



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	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
62/008,561	06/06/2014		130	0813EBDD-1		

CONFIRMATION NO. 6709

17012
CipherLaw
PO Box 34783
Bethesda, MD 20827

FILING RECEIPT



OC000000069182398

Date Mailed: 06/25/2014

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Aviel David Rubin, Pikesville, MD;

Applicant(s)

Aviel David Rubin, Pikesville, MD;

Power of Attorney:

James Denaro--54063

If Required, Foreign Filing License Granted: 06/23/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 62/008,561**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

UTILIZATION OF MULTIPLE DEVICES TO SECURE ONLINE TRANSACTIONS

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international

application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national

security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

To: james.denaro@cipherlawgroup.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 17012

Jun 25, 2014 05:20:56 AM

Dear PAIR Customer:

CipherLaw
PO Box 34783
Bethesda, MD 20827
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 17012 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
62008561	APP.FILE.REC	06/25/2014	0813EBDD-1

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Aviel

David

Rubin

Pikesville

MD

US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention

UTILIZATION OF MULTIPLE DEVICES TO SECURE ONLINE TRANSACTIONS

Attorney Docket Number (if applicable)

0813EBDD-1

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number

☐ Firm or Individual Name

Customer Number

17012

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the invention was made by an agency of the United States Government. The U.S. Government agency name is:

☐ Yes, the invention was under a contract with an agency of the United States Government. The name of the U.S. Government agency and Government contract number are:

Entity Status

Applicant asserts small entity status under 37 CFR 1.27 or applicant certifies micro entity status under 37 CFR 1.29

- ☒ Applicant asserts small entity status under 37 CFR 1.27
- ☐ Applicant certifies micro entity status under 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
- ☐ No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/James M. Denaro/			Date (YYYY-MM-DD)	2014-06-06
First Name	James	Last Name	Denaro	Registration Number (If appropriate)	54063

This collection of information is required by 37 CFR 1.51. 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 8 hours 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. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

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.

UNITED STATES PROVISIONAL PATENT APPLICATION

FOR

UTILIZATION OF MULTIPLE DEVICES TO SECURE ONLINE TRANSACTIONS

INVENTOR

AVIEL DAVID RUBIN

Field of the Invention

[1] This application relates generally to securing communications against malware by utilizing two devices with differential or application-specific components during an online session.

Background

[2] Online applications run locally on computers or other devices such as tablets or smartphones. It is common for these devices to become infected with malware (*i.e.*, malicious code that runs on the user's device). Malware can compromise the security of a user's device. When online applications involve the transfer of money, the consequences are that the attacker can steal money. For example, there are documented instances where malicious code on a user's computer has revealed confidential information to an attacker in an online game, and the attacker was able to use this information to defeat the other player and thus steal money from the victim.

[3] Efforts to secure online applications have focused on requiring the user to install anti-virus or firewall technologies on the electronic devices to attempt to keep the malicious code from being installed or from running. However, it is not realistic to assume that average users can administer their computers and other electronic devices adequately.

[4] Further efforts to secure online applications have involved two-factor authentication. Two-factor authentication is utilized to authenticate users, authorize transactions, or to notify users of irregularities in their accounts. In two-factor authentication, a user logs into a first device (*e.g.*, a computer) and then uses a second device (*e.g.*, a smartphone) as part of the authentication process. The second device receives code, for example by text or email, and the user is instructed to enter that code into the first device, where the rest of the interaction with the application takes place. Examples of two-factor authentication include RSA tokens and SMS notification systems. In two-factor authentication, the second device is no longer needed once the authentication takes place. Accordingly, two-factor authentication will not offer protection against malware after the authentication takes place.

Brief Description of the Drawings

[5] Fig. 1 illustrates the current state of the art. It depicts architecture in online games. A game server communicates with the players in the game. Each of the players utilizes a single computing device (*e.g.*, computer, phone, or tablet), and the players can communicate with the game server or with each other over the Internet.

[6] Fig. 2 illustrates a preferred embodiment of the invention. Specifically, in this example, a user is playing online poker, and the user sees the same view of a table as is common in online poker, but the hole cards are not displayed. In this embodiment, the user runs a separate app on a second device that requires its own authentication (which can be different from the authentication required on the first device), and over that channel, the game server sends the user the hole cards for that hand. An identifier is used to link the current hand on the first device to the hole cards that are displayed on the second device.

[7] Fig. 3 illustrates another example of the preferred embodiment of the invention in which a game server can use the Internet to communicate with the first device. The game server sends the information about the user's hole cards to the second device over the cellular network as a text message.

[8] Fig. 4 illustrates another example of the preferred embodiment of the invention where the game server sends the user hole cards over a separate Internet connection.

[9] Fig. 5 illustrates the flow of control for a poker hand at the game server in the preferred embodiment.

[10] Fig. 6 illustrates the architecture for an embodiment of the present invention in a banking application. In this example, the banking application is split into two components. On a first device, a user with a web browser logs in and initiates a transaction. The bank then communicates with the user's second device over an independent Internet channel to obtain details about the desired transaction.

[11] Fig. 7 illustrates an example of the communication among the central banking server, the user's first device and the user's second device.

[12] Fig. 8 illustrates an example of a database entry on the central server for a particular user in the banking example. The central server stores hashes of the passwords that are used on the first device and the second device. When a user submits a password on a device, the device hashes the password and sends the hash to the central server over a secure connection (*e.g.*, SSL). The central server extracts the stored password from the database shown in the figure and compares the two. If they match, then authentication is successful. The figure shows that the database may store the authentication token as described above, as well as information about the user's preferences, such as the dollar amount above which use of a second device is required for funds transfers.

Detailed Description

[13] The present invention describes a system where the user has persistent use of a first device and a second device throughout the use of an online application to prevent a compromise of the transaction if malware infects either device. Whereas two-factor authentication in the prior art is application-agnostic and takes place before a user engages in the specific functionality of a particular application, the present invention includes a system that utilizes the two devices throughout an online session and includes application-specific components in each of the devices.

[14] The present invention includes an architecture whereby a user's interaction with an application includes a first device, which can be a computer, a tablet, a smartphone or other electronic device and second device, such as a computer, tablet, smartphone or another type of electronic device. Any combination of electronic devices can be used.

[15] Preferred Embodiment

[16] The preferred embodiment of the invention includes online games. However, the invention may also apply to any other domain, such as online banking, mobile healthcare, online investing, and other online activities that require security against malware on a user's computing device. Although the preferred embodiment is described using the game of poker as an example, this example is non-limiting and the preferred embodiment could apply to any online game.

[17] In the preferred embodiment, a player runs gaming software on a first device. In the case of the poker example used here, the game server does not communicate certain sensitive information (such as, for example, the user's hole cards) to the first device. The player's sensitive information (*e.g.*, the user's hole cards) are therefore not displayed on the first device. Accordingly, because the sensitive information is not displayed or transmitted to the first device, an attacker using malware cannot gain access to the sensitive information.

[18] In the preferred embodiment, the user also utilizes a second device. Everything that is known and displayed on the first device is considered to be public information, and the only private, sensitive information exists on or is transmitted to a separate electronic device.

[19] The game server communicates the user's sensitive information (*e.g.*, the user's hole cards) to the second device via a separate communication channel, such as a different Internet connection, or via the cellular phone network. The second device then displays the sensitive information to the user. The game server may communicate additional sensitive information to the second device.

[20] In one example of the preferred embodiment, the user can receive the information about sensitive information cards as a text message and does not have to run another application on a second device. In this example, the user can register a cell phone number on which to receive text messages and can see the cards as a text message. For example, Ah3c would be the ace of hearts and the three of clubs. Alternatively, the user can utilize an application that would translate this text into pictures of the cards that are displayed to the user. In another example of

the preferred embodiment, the user runs an app on a smartphone that communicates with the game server and receives and displays the user's hole cards.

[21] In the preferred embodiment, each user of an online game site can choose from several alternatives on how the user wants to receive sensitive information, thus balancing security needs with convenience. The choices can include, but are not limited to:

(1) no change from the status quo – the sensitive information is visible at the poker table on one device;

(2) receiving the sensitive information over the Internet on a second, networked device by running an application (app) on that second device;

(3) receiving the sensitive information as a cellular text message on a second device, which can be display as text or as an image or images.

[22] The user may also elect to change the choice every time the user plays, based on the user's circumstances and perceived level of risk. For example, if playing a low stakes game, the user may elect to receive and view the user's sensitive information on the first device, or if there is an area of low cellular coverage, the user may elect not to receive the sensitive information on a second device as a text message.

[23] These examples of the preferred embodiment are for illustration and are not limiting, and there may be many other ways in which the user can elect to receive sensitive information on a second device.

[24] The preferred embodiment of the invention can be utilized by some players, but need not necessarily be utilized by all players. Thus, in this embodiment of the invention, each player can decide what level of security the user is most comfortable with, and the game server can support either one. At any time, any player may elect to switch to a different level of security by receiving the user's sensitive information in a different way.

[25] Multi-Tabling Function of the Preferred Embodiment

[26] The preferred embodiment of the invention contemplates that there may be players who play at more than one virtual table at a time. This is a common practice in online poker and is called multi-tabling.

[27] If the second device has a big enough screen, and if there are few enough tables, the second device may be able to display the sensitive information for all of the tables at the same time. However, the preferred embodiment of the present invention includes mechanisms for supporting multi-tabling, even where the user can only see one poker hand at a time on a second device, which might be the case on a smartphone with a small screen.

[28] The preferred embodiment of the present invention includes several ways of synchronizing the active poker table on the first device with the second device. One way to link the active table on the first device with the cards displayed on the second device is to perform a visual enhancement to each table, such as a special border or a color scheme, and then to match that on the second device. For example, if the second device is a smartphone, and the smartphone displays a pair of hole cards on the screen, the user can swipe to the left or right within the smartphone application and thus scroll through hole cards for different hands. Each hand may have a visual cue that is similar to a visual cue (*e.g.*, color, a border, or some other marking) that matches a similar visual cue on that poker table on the first device.

[29] Another way to keep the two devices synchronized is for the first device to communicate to the game server which table currently has the focus, and the game server can then relay that information to the second device over the independent channel.

[30] Yet another way that the two devices can remain synchronized is for the application on the first device and the application on the second device to share a direct communication line such as Bluetooth, WiFi, or some other way of communicating. The first device would then send the second device the information about which poker hand is currently active. It is important

that this channel not be utilized for any other purpose and that the communication be one way – from the first device to the second device, to avoid creating a vector of attack.

[31] Yet another way that the user can keep track of which poker hand corresponds to which table is to display additional information in the second device, such as the names of the other players at the table and/or the community cards and/or the pot size, or any other information that would help the user associate the current hole cards on the second device to a particular poker table on the first device. In this example of the preferred embodiment, the game server communicates the additional information to the second device, in addition to the hole cards.

[32] Any of the foregoing synchronization methods can be utilized alone or in conjunction with any of the other synchronization methods described above.

[33] On-Line Banking Embodiment

[34] Another embodiment of the present invention can be applied to online banking applications. This embodiment includes a system and method for users to use their first device and their second device at the same time, to protect against malware on either one.

[35] In one example of this embodiment, a banking application can require that users log into their bank account from their first device and also from their second device, and that the user perform some action on each of those devices before the action is authorized.

[36] In another example of this embodiment, the user requests some information on the first device and can only view it on the second device. For example, the user can use the bank's website on their computer to request a balance in an account, and the user can then view the balance on the second device, but not on the first device.

[37] This embodiment involves splitting the application into different components, where at least one of the application-specific components of the application requires a first device and one of the other application-specific components requires a second device. The use of the two

devices is related to an application-specific activity, such as viewing an account balance or performing a funds transfer, or performing a bill payment.

[38] In the example of a transaction, if the user wants to perform a funds transfer in a banking application. The application is split up into two components, one of which runs on the user's first device, and the other runs on a second device. It is understood that this is one example, and that the two application components can run on two computers or on a combination of smartphones, tablets or computers.

[39] Continuing the example of splitting the banking application, the user indicates, via the first device, that the user wishes to perform a transfer. Next, using the second device component of the application, the user can select the accounts to transfer to/from as well as the amount. In this manner, different parts of the experience of performing a banking transaction occur on different devices.

[40] No restriction is placed on the account, and there is no re-authentication of the user. The present invention, however, includes a seamless application where the user utilizes an application that has been designed to utilize two different devices, to avoid the threat of malware, not explicitly for user authentication.

[41] The communication with the first device could be over the Internet, and the communication with the second device could be over a separate Internet connection or via text message, or some other communication channel their smartphones and tablets, in addition to logging into their account on their computers.

[42] Similarly, an online investment application where the user purchases stocks could be split in such a way where the user performs an application-specific action on a first device and another application-specific action on a second device, where sensitive information is not displayed on the first device, but instead is displayed to the user on the second device. Any number of application domains could utilize the present invention to provide security against

malware on a user's first device and thus hide sensitive information from an attacker who has compromised the first device.

[43] Below are some non-limiting, illustrative examples of different types of banking transactions and how they can be split using the present invention into steps performed on two separate devices that communicate with a bank server over independent communication channels to protect the user's banking information and the user's funds against malware on the user's devices. Of course, there are many other ways in which the transactions can be split.

[44] Account balance inquiry: A user initiates a request to view the account balance on a first device, and the account balance is displayed on the second device. Thus, malware on the first device cannot obtain or view account balances.

[45] Funds transfer: This example is illustrated and described above where a user initiates a funds transfer on a first device, and the amount and designated recipient are entered on the second device. It should be noted that other combinations of splitting are possible, for example, in another embodiment the user may indicate the recipient on the first device and the amount on the second device.

[46] Bill Payment: In this example, a user initiates a request to pay a bill in online bill pay on a first device, and then on the second device, the user chooses a recipient and the amount. Another way this could be implemented is to choose the recipient on the first device and the amount of the bill and the date of payment on the second device. The present invention can also be utilized to add a new payee to online bill pay. The user could request to add a new payee on the first device, and then enter the name and address of the payee on the second device. Other ways of splitting up the various tasks in the bill pay activities are possible.

[47] Linking to an external account: In this example, a user wants to link an external bank account to the user's bank account. In one embodiment, the user initiates a request to link accounts on the first device. Then, the user enters the account details for the external account on the second device.

[48] Other banking activities: Other activities that the user performs with the user's online bank can be split up in a similar manner to the examples given above, where the user performs part of the activity on the first device such that even if an attacker compromised the first device, the attacker would not be able to do anything damaging, and part of the activity is performed on a second device. Only the combination of the actions performed on the two devices will cause the user action to succeed.

[49] There are many ways that the central banking server can implement the present invention. For example, the banking server could implement a system-wide threshold for funds transfers. A bank could specify that, for any transaction over \$3,000 in this example, the user must use a second device and a split application. (A split application refers to an application as described above where part of the transaction is performed on a first device and part of the transaction is performed on a second device.) Individual users may specify lower thresholds for their accounts. For example, a user may specify that any funds transfer over \$500 requires a second device and a split application. Thus, in this example, some users who may be more security conscious and who may be comfortable using their smartphone more often may set their own thresholds for certain activities, and other users may default to the system-wide threshold set by the bank.

[50] The splitting up of applications in banking transactions, as described above, can operate in conjunction with other security mechanisms known in the prior art such as two-factor authentication or two-factor transaction confirmations.

[51] Another way that a bank can improve its security with the present invention is by using its existing or new heuristics for detecting possible suspicious activity to increase its level of security requirements. For example, the bank may detect an abnormal amount of activity in one account that normally only performs a few transactions a month. In that instance, the bank could require that all future transactions in that account utilize a split application and two devices as per the present invention until there is a satisfactory explanation for the increased activity. Once the bank is satisfied that the activity is legitimate, it can reduce the need for increased security

and allow standard transactions through its web server. In this manner, the present invention allows suspicious accounts that are actually not involved in anything inappropriate to continue to function instead of locking those accounts and inconveniencing its customers.

[52] Sensitive Healthcare Information Embodiment

[53] In another embodiment of the present invention, the invention is utilized to help protect sensitive healthcare information. In this embodiment, a user logs into a healthcare portal to access the user's medical records. The application is split such that most of the interaction between the user and the healthcare records system is via the user's first device. Additionally, the user also utilizes a second device, and the healthcare information server communicates over an independent channel with the user's second device.

[54] For example, if a user wishes to view sensitive medical records, the user would log into the healthcare information portal via a first device and request the specific information that is desired to view. Once the user has indicated which records are desired, the healthcare information server sends those records either via text message or over an independent Internet connection to the user's second device. Thus, if the user's first device is infected with malware that allows an attacker to view the screen, the attacker will still not be able to see any sensitive records. The only way to compromise the user's healthcare information would be to compromise both the user's first device and the user's second device, in this example.

[55] Examples of Second Device Customization Options

[56] The invention contemplates that the second device can be off-the-shelf or customized. The user's second device may be, for example, a custom electronic device that is specifically built to help secure applications. This type of second device can be built with security as the motivating factor, and it can be a stripped down electronic system that is not running full versions of a standard operating system. In this embodiment, the second device runs only software and hardware necessary to provide a split application functionality according to the

present invention. A single such second device can be designed to support multiple types of applications at the same time.

[57] An example second device is an electronic device with a processor, a screen and a network interface that can communicate with a central application server to display content related to a particular networked application, but which is not a general-purpose machine in that it is designed not to allow the user to download new applications. In this fashion, the custom second device may be less vulnerable to malware.

[58] Application developers can split their application such that the user can use the first device for part of the communication with the user, and the custom second device over an independent communication channel, for the remainder of the communication with the user, as described below.

[59] One example of this is where the user performs most of the actions in an application using the first device, but then when it is time for the central server to communicate sensitive information to the user, that information is sent to the second device, which displays it to the user. The custom second device can be built such that it has a keyboard and other data entry mechanisms, such as a mouse or a touch sensor, allowing additional functionality in the second device.

[60] The custom second device can optionally be initialized with security keys and cryptographic tokens, allowing the second device authentication capabilities, in addition to or instead of authentication by the user. For example, the device can be loaded with client SSL private keys and certificates, allowing the server to directly authenticate the custom second device. Additionally, user authentication inside of an application can allow for even greater security. Since the custom second device may be much less vulnerable to malware than a standard computer, tablet or smartphone, these pre-loaded keys and cryptographic tokens are correspondingly less vulnerable to malware infections.

[61] Examples of Independent Communication Channels

[62] The present invention contemplates using the first and second devices through a single or a plurality of communication channels between a central server and the devices of the user. By utilizing independent communication channels, the devices are further protected from each other.

[63] In one example, the first device is connected to the Internet in a user's home. This type of a connection typically involves an Internet Service Provider (ISP) that links the user's home to the Internet, such as over fiber optics (*e.g.*, Verizon FIOS), cable modem (*e.g.*, Comcast Infinity), DSL, or any other means of connecting users to the Internet. In the home, the user typically utilizes a modem that provides for a Local Area Network (LAN) for the devices in the home. The user may connect to the LAN via Ethernet cable or wirelessly via WiFi or via some combination of wired and wireless connections.

[64] The second device may communicate with the central server via any one of multiple mechanisms. For example, the central server may utilize text messages via SMS to communicate with the second device. Or, the user can connect the second device to the Internet either via the cellular network's Internet service such as a 3G or 4G (*e.g.*, LTE) network or similar networks of the cellular provider, or using WiFi. There are some security benefits to connecting the second device to the Internet via a network other than the home network, but the protection from malware is achieved even if the first and second device are on the same WiFi home network, and the network paths to the central server are still independent.

[65] Examples of Device Registration

[66] The present invention contemplates that the first and second devices can either be unregistered or can be registered with the central server.

[67] For example, while interacting with the central server via use of the first device, the user can indicate via an application menu selection or by entering a configuration mode or preferences screen in the application that he or she wishes to add a device and to require the use

of the new device in the application. The user can then include information about the device, such as whether it is a computer, a tablet or a smartphone.

[68] At registration time, upon receiving a request to add a second device from a user's first device, the central server then creates a new database entry or adds fields to an existing database record for the user, for storing information about the user's second device.

[69] Next, in this example, the user initiates a connection to the central server from the second device, and the central server correlates the communication from the second device with the database entry created or modified based on earlier communication with the first device. In this preferred embodiment, the central server creates authentication information, such as a 256 bit random number and sends that authentication information to the first device. Upon registering the second device, the user enters the authentication information into the second device to complete the registration. The authentication information, consisting of a 256 bit random string, in this example, can be converted into a human readable ASCII string using, for example, uuencoding, such that the user can read it and enter it into the second device. The central server uses the authentication information to ensure that only the actual user adds a new device, and that the new device that is added is added to the account of the correct user.

[70] It is preferable that the central server store two different means of authenticating the user. One means of authentication, in some cases a password, is stored for authenticating the user on the first device, and a second means of authentication, perhaps a different password, is stored to authenticate the user on the second device. The reason for this is that if the first device is compromised by malware, then the attacker controlling the malware can learn the user's password. If the same authentication means is used for both devices, then the attacker could conceivably connect to the server with a illegitimate second device and impersonate the user. While this may be discovered when the legitimate user attempts to connect with the second device, it is simpler to require two separate authentications to prevent this attack. In another embodiment, the central server and the second device can agree on a secret value, an

authentication token, that is stored on the second device and in the central server database. Whenever the second device communicates with the central server, the authentication token is used, such that any device without the authentication token cannot act as the second device.

[71] The authentication token can be derived by combining (via xor or Diffie Helman key exchange or similar protocol) a secret value generated on the second device and a secret value generated on the secure server, during device registration.

[72] It should be noted that if an authentication token is used on the second device, then the user will be limited to using that specific device whenever using the application with the central server. If it is desired to be able to use different devices to serve as the second device in the application, then the authentication should be limited to the user entering authentication information, such as a password, into the second device, which can then be any device that contains the appropriate application software.

[73] In addition to creating a database entry or adding to an existing database record for the user, the central server may also store in its database, user preferences, such as in the game of poker, whether or not the user prefers to receive hole cards on the first device or on the second device. Or, for example, in the banking application, the central server can store user-specific information in the database corresponding to the user's threshold for transaction amounts that require performing some part of a transaction in a split way on a first device and on a second device to protect the user from malware on either of the devices as described in detail above.

[74] Example System Components

[75] The systems and methods described herein can be implemented in software or hardware or any combination thereof. The systems and methods described herein can be implemented using one or more computing devices which may or may not be physically or logically separate from each other. Additionally, various aspects of the methods described herein may be combined or merged into other functions.

[76] In some embodiments, the illustrated system elements could be combined into a single hardware device or separated into multiple hardware devices. If multiple hardware devices are used, the hardware devices could be physically located proximate to or remotely from each other.

[77] The methods can be implemented in a computer program product accessible from a computer-usable or computer-readable storage medium that provides program code for use by or in connection with a computer or any instruction execution system. A computer-usable or computer-readable storage medium can be any apparatus that can contain or store the program for use by or in connection with the computer or instruction execution system, apparatus, or device.

[78] A data processing system suitable for storing and/or executing the corresponding program code can include at least one processor coupled directly or indirectly to computerized data storage devices such as memory elements. Input/output (I/O) devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system. Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. To provide for interaction with a user, the features can be implemented on a computer with a display device, such as a CRT (cathode ray tube), LCD (liquid crystal display), or another type of monitor for displaying information to the user, and a keyboard and an input device, such as a mouse or trackball by which the user can provide input to the computer.

[79] A computer program can be a set of instructions that can be used, directly or indirectly, in a computer. The systems and methods described herein can be implemented using programming languages such as Ruby™, Flash™, JAVA™, C++, C, C#, Visual Basic™, JavaScript™, PHP, XML, HTML, etc., or a combination of programming languages, including compiled or interpreted languages, and can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment.

The software can include, but is not limited to, firmware, resident software, microcode, etc. Protocols such as SOAP/HTTP may be used in implementing interfaces between programming modules. The components and functionality described herein may be implemented on any operating system or environment executing in a virtualized or non-virtualized environment, using any programming language suitable for software development, including, but not limited to, different versions of Microsoft Windows™, Android™, Apple™ Mac™, iOS™, Unix™/X-Windows™, Linux™, etc. The system could be implemented using a web application framework, such as Ruby on Rails.

[80] The processing system can be in communication with a computerized data storage system. The data storage system can include a non-relational or relational data store, such as a MySQL™ or other relational database. Other physical and logical database types could be used. The data store may be a database server, such as PostgreSQL™, MongoDB™, Microsoft SQL Server™, Oracle™, IBM DB2™, SQLITE™, or any other database software, relational or otherwise. The data store may store the information identifying syntactical tags and any information required to operate on syntactical tags. In some embodiments, the processing system may use object-oriented programming and may store data in objects. In these embodiments, the processing system may use an object-relational mapper (ORM) to store the data objects in a relational database.

[81] Suitable processors for the execution of a program of instructions include, but are not limited to, general and special purpose microprocessors, and the sole processor or one of multiple processors or cores, of any kind of computer. A processor may receive and store instructions and data from a computerized data storage device such as a read-only memory, a random access memory, both, or any combination of the data storage devices described herein. A processor may include any processing circuitry or control circuitry operative to control the operations and performance of an electronic device.

[82] The processor may also include, or be operatively coupled to communicate with, one or more data storage devices for storing data. Such data storage devices can include, as non-limiting examples, magnetic disks (including internal hard disks and removable disks), magneto-optical disks, optical disks, read-only memory, random access memory, and/or flash storage. Storage devices suitable for tangibly embodying computer program instructions and data can also include all forms of non-volatile memory, including, for example, semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, ASICs (application-specific integrated circuits).

[83] The systems, modules, and methods described herein can be implemented using any combination of software or hardware elements. The systems, modules, and methods described herein can be implemented using one or more virtual machines operating alone or in combination with each other. Any applicable virtualization solution can be used for encapsulating a physical computing machine platform into a virtual machine that is executed under the control of virtualization software running on a hardware computing platform or host. The virtual machine can have both virtual system hardware and guest operating system software.

[84] The systems and methods described herein can be implemented in a computer system that includes a back-end component, such as a data server, or that includes a middleware component, such as an application server or an Internet server, or that includes a front-end component, such as a client computer having a graphical user interface or an Internet browser, or any combination of them. The components of the system can be connected by any form or medium of digital data communication such as a communication network. Examples of communication networks include, *e.g.*, a LAN, a WAN, and the computers and networks that form the Internet.

[85] One or more embodiments of the invention may be practiced with other computer system configurations, including hand-held devices, microprocessor systems, microprocessor-based or

programmable consumer electronics, minicomputers, mainframe computers, etc. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a network.

[86] While one or more embodiments of the invention have been described, various alterations, additions, permutations and equivalents thereof are included within the scope of the invention.

[87] In the description of embodiments, reference is made to the accompanying drawings that form a part hereof, which show by way of illustration specific embodiments of the claimed subject matter. The figures herein represent example use cases for the syntactic tagging system and are not intended to be limiting on the scope of the invention. It is to be understood that other embodiments may be used and that changes or alterations, such as structural changes, may be made. Such embodiments, changes or alterations are not necessarily departures from the scope with respect to the intended claimed subject matter. While the steps herein may be presented in a certain order, in some cases the ordering may be changed so that certain inputs are provided at different times or in a different order without changing the function of the systems and methods described. The disclosed procedures could also be executed in different orders. Additionally, various computations that are herein need not be performed in the order disclosed, and other embodiments using alternative orderings of the computations could be readily implemented. In addition to being reordered, the computations could also be decomposed into sub-computations with the same results.

FIG. 1

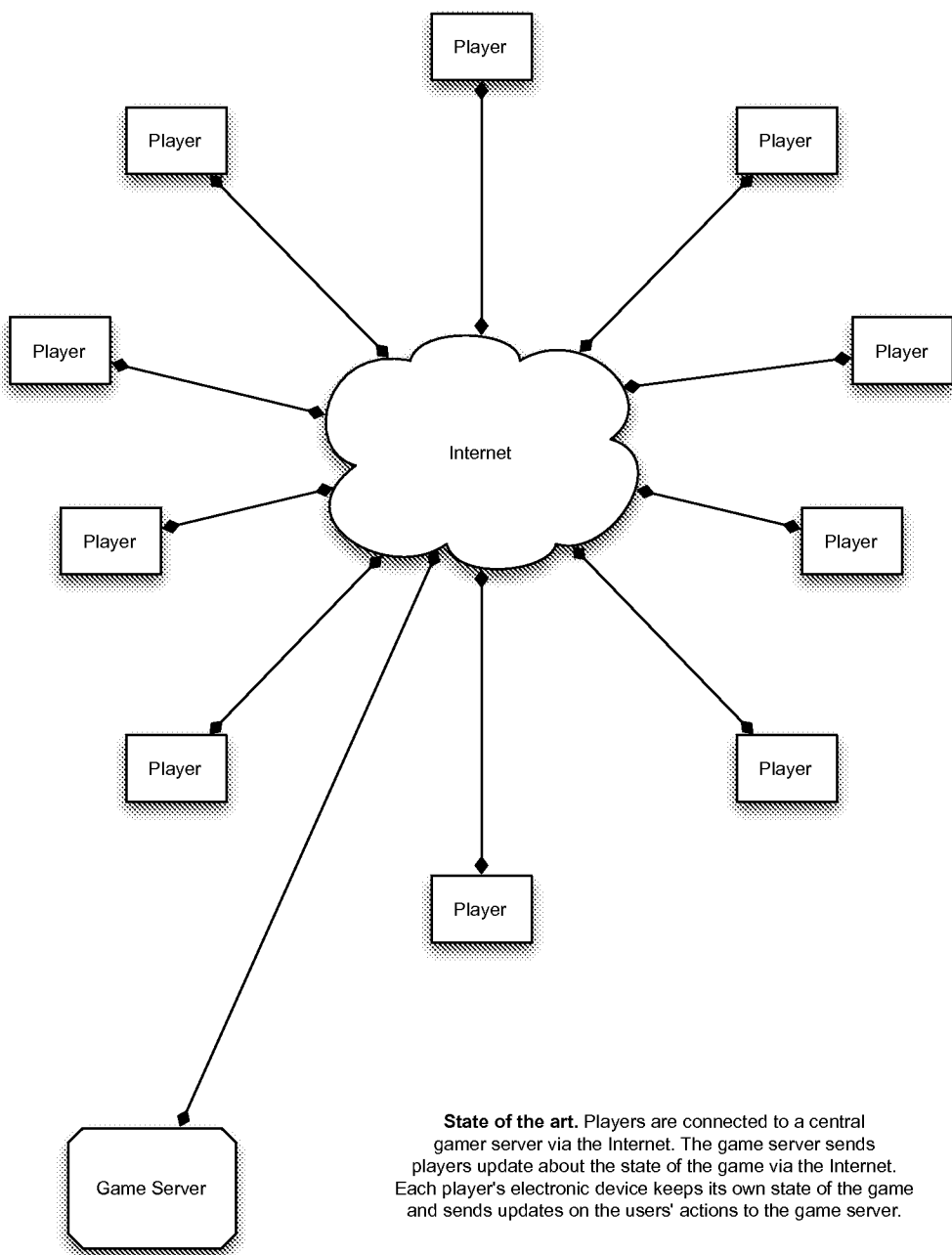


FIG. 2

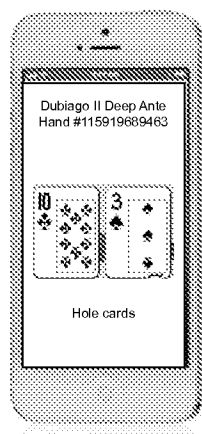
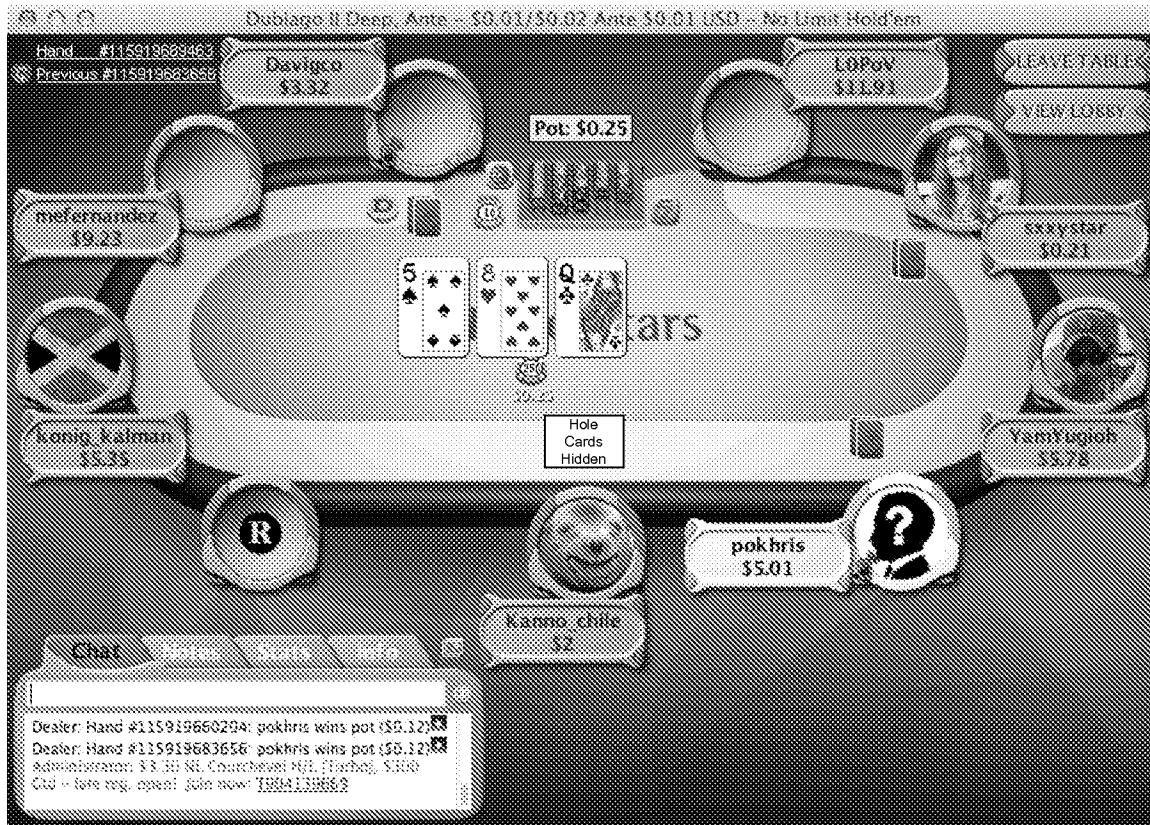


FIG. 3

**Player who elects to receive
hole cards over cellular network:**
The game server sends the same
information to the user's first device
as was sent in prior art systems, but
the user's hole cards are excluded. At
the same time, the hole cards are
sent to the user's smartphone over
the cellular network.

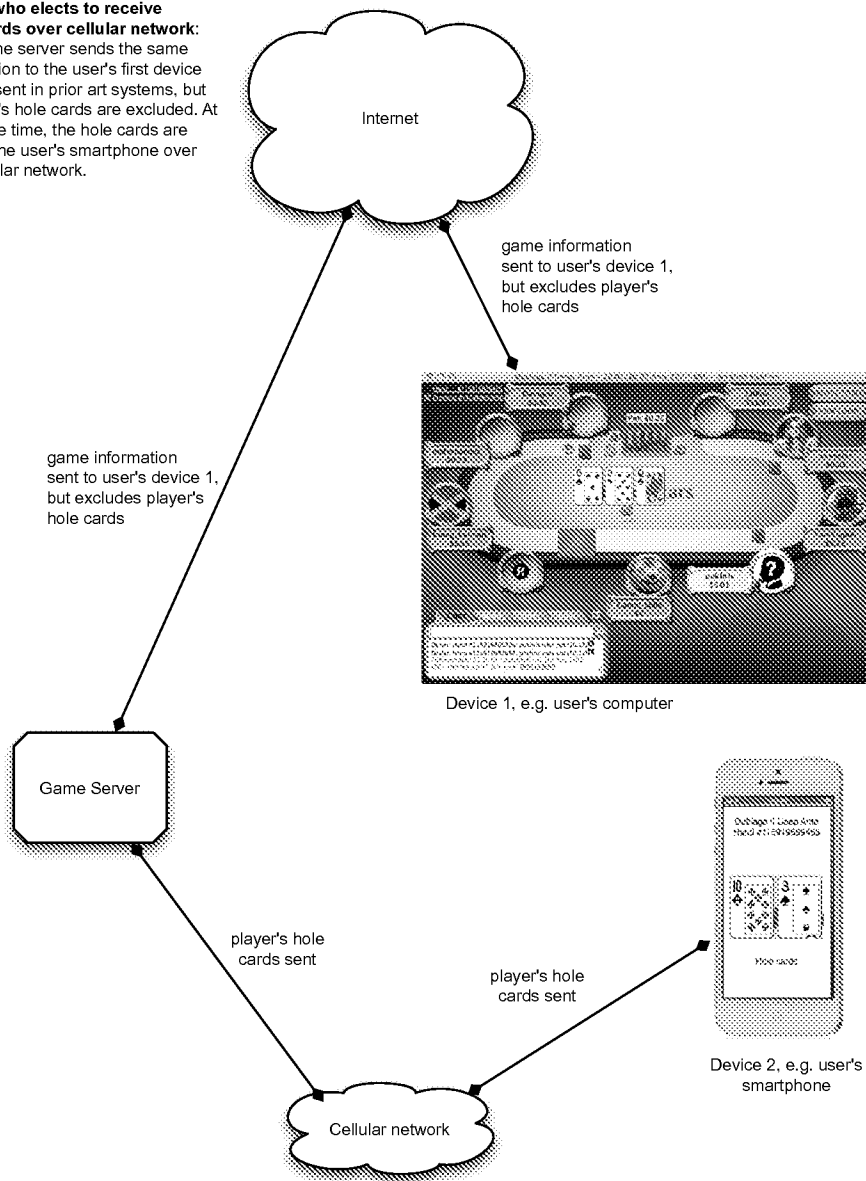


FIG. 4

**Player who elects to receive
hole cards over the Internet:**

The game server sends the same
information to the user's first device
as was sent in prior art systems, but
the user's hole cards are excluded. At
the same time, the hole cards are
sent to the user's smartphone over
the Internet.

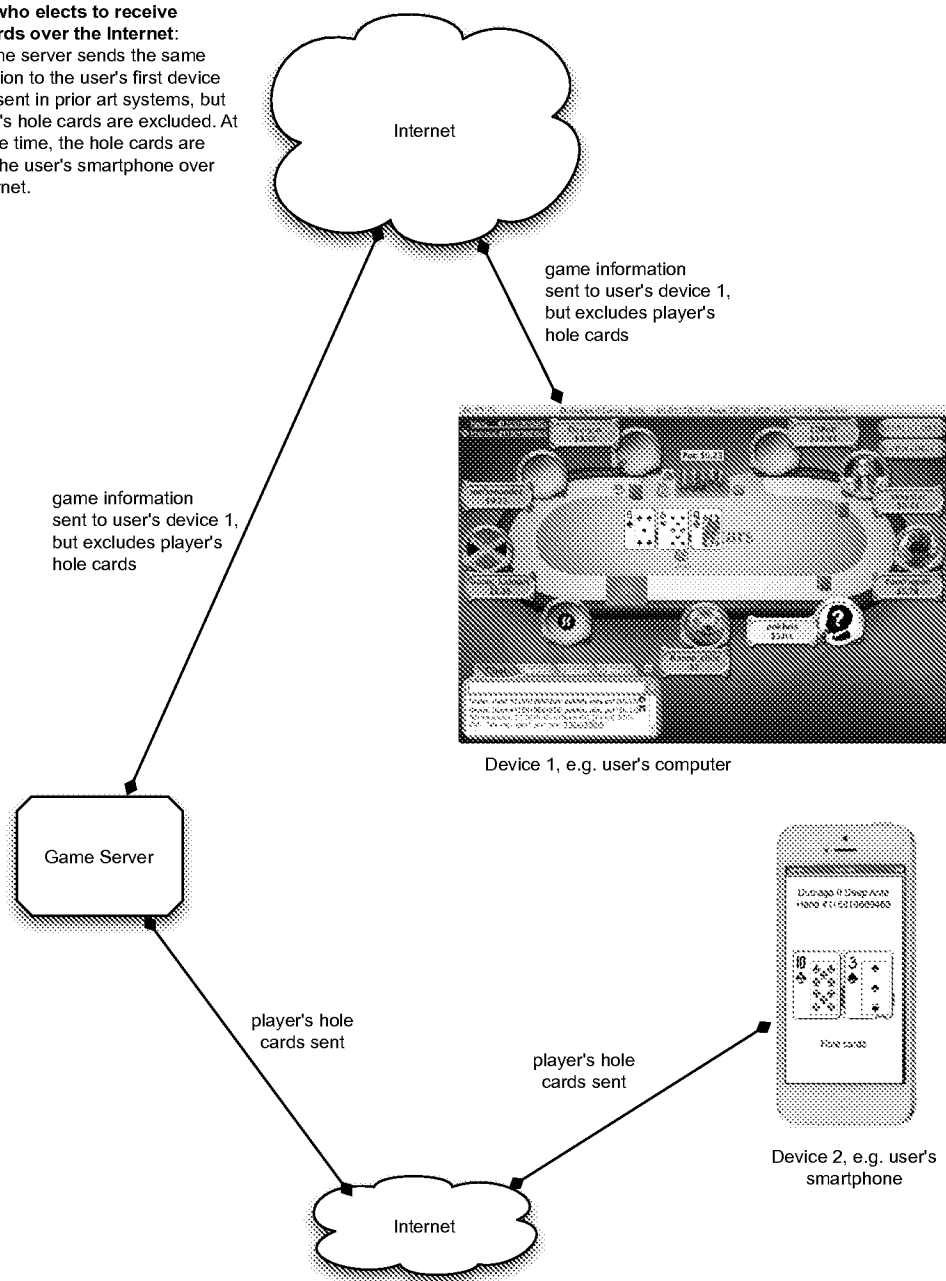


FIG. 5

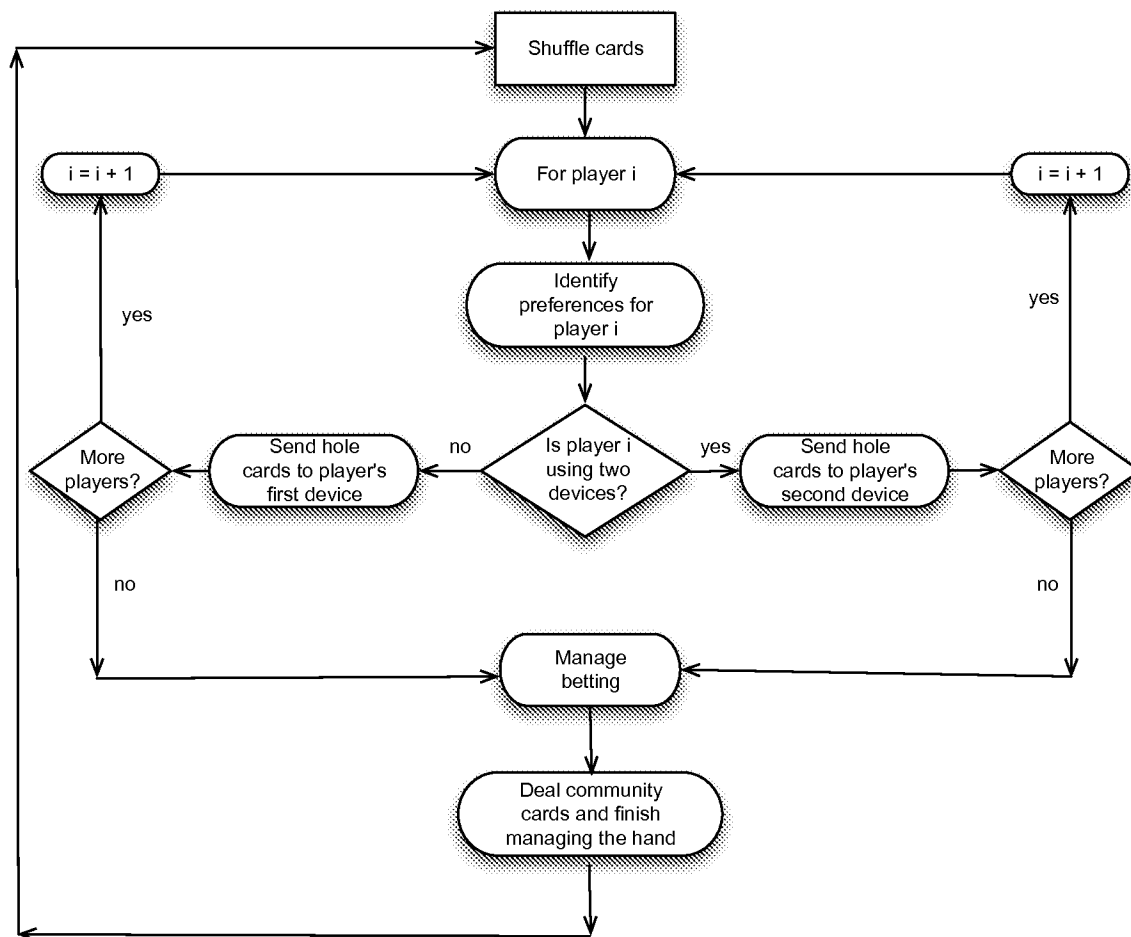


FIG. 6

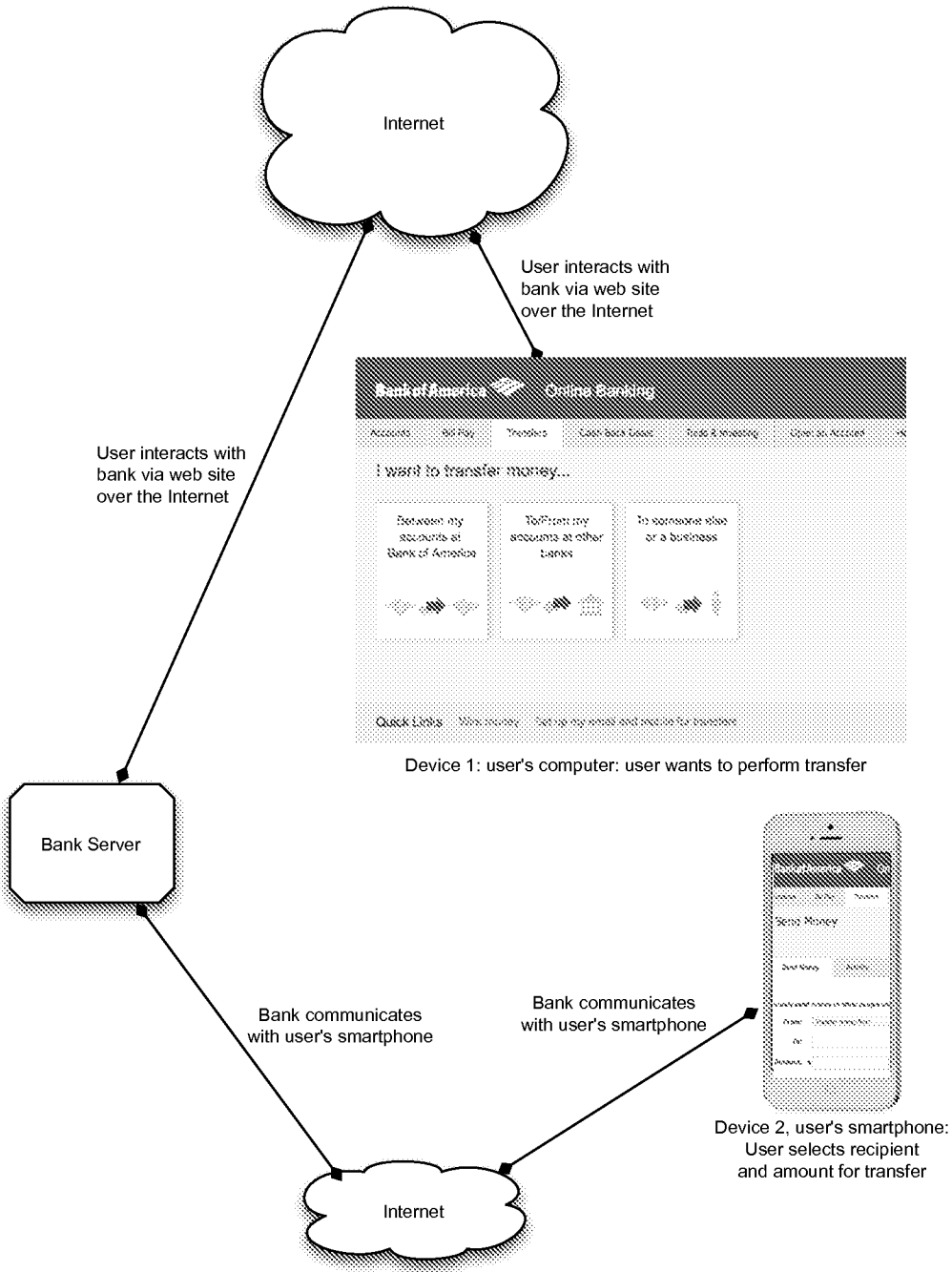


FIG. 7

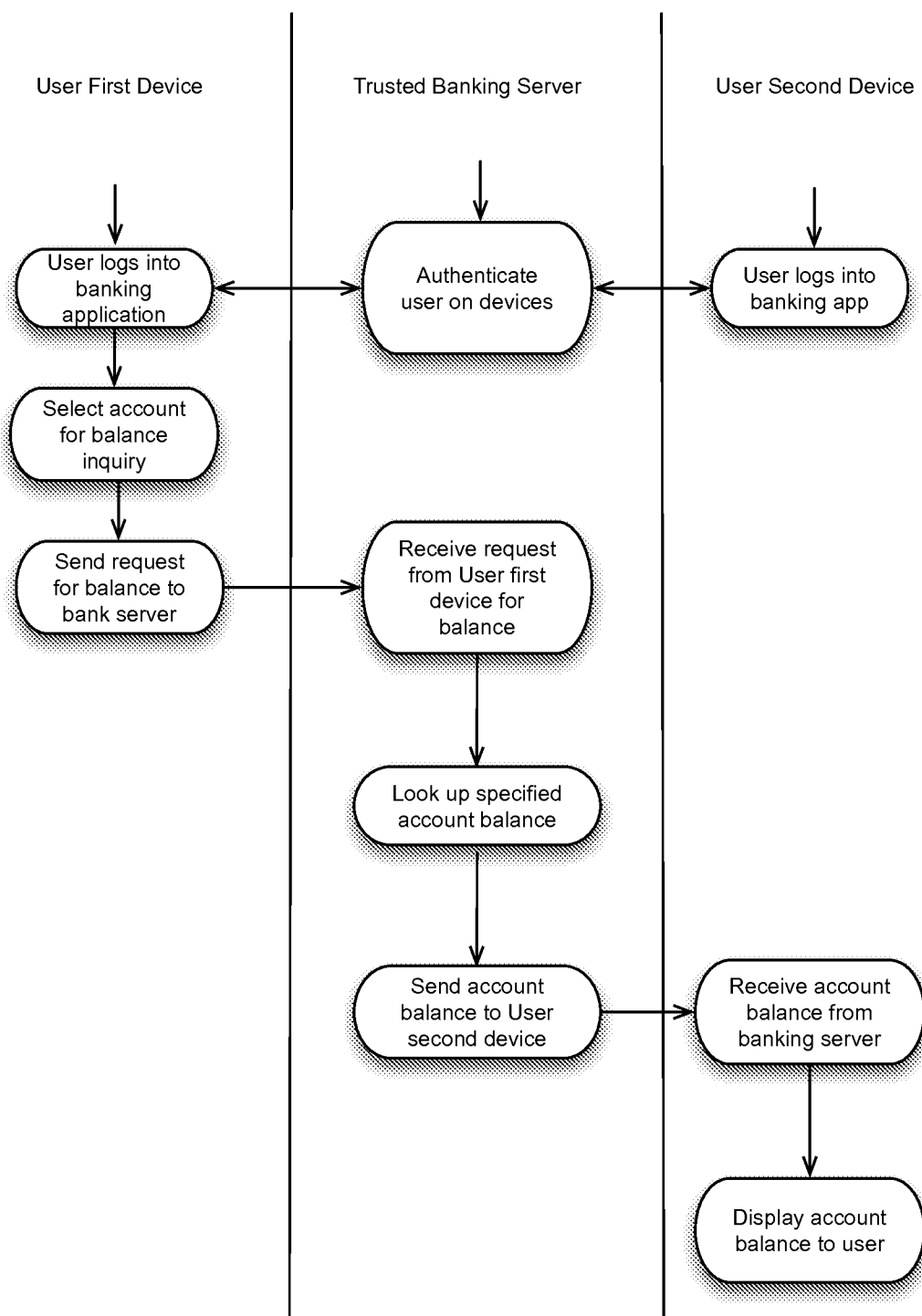


FIG. 8

username	John Doe
requires second device	Yes
hashed pw for first device	3987a87b87c73f3490c9d0
hashed pw for second device	98b7c73a347e789f98d342
authentication token	98234f342e324a7cd98b2a
funds transfer threshold	\$800
link to bank account info	Pointer to banking database: 0x00123adf32 Key to user entry in bank database: 3a98c3243f

Example database entry on central server
for user John Doe in banking example

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

UTILIZATION OF MULTIPLE DEVICES TO SECURE ONLINE TRANSACTIONS

First Named Inventor/Applicant Name:

Aviel David Rubin

Filer:

James M. Denaro

Attorney Docket Number:

0813EBDD-1

Filed as Small Entity

Provisional Filing Fees

Description

Fee Code

Quantity

Amount

**Sub-Total in
USD(\$)**

Basic Filing:

Provisional Application Filing Fee

2005

1

130

130

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Ex. 2006-036

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	19230297
Application Number:	62008561
International Application Number:	
Confirmation Number:	6709
Title of Invention:	UTILIZATION OF MULTIPLE DEVICES TO SECURE ONLINE TRANSACTIONS
First Named Inventor/Applicant Name:	Aviel David Rubin
Customer Number:	17012
Filer:	James M. Denaro
Filer Authorized By:	
Attorney Docket Number:	0813EBDD-1
Receipt Date:	06-JUN-2014
Filing Date:	
Time Stamp:	10:48:35
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	10790
Deposit Account	506129
Authorized User	DENARO, JAMES

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 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Ex. 2006-038

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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	Provisional Cover Sheet (SB16)	ProvisionalSB.pdf	1477166	no	3
			c44f1fd3fe90f089b99e5393a30652e51799cc6f		

Warnings:

Information:

2		Securing_Transactions_Provisional_PTO.pdf	2605178	yes	28
			b45cdfcc972b9d48de2cfaa83fec1780029938af		

Multipart Description/PDF files in .zip description

	Document Description	Start	End
	Specification	1	20
	Drawings-only black and white line drawings	21	28

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	29617	no	2
			3969527e6fd9e3fdbbc15cef1947b358b814c60b3		

Warnings:

Information:

Total Files Size (in bytes):			4111961
------------------------------	--	--	---------

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.

Ex. 2006-039