts a request to reconstruct the secured data. Step 304 queries a local map and the security system or protocol. In a preferred embodiment the user would have to input several passwords, one of them being a local password on computer 140. A local map which may be accessed only through the password, may simply identify the URL of server 152. Decision step 306 determines whether the local password is acceptable. If not, an error step is indicated in step 307, the attempt to log on to the security system is noted in step 309 (an audit trail), and the system either branches to repeat step 311 or bars the user from further activity in step 313.

[0100] Returning to decision step 306, if the password is locally acceptable, the YES branch is taken and the system executes step 308 which releases a reconstruction request to the common storage facility I-com 154 or A-com 108 (FIGS. 2 and 1A-B). The system in step 310 logs the user

in, as well as time and date and the data regarding the request. In step 312, a download from the common data storage is provided to RAM 166 or hard drive 168.

[0101] In step 314, a query is made to obtain the remote map from the remote security system. The decision step 316 indicates that the user again successfully inputs his or her security code. If not, error routine 317 is activated, the password failure is noted in step 319 (an audit trail), and the user is given an opportunity to repeat in step 321 or is barred or prohibited from further activity in step 323. If the user has correctly input the security code, the system in step 318 releases the keys (to decrypt) and the map and releases the reconstruction request to the remote storage for the extracted data. This could be computer storage I-ext 156 or computer storage B-ext 110. In step 320, the user's access to the extracted data is logged in along with the time and day and type of data request. In step 322, the system downloads the extracted data into RAM 166 and/or hard drive 168 of computer 140. In step 324, an error routine is operated on the extracted data in order to insure that the extracted data properly matches the common or remainder previously stored. Decision step 326 determines whether the error routine properly generates the correct count or output. If not, the system in step 327 indicates an error, in step 329 the system deletes the common files and the extracted files and the system in step 331 logs in the failed attempt. If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to integrate the plaintext document pursuant to the security clearance initially input by the user. Step 330 ends this process. The end process may entail encrypting the data again and swiping clean all traces of data objects from the memory stores and computer handling units. Of course, every use of encryption requires decryption of the data prior to reconstruction.

[0102] The system may incorporate various types of security systems or routines.

pass word

pass phrase

multiple choice questions and answers

initial, intermediate and subsequent security clearance routines

biometric security routines (voice, fingerprint, signature, eye or retina scan)

[0103] The reconstruction routines may be interrupted or the security system automatically activated or initiated upon the occurrence of externally generated triggers or upon certain predetermined conditions or conditional events. Limited extraction, security clearance, release of data and reconstruction limits may be imposed.

[0104] The display systems 220, 222 in FIG. 3 include CRT monitors, LCD screens, projection screens and combinations of those systems.

[0105] The audit trail to monitor reconstruct and reconstruction attempts may include adding a time/data stamp to the remainder data and/or the extracted data prior to storage and a cross-check to the audit trail log during the reconstruction process.

[0106] Placeholders in the remainder document may be:

blank spaces

data symbols or elements “---“ or “xxx”

false data

clearly erroneous data “ABC Company” or “Baker”

chaff or hash marks

messages

bar code

serialization data

alerts

links to other data objects

null set indicators “[]”

URL or website addresses

[0107] It is believed that the present invention is faster, during reconstruction, than standard encryption techniques, on the order of 100 to 1,000 faster.

[0108] The system and method described herein may operate substantially automatically, that is, without operator intervention, other than the security clearance function. The clearance function does require some type of operator authentication prior to retrieval of the extracted and remainder data.

[0109] The system and the method may operate automatically in that the plaintext or originating data could be identified by a party desiring security. The system could obtain that data from any data input device (hard drive memory, floppy drive memory, flash card memory, personal data assistant (PDA), or any other type of data input device), filter the data, separate the extracted text or the remainder text, encrypt (or not encrypt) the data, separately store the extract and remainder data (all automatically, that is, without operator intervention). Hence, it is not necessary that the system operate with significant operator or manual intervention. Of course, the system may also operate on a plaintext document or data object that is being created “in real time” by an operator and keyboard, mouse or other type of data input device. Since the present system can be configured

to operate in real time, the system works on data packets of sensitive text, characters, icons, images or a combination thereof, sound, video, and data objects in general

[0110] The automatic operation of the system and the method can be caused by a triggering event. This triggering event may be a security attack (generating a trigger to start the gathering of plaintext, filtering, extraction and storing) or may be any other type of trigger such as a building burglar alarm, door alarm, fire alarm, or virus detection algorithm trigger. The event may be a time of day, week or month. It may be n seconds after the user stops typing on a keyboard. It may be a timed back-up feature.

[0111] Multiple filters may be utilized in the system and in connection with the method. These multiple filters may be useful in the operation of the system with a plurality of security levels. Each filter could filter out different levels of security sensitive items and each bundle or group of security sensitive items (from each distinct filter) could be stored at different computer storage locations. Multiple filters, multiple security levels and multiple storage areas may also include multiple encryption routines and decryption routines. Encryption and decryption routines can be related to the level of security of a particular group of data.

[0112] Multiple maps may also be provided for singular or multiple storage of extracted data and remainder data. These maps may or may not indicate the originating point of the data. Maps can be parsed such that an intruder, upon discovery of a single map or map portion, could not locate the storage locations of all piece of the extracted data and remainder data.

[0113] The concept of partial reconstruction also includes the concept that a portion of the plaintext would be reconstructed and the unreconstructed portions of the plaintext could be encrypted or could show blanks or other symbolic indicators. See the placeholder table above.

[0114] Partial reconstruction of the plaintext also includes a concept that the security sensitive items or materials may be subject to different types of encryption. Hence, a single plaintext document may have multiple levels of security and multiple levels of encryption wherein each encryption has a different level of security assigned to it.

[0115] The claims appended hereto are meant to cover modifications and changes within the scope and spirit of the present invention.

[0116] What is claimed is:

1. A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

accepting data input which includes security sensitive content via said client computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

2. A method as claimed in claim 1 wherein accepting occurs at one of said client computer and said server computer.

3. A method as claimed in claim 1 wherein extracting occurs at one of said client computer and said server computer.

4. A method as claimed in claim 1 wherein one or both of extracting and storing occurs at said server computer.

5. A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system..

6. A method as claimed in claim 1 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

7. A method as claimed in claim 6 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

8. A method as claimed in claim 1 wherein permitting full or partial reconstruction of said data occurs at one of said client computer and said server computer.

9. A method as claimed in claim 1 wherein said client-server computer system includes at least first and second client computers, said first client computer being said at least one client computer, and wherein accepting data input occurs at said first client computer and permitting full or partial reconstruction of said data occurs at said second client computer.

10. A method as claimed in claim 9 wherein extracting occurs at one of said first client computer and said server computer.

11. A method as claimed in claim 10 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

12. A method as claimed in claim 10 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

13. A method as claimed in claim 1 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

14. A method as claimed in claim 13 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

15. A method as claimed in claim 14 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

16. A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer and said client computer.

17. A method as claimed in claim 1 wherein storing of said remainder data occurs at said client computer on one of a fixed memory and a removable memory at said client computer.

18. A method as claimed in claim 16 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

19. A method as claimed in claim 1 including storing a map or locating data for said respective extract stores.

20. A method as claimed in claim 19 wherein the storing of said map or locating data occurs at one of said client computer and said server computer.

21. A method as claimed in claim 20 wherein the storing of said map or locating data occurs at said client computer in one of a fixed memory and a removable memory at said client computer.

22. A method as claimed in claim 20 wherein the storing of said map or locating data via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

23. A method as claimed in claim 19 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

24. A method as claimed in claim 23 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

25. A method as claimed in claim 24 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer and said map locates said remainder store.

26. A method as claimed in claim 1 including establishing a plurality of filters for groups of security sensitive content corresponding to respective ones of said plurality of security levels and using said filter during the extraction of security sensitive content.

27. A method as claimed in claim 26 including storing said plurality of filters on one of said client computer and said server computer in one of fixed memory and removable memory.

28. A method as claimed in claim 27 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

29. A method as claimed in claim 27 including one of destroying or storing the filter after extraction.

30. A method as claimed in claim 2 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon accepting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

31. A method as claimed in claim 3 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon extracting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

32. A method as claimed in claim 4 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on said server computer in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

33. A method as claimed in claim 26 wherein said filters identify either by inclusion or exclusion said security sensitive content.

34. A method as claimed in claim 1 including deleting said data input after storing.

35. A method as claimed in claim 24 including deleting said map after full reconstruction.

36. A method as claimed in claim 1 wherein said client-server computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

37. A method as claimed in claim 1 wherein said client-server computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

38. A method as claimed in claim 1 wherein extracting occurs at said client computer either automatically or manually with operator input.

39. A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security

clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

from input data, extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

separately storing said extracted data, for each corresponding security level, in the respective extract store, apart from said remainder data stored in one or both of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

40. A method as claimed in claim 39 wherein extracting occurs at one of said client computer and said server computer.

41. A method as claimed in claim 39 wherein one or both of extracting and storing occurs at said server computer.

42. A method as claimed in claim 39 wherein extracting includes filtering security sensitive content at one of said client computer and said server computer.

43. A method as claimed in claim 39 wherein said server computer stores said remainder data thereat or in remotely disposed remainder stores in said client-server computer system.

44. A method as claimed in claim 43 including storing a map of said respective extract stores.

45. A method as claimed in claim 44 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

46. A method as claimed in claim 45 wherein said map is stored on one of said client computer and said server computer.

47. A method as claimed in claim 46 including the step of decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

48. A method as claimed in claim 39 wherein said computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

49. A method as claimed in claim 39 wherein said computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

50. A method as claimed in claim 39 including deleting said input data after storing.

51. A method as claimed in claim 39 including mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

52. A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one

server computer and a plurality of extract data stores for respective ones of said plurality of security levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

extracting security sensitive content from a data input via said server computer to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

53. A method as claimed in claim 52 wherein said reconstruction is a download operation adapted to be directed at said client computer.

54. A method as claimed in claim 53 wherein said client-server computer system includes first and second client computers, said extracting is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

55. A method as claimed in claim 52 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

56. A method as claimed in claim 52 wherein said client-server computer system includes first and second client computers, said remainder data store is part of said first client computer and the storing of remainder data includes a store download operation adapted to be directed at said first client computer.

57. A method as claimed in claim 56 said extracting is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

58. A method as claimed in claim 52 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

59. A method as claimed in claim 58 wherein storing or reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

60. A method as claimed in claim 52 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

61. A method as claimed in claim 60 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

62. A method as claimed in claim 61 wherein reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

63. A method as claimed in claim 52 wherein storing of said remainder data occurs upon server instruction adapted to be directed at said client computer on one of a fixed memory and a removable memory at said client computer.

64. A method as claimed in claim 60 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

65. A method as claimed in claim 52 including storing a map or locating data for said respective extract stores.

66. A method as claimed in claim 65 wherein the storing of said map or locating data occurs at one of a map store and said server computer.

67. A method as claimed in claim 66 wherein the storing of said map or locating data occurs via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

68. A method as claimed in claim 65 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

69. A method as claimed in claim 68 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

70. A method as claimed in claim 52 wherein a plurality of filters are provided for groups of security sensitive content corresponding to respective ones of said plurality of security levels, downloading, from said server computer, one or more of said filters to facilitate extraction of security sensitive content.

71. A method as claimed in claim 70 including storing said plurality of filters on said server computer in one of fixed memory and removable memory.

72. A method as claimed in claim 71 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

73. A method as claimed in claim 71 including one of destroying or storing the filter after extraction.

74. A method as claimed in claim 54 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a

respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

75. A method as claimed in claim 55 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

76. A method as claimed in claim 70 wherein said filters identify either by inclusion or exclusion said security sensitive content.

77. A method as claimed in claim 52 including deleting said data input after storing.

78. A method as claimed in claim 69 including deleting said map after full reconstruction.

79. A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security

levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

facilitating the extraction of security sensitive content from a data input to obtain extracted data for each corresponding security level and remainder data;

at said server computer, storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

80. A method as claimed in claim 79 wherein said reconstruction is a download operation adapted to be directed at said client computer.

81. A method as claimed in claim 80 wherein said client-server computer system includes first and second client computers, said facilitating the extraction is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

82. A method as claimed in claim 79 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

83. A method as claimed in claim 79 wherein said client-server computer system includes first and second client computers, said remainder data store is part of said first client computer and the storing of remainder data includes a store download operation adapted to be directed at said first client computer.

84. A method as claimed in claim 83 said facilitating the extraction is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

85. A method as claimed in claim 79 wherein storing or said facilitating the extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

86. A method as claimed in claim 85 wherein storing or reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

87. A method as claimed in claim 79 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

88. A method as claimed in claim 87 wherein storing or said facilitating the extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

89. A method as claimed in claim 88 wherein reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

90. A method as claimed in claim 79 wherein storing of said remainder data occurs upon server instruction adapted to be directed at said client computer on one of a fixed memory and a removable memory at said client computer.

91. A method as claimed in claim 79 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

92. A method as claimed in claim 79 including storing a map or locating data for said respective extract stores.

93. A method as claimed in claim 92 wherein the storing of said map or locating data occurs at one of a map store and said server computer.

94. A method as claimed in claim 93 wherein the storing of said map or locating data occurs via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

95. A method as claimed in claim 94 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

96. A method as claimed in claim 95 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

97. A method as claimed in claim 92 wherein a plurality of filters are provided for groups of security sensitive content corresponding to respective ones of said plurality of security levels, downloading, from said server computer, one or more of said filters to facilitate extraction of security sensitive content.

98. A method as claimed in claim 97 including storing said plurality of filters on said server computer in one of fixed memory and removable memory.

99. A method as claimed in claim 98 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

100. A method as claimed in claim 98 including one of destroying or storing the filter after extraction.

101. A method as claimed in claim 81 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a

respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

102. A method as claimed in claim 82 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

103. A method as claimed in claim 97 wherein said filters identify either by inclusion or exclusion said security sensitive content.

104. A method as claimed in claim 79 including deleting said data input after storing.

105. A method as claimed in claim 96 including deleting said map after full reconstruction.

106. A computer readable medium containing programming instructions for securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at

least one client computer and said extract data stores over a communications network, the programming instructions comprising:

accepting data input which includes security sensitive content via said client computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

107. A computer readable medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system.

108. A computer readable medium containing programming instructions as claimed in claim 106 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

109. A computer readable medium containing programming instructions as claimed in claim 108 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

110. A computer readable medium containing programming instructions as claimed in claim 106 wherein extract data stores are remotely disposed, via said communications network, with

respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

111. A computer readable medium containing programming instructions as claimed in claim 110 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

112. A computer readable medium containing programming instructions as claimed in claim 111 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

113. A computer readable medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer and said client computer.

114. A computer readable medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at said client computer on one of a fixed memory and a removable memory at said client computer.

115. A computer readable medium containing programming instructions as claimed in claim 113 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

116. A computer readable medium containing programming instructions as claimed in claim 106 including storing a map or locating data for said respective extract stores.

117. A computer readable medium containing programming instructions as claimed in claim 116 wherein the storing of said map or locating data occurs at one of said client computer and said server computer.

118. A computer readable medium containing programming instructions as claimed in claim 117 wherein the storing of said map or locating data occurs at said client computer in one of a fixed memory and a removable memory at said client computer.

119. A computer readable medium containing programming instructions as claimed in claim 117 wherein the storing of said map or locating data via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

120. A computer readable medium containing programming instructions as claimed in claim 116 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

121. A computer readable medium containing programming instructions as claimed in claim 120 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

122. A computer readable medium containing programming instructions as claimed in claim 121 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer and said map locates said remainder store.

123. A computer readable medium containing programming instructions as claimed in claim 106 including establishing a plurality of filters for groups of security sensitive content corresponding to respective ones of said plurality of security levels and using said filter during the extraction of security sensitive content.

124. A computer readable medium containing programming instructions as claimed in claim 123 including storing said plurality of filters on one of said client computer and said server computer in one of fixed memory and removable memory.

125. A computer readable medium containing programming instructions as claimed in claim 124 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

126. A computer readable medium containing programming instructions as claimed in claim 124 including one of destroying or storing the filter after extraction.

127. A computer readable medium containing programming instructions as claimed in claim 106 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon accepting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

128. A computer readable medium containing programming instructions as claimed in claim 106 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon extracting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

129. A computer readable medium containing programming instructions as claimed in claim 108 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on said server computer in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

130. A computer readable medium containing programming instructions as claimed in claim 123 wherein said filters identify either by inclusion or exclusion said security sensitive content.

131. A computer readable medium containing programming instructions as claimed in claim 106 including deleting said data input after storing.

132. A computer readable medium containing programming instructions as claimed in claim 121 including deleting said map after full reconstruction.

133. An information processing system for securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

a filter adapted to receive said data input from said communications network and to separate, from said data input, said security sensitive content as extracted data for each corresponding security level, leaving remainder data;

means for storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer;

an access controller for permitting access to said respective extract stores for corresponding security levels with said associated security clearances; and,

a compiler, coupled to said means for storing and access controller, for permitting full or partial reconstruction of said data via said respective extract stores and remainder data based upon said corresponding security levels and associated security clearances.

134. An information processing system as claimed in claim 133 wherein said filter is on one of said client computer and said server computer.

135. An information processing system as claimed in claim 133 wherein server computer has a downloader and said filter is downloaded to said client computer.

136. An information processing system as claimed in claim 133 wherein said means for storing is on said server computer.

137. An information processing system as claimed in claim 133 wherein said server computer includes a remainder store and said means for storing operates on said remainder data at said server computer.

138. An information processing system as claimed in claim 133 wherein said client computer includes a remainder store and said means for storing operates on said remainder data at said client computer.

139. An information processing system as claimed in claim 133 including an encryptor coupled to said means for storing enabling encryption for said extracted data corresponding to said respective ones of said plurality of security levels.

140. An information processing system as claimed in claim 139 including a decryptor coupled to said compiler, for decryption with said means for storing and said compiler during reconstruction, said decryption corresponding to said respective ones of said plurality of security levels.

141. An information processing system as claimed in claim 133 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein said means for storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

142. An information processing system as claimed in claim 141 including an encryptor coupled to said means for storing enabling encryption for said extracted data corresponding to said respective ones of said plurality of security levels.

143. An information processing system as claimed in claim 142 including a decryptor coupled to said compiler, for decryption with said means for storing or and compiler during reconstruction, said decryption corresponding to said respective ones of said plurality of security levels.

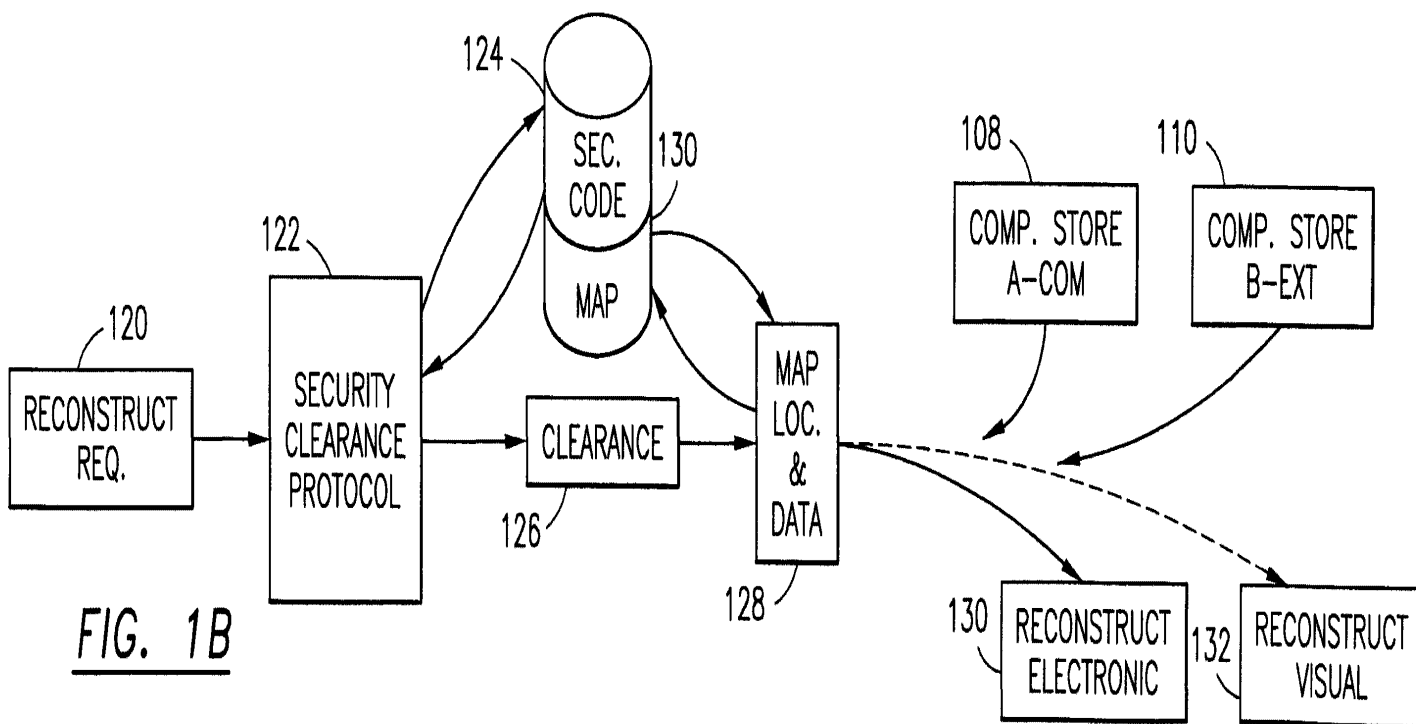
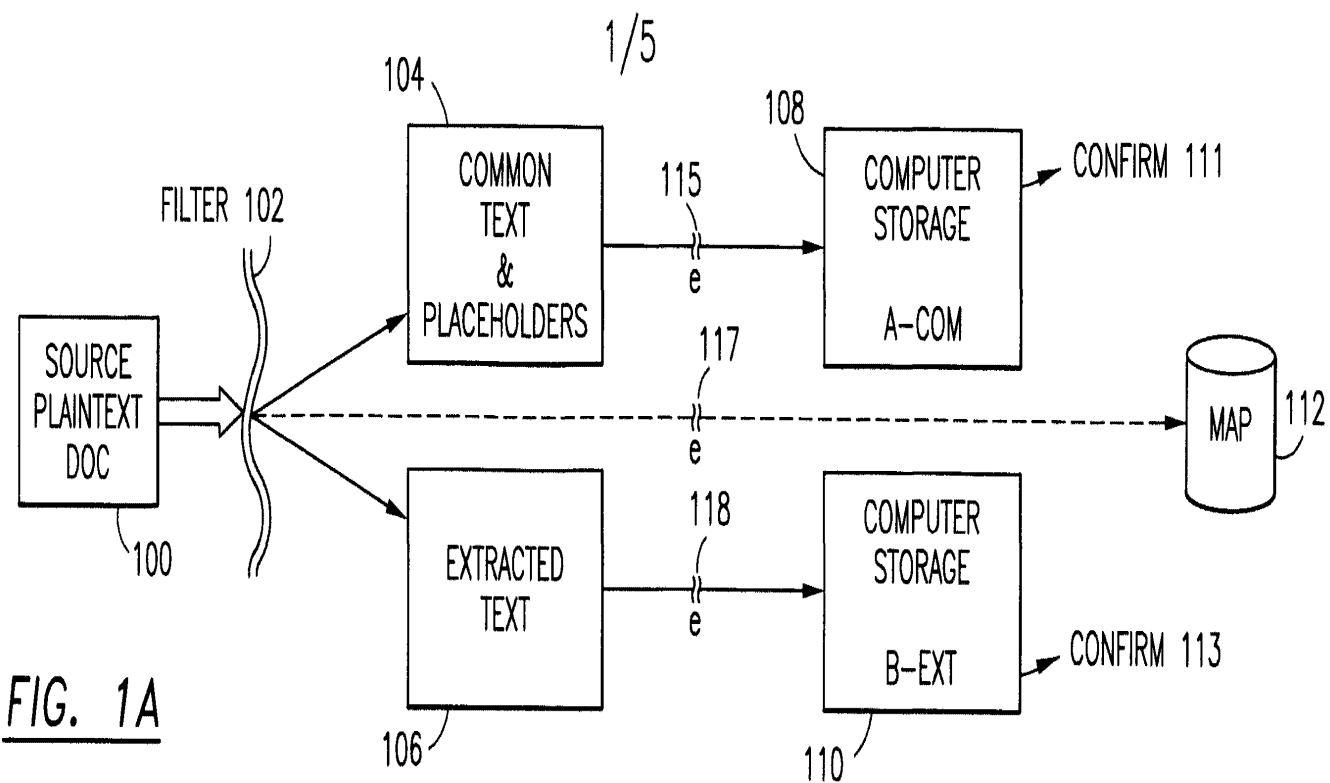
144. An information processing system as claimed in claim 133 wherein means for storing directs storage of said remainder data at said client computer on one of a fixed memory and a removable memory at said client computer.

145. An information processing system as claimed in claim 133 wherein means for storing directs storage of said remainder data at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

ABSTRACT

The method for securing data in a server-client computer system for security sensitive content includes extracting sensitive content and separating the security sensitive content from remainder data. The security sensitive content is grouped into security levels, each with a security clearance. The extracted data, for each security level, is remotely stored in extract stores. A map of storage sites may be generated. The filter and/or map may be destroyed or stored. The data input, extracted data and remainder data may be deleted from the originating computer. Encryption may be utilized to enhance security (including transfers of data, filter and map). Full or partial reconstruction of the data is permitted only in the presence of predetermined security clearances. The extraction and storage can be done on the input client computer or the web-based server. A computer readable medium containing programming instructions and an information processing system is encompassed.

H:\RCK\CLIENTS\Redlich\Patents\6851-02-div2-pa.wpd



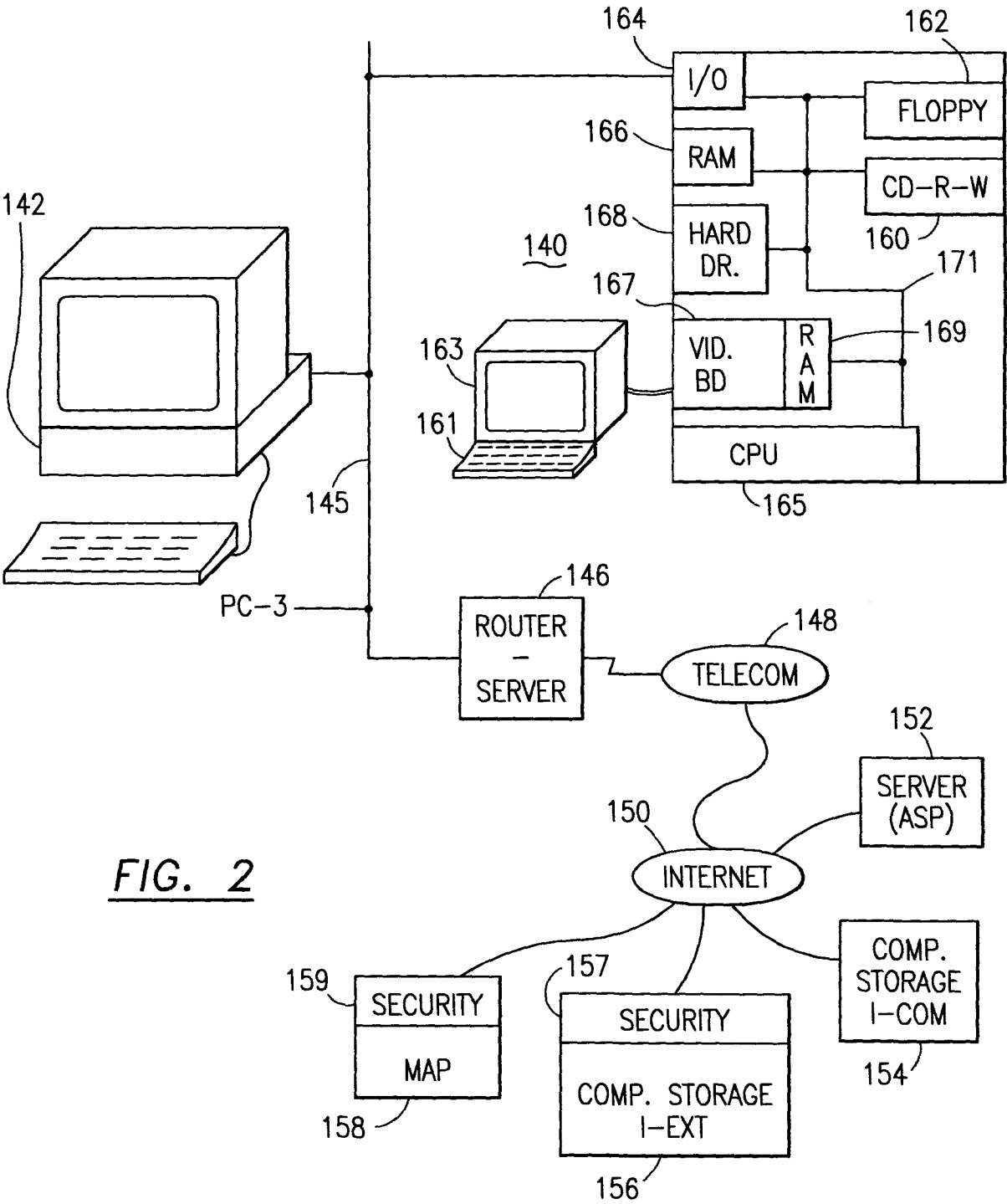
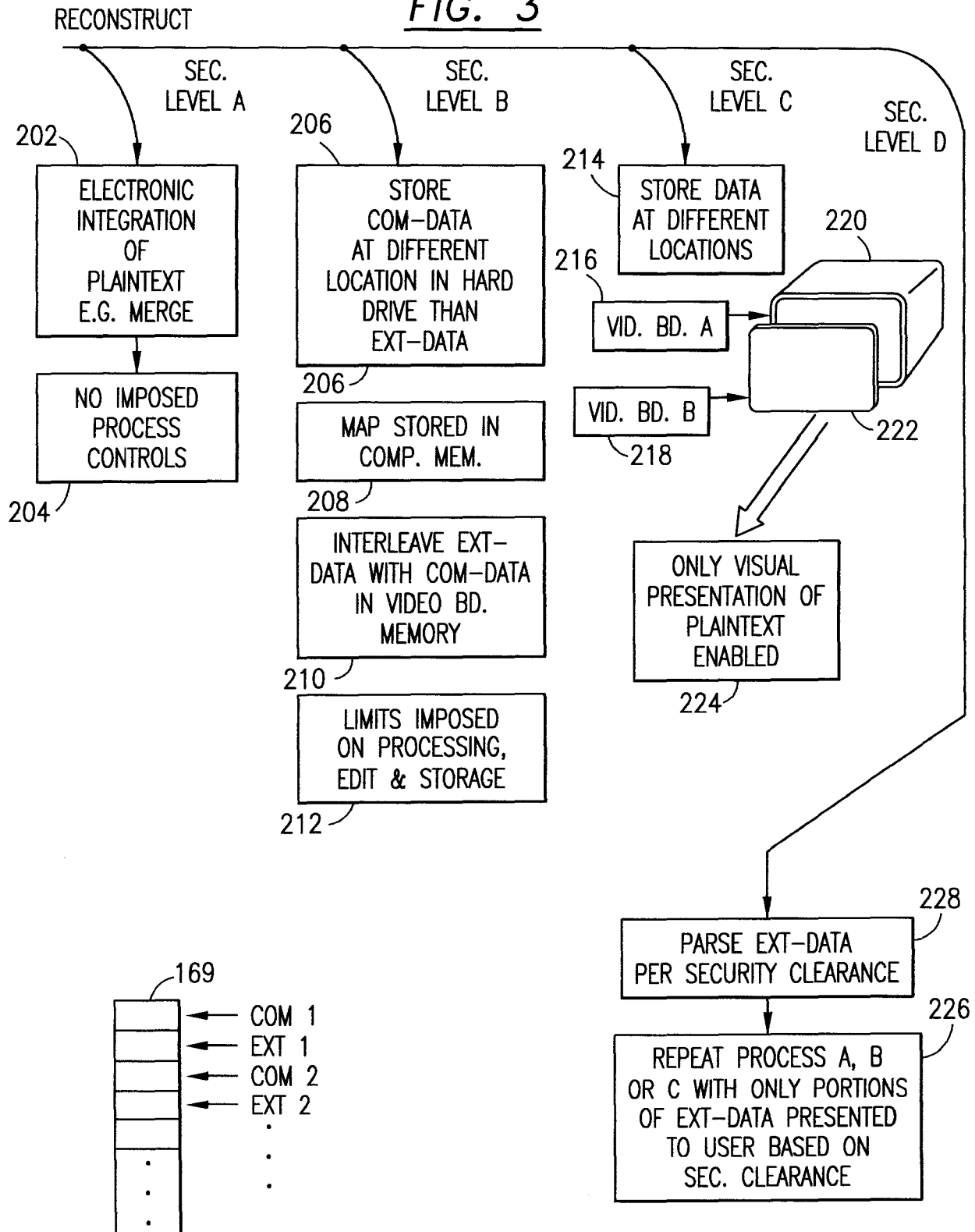
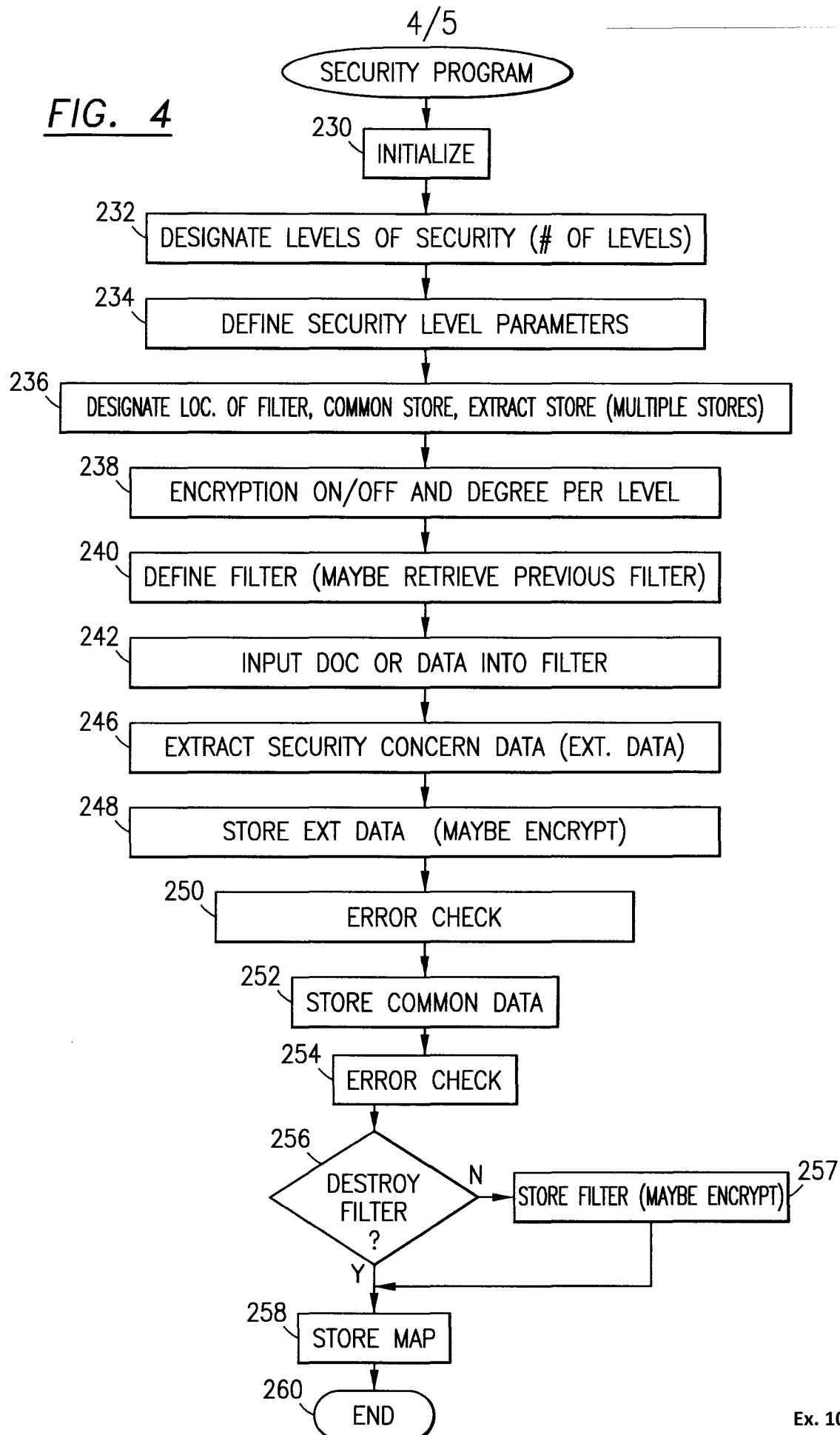


FIG. 2

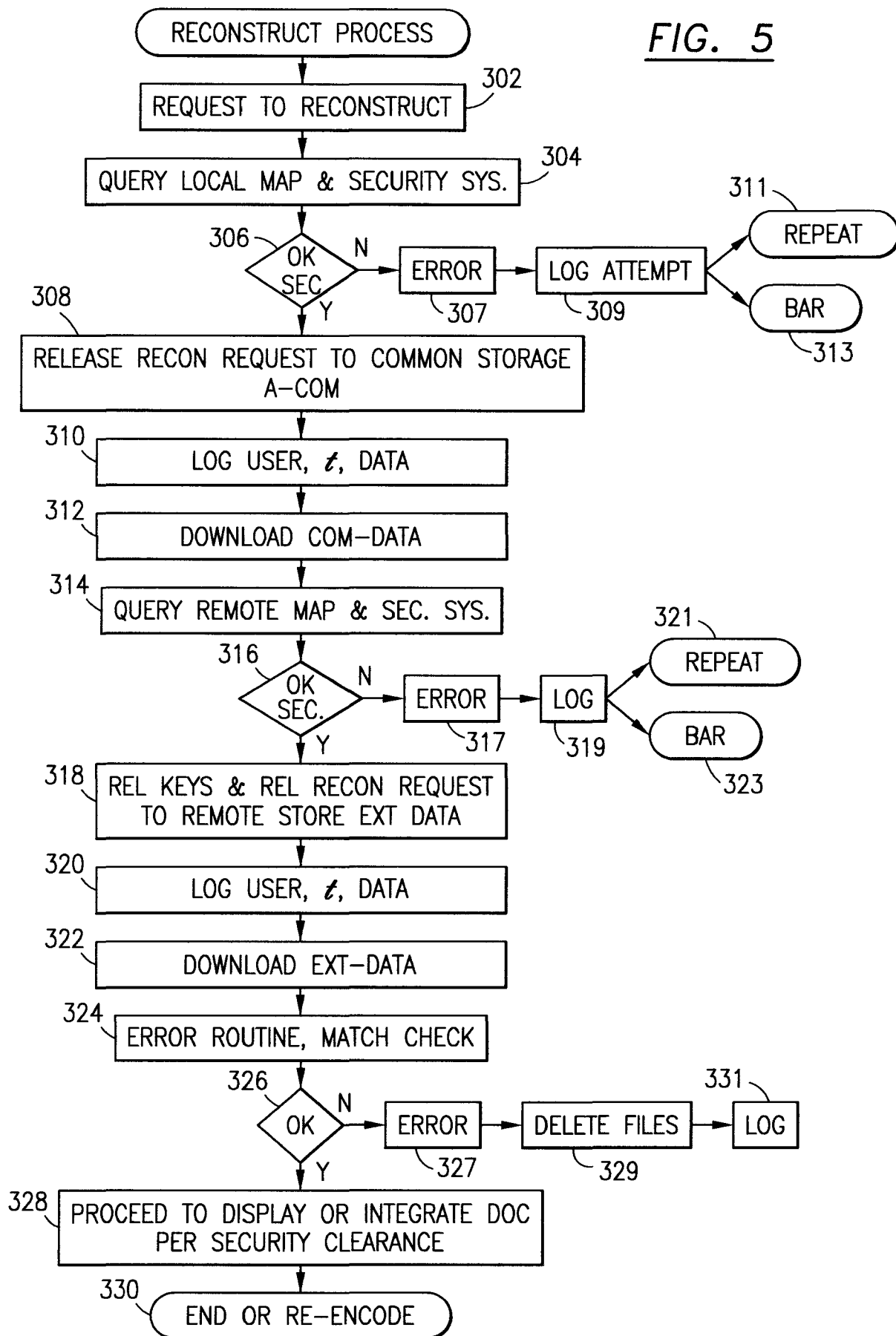
3/5

FIG. 3FIG. 3A

4/5

FIG. 4

5/5

FIG. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled DATA SECURITY SYSTEM AND METHOD
the specification of which

(check one) ☒ is attached hereto.
☐ was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐ Yes	☐ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐ Yes	☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>09/916,397</u> (Application Serial No.)	<u>July 27, 2001</u> (Filing Date)	<u>Pending</u> (Status) (patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

(Provisional Application No.)

(Filing Date)

(Provisional Application No.)

(Filing Date)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman, Reg. No. 35,171; and Steve Bongini, Reg. No. 40,917; Paul D. Bianco, Reg. No. 43,500.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**

Fleit, Kain, Gibbons, Gutman & Bongini, P.L.

750 Southeast Third Avenue, Suite 100

Ft. Lauderdale, Florida 33316-1153

Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich

Full name of sole or first inventor

Inventor's signature

Date

Miami Beach, FL

Residence

U.S.

Citizenship

4201 Collins Avenue, Apt. 2103

Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow

Full name of second joint inventor, if any

Inventor's signature

Date

Miami Beach, FL

Residence

U.S.

Citizenship

2915 Flamingo Drive

Post Office Address

Miami Beach, FL 33140

(Supply similar information and signature for third and subsequent joint inventors.)

\\Tiger\data share\IRCK\CLIENTS\Redlich\6851-02-div2-dec3.wpd

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No.

Filed: Herewith

For: Data Security System and Method

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

Patent No.	Inventor	Issue Date
6192472	Garay et al.	Feb. 20, 2001
6148342	Ho	Nov. 14, 2000
6094483	Fidrich et al.	Jul. 25, 2000
6055544	DeRose et al.	Apr. 25, 2000
5996011	Humes	Nov. 30, 1999
5905980	Masuichi et al.	May 18, 1999
5832212	Cragun et al.	Nov. 3, 1998
5485474	Rabin	Jan. 16, 1996

5933498	Schneck et al	Aug. 3, 1999
US2002/0073313	Brown et al.	Jun. 13, 2002
WO 00/75779-A2	Lambert	Dec. 14, 2000

-Ingrian i100, Content Security Appliance (2 pages)

-Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)

-Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)

-ZD Net Interactive Week - IBS, SAP: XML to Boost Security, integration.

-Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999.

-MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001.

-Cisco IDS Host Sensor Product, October 16, 2001.

The examiner in Serial No. 09/916,397 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
 U.S. Patent No. 5,581,682 to Anderson
 U.S. Patent No. 6,389,542 to Flyntz
 U.S. Patent No. 6,602,298 to Kirshenbaum
 U.S. Patent No. 6,078,907 to Lamm
 U.S. Patent No. 6,598,161 to Kluttz
 U.S. Patent No. 5,036,315 to Gurley
 The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
 The Uniform Resource Locator article "FOLD OC" (attached to Office Action)

The examiner in Serial No. 10/008,209 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
 U.S. Patent No. 5,581,682 to Anderson
 U.S. Patent No. 6,389,542 to Flyntz
 U.S. Patent No. 6,078,907 to Lamm (PRIMARY REFERENCE)
 U.S. Patent No. 6,598,161 to Kluttz

U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
The Uniform Resource Locator article "FOLD OC" (attached to Office Action)

The examiner in Serial No. 10/008,218 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,301,668 to Gleichauf
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
U.S. Patent No. 6,714,977 to Fowler
The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
The Uniform Resource Locator article "FOLD OC" (attached to Office Action)
Wylie "Survivable Information Storage Systems" (cited by Redlich)

The examiner in Serial No. 10/155,192 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman (PRIMARY REFERENCE)
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Patent No. 6,487,538 to Gupta
U.S. Patent No. 6,771,290 to Hoyle
Published U.S. Application 2002/0116641 to Mastrianni

The examiner in Serial No. 10/155,525 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman (PRIMARY REFERENCE)
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Published Patent Application 2002/0116641 to Mastrianni
U.S. Published Patent Application 2004/0054630 to Ginter
Microsoft Word "Learning Microsoft Word 7.0"

The examiner in Serial No. 10/277,196 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,253,203 to O'Flaherty
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 6,044,375 to Shmueli
U.S. Patent No. 6,662,189 to Oyanagi
U.S. Patent No. 5,036,315 to Gurley

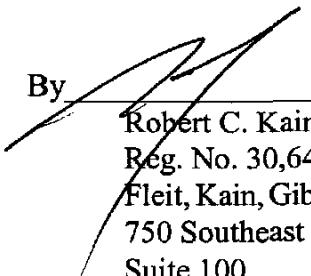
Related Cases

<u>Our Ref.</u>	<u>Serial No.</u>	<u>Filed</u>
-02-div1	tba	tba
-02-div2	tba	tba
-02-con	tba	tba
-02-cip5	10/390,807	March 19, 2004
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-03	10/396,088	Mar. 25, 2003

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-div2-IDS.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	MIMESweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingrian i100, Content Security Appliance (1 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigrigg, John D. Strunk, Gregory R. Ganger, Han Kiloccote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Exami ner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s)	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Data Security System and Method		
First Named Inventor:		Ron M. Redlich		
Filer:		Robert C. Kain		
Attorney Docket Number:		6851-02-DIV2		
Filed as Small Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Claims in excess of 20	2202	125	25	3125
Independent claims in excess of 3	2201	3	100	300
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				3850

Electronic Acknowledgement Receipt

EFS ID:	1159924
Application Number:	11465350
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	17-AUG-2006
Filing Date:	
Time Stamp:	17:20:06
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 3850
RAM confirmation Number	396
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
-----------------	----------------------	-----------	------------------	------------	-------

1	Transmittal letter	6851-02-div2-Transmittal.pdf	25732	no	1
Warnings:					
Information:					
2	Specification	6851-02-div2-pa-spec.pdf	104017	no	46
Warnings:					
Information:					
3	Claims	6851-02-div2-pa-clms.pdf	47666	no	24
Warnings:					
Information:					
4	Abstract	6851-02-div2-pa-abstr.pdf	16695	no	1
Warnings:					
Information:					
5	Drawings	6851-02-div2-dwgs.pdf	125017	no	5
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
6	Oath or Declaration filed	6851-02-div2-dec3.pdf	91991	no	2
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Filed	6851-02-div2-IDS.pdf	265738	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Information Disclosure Statement (IDS) Filed	PA-Ingrian-I100-content-security-appliance.pdf	104559	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

9	Information Disclosure Statement (IDS) Filed	PA-Element-Wise-XML-Encryption.pdf	235982	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
10	Information Disclosure Statement (IDS) Filed	PA-Survivable-Information-Storage-Systems.pdf	548011	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
11	Information Disclosure Statement (IDS) Filed	PA-ZD-Net-Interactive-Week.pdf	67921	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
12	Information Disclosure Statement (IDS) Filed	PA-Mostly-Static-Decentralized-Myers.pdf	2216378	no	43
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
13	Information Disclosure Statement (IDS) Filed	PA-Mimesweeper.pdf	630873	no	12
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
14	Information Disclosure Statement (IDS) Filed	PA-Cisco-IDS-Host-Sensor-Product.pdf	510120	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
15	Information Disclosure Statement (IDS) Filed	PA-Applied-Cryptography-Schneier.pdf	362813	no	5
Warnings:					
Information:					

This is not an USPTO supplied IDS fillable form					
16	Information Disclosure Statement (IDS) Filed	PA-FOLDOC.pdf	87383	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
17	Information Disclosure Statement (IDS) Filed	PA-Learning-Microsoft-Word.pdf	228594	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
18	Fee Worksheet (PTO-875)	fee-info.pdf	8513	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			5678003		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number

11/465,350**APPLICATION AS FILED – PART I**

(Column 1)

(Column 2)

SMALL ENTITY

OR

OTHER THAN
SMALL ENTITY

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		
TOTAL CLAIMS (37 CFR 1.16(i))	145 minus 20 =	125
INDEPENDENT CLAIMS (37 CFR 1.16(h))	6 minus 3 =	* 3
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

RATE (\$)	FEE (\$)
	150
	250
	100
X\$ 25	3125
X\$100	300
180	
TOTAL	3925

RATE (\$)	FEE (\$)
	300
	500
	200
X\$50	100
X\$200	
360	
TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

(Column 1)

(Column 2)

(Column 3)

SMALL ENTITY

OR

OTHER THAN
SMALL ENTITY

AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(i))	*	Minus **	=
Independent (37 CFR 1.16(h))	*	Minus ***	=
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
180	
TOTAL	
ADD'T FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
360	
TOTAL	
ADD'T FEE	

(Column 1)

(Column 2)

(Column 3)

OR

AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(i))	*	Minus **	=
Independent (37 CFR 1.16(h))	*	Minus ***	=
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
N/A	
TOTAL	
ADD'T FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
N/A	
TOTAL	
ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled DATA SECURITY SYSTEM AND METHOD
the specification of which

(check one) ☐ is attached hereto.

☒ was filed on 17-Aug-2006

as Application Serial No. 11/465,350

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)

(Country)

(Day/Month/Year Filed)

☐ Yes ☐ No

(Number)

(Country)

(Day/Month/Year Filed)

☐ Yes ☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

09/916,397
(Application Serial No.)

July 27, 2001
(Filing Date)

Pending
(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

(Provisional Application No.)

(Filing Date)

(Provisional Application No.)

(Filing Date)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman, Reg. No. 35,171; and Steve Bongini, Reg. No. 40,917; Paul D. Bianco, Reg. No. 43,500.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**

Fleit, Kain, Gibbons, Gutman & Bongini, P.L.

750 Southeast Third Avenue, Suite 100

Ft. Lauderdale, Florida 33316-1153

Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich

Full name of sole or first inventor

Ron Redlich
Inventor's signature

08-23-2006
Date

Miami Beach, FL

Residence

U.S.

Citizenship

4201 Collins Avenue, Apt. 2103

Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow

Full name of second joint inventor, if any

Martin A. Nemzow
Inventor's signature

08-23-2006
Date

Miami Beach, FL

Residence

U.S.

Citizenship

2915 Flamingo Drive

Post Office Address

Miami Beach, FL 33140

(Supply similar information and signature for third and subsequent joint inventors.)

\\Tiger\data\share\RCK\CLIENTS\Redlich\6851-02-div2-dec3.wpd

Electronic Acknowledgement Receipt

EFS ID:	1169907
Application Number:	11465350
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	24-AUG-2006
Filing Date:	
Time Stamp:	13:13:08
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Oath or Declaration filed	6851-02-div2-dec-signed.pdf	95651	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	95651
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.	

Electronic Acknowledgement Receipt

EFS ID:	1169907
Application Number:	11465350
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	24-AUG-2006
Filing Date:	
Time Stamp:	13:13:08
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Oath or Declaration filed	6851-02-div2-dec-signed.pdf	95651	no	2

09/26/2006 MNGUYEN 00000005 031231 11465350

01 FC:2051 65.00 DA



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/465,350	08/17/2006	Ron M. Redlich	6851-02-DIV2

CONFIRMATION NO. 1129

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL333161153

Title: Data Security System and Method

Publication No. US-2007-0006326-A1

Publication Date: 01/04/2007

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 703-305-3028.

Pre-Grant Publication Division, 703-605-4283

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No 11/465,350

Group Art 2176

Confirmation No.: 1129

Filed: August 17, 2006

For: Data Security System and Method

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

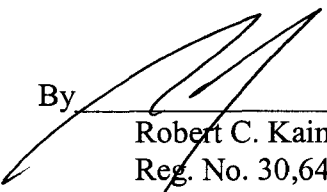
Patent No.	Inventor	Issue Date
6,922,696	Lincoln et al.	Jul. 26, 2005
7,031,961	Pitkow et al.	Apr. 18, 2006

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the

pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-DIV2-IDS1.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date Aug. 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,922,696	07/26/2005	Lincoln et al.	707	101	
	7,031,961	04/18/2006	Pitkow et al.	707	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form PTO-1449-1.wpd

Electronic Acknowledgement Receipt

EFS ID:	2638544
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	26-DEC-2007
Filing Date:	17-AUG-2006
Time Stamp:	12:45:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6851-02-div2-ids-1449.pdf	59240 10ffb85064dcbc7e94fa8f92ffa1d895905b05d6	no	3

Warnings:

Information:

Total Files Size (in bytes):

59240

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Group Art 2176

Confirmation No.: 1129

Filed: August 17, 2006

For: Data Security System and Method

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this supplemental Information Disclosure Statement pursuant to 37 C.F.R. §1.97 which represents foreign search results.

Patent No.	Inventor	Issue Date
6,078,907	Lamm	Jun. 20, 2000
6,253,203	O'Flaherty et al.	Jun. 26, 2001
5,960,080	Fahlman et al.	Sep. 28, 1999

-Published Canadian Patent Application CA 2 345 148 June 4, 2000.

-"Processing of confidential information in distributed systems by fragmentation" by

J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997).

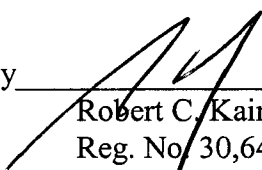
-“Secure External References in Multimedia Email Messages” B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996.

-“Element-Wise XML Encryption” H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000.

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.

Reg. No. 30,648

Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.

750 Southeast Third Avenue

Suite 100

Ft. Lauderdale, Florida 33316-1153

Telephone: 954-768-9002

Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-div2-Supp-IDS-030408.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-div2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date August 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	06/20/2000	Lamm	705	40	
	6,253,203	06/26/2001	O'Flaherty et al.	707	9	
	5,960,808	09/28/1999	Fahlman et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	CA 2 345 148	06/04/2000	Canada			X

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Processing of confidential information in distributed systems by fragmentation" by J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997)	
	"Secure External References in Multimedia Email Messages" B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996	
	"Element-Wise XML Encryption" H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000	

EXAMINER

DATE CONSIDERED

Electronic Acknowledgement Receipt

EFS ID:	2953877
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	05-MAR-2008
Filing Date:	17-AUG-2006
Time Stamp:	16:01:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6851-02-div2-Supp-IDS-144 9-030408.pdf	157997 69ac9e981264565de47148efce01ed8304bf6861	no	3

Warnings:

Information:

Total Files Size (in bytes):

157997

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Confirmation No.: 1129

Group Art 2176

Filed: August 17, 2006

For: Data Security System and Method

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R.

§1.97. Applicant's related cases are listed below.

The examiner in Serial No. 11/465309 cited the following references:

U.S. Patent No. 6,845,448 to Chaganti (Jan. 2005; 713/166)
U.S. Patent No. 6,941,459 to Hind (Sept., 2005; 713/167)
U.S. Patent No. 7,010,681 to Fletcher (Mar. 2006; 713/154)

The examiner in Serial No. 10/396,088 cited the following references:

U.S. Patent No. 6,922,696 to Lincoln
U.S. Patent No. 7,031,961 to Pitkow
U.S. Patent No. 7,089,428 to Farley
U.S. Patent No. 7,188,107 to Moon

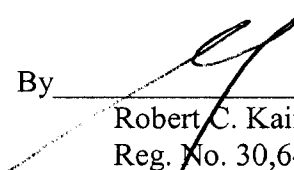
Related Cases

<u>Our Ref.</u>	<u>Serial No.</u>	<u>Filed</u>
-02-div1	11/465309	08.17.2006
-02-div2	11/465350	08.17.2006
-02-con	11/465388	08.17.2006
-02-cip4-con	11/682941	03.07.2007
-02-cip5	10/390,807	March 19, 2004
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-02-cip10	11/829207	09.06.2007
-03	10/396,088	Mar. 25, 2003

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al	
	Filing Date August 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form-PTO-1449-Master.wpd

Electronic Acknowledgement Receipt

EFS ID:	4738930
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	05-FEB-2009
Filing Date:	17-AUG-2006
Time Stamp:	11:53:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	6851-02-div2-IDS-020409- update-pendng-IDS.pdf	78100 60f5f196558e40fa82f5c14525db115aab583347	no	3

Warnings:

Information:

Total Files Size (in bytes):

78100

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	5043058
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	26-MAR-2009
Filing Date:	17-AUG-2006
Time Stamp:	16:51:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	6851-02-div2-IDS-Supple- F1449-032409.pdf	69082 05b3e833369e7f0cb0b2e0f7cc377a72cf92 ae2b	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Secure-External.pdf	1060497	no	8
			9ab51ddd72a1c4fe818829f9fbf8942e9a1c29b		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Proces-Confid-Info.pdf	812445	no	12
			687b4d764bade290dde95a47f4c85b8aac2c26c6		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Canada-2345148-Silanis. pdf	1113678	no	28
			52f3e78f2267c62b1f79ceb703fa830d01646c99		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
Total Files Size (in bytes):			3055702		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Confirmation No.: 1129

Examiner Kim Y Vu

Filed: August 17, 2006

Group Art 2435

For: Data Security System and Method

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97. The prior art cited below was cited in a pending, non-U.S. patent application as being technical background.

-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.

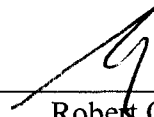
-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.

-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-div2-IDS-Supple-032409.wpd

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-div2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date August 17, 2006	Group Art Unit 2435

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.	
	-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.	
	-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.	

EXAMINER

DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form-PTO-1449-supple.wpd



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/465,350

08/17/2006

Ron M. Redlich

6851-02-DIV2

1129

4897 7590 08/25/2009
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2437

MAIL DATE

DELIVERY MODE

08/25/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/465,350	Applicant(s) REDLICH ET AL.	
	Examiner MICHAEL PYZOSHA	Art Unit 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-145 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-145 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 August 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☐ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413) |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) ☒ Information Disclosure Statement(s) (PTO/SB/08) | 5) ☐ Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>See Continuation Sheet</u> . | 6) ☐ Other: _____ |

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :8/17/06, 12/26/07, 3/5/08, 2/5/09, 3/26/09.

DETAILED ACTION

1. Claims 1-145 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 106-132 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 106-132 relate to a computer readable medium containing instructions to perform certain actions. Referring to the specification paragraphs [0069] and [0070] the computer readable medium can be either tangible media (e.g. memory) or non-tangible media (e.g. wireless networks). As such, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the mean of 35 USC §101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

It is recommended to change “computer readable medium” to “computer readable storage medium” to restrict the claims to the tangible media thereby making the claims statutory.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-73 of U.S. Patent No. 7103915.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the ‘915 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

6. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-73 of U.S. Patent No. 7140044.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data a client while

Art Unit: 2437

storing data on a server, while the '044 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

7. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 7146644. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '644 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

8. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-85 of U.S. Patent No. 7191252. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '252 claims relate to securing email and browser data, using the same steps, and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

9. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-143 of U.S. Patent No. 7313825. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '825 claims relate to securing data, using the same

Art Unit: 2437

steps, based on location and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data based on location in order to prevent unauthorized divulgence of secret data.

10. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-90 of U.S. Patent No. 7322047.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '047 claims relate to securing data, using the same steps, in a computer database and one of ordinary skill in the art would recognize that the client storing data on a server could contain a database that is protected by the steps.

11. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-27 of U.S. Patent No. 7349987.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application stores the extracted data remotely while '987 stores the data locally; one of ordinary skill would recognize that extracted data can be stored locally or remotely in order to provide access to the extracted data only on a single machine or access to many machines.

12. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-72 of U.S. Patent No. 7546334.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the '334 application uses contextual information to filter the security

related data, one of ordinary skill in the art recognizes that using contextual information is a well-know method of extracting data in order to extract the proper data.

13. Claims 1-145 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-54 of U.S. Patent no. 7552482. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '482 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

14. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-108 of copending Application No. 10998363. Although the conflicting claims are not identical, they are not patentably distinct from each other because the '363 application uses tags to filter the security related data, one of ordinary skill in the art recognizes that tags are a well-know method of extracting data in order to specify exactly what to be extracted.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 10998365. Although the conflicting claims are not identical, they are not patentably distinct from each other because the '365 application uses contextual information to filter the security related data, one of ordinary skill in the art

recognizes that using contextual information is a well-know method of extracting data in order to extract the proper data.

15. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-12 of copending Application No. 10988366. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application stores the extracted data remotely while '366 stores the data in independent storage locations coupled by independent networks; one of ordinary skill would recognize that extracted data can be stored remotely using independent networks in order to provide specific security via the independent networks.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

16. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-45 of copending Application No. 11465388. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '388 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

17. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-44 of copending Application No. 11682941. Although the conflicting claims are not identical, they are not patentably distinct from each other because the present application relates to securing data on a client while storing data on a server, while the '941 claims relate to securing data, using the same steps, in a computer network and one of ordinary skill in the art would recognize that the steps could be performed on a client while storing data on a server to protect its data.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

18. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 11829207. Although the conflicting claims are not identical, they are not patentably distinct from each other because each application relates to the same method of filtering data and storing the data based on security level.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

19. Claims 1-145 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 12403850. Although the conflicting claims are not identical, they are not patentably distinct from each other because the '850 application uses contextual information to filter the security related data, one of ordinary skill in the art

recognizes that using contextual information is a well-know method of extracting data in order to extract the proper data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 11/465,350
Art Unit: 2437

Page 10

/Michael Pyzocha/
Examiner, Art Unit 2437



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1129

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
11/465,350	08/17/2006	715	2437	6851-02-DIV2		
RULE						
APPLICANTS Ron M. Redlich, Miami Beach, FL; Martin A. Nemzow, Miami Beach, FL;						
** CONTINUING DATA ***** This application is a DIV of 09/916,397 07/27/2001 PAT 7,103,915 which claims benefit of 60/260,398 01/09/2001 * and claims benefit of 60/287,813 05/02/2001 and claims benefit of 60/267,944 02/12/2001 and claims benefit of 60/247,242 11/13/2000 and claims benefit of 60/247,232 11/13/2000 (*)Data provided by applicant is not consistent with PTO records.						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 09/25/2006						
Foreign Priority claimed	☐ Yes ☒ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☐ Yes ☒ No		FL	5	145	6
Verified and	/MICHAEL J PYZOCHA/	Initials				
Acknowledged	Examiner's Signature					
ADDRESS ROBERT C. KAIN, JR. 750 SOUTHEAST THIRD AVENUE SUITE 100 FT LAUDERDALE, FL 333161153						
TITLE Data Security System and Method						
FILING FEE RECEIVED 3915	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		☐ All Fees			
			☐ 1.16 Fees (Filing)			
			☐ 1.17 Fees (Processing Ext. of time)			
			☐ 1.18 Fees (Issue)			
			☐ Other _____			
			☐ Credit			

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S35	39	(REDLICH near RON) (NEMZOW near MARTIN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S36	1538	(726/27).OCLS.	US-PGPUB; USPAT	OR	OFF	2009/08/19 09:39
S37	641	713/166.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S38	2845	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S39	7099	(extract\$4 filter\$4) with (separat\$4 distinct\$4) with (database memory location)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S40	58	S39 same security	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S41	32	S40 not redlich.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S42	2803	security near level same (separat\$4 distinct\$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S43	28	(digital adj doors).as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39

S44	440754	(redact\$4 filter\$4 extract \$4) with separat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S45	4832	S44 same partial	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S46	39	S44 same partial with reconstruct\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S47	9393	(redact\$4 filter\$4 extract \$4) with separat\$4 with (database storage memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S48	211	S47 same partial\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S49	91	S48 and @ad< "20001113"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S50	237	S47 and partial\$4 with (combin\$6 reconstruct\$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S51	118	security with clearance same (filter\$4 redact\$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S52	484	multiple with (stor\$4 memory server) with security with level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S53	28	partial with reconstruct\$4 same security with level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39

S54	166	security same filter\$4 same extract\$4 same stor \$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S55	33	filter\$4 same security near sensitive near word	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S56	54	automatic\$5 with redact \$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S57	32	("20020073313" "20020116641" "20040054630" "5036315" "5485474" "5532950" "5581682" "5832212" "5905980" "5933498" "5960080" "5960808" "5996011" "6044375" "6055544" "6073165" "6078907" "6094483" "6148342" "6253203" "6301668" "6389542" "6487538" "6598161" "6602298" "6662189" "6714977" "6771290" "6922696" "0619472" "7031961" "0075779").PN.	US-PGPUB; USPAT	OR	OFF	2009/08/19 09:39
S58	1999	(715/255).ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S59	4	S58 and redact\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/08/19 09:39
S60	736	(redact\$4 filter\$4 extract \$4) same security adj level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S61	109	S60 and @ad<"20001113"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39

S62	354	(redact\$4 filter\$4 extract \$4) with security adj level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S63	51	S62 and @ad<"20001113"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39
S64	50	S63 not S57	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/19 09:39

EAST Search History (Interference)

< This search history is empty >

8/ 19/ 09 10:25:59 AM**C:\ Documents and Settings\ mpyzocha1\ My Documents\ EAST\ Workspaces\ 11465350.w sp**

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al	
	Filing Date August 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

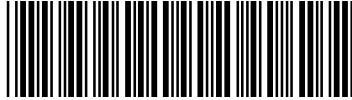
FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

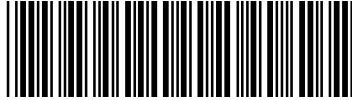
EXAMINER	/Michael Pyzocha/	DATE CONSIDERED	08/19/2009
----------	-------------------	-----------------	------------

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form-PTO-1449-Master.wpd

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

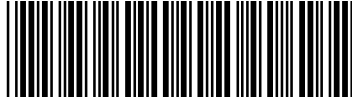
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	08/19/2009									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									
	31	✓									
	32	✓									
	33	✓									
	34	✓									
	35	✓									
	36	✓									

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

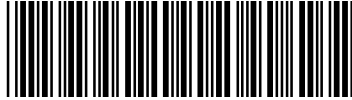
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	08/19/2009									
	37	✓									
	38	✓									
	39	✓									
	40	✓									
	41	✓									
	42	✓									
	43	✓									
	44	✓									
	45	✓									
	46	✓									
	47	✓									
	48	✓									
	49	✓									
	50	✓									
	51	✓									
	52	✓									
	53	✓									
	54	✓									
	55	✓									
	56	✓									
	57	✓									
	58	✓									
	59	✓									
	60	✓									
	61	✓									
	62	✓									
	63	✓									
	64	✓									
	65	✓									
	66	✓									
	67	✓									
	68	✓									
	69	✓									
	70	✓									
	71	✓									
	72	✓									

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

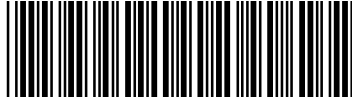
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	08/19/2009								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓								
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	08/19/2009								
	109	✓								
	110	✓								
	111	✓								
	112	✓								
	113	✓								
	114	✓								
	115	✓								
	116	✓								
	117	✓								
	118	✓								
	119	✓								
	120	✓								
	121	✓								
	122	✓								
	123	✓								
	124	✓								
	125	✓								
	126	✓								
	127	✓								
	128	✓								
	129	✓								
	130	✓								
	131	✓								
	132	✓								
	133	✓								
	134	✓								
	135	✓								
	136	✓								
	137	✓								
	138	✓								
	139	✓								
	140	✓								
	141	✓								
	142	✓								
	143	✓								
	144	✓								

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	08/19/2009							
	145	✓							

Search Notes 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

SEARCHED			
Class	Subclass	Date	Examiner
726	27	8/19/09	MJP
713	166	8/19/09	MJP
713	193	8/19/09	MJP
715	255	8/19/09	MJP

SEARCH NOTES		
Search Notes	Date	Examiner
BRS search in USPAT, USPGPUB, EPO, JPO, IBM, DERWENT, see attached search history; inventor name search; all claims have been reviewed for 35 USC non-statutory subject matter	8/19/09	MJP

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-div2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date August 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	06/20/2000	Lamm	705	40	
	6,253,203	06/26/2001	O'Flaherty et al.	707	9	
	5,960,808	09/28/1999	Fahlman et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	CA 2 345 148	06/04/2000	Canada			X

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Processing of confidential information in distributed systems by fragmentation" by J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997)	
	"Secure External References in Multimedia Email Messages" B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996	
	"Element-Wise XML Encryption" H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000	

EXAMINER

/Michael Pyzocha/

DATE CONSIDERED

08/19/2009

G:\RCK\CLIENTS\Redlich\6851-02-div2-Supp-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-div2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date August 17, 2006	Group Art Unit 2435

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.	
	-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.	
	-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.	

EXAMINER /Michael Pyzocha/

DATE CONSIDERED 08/19/2009

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form-PTO-1449-supple.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	MIMESweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER

/Michael Pyzocha/

DATE CONSIDERED

08/19/2009

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingrian i100, Content Security Appliance (1 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigg, John D. Strunk, Gregory R. Ganger, Han Kilocote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER

/Michael Pyzocha/

DATE CONSIDERED

08/19/2009

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER /Michael Pyzocha/

DATE CONSIDERED 08/19/2009

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number
Title: Data Security System and Method	Applicant(s)	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

/Michael Pyzocha/

DATE CONSIDERED 08/19/2009

\\Tiger\data\share\RCK\CLIENTS\Redlich\6851-02-div2-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-DIV2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date Aug. 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,922,696	07/26/2005	Lincoln et al.	707	101	
	7,031,961	04/18/2006	Pitkow et al.	707	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER /Michael Pyzocha/ DATE CONSIDERED 08/19/2009

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form PTO-1449-1.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Group Art 2176

Confirmation No.: 1129

Filed: August 17, 2006

For: Data Security System and Method

AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Amendment responds to the Office Action dated April 3, 2009. Please charge Deposit Account No. 03-1231 for the Terminal Disclaimer fee of \$70.00. Applicant is a small entity. Please debit or credit Deposit Account No. 03-1231 for any underpayment or overpayment. This amendment includes:

- (a) Transmittal (1 pg., p. 1)
- (b) Claims (26 pgs., pp. 2 - 27)
- (c) Remarks (2 pgs., pp. 28 - 29)
- (d) Terminal Disclaimer (4 pgs.)

[space left blank]

CLAIMS

1. (original) A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

accepting data input which includes security sensitive content via said client computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

2. (original) A method as claimed in claim 1 wherein accepting occurs at one of said client computer and said server computer.

3. (original) A method as claimed in claim 1 wherein extracting occurs at one of said client computer and said server computer.

4. (original) A method as claimed in claim 1 wherein one or both of extracting and storing occurs at said server computer.

5. (original) A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system..

6. (original) A method as claimed in claim 1 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

7. (original) A method as claimed in claim 6 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

8. (original) A method as claimed in claim 1 wherein permitting full or partial reconstruction of said data occurs at one of said client computer and said server computer.

9. (original) A method as claimed in claim 1 wherein said client-server computer system includes at least first and second client computers, said first client computer being said at least one client computer, and wherein accepting data input occurs at said first client computer and permitting full or partial reconstruction of said data occurs at said second client computer.

10. (original) A method as claimed in claim 9 wherein extracting occurs at one of said first client computer and said server computer.

11. (original) A method as claimed in claim 10 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

12. (original) A method as claimed in claim 10 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

13. (original) A method as claimed in claim 1 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

14. (original) A method as claimed in claim 13 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

15. (original) A method as claimed in claim 14 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

16. (original) A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer and said client computer.

17. (original) A method as claimed in claim 1 wherein storing of said remainder data occurs at said client computer on one of a fixed memory and a removable memory at said client computer.

18. (original) A method as claimed in claim 16 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

19. (original) A method as claimed in claim 1 including storing a map or locating data for said respective extract stores.

20. (original) A method as claimed in claim 19 wherein the storing of said map or locating data occurs at one of said client computer and said server computer.

21. (original) A method as claimed in claim 20 wherein the storing of said map or locating data occurs at said client computer in one of a fixed memory and a removable memory at said client computer.

22. (original) A method as claimed in claim 20 wherein the storing of said map or locating data via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

23. (original) A method as claimed in claim 19 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

24. (original) A method as claimed in claim 23 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

25. (original) A method as claimed in claim 24 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer and said map locates said remainder store.

26. (original) A method as claimed in claim 1 including establishing a plurality of filters for groups of security sensitive content corresponding to respective ones of said plurality of security levels and using said filter during the extraction of security sensitive content.

27. (original) A method as claimed in claim 26 including storing said plurality of filters on one of said client computer and said server computer in one of fixed memory and removable memory.

28. (original) A method as claimed in claim 27 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

29. (original) A method as claimed in claim 27 including one of destroying or storing the filter after extraction.

30. (original) A method as claimed in claim 2 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon accepting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

31. (original) A method as claimed in claim 3 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon extracting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

32. (original) A method as claimed in claim 4 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on said server computer in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

33. (original) A method as claimed in claim 26 wherein said filters identify either by inclusion or exclusion said security sensitive content.

34. (original) A method as claimed in claim 1 including deleting said data input after storing.

35. (original) A method as claimed in claim 24 including deleting said map after full reconstruction.

36. (original) A method as claimed in claim 1 wherein said client-server computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

37. (original) A method as claimed in claim 1 wherein said client-server computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

38. (original) A method as claimed in claim 1 wherein extracting occurs at said client computer either automatically or manually with operator input.

39. (original) A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

from input data, extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

separately storing said extracted data, for each corresponding security level, in the respective extract store, apart from said remainder data stored in one or both of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

40. (original) A method as claimed in claim 39 wherein extracting occurs at one of said client computer and said server computer.

41. (original) A method as claimed in claim 39 wherein one or both of extracting and storing occurs at said server computer.

42. (original) A method as claimed in claim 39 wherein extracting includes filtering security sensitive content at one of said client computer and said server computer.

43. (original) A method as claimed in claim 39 wherein said server computer stores said remainder data thereat or in remotely disposed remainder stores in said client-server computer system.

44. (original) A method as claimed in claim 43 including storing a map of said respective extract stores.

45. (original) A method as claimed in claim 44 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

46. (original) A method as claimed in claim 45 wherein said map is stored on one of said client computer and said server computer.

47. (original) A method as claimed in claim 46 including the step of decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

48. (original) A method as claimed in claim 39 wherein said computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

49. (original) A method as claimed in claim 39 wherein said computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

50. (original) A method as claimed in claim 39 including deleting said input data after storing.

51. (original) A method as claimed in claim 39 including mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

52. (original) A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality

of security levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

extracting security sensitive content from a data input via said server computer to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

53. (original) A method as claimed in claim 52 wherein said reconstruction is a download operation adapted to be directed at said client computer.

54. (original) A method as claimed in claim 53 wherein said client-server computer system includes first and second client computers, said extracting is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

55. (original) A method as claimed in claim 52 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

56. (original) A method as claimed in claim 52 wherein said client-server computer system includes first and second client computers, said remainder data store is part of said first client computer and the storing of remainder data includes a store download operation adapted to be directed at said first client computer.

57. (original) A method as claimed in claim 56 said extracting is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

58. (original) A method as claimed in claim 52 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

59. (original) A method as claimed in claim 58 wherein storing or reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

60. (original) A method as claimed in claim 52 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

61. (original) A method as claimed in claim 60 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

62. (original) A method as claimed in claim 61 wherein reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

63. (original) A method as claimed in claim 52 wherein storing of said remainder data occurs upon server instruction adapted to be directed at said client computer on one of a fixed memory and a removable memory at said client computer.

64. (original) A method as claimed in claim 60 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

65. (original) A method as claimed in claim 52 including storing a map or locating data for said respective extract stores.

66. (original) A method as claimed in claim 65 wherein the storing of said map or locating data occurs at one of a map store and said server computer.

67. (original) A method as claimed in claim 66 wherein the storing of said map or locating data occurs via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

68. (original) A method as claimed in claim 65 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

69. (original) A method as claimed in claim 68 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

70. (original) A method as claimed in claim 52 wherein a plurality of filters are provided for groups of security sensitive content corresponding to respective ones of said plurality of security levels, downloading, from said server computer, one or more of said filters to facilitate extraction of security sensitive content.

71. (original) A method as claimed in claim 70 including storing said plurality of filters on said server computer in one of fixed memory and removable memory.

72. (original) A method as claimed in claim 71 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

73. (original) A method as claimed in claim 71 including one of destroying or storing the filter after extraction.

74. (original) A method as claimed in claim 54 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

75. (original) A method as claimed in claim 55 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

76. (original) A method as claimed in claim 70 wherein said filters identify either by inclusion or exclusion said security sensitive content.

77. (original) A method as claimed in claim 52 including deleting said data input after storing.

78. (original) A method as claimed in claim 69 including deleting said map after full reconstruction.

79. (original) A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

facilitating the extraction of security sensitive content from a data input to obtain extracted data for each corresponding security level and remainder data;

at said server computer, storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

80. (original) A method as claimed in claim 79 wherein said reconstruction is a download operation adapted to be directed at said client computer.

81. (original) A method as claimed in claim 80 wherein said client-server computer system includes first and second client computers, said facilitating the extraction is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

82. (original) A method as claimed in claim 79 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

83. (original) A method as claimed in claim 79 wherein said client-server computer system includes first and second client computers, said remainder data store is part of said first client computer and the storing of remainder data includes a store download operation adapted to be directed at said first client computer.

84. (original) A method as claimed in claim 83 said facilitating the extraction is part of an upload operation adapted to be associated with said first client computer and said download reconstruction is adapted to be directed at said second client computer.

85. (original) A method as claimed in claim 79 wherein storing or said facilitating the extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

86. (original) A method as claimed in claim 85 wherein storing or reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

87. (original) A method as claimed in claim 79 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

88. (original) A method as claimed in claim 87 wherein storing or said facilitating the extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

89. (original) A method as claimed in claim 88 wherein reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

90. (original) A method as claimed in claim 79 wherein storing of said remainder data occurs upon server instruction adapted to be directed at said client computer on one of a fixed memory and a removable memory at said client computer.

91. (original) A method as claimed in claim 79 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

92. (original) A method as claimed in claim 79 including storing a map or locating data for said respective extract stores.

93. (original) A method as claimed in claim 92 wherein the storing of said map or locating data occurs at one of a map store and said server computer.

94. (original) A method as claimed in claim 93 wherein the storing of said map or locating data occurs via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

95. (original) A method as claimed in claim 94 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

96. (original) A method as claimed in claim 95 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

97. (original) A method as claimed in claim 92 wherein a plurality of filters are provided for groups of security sensitive content corresponding to respective ones of said plurality of security levels, downloading, from said server computer, one or more of said filters to facilitate extraction of security sensitive content.

98. (original) A method as claimed in claim 97 including storing said plurality of filters on said server computer in one of fixed memory and removable memory.

99. (original) A method as claimed in claim 98 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

100. (original) A method as claimed in claim 98 including one of destroying or storing the filter after extraction.

101. (original) A method as claimed in claim 81 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

102. (original) A method as claimed in claim 82 including
establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and downloading, from said server computer, a

respective filter to facilitate extraction of security sensitive content for said each corresponding security level;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of instructing the destruction or storage of the respective filter after extraction.

103. (original) A method as claimed in claim 97 wherein said filters identify either by inclusion or exclusion said security sensitive content.

104. (original) A method as claimed in claim 79 including deleting said data input after storing.

105. (original) A method as claimed in claim 96 including deleting said map after full reconstruction.

106. (currently amended) A computer readable storage medium containing programming instructions for securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network, the programming instructions comprising:

accepting data input which includes security sensitive content via said client computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

107. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system.

108. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

109. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 108 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

110. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

111. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 110 wherein storing or extraction occurs with encryption corresponding to said respective ones of said plurality of security levels.

112. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 111 wherein accepting or storing or permitting reconstruction occurs with decryption corresponding to said respective ones of said plurality of security levels.

113. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer and said client computer.

114. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at said client computer on one of a fixed memory and a removable memory at said client computer.

115. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 113 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

116. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 including storing a map or locating data for said respective extract stores.

117. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 116 wherein the storing of said map or locating data occurs at one of said client computer and said server computer.

118. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 117 wherein the storing of said map or locating data occurs at said client computer in one of a fixed memory and a removable memory at said client computer.

119. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 117 wherein the storing of said map or locating data via said server computer in one of a server memory store and a remote memory map store, remotely disposed over said communications network with respect to said server computer.

120. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 116 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

121. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 120 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

122. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 121 wherein storing of said remainder data occurs at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer and said map locates said remainder store.

123. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 including establishing a plurality of filters for groups of security sensitive content corresponding to respective ones of said plurality of security levels and using said filter during the extraction of security sensitive content.

124. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 123 including storing said plurality of filters on one of said client computer and said server computer in one of fixed memory and removable memory.

125. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 124 including encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels.

126. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 124 including one of destroying or storing the filter after extraction.

127. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon accepting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

128. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on one of said client computer and said server computer, dependent upon extracting at one of said client computer and said server computer, in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

129. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 108 including

establishing a plurality of filters corresponding to groups of security sensitive content for respective ones of said plurality of security levels and using a respective filter during the extraction of security sensitive content for said each corresponding security level;

storing said plurality of filters on said server computer in one of fixed memory and removable memory;

encrypting and decrypting said plurality of filters for respective ones of said plurality of security levels; and

one of destroying or storing the filter after extraction.

130. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 123 wherein said filters identify either by inclusion or exclusion said security sensitive content.

131. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 106 including deleting said data input after storing.

132. (currently amended) A computer readable storage medium containing programming instructions as claimed in claim 121 including deleting said map after full reconstruction.

133. (currently amended) An information processing system for securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the ~~method of securing data~~ information processing system deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:

a filter adapted to receive ~~said~~ a data input from said communications network and to separate, from said data input, said security sensitive content as extracted data for each corresponding security level, leaving remainder data;

means for storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer;

an access controller for permitting access to said respective extract stores for corresponding security levels with said associated security clearances; and,

a compiler, coupled to said ~~means for storing and~~ access controller, for permitting full or partial reconstruction of said data via said respective extract stores and remainder data based upon said corresponding security levels and associated security clearances.

134. (original) An information processing system as claimed in claim 133 wherein said filter is on one of said client computer and said server computer.

135. (original) An information processing system as claimed in claim 133 wherein server computer has a downloader and said filter is downloaded to said client computer.

136. (original) An information processing system as claimed in claim 133 wherein said means for storing is on said server computer.

137. (original) An information processing system as claimed in claim 133 wherein said server computer includes a remainder store and said means for storing operates on said remainder data at said server computer.

138. (original) An information processing system as claimed in claim 133 wherein said client computer includes a remainder store and said means for storing operates on said remainder data at said client computer.

139. (original) An information processing system as claimed in claim 133 including an encryptor coupled to said means for storing enabling encryption for said extracted data corresponding to said respective ones of said plurality of security levels.

140. (currently amended) An information processing system as claimed in claim 139 including a decryptor coupled to said compiler, for decryption ~~with said means for storing and said compiler~~ during reconstruction, said decryption corresponding to said respective ones of said plurality of security levels.

141. (original) An information processing system as claimed in claim 133 wherein extract data stores are remotely disposed, via said communications network, with respect to said server computer and wherein said means for storing said extracted data employs said server computer to store the respective extracted data into said corresponding extract stores.

142. (original) An information processing system as claimed in claim 141 including an encryptor coupled to said means for storing enabling encryption for said extracted data corresponding to said respective ones of said plurality of security levels.

143. (currently amended) An information processing system as claimed in claim 142 including a decryptor coupled to said compiler, for decryption ~~with said means for storing or and~~ ~~compiler~~ during reconstruction, said decryption corresponding to said respective ones of said plurality of security levels.

144. (original) An information processing system as claimed in claim 133 wherein means for storing directs storage of said remainder data at said client computer on one of a fixed memory and a removable memory at said client computer.

145. (original) An information processing system as claimed in claim 133 wherein means for storing directs storage of said remainder data at one of said server computer and a remainder store remotely disposed via said communications network with respect to said server computer.

REMARKS

This Amendment responds to the Office Action dated April 3, 2009.

TERMINAL DISCLAIMER

Applicant submits, under protest, a Terminal Disclaimer. First, the Patent Office required that Applicant restrict the present claims from other claims in the parent application, U.S. Patent No. 7,103,915, and therefore it should not be necessary to disclaim. Second, since the present case claims priority based upon the earlier cases and the term of the present case is coextensive with the Parent Case, U.S. Patent No. 7,103,915, and therefore the present case could never be longer in duration compared to other “sibling” cases.

If a “provisional” nonstatutory obviousness-type double patenting (ODP) rejection is the only rejection remaining in the earlier filed of the two pending applications, while the later-filed application is rejectable on other grounds, the examiner should withdraw that rejection and permit the earlier-filed application to issue as a patent without a terminal disclaimer.

MPEP 804 (I)(B)(1), p. 800-17.

The filing of a terminal disclaimer to obviate a rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991). The court indicated that the “filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppel on the merits of the rejection.”

MPEP 804.02(II), p. 800-32.

Applicant is submitting this terminal disclaimer in order to expedite prosecution. Applicant disagrees that the Examiner adequately explained the obviousness link or combination of the present claims with those claims in one or more of the cited patents and patent applications with the cited art.

Since the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection, the factual

inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are employed when making an obvious-type double patenting analysis. These factual inquiries are summarized as follows: (A) Determine the scope and content of a patent claim relative to a claim in the application at issue; (B) Determine the differences between the scope and content of the patent claim as determined in (A) and the claim in the application at issue; (C) Determine the level of ordinary skill in the pertinent art; and (D) Evaluate any objective indicia of nonobviousness.

The conclusion of obviousness-type double patenting is made in light of these factual determinations. Any obviousness-type double patenting rejection should make clear: (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue would have been an obvious variation of the invention defined in a claim in the patent.

MPEP § 804(II)(B)(1) p. 800-21

It is respectfully submitted that the Examiner accept the enclosed Terminal Disclaimer and withdraw the rejection.

Applicant has amended claims 106 - 132 to overcome the rejection by adding “storage” to the term “medium.” Applicant requests that the Examiner withdrawal the rejection. Applicant has amended claims 133, 140 and 144 to better clarify the claim language therein and correct typographic errors (see the reference to “method” in claim 133). Allowance is requested.

Respectfully submitted,

By____/Robert Kain/_____

Robert C. Kain, Jr.

Reg. No. 30,648

Kain & Associates, Attorneys at Law, P.A.

750 Southeast Third Avenue, Suite 100

Ft. Lauderdale, Florida 33316-1153

Telephone: 954-768-9002

Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\Patents\6851-02-div2-Amdt-1st-100709.wpd

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Group Art 2176

Confirmation No.: 1129

Filed: August 17, 2006

For: Data Security System and Method

TERMINAL DISCLAIMER

Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

Petitioner, Digital Doors, Inc., a Florida corporation, having its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, FL 33140, represents that it is the owner by assignment of all rights to (i) the captioned application and (ii) the following:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/988,365 filed November 26, 2004;
U.S. Patent No. 7,546,334, Serial No. 11/465,309 filed August 17, 2007;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/988,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006 (captioned case);
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

The captioned application was assigned to Digital Doors, Inc. and the assignment was filed with the original parent application. The evidentiary document accompanying or referred to in the instant terminal disclaimer has been reviewed by the undersigned and it is certified that to the best of assignee, Digital Doors, Inc.'s knowledge and belief, title is in the assignee. Assignee is a small entity.

Petitioner, Digital Doors, Inc., hereby disclaims the terminal part of any patent granted on the above identified application, which would extend beyond the expiration date of any patent granted on any application listed below or any of the below-listed patents:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/988,365 filed November 26, 2004;
U.S. Patent No. 7,546,334, Serial No. 11/465,309 filed August 17, 2007;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/988,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

AND, except as provided below, hereby agrees that any patent so granted on the above identified applications shall be enforceable only for and during such period and that the listed patents remain commonly owned. Petitioner, Digital Doors, Inc., is a small entity.

Petitioner does not disclaim any terminal part of any patent granted on the above identified application prior to the expiration date of the full statutory term of any patent granted on:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;

U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/988,365 filed November 26, 2004;
U.S. Patent No. 7,546,334, Serial No. 11/465,309 filed August 17, 2007;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/988,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

IN THE EVENT that any latter patent: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. §1.321(a), has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its statutory term as presently shortened by any terminal disclaimer, except for the separation of legal title stated above.

Petitioner expressly reserves and does not waive the right to extend the term of any patent granted on:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/988,365 filed November 26, 2004;
U.S. Patent No. 7,546,334, Serial No. 11/465,309 filed August 17, 2007;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/988,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

OR ANY patent granted on the above identified application under any statute which permits such an extension of term.

I hereby declare that all statements made herein of our own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Dated: Oct. 7, 2009

Digital Doors, Inc.
By: ___/Robert C. Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

\\srv1\datashare\RCK\CLIENTS\Redlich\6851-02-div2-Term-Disc1-100709.wpd

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Group Art 2176

Confirmation No.: 1129

Examiner Michael J. Pyzocha

Filed: August 17, 2006

For: Data Security System and Method

REQUEST TO AMEND DRAWINGS

Mail Stop Non-Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a request to amend drawings pursuant to 37 CFR 1.123. It is respectfully requested that the examiner approve the drawing changes identified on FIG. 3 attached.

Respectfully submitted,

Dated: Oct. 7, 2009

By: /Robert C. Kain/
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

G:\RCK\CLIENTS\Redlich\6851-02-div2-Amend-drawings-corr-100709.wpd

FIG. 3

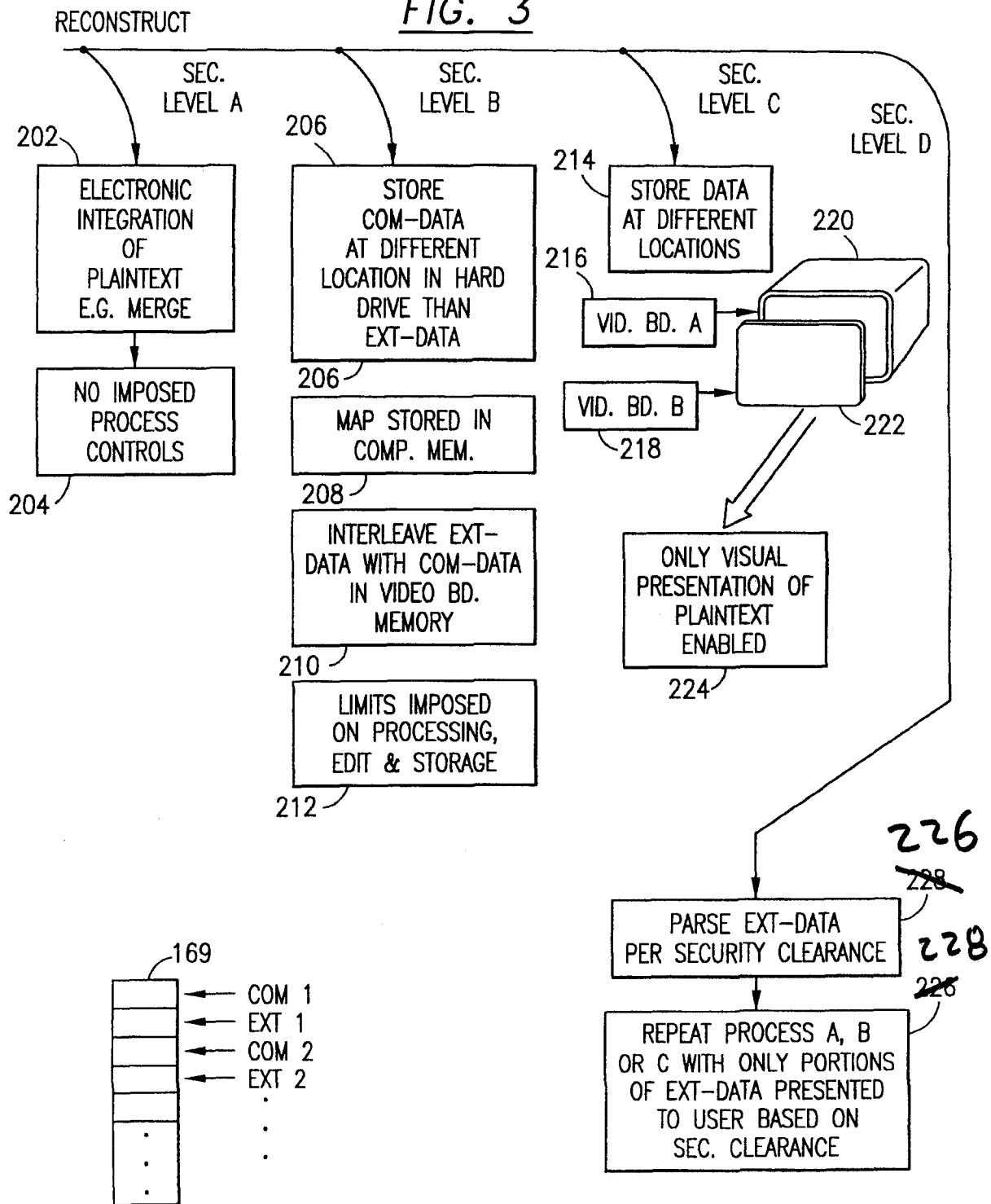


FIG. 3A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/465,350

Group Art 2176

Confirmation No.: 1129

Examiner Michael J. Pyzocha

Filed: August 17, 2006

For: Data Security System and Method

SUBMISSION OF REPLACEMENT FORMAL DRAWINGS

Mail Stop Non-Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed please find one (1) sheet (FIGS. 3 and 3A) of replacement formal drawings for the captioned case.

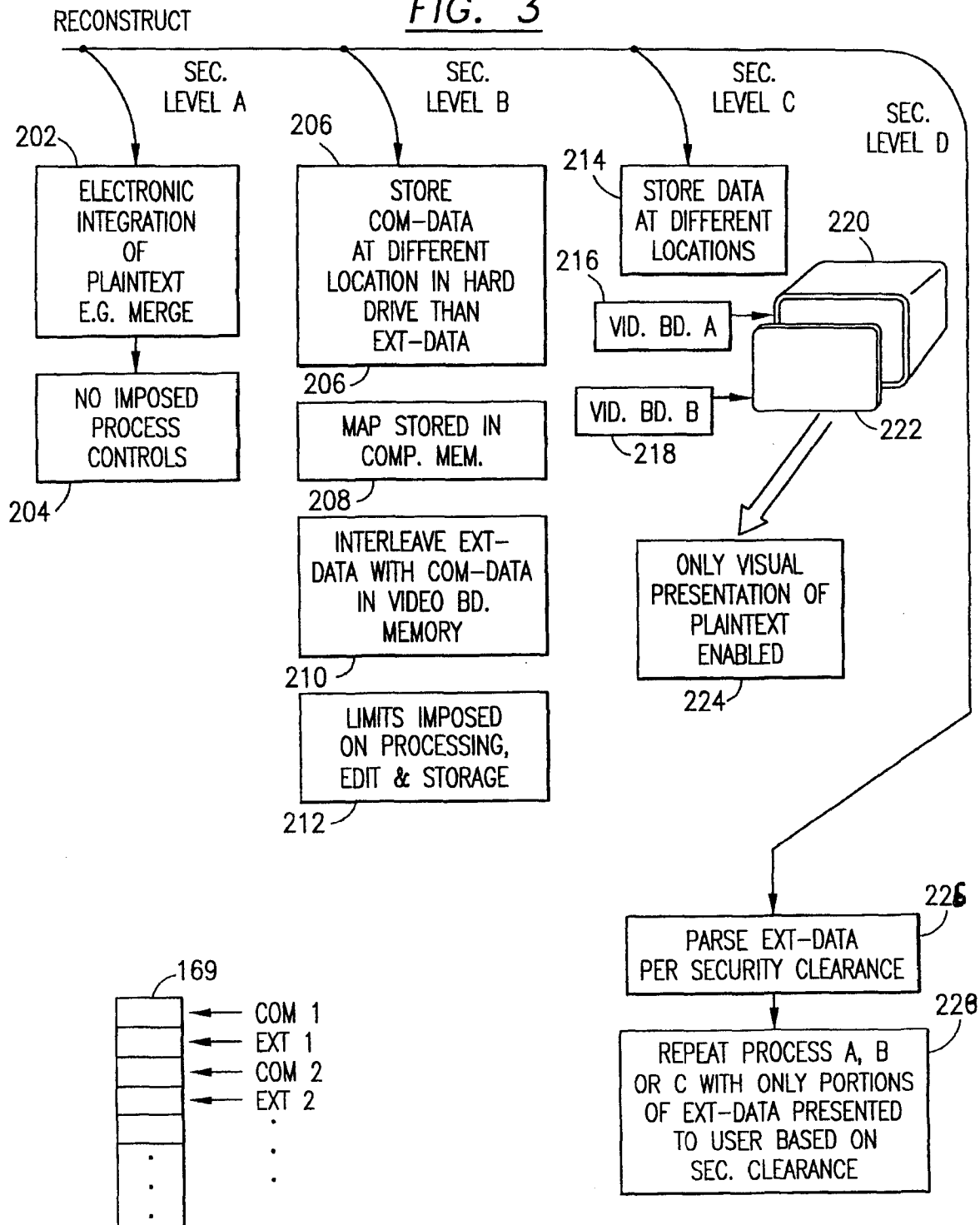
Respectfully submitted,

Dated: Oct. 7, 2009

By: /Robert C. Kain/
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002

G:\RCK\CLIENTS\Redlich\6851-02-div2-formal-drawings-subm-100709.wpd

3/5

FIG. 3**FIG. 3A**

Electronic Patent Application Fee Transmittal

Application Number:	11465350			
Filing Date:	17-Aug-2006			
Title of Invention:	Data Security System and Method			
First Named Inventor/Applicant Name:	Ron M. Redlich			
Filer:	Robert C. Kain			
Attorney Docket Number:	6851-02-DIV2			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory disclaimer	2814	1	70	70
Total in USD (\$)				70

Electronic Acknowledgement Receipt

EFS ID:	6221768
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	07-OCT-2009
Filing Date:	17-AUG-2006
Time Stamp:	17:28:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$70
RAM confirmation Number	3896
Deposit Account	031231
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	6851-02-div2-Amdt-1st-100709-trans.pdf	14641	no	1
			f55ce25a3c1f6db8b0799928b40b3ed133cd9ba0		
Warnings:					
Information:					
2	Claims	6851-02-div2-Amdt-1st-100709-clms.pdf	47627	no	26
			61a5db8a61876d6d1377f10c5778bea68b6e7d8a		
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	6851-02-div2-Amdt-1st-100709-rem.pdf	24546	no	2
			0464a8e6a770d953c1bf601e1ead8568970d3c62		
Warnings:					
Information:					
4	Terminal Disclaimer Filed	6851-02-div2-Term-Discl-100709.pdf	24325	no	4
			65960c810e0d41ad059e330d75eabe2162d72310		
Warnings:					
Information:					
5	Miscellaneous Incoming Letter	6851-02-div2-Amend-drawings-corr-100709.pdf	17939	no	1
			fedb783a501cb3aa305159095dcd20a3489e2d23		
Warnings:					
Information:					
6	Miscellaneous Incoming Letter	6851-02-div2-dwgs-marked.pdf	21990	no	1
			641577f5afa2f8136c771b5a2ec1e84185770774		
Warnings:					
Information:					
7	Miscellaneous Incoming Letter	6851-02-div2-formal-drawings-subm-100709.pdf	16737	no	1
			28ad0a0af7bb468a958a277c3b44dcd771e5f68f		
Warnings:					
Information:					
8	Drawings-only black and white line drawings	6851-02-div2-dwgs-replace.pdf	22078	no	1
			67b9210aac70d846a67b9d0500bdec76f6d36113		
Warnings:					
Information:					

9	Fee Worksheet (PTO-875)	fee-info.pdf	29541 4b8bb9db854c8853eade6a554dfcd00a0d76ddc6	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				219424	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/465,350		Filing Date 08/17/2006		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY ☒ OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	10/07/2009	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 145	Minus	** 145	= 0	X \$26 =	0		X \$	=
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X \$110 =	0		X \$	=
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE	0		TOTAL ADD'L FEE	
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=		X \$	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=		X \$	=
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
/EVELYN G. NIMMONS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**CHANGE OF
CORRESPONDENCE ADDRESS**
*Application*Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/465,350
Filing Date	8/17/2006
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	6851-02-div2

Please change the Correspondence Address for the above-identified patent application to:

The address associated with
Customer Number:

004897

ORFirm or
Individual Name

Address

City

State

Zip

Country

Telephone

Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:



Applicant/Inventor

Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).Attorney or agent of record. Registration Number 30,648.

Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number _____.

Signature

Typed or Printed
Name

Robert C. Kain, Jr.

Date 10/28/2009

Telephone

954-768-9002

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	6357746
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	Data Security System and Method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	29-OCT-2009
Filing Date:	17-AUG-2006
Time Stamp:	16:24:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Change of Address	6851-02-div2-change-address-sb0122_fill.pdf	317879 d48cc794fdc48847f57e5455b465bd2dffa6bd97	no	2

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Application Number 	Application/Control No. 11/465,350	Applicant(s)/Patent under Reexamination REDLICH ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 10/07/09	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
j.proctor



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

4897 7590 12/28/2009

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2437

DATE MAILED: 12/28/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/465,350

08/17/2006

Ron M. Redlich

6851-02-DIV2

1129

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$755	\$300	\$0	\$1055	03/29/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

4897 7590 12/28/2009

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/465,350	08/17/2006	Ron M. Redlich	6851-02-DIV2	1129

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$755	\$300	\$0	\$1055	03/29/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
PYZOCHA, MICHAEL J	2437	713-166000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/465,350

08/17/2006

Ron M. Redlich

6851-02-DIV2

1129

4897

7590

12/28/2009

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2437

DATE MAILED: 12/28/2009

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 678 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 678 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	11/465,350	REDLICH ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOSHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment filed 10/07/2009.
2. ☒ The allowed claim(s) is/are 1-145.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 - * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. ☐ Notice of References Cited (PTO-892) 2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. ☐ Notice of Informal Patent Application 6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____. 7. ☐ Examiner's Amendment/Comment 8. ☒ Examiner's Statement of Reasons for Allowance 9. ☐ Other _____. |
|---|--|

DETAILED ACTION

1. Amendment filed 10/07/2009 has been received and considered.
2. Claims 1-145 are pending.

Claim Rejections - 35 USC § 101

3. The rejections under 35 U.S.C. 101 have been withdrawn based on the filed amendment.

Double Patenting

4. The Double Patenting rejections have been withdrawn based on the approved terminal disclaimer filed 10/07/2009.

Allowable Subject Matter

5. Claims 1-145 are allowed.
6. The following is an examiner's statement of reasons for allowance: The prior art teaches filtering data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance when in combination with the remaining claim limitations. The prior art also fails to teach storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store when in combination with the remaining claim limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

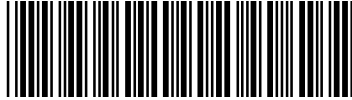
Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2437

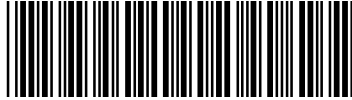
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOSKA	Art Unit 2437

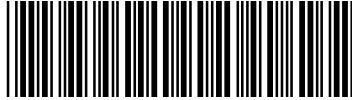
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant				☐ CPA				☒ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	08/19/2009	12/09/2009												
	1	✓	=												
	2	✓	=												
	3	✓	=												
	4	✓	=												
	5	✓	=												
	6	✓	=												
	7	✓	=												
	8	✓	=												
	9	✓	=												
	10	✓	=												
	11	✓	=												
	12	✓	=												
	13	✓	=												
	14	✓	=												
	15	✓	=												
	16	✓	=												
	17	✓	=												
	18	✓	=												
	19	✓	=												
	20	✓	=												
	21	✓	=												
	22	✓	=												
	23	✓	=												
	24	✓	=												
	25	✓	=												
	26	✓	=												
	27	✓	=												
	28	✓	=												
	29	✓	=												
	30	✓	=												
	31	✓	=												
	32	✓	=												
	33	✓	=												
	34	✓	=												
	35	✓	=												
	36	✓	=												

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

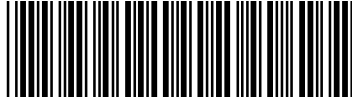
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant				☐ CPA				☒ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	08/19/2009	12/09/2009												
	37	✓	=												
	38	✓	=												
	39	✓	=												
	40	✓	=												
	41	✓	=												
	42	✓	=												
	43	✓	=												
	44	✓	=												
	45	✓	=												
	46	✓	=												
	47	✓	=												
	48	✓	=												
	49	✓	=												
	50	✓	=												
	51	✓	=												
	52	✓	=												
	53	✓	=												
	54	✓	=												
	55	✓	=												
	56	✓	=												
	57	✓	=												
	58	✓	=												
	59	✓	=												
	60	✓	=												
	61	✓	=												
	62	✓	=												
	63	✓	=												
	64	✓	=												
	65	✓	=												
	66	✓	=												
	67	✓	=												
	68	✓	=												
	69	✓	=												
	70	✓	=												
	71	✓	=												
	72	✓	=												

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOSKA	Art Unit 2437

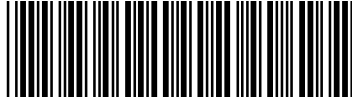
✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant				☐ CPA				☒ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	08/19/2009	12/09/2009												
	73	✓	=												
	74	✓	=												
	75	✓	=												
	76	✓	=												
	77	✓	=												
	78	✓	=												
	79	✓	=												
	80	✓	=												
	81	✓	=												
	82	✓	=												
	83	✓	=												
	84	✓	=												
	85	✓	=												
	86	✓	=												
	87	✓	=												
	88	✓	=												
	89	✓	=												
	90	✓	=												
	91	✓	=												
	92	✓	=												
	93	✓	=												
	94	✓	=												
	95	✓	=												
	96	✓	=												
	97	✓	=												
	98	✓	=												
	99	✓	=												
	100	✓	=												
	101	✓	=												
	102	✓	=												
	103	✓	=												
	104	✓	=												
	105	✓	=												
	106	✓	=												
	107	✓	=												
	108	✓	=												

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant				☐ CPA		☒ T.D.		☐ R.1.47	
CLAIM		DATE							
Final	Original	08/19/2009	12/09/2009						
	109	✓	=						
	110	✓	=						
	111	✓	=						
	112	✓	=						
	113	✓	=						
	114	✓	=						
	115	✓	=						
	116	✓	=						
	117	✓	=						
	118	✓	=						
	119	✓	=						
	120	✓	=						
	121	✓	=						
	122	✓	=						
	123	✓	=						
	124	✓	=						
	125	✓	=						
	126	✓	=						
	127	✓	=						
	128	✓	=						
	129	✓	=						
	130	✓	=						
	131	✓	=						
	132	✓	=						
	133	✓	=						
	134	✓	=						
	135	✓	=						
	136	✓	=						
	137	✓	=						
	138	✓	=						
	139	✓	=						
	140	✓	=						
	141	✓	=						
	142	✓	=						
	143	✓	=						
	144	✓	=						

<i>Index of Claims</i> 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant				☐ CPA				☒ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	08/19/2009	12/09/2009												
	145	✓	=												

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	40	(REDLICH near RON) (NEMZOW near MARTIN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:53
L2	1664	(726/27).CCLS.	US-PGPUB; USPAT	OR	OFF	2009/12/09 06:53
L3	4	L2 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:53
L4	663	713/166.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:53
L5	1	L4 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:53
L6	2962	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:53
L7	7	L6 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:53
L8	7312	(extract\$4 filter\$4) with (separat\$4 distinct\$4) with (database memory location)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L9	35	L8 same security with level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54

L10	0	L9 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L11	67	L8 same security	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L12	0	L11 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L13	326	security near level same (separat\$4 distinct\$4) with (location database memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L14	1	L13 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L15	452935	(redact\$4 filter\$4 extract \$4) with separat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L16	41	L15 same partial with reconstruct\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L17	0	L16 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L18	9693	(redact\$4 filter\$4 extract \$4) with separat\$4 with (database storage memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L19	215	L18 same partial\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54

L20	0	L19 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L21	128	security with clearance same (filter\$4 redact\$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L22	1	L21 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L23	508	multiple with (stor\$4 memory server) with security with level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L24	0	L23 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L25	29	partial with reconstruct\$4 same security with level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L26	0	L25 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L27	173	security same filter\$4 same extract\$4 same stor \$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:54
L28	0	L27 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L29	34	filter\$4 same security near sensitive near word	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54

L30	0	L29 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L31	59	automatic\$5 with redact\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:54
L32	0	L31 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:54
L33	2057	(715/255).ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/12/09 06:55
L34	6	L33 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:55
L35	768	(redact\$4 filter\$4 extract \$4) same security adj level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:55
L36	0	L35 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:55
L37	371	(redact\$4 filter\$4 extract \$4) with security adj level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:55
L38	0	L37 and @ad< "20001113" and @pd> "20090122"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/09 06:55

EAST Search History (I nterference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L39	13	(extract\$4 with security adj level).clm.	USPAT; UPAD	OR	ON	2009/12/09 06:56

L40	80	(stor\$4 with data with security adj level).clm.	USPAT; UPAD	OR	ON	2009/12/09 06:58
L41	9	(stor\$4 with remainder with data with security adj level).clm.	USPAT; UPAD	OR	ON	2009/12/09 06:58
L42	8	(reconstruct\$4 with data with security adj level).clm.	USPAT; UPAD	OR	ON	2009/12/09 06:59
L43	2	(content with security adj level with security adj clearance).clm.	USPAT; UPAD	OR	ON	2009/12/09 07:00

12/ 9/ 09 7:00:48 AM

C:\ Documents and Settings\ mpyzocha1\ My Documents\ EAST\ Workspaces\ 11465350-1.wsp

Search Notes 	Application/Control No. 11465350	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner MICHAEL PYZOCHA	Art Unit 2437

SEARCHED			
Class	Subclass	Date	Examiner
726	27	8/19/09	MJP
713	166	8/19/09	MJP
713	193	8/19/09	MJP
715	255	8/19/09	MJP
updated	search	12/09/09	MJP

SEARCH NOTES		
Search Notes	Date	Examiner
BRS search in USPAT, USPGPUB, EPO, JPO, IBM, DERWENT, see attached search history; inventor name search; all claims have been reviewed for 35 USC non-statutory subject matter	8/19/09	MJP
updated BRS search, see attached search history	12/09/09	MJP

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
726	27	12/9/09	MJP
713	166	12/9/09	MJP
713	193	12/9/09	MJP
715	255	12/9/09	MJP

--	--

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-div2	Application Number 11/465,350
Title: Data Security System and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date August 17, 2006	Group Art Unit 2176

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	06/20/2000	Lamm	705	40	
	6,253,203	06/26/2001	O'Flaherty et al.	707	9	
	~~5,960,808~~ 5,960,080	09/28/1999	Fahlman et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	CA 2 345 148	06/04/2000	Canada			X

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Processing of confidential information in distributed systems by fragmentation" by J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997)	
	"Secure External References in Multimedia Email Messages" B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996	
	"Element-Wise XML Encryption" H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000	

EXAMINER /Michael Pyzocha/ DATE CONSIDERED 08/19/2009

G:\RCK\CLIENTS\Redlich\6851-02-div2-Supp-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MP/

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Robert C. Kain, Jr.
9000 Southeast Third Avenue
Suite 205
Ft. Lauderdale, Florida 33316

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Robert C. Kain, Jr.	(Depositor's name)
/rck/	(Signature)
03/26/2010	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
011/465,350	08/17/2006	Ron M. Redlich	6851-02-div2	1129

TITLE OF INVENTION:

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$755	\$300	\$0	\$1055	03/29/10

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.563).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 Robert C. Kain, Jr.
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Digital Doors, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Miami Beach, Florida

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 031231 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /rck/

Date 03/26/2010

Typed or printed name Robert C. Kain, Jr.

Registration No. 30648

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	11465350			
Filing Date:	17-Aug-2006			
Title of Invention:	DATA SECURITY SYSTEM AND METHOD			
First Named Inventor/Applicant Name:	Ron M. Redlich			
Filer:	Robert C. Kain/Ellen Kotler			
Attorney Docket Number:	6851-02-DIV2			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	755	755
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1055

Electronic Acknowledgement Receipt

EFS ID:	7290531
Application Number:	11465350
International Application Number:	
Confirmation Number:	1129
Title of Invention:	DATA SECURITY SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain/Ellen Kotler
Filer Authorized By:	Robert C. Kain
Attorney Docket Number:	6851-02-DIV2
Receipt Date:	26-MAR-2010
Filing Date:	17-AUG-2006
Time Stamp:	07:22:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$ 1055
RAM confirmation Number	9700
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Issue Fee Payment (PTO-85B)	6851-02-div2-issue-fee-transmittal-032610.pdf	64399 e73f0c6b5550a6090668540576fdbd066cf558fb	no	1
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	31685 4c12c909ef9412da6a5947318b1ecb2014f45b4b	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			96084		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/465,350	05/18/2010	7721344	6851-02-DIV2	1129

4897 7590 04/28/2010

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 944 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;