

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PLAID INC.,
Petitioner,

v.

SIX TREES CAPITAL LLC,
Patent Owner According to PTO Assignment Records, and

SECURE AUTHENTICATION TECHNOLOGIES LLC,
Patent Owner Identified in Patent Complaint.

Case No. IPR2026-00157
U.S. Patent No. 11,315,090

**DECLARATION OF DR. MARY K. BOLIN
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,315,090**

I, Mary K. Bolin, declare as follows:

1. I am Emeritus Professor at the University of Nebraska, Lincoln Libraries. I have held the following positions: Professor and Catalog and Metadata Librarian, Digital Initiatives and Special Collections Department, University of Nebraska—Lincoln Libraries (2015–2020); Professor and Chair, Discovery and Resource Management and Coordinator of Collection Development, University of Nebraska, Lincoln Libraries (2004–2015); San Jose State University School of Information: Lecturer (2008–present); Head of the Technical Services Department, University of Idaho Library (1993–2003; promoted to Professor in 1999); Head of the Cataloging Department, University of Idaho Library (1986–1993; promoted to Associate Professor and tenured in 1991); and Head of Records Maintenance Section, Cataloging Department, University of Georgia Libraries (1981–1986).

2. Over the course of my work as a librarian, professor, researcher, student research supervisor, and author of numerous scholarly papers and other publications, I have had extensive experience with cataloging records and online library management systems built around Machine-Readable Cataloging (MARC) standards. I also have substantial experience in authenticating printed documents and establishing the date when they were accessible to ordinarily skilled researchers.

3. Attachment A is my full resume.

4. I have been retained by counsel for Plaid Inc. (“Petitioner”) to evaluate, authenticate, and establish the date of public availability of a document relevant to the above-captioned Petition for *Inter Partes* Review. For my time performing this service, I am being paid my usual hourly fee. I have no financial interest in this action, or affiliation with Petitioner. My compensation is not dependent upon the outcome of, or my testimony in, this proceeding or any other proceeding, including before the U.S. Patent Office.

A. Document of Interest

5. The document that is the subject of this Declaration (“Document”) is the following: Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & De Sousa, R. T. (2011). A formal classification of internet banking attacks and vulnerabilities. *International Journal of Computer Science & Information Technology*, 3(1), 186-197.

B. Methodology

6. I searched for the Document in the OCLC database, Google Scholar, and subscription databases such as IEEE Xplore and ACM Digital Library. I also searched the library catalogs of institutions such as the University of Nebraska—Lincoln and other large research libraries. My goal was to find a record in one of these databases that contained a date indicating when the Document was available to the public.

7. *Use of MARC Records.* The “Machine Readable Cataloging” standard, also known as “MARC,” is an industry-wide standard method of organizing library catalog information. The Library of Congress first developed MARC in the 1960s. A MARC-compatible library is one that has a catalog consisting of individual MARC records for each of its works. Today, MARC is the primary communication protocol for the transfer and storage of bibliographic metadata in libraries.

8. OCLC is a database of MARC records used by libraries worldwide. When an OCLC-participating institution acquires a work, it creates a MARC record for this work in its computer catalog system, and OCLC automatically supplies the date of creation. The MARC record creation date reflects the date on which (or shortly after) the item was first acquired and cataloged. Once the MARC record is created by a cataloger at an OCLC-participating member institution, it is instantaneously available to any OCLC-participating members and, therefore, available to the public.

9. A MARC record comprises several fields, each of which contains specific data about the work. Each field is identified by a standardized, unique, three-digit code corresponding to the type of data that follows. For example, a work’s title is recorded in field 245, the primary author of the work is recorded in field 100, an item’s International Standard Book Number (“ISBN”) is recorded in field 020, an item’s Library of Congress call number is recorded in field 050, and

the publication date is recorded in field 260 or 264 under the subfield “c.” If a work is a periodical, then its publication frequency is recorded in field 310, and the publication dates (*e.g.*, the first and last publication) are recorded in field 362, which is also referred to as the enumeration/chronology field. The library that created the record is recorded in field 040 in subfield “a” with a unique library code. When viewing the MARC record online via OCLC’s Worldshare Record Manager database, hovering over this code with the mouse reveals the name of the library. I used this method of “mousing over” the library codes in the OCLC database to identify the originating library for all of the MARC records in this Declaration, as well as the “display holdings” command to see a list of libraries that own the item. In the MARC records in the OCLC Worldshare Record Manager database, MARC field 040 contains the OCLC symbols of institutions transcribing, creating, and modifying the record.

10. OCLC was created “to establish, maintain and operate a computerized library network and to promote the evolution of library use, of libraries themselves, and of librarianship, and to provide processes and products for the benefit of library users and libraries, including such objectives as increasing availability of library resources to individual library patrons and reducing the rate of rise of library per-unit costs, all for the fundamental public purpose of furthering ease of access to and use of the ever-expanding body of worldwide scientific, literary and educational

knowledge and information.”¹ Among other services, OCLC and its members are responsible for maintaining the WorldCat database (<http://www.worldcat.org/>), which is used by independent and institutional libraries throughout the world. OCLC is the international cooperative to which libraries catalog records and others pay to access MARC records. The MARC records referenced in this Declaration, extracted from the OCLC database, were generated in the ordinary course of business. Further, I personally located and downloaded each of these records associated with the Document on which this Declaration focuses.

11. OCLC provides its members online access to MARC records through its OCLC Worldshare Record Manager database. When an OCLC member institution acquires a work, it creates a MARC record for this work in its computer catalog system in the ordinary course of its business. MARC records created at the Library of Congress are batch-loaded into the OCLC database through a subscription to MARC Distribution Services daily or weekly. Once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress, it is then made available to any other OCLC members online, and, therefore, made available to the public.

¹ Third Article, Amended Articles of Incorporation of OCLC Online Computer Library Center, Incorporated (available at <http://www.oclc.org/en-US/membership/councils.html>).

12. When an OCLC member institution creates a new record, OCLC automatically supplies the date of creation for that record. The MARC record creation date reflects the date on which, or shortly after which, the item was first acquired or cataloged.

13. The date of creation for the MARC record appears in the fixed field (008), characters 00 through 05. Field 005 is a 16 digit field that records the date characters `yyyymmdd` including 4 for the year, 2 for the month, and 2 for the day. The date entered on file never changes. These dates are automatically supplied by the OCLC system and cannot be changed by the user. When the MARC record is created in OCLC, it is available throughout the world to other libraries and in WorldCat, the public version of OCLC Connexion. Thus, the date of creation of the MARC record by a cataloger at an OCLC member institution reflects when the underlying item is accessible to the public.

14. MARC records also include several fields that include subject matter classification information. An overview of MARC record fields is available through the Library of Congress.² For example, 6XX fields are termed “Subject Access Fields.”³ Among these, for example, is the 650 field, which is the “Subject Added Entry – Topical Term” field.⁴ The 650 field is a “[s]ubject added entry in which the

² See <http://www.loc.gov/marc/bibliographic/>.

³ See <http://www.loc.gov/marc/bibliographic/bd6xx.html>.

⁴ See <http://www.loc.gov/marc/bibliographic/bd650.html>.

entry element is a topical term.” *Id.* The 650 field entries “are assigned to a bibliographic record to provide access according to generally accepted thesaurus-building rules (e.g., *Library of Congress Subject Headings* (LCSH), *Medical Subject Headings* (MeSH)).” *Id.* Thus, a researcher can easily discover material relevant a topic of interest with a search using the terms employed in the MARC Fields 6XX.

15. For the Document, I performed a search of OCLC (www.oclc.org), which is a large shared database used by libraries around the world to create and exchange cataloging data, using MARC format, which is a universal communications format for that data.

16. Using the records from OCLC, I determined when each record was created, and which libraries own the items. I then visited the website of the library or libraries that own the items, searched their library catalog, and determined when the items were added to the library’s collection.

17. I am familiar with many online catalogs, databases, and search engines. In preparing for this Declaration, I used authoritative information systems such as the above-mentioned WorldCat (<https://www.worldcat.org>), the online catalog of the Library of Congress (<https://catalog.loc.gov>), shared research databases such as ResearchGate and CiteSeerX (formerly known as CiteSeer), the online catalog of a number of large research libraries such as the University of Nebraska—Lincoln,

IEEEExplore, and Google Scholar search for records. These records are identified and discussed in this Declaration.

18. The IEEE Xplore⁵ research database is a vital resource for undergraduate and graduate students, researchers, scientists, and the public, offering access to high-quality, peer-reviewed publications. IEEE Xplore serves as a repository for IEEE's ebooks, standards, conference proceedings, technical reports, and journal articles, with content dating back to 1988 and selectively covering materials from 1913 to 1987. The database currently includes over 5.5 million full-text documents and is recognized for its rigorous curation and accurate bibliographic records. IEEE Xplore ensures precise reporting of publication dates and event locations in alignment with industry standards for major scholarly and technical journals. Approximately 20,000 new documents are added each month. While abstracts are freely available, full-text access requires a subscription or institutional login.

19. I am familiar with the Internet Archive, a digital library formally certified by the State of California as a public library. Among other services that the Internet Archive makes available to the general public, is the Wayback Machine, an online archive. The Internet Archive's Wayback Machine service archives webpages as of a certain capture date to track changes in the web over time. The Internet

⁵ See <https://ieeexplore.ieee.org/Xplore/home.jsp>.

Archive has been in operation as a nonprofit library since 1996 and has hosted the Wayback Machine service since its inception in 2001. I consider the Internet Archive's records keeping to be as rigorous and detailed as other formal library records keeping practices such as MARC records and OCLC records.

C. Opinions Regarding the Document

20. The following are my opinions with respect to the authenticity and public availability of the Document—Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & De Sousa, R. T. (2011). A formal classification of internet banking attacks and vulnerabilities. *International Journal of Computer Science & Information Technology*, 3(1), 186-197.

1. Authentication of the Document

21. Attachment B is a PDF of the Document, downloaded from Research Gate at https://www.researchgate.net/publication/50211018_A_Formal_Classification_of_Internet_Banking_Attacks_and_Vulnerabilities, and showing a publication date of February 2011.

22. Attachment C is a screenshot of the PDF properties of the Document retrieved from Research Gate, showing a creation date of February 22, 2011.

23. Attachment D is a PDF of the search results for the Document, in WorldCat.org, the open access public version of OCLC, showing a publication date of February 2011.

24. Attachment E is a PDF of the website of the *International Journal of Computer Science & Information Technology* (“IJCSIT”), where the Document was published, showing a publication date of February 2011.

25. Attachment F is a PDF of the Document, downloaded from the IJCSIT website at <https://airccse.org/journal/jcsit/0211ijcsit13.pdf>, and showing a publication date of February 2011.

26. Attachment G is a screenshot of the PDF properties of the Document found at the IJCSIT, showing a creation date of February 22, 2011.

27. Attachment H is a PDF of the website of the IJCSIT, archived by Internet Archive’s Wayback Machine at https://web.archive.org/web/20110302081810/https://airccse.org/journal/ijcsit2011_curr.html, showing that the Document was publicly available for download from the IJCSIT website on March 2, 2011.

28. Attachment I is a PDF of the Document’s citations page from Google Scholar at https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NjtpR1

IAAAAJ&pagesize=80&citation_for_view=NjtpR1IAAAAJ:BJbdYPG6LGMC, showing that the Document was cited four times in 2012 and three in 2013.

2. *Public Availability of the Document*

29. Based on the fact that the Document is found on a March 2, 2011 archived version of the IJCSIT website, in the Research Gate repository, and WorldCat.org, with each indicating a publication date of February 2011, and a PDF creation date of February 22, 2011, it is my conclusion that the Document was available prior to January 28, 2014, and could have been found by a skilled researcher.

30. Public availability of the Document before January 28, 2014 is also confirmed via the seven citations listed in Google Scholar in articles published in 2012 and 2013.

3. *Locating the Document*

31. Attachment J is a PDF of the website of the IJCSIT, archived by Internet Archive's Wayback Machine at https://web.archive.org/web/20110917052615/https://airccse.org/journal/jcsit_index.html, showing that the "articles of IJCSIT" were "indexed/abstracted" in numerous index services, including Google Scholar, CiteSeerX, WorldCat, and ProQuest, by September 17, 2011.

32. In my professional experience as a librarian, academic libraries have had access to WorldCat.org since it was launched in January 1998. A skilled researcher could have searched WorldCat.org for the Document and located it from its publication in February 2011 and prior to January 28, 2014.

33. For example, the Document could have been located using words from the title, the abstract, the authors' names, and the journal title.

34. Moreover, Google Scholar has been freely accessible since its launch in 2004. A skilled researcher could have searched Google Scholar for the Document and located it prior to January 28, 2014.

35. For example, the Document could have been located using words from the title, abstract, or full-text of the Document.

36. Thus, it is my opinion that someone searching the Document would have been able to locate the Document prior to January 28, 2014.

* * *

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 are made with the knowledge that willful false statements and the like are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the U.S. Code. I state under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 7th day of January, 2026, in Minneapolis, Minnesota.

A handwritten signature in cursive script, appearing to read "Mary K. Bolin". The signature is written in dark ink on a light background.

Mary K. Bolin

ATTACHMENT A

Mary K. Bolin, PhD
201 25th Ave S
Minneapolis, Minnesota 55406
mary@marykbolin.com

Mary K. Bolin, PhD

Professor Emeritus
University Libraries
University of Nebraska—Lincoln
mbolin2@unl.edu

Lecturer,
School of Information
San José State University
mary.bolin@sjsu.edu

EDUCATION

PhD, Educational Studies (Educational Leadership and Higher Education), 2007, University of Nebraska

Dissertation: *A Typology and Discourse Analysis of the Status and Appointments of Librarians at Land Grant Universities* (available at digitalcommons.unl.edu)

MA, English, 1999, University of Idaho

Thesis: *Grace: A Contrastive Analysis of a Biblical Semantic Field* (available at digitalcommons.unl.edu)

MSLS, 1981, University of Kentucky

BA, Linguistics, 1976, University of Nebraska—Lincoln

WORK EXPERIENCE

Center for Digital Research in the Humanities. Fellow, 2019- Emeritus, 2020-

University of Nebraska--Lincoln Libraries: Professor and Catalog and Metadata Librarian, Digital Initiatives and Special Collections, 2015-2020. Emeritus, 2020-

University of Nebraska—Lincoln Libraries: Professor and Chair, Discovery and Resource Management, 2004-2015; Coordinator of Collection Development, 2012-2015

University of Idaho Library: Head, Technical Services Department, 1993-2003. Promoted to Professor in 1999

University of Idaho Library: Head, Cataloging Department, 1986-1993. Promoted to Associate Professor and tenured, 1991

University of Georgia Libraries: Head, Records Maintenance Section, Cataloging Department, 1981-1986

Teaching:

San José State University School of Information:

LIBR 281, Metadata. 2009-

LIBR 248, Introduction to Cataloging and Classification. 2013-

LIBR 202, Information Retrieval. 2008-2013

Associate Coordinator, Gateway PhD program, San Jose State University, 2021-2022

American Library Association:

Cataloging for Non-Catalogers, Online Continuing Education Course, 2017- Intermediate

Cataloging for Non-Catalogers, Online Continuing Education Course, 2018-

Lyrasis:

Webinar on BibFrame, taught twice a year, 2020-

Quick and Clean Cataloging, Parts 1, 2, and 3. 2022-

Independent Study in Idaho:

Library Science C415, Technical Services for Small Libraries, 2004-2013

Library Science C416, Library Services to Rural Libraries, 2004-2013
Library Science C422, Use of the School Library, 1999-2013
Library Science C425/525, Organization and Management of Small Libraries,
1988-2013
Library Science C427, Library or Media Center Practicum, 1995-2013

Gateway PhD Program (San Jose State University and Queensland University of Technology).
SJSU supervisor for two PhD students, 2015-

Gateway PhD Program (San Jose State University and Manchester Metropolitan University).
Associate Coordinator, 2021-2022

Consulting

Expert witness for multiple attorneys employed by Wolf, Greenfield & Sacks, P.C.,
Hughes Hubbard & Reed LLP, and other firms. 2017-

Editing

Language and academic editing for [EditSprings](#), a service for international scholars, 2020-

SCHOLARSHIP

Refereed Publications:

(Publications available from digitalcommons.unl.edu)

Pytlík Zillig, Brian, and Mary K. Bolin. (Forthcoming 2024). “Visualization of Semantic Primes in Texts from Early Modern English Drama.” *Journal of the Japanese Association for the Digital Humanities*.

Bolin, Mary K. (2022). “Academic Libraries and Writing Centers: Collaborations at US Public Research Universities.” *School of Information Student Research Journal*, 11(2). Retrieved from <https://scholarworks.sjsu.edu/ischoolsrj/vol11/iss2/2>

Bolin, Mary K. (2022). *Refocusing Academic Libraries through Learning and Discourse: The Idea of a Library*. Oxford, UK: Chandos/Elsevier.

Bolin, Mary K. (2022). “Metadata, Catalog Systems, Linked Data, and the Evolving ILS.” In: Sandra Hirsh (Ed.), *Information Services Today: An Introduction*. 3rd ed. New York: Rowman

and Littlefield.

Wintermute, Harriet E., and Bolin, Mary K. (2018). "Metadata Generators for Backlog Reduction: Metadata Maker Streamlines Cataloging and Facilitates Transition. *Technical Services Quarterly* 35(2) doi: <https://doi.org/10.1080/07317131.2018.1422879>

Bolin, Mary K. (2018). "Metadata, Catalog Systems, Linked Data, and the Evolving ILS." In: Sandra Hirsh (Ed.), *Information Services Today: An Introduction*. 2nd ed. New York: Rowman and Littlefield.

Bolin Mary K. (2017). *The 21-century Academic Library: Global Patterns of Organization and Discourse*. Oxford: Chandos Publishing. (Chandos Information Professional Series)

Bolin, Mary K. (2017). Linguistics and LIS: A Research Agenda." *SLIS Student Research Journal*, 7:1.

Retrieved from <http://scholarworks.sjsu.edu/slissrj/vol7/iss1/2>

Bolin, Mary K. (2014). "Open Access Web Resources for Library Continuing Education and Training." In S. Hines (Ed.), *Revolutionizing the Development of Library and Information Professionals: Planning for the Future* (pp. 107- 124). Hershey, PA: . doi:10.4018/978-1-4666-4675-9.ch008.

Bolin, Mary K. (2014). "The Language of Academic Librarianship: The Discourse of Promotion and Tenure. " *Advances in Library Administration and Organization* 32.

Bolin, Mary K. "Librarian Status at US Research Universities: Extending the Typology." *Journal of Academic Librarianship* 34:4 (September 2008)

Bolin, Mary K. "A Typology of Librarian Status at Land Grant Universities." *Journal of Academic Librarianship*, 34: 3 (May 2008)220:230.

Bolin, Mary K. "The Library and the Computer Center: Organizational Patterns at Land Grant Universities." *Journal of Academic Librarianship*, 31:1 (2005)

Eckwright, Gail Z. and Mary K. Bolin. "The Hybrid Librarian: The Affinity of Collection Management with Technical Services and the Organizational Benefits of an Individualized Assignment." *Journal of Academic Librarianship*, 27:6 (2001)452:457.

Bolin, Mary K. "Catalog Design, Catalog Maintenance, Catalog Governance," *Library*

Collections, Acquisitions, and Technical Services. 24: (2000)53-63.

Bolin, Mary K. "The Collegial Environment and the Functional Organization," *Journal of Library Administration*. 29:2(1999):49-61.

Bolin, Mary K. "Cataloging Environmental Impact Statements and Related Documents," *Resource Sharing and Library Networks*. 14:1(1999): 21-40.

Bolin, Mary K. "Waiting for the Electrician or Someone like Him: Client-Centered Technical Services" Proceedings of the Association of College and Research Libraries National Conference, Nashville, April 1997.

< http://www.ala.org/Content/ContentGroups/ACRL1/Nashville_1997_Papers/Bolin.htm >

Grants:

Electronic Theses and Dissertations. Seed Grant from University of Idaho Office of Research, 2002. Co PI with Gail Z. Eckwright. \$6500.

Interoperability of Metadata for Thematic Research Collections. Grant to the Center for Digital Research in the Humanities from the Institute of Museum and Library Services 2005-2008. Project Team Member.

http://unlcms.unl.edu/cas/center-for-digital-research-in-the-humanities/projects/pages/iom_files/IOM_Final_Narrative_Report_July_2008.pdf

Other Publications:

Library Philosophy & Practice. Peer-reviewed electronic library science journal. Mary K. Bolin and Gail Z. Eckwright, founders and editors. <http://digitalcommons.unl.edu/libphilprac>

Library Science C415, Technical Services for Small Libraries, through Independent Study in Idaho. 2004.

Library Science C416, Library Services to Rural Libraries, through Independent Study in Idaho. 2004.

Library Science C422, Use of the School Library, through Independent Study in Idaho. Revised 1999.

Library Science C425/525, Organization and Management of Small Libraries through

Independent Study in Idaho. Revised 2005.

Library Science C427, Library or Media Center Practicum, Independent Study in Idaho. Revised 1999.

Presentations:

Bolin, Mary K. "BibFrame and the MARC Cataloging Environment: an Introduction." Lyrisis Webinar, June 16, 2020, August 17, 2021.. Recording available <http://lyrisis.adobeconnect.com/paufo9e0dm30/>

Pytlik Zillig, Brian, and Mary K. Bolin. "A Little More than Kin, a Little Less than Kind": the Semantic Field Grace in Early Modern English" Poster Session, Text Encoding Initiative Meeting, Graz, Austria, September 18, 2019

Pytlik Zillig, Brian, and Mary K. Bolin. "Shakespeare and the Enumeration of Semantic Primes." Research Paper Presentation, Text Encoding Initiative Meeting, Tokyo, Japan, September 13, 2018

"Library Philosophy and Practice: Creating and Maintaining an Open-Access E-Journal," Presentation to UNCL meeting (libraries at campuses of the University of Nebraska), Lincoln, Nebraska, March 20, 2008.

Presentation to "Thinking outside the Borders" participants on the open-access electronic journal Library Philosophy and Practice and its role in the international library community. University of Nebraska—Lincoln Libraries, October 24, 2007

Panel discussion on open access electronic journals. GWLA directors' meeting. Linda K. Hall Library, Kansas City, Missouri. April 2007.

"Waiting for the Electrician or Someone Like Him: Client-Centered Technical Services." Association of College and Research Libraries National Conference, Nashville, April 5, 1997.

" 'Some Problems of an Editor': the Idaho Librarian from Manuscript to Published Issue," Joint Annual Conference of the Idaho Library Association and the Washington Library Association, Spokane, Washington, April 6, 1995.

"Automating Idaho's Libraries: a Historical Perspective." Idaho Library Association Annual Conference, Idaho Falls, October 4, 1990.

"Small Library Management." Idaho Library Association Spring Conference, Lewiston, Idaho, May 13, 1989.

"No More 'Good Workers': Excellence and Academic Library Classified Staff." Association of College and Research Libraries 5th Annual Conference, Cincinnati, April 7, 1989.

"Communication to and from Cataloging Departments." Heads of Cataloging Discussion Group, American Library Association Midwinter Meeting, San Antonio, January 1988.

Discussion Leader at the LAMA (Library Administration and Management) Management Exchange. American Library Association Annual Meeting, San Francisco, June 1987.

"Staff Turnover." Heads of Cataloging Discussion Group, American Library Association Midwinter Meeting, Chicago, January 1987.

SELECTED PROFESSIONAL SERVICE

Reviewer. *Resources for College Libraries*. Linguistics bibliography, Spring 2020.

Peer reviewer for ALISE National Conference presentations, Spring 2020. Peer

reviewer for *Journal of Academic Librarianship*, 2012-

Peer reviewer for refereed journal, *Western Nigerian Journal of Medical Sciences* (<http://www.wnjms.org/>), a publication of Ladoke Akintola University of Technology (LAUTECH) Teaching Hospital, 2008-

PhD Reviewer for students from Aligarh Muslim University, India, 2010- Outside reviewer for numerous library faculty promotion and tenure cases in US universities.

University of Nebraska--Lincoln

Chair, University Libraries Faculty, 2018

Faculty Senate Academic Rights and Responsibilities Committee, 2016- Chair, 2018-19

Faculty Senate – 2004-2008; 2008-2011

Faculty Senate Executive Committee 2004-2008
Academic Planning Committee (APC), 2005-2008; Vice Chair, 2006-2007; Chair,
2007-2008

Aesthetic Review Committee 2006-2007

APC monitor for academic program reviews: Department of Political Science, 2005;
Department of Educational Psychology 2006
Pacific Northwest Library Association:

Editor, *PNLA Quarterly*, December 2002-December 2013

Idaho Library Association:

Editor, *The Idaho Librarian*, September 1990-January 1996

ATTACHMENT B

A FORMAL CLASSIFICATION OF INTERNET BANKING ATTACKS AND VULNERABILITIES

Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo de Sousa Jr.

Electrical Engineering Department, University of Brasilia (UnB)
Campus Universitario Darcy Ribeiro -- Asa Norte -- 70910-900 -- Brasília, DF -- Brazil
{peotta,holtz,bernardo.david,desousa}@redes.unb.br

Abstract

A formal classification of attacks and vulnerabilities that affect current internet banking systems is presented along with two attacks which demonstrate the insecurity of such systems. Based on a thorough analysis of current security models, we propose a guidelines for designing secure internet banking systems which are not affected by the presented attacks and vulnerabilities.

KEYWORDS

Internet banking, e-bank, online bank, identification, authentication, authorization.

1. INTRODUCTION

Currently there is a clear need for efficient security models by banks which offer online access to their banking systems [20]. In face of the growing number of transactions processed through online banking systems, several new security technologies and models which aim at providing authenticated secure communications through known insecure channels have been introduced in current literature [16].

The number of malware and exploits focused on online banking systems vulnerabilities has been steadily growing during past years [19]. Recent reports [22] indicate that banking trojans were among the 50 main security threats in 2009, while Brazil figures as the source and destination of most of those attacks performed in Latin America[30].

In order to propose security models and solutions in general it is first necessary to understand and properly classify the existing attack techniques and the vulnerabilities on which they are based. Such characterization must be conducted taking into consideration the external factors that affect security and the intrinsic trust relation between users and providers of online banking services. Furthermore, it must be considered the responsibility for maintaining security is always transferred to the weakest link in the security chain, which means, in most cases, the final user. In this paper we present a formal analysis and classification of the several vulnerabilities and attacks that affect online banking systems.

The rest of this paper is organized as follows: the current security models for online banking are discussed in sections 2 and 3. In section 4, we present a comparative analysis of the solutions currently adopted by banking institutions and their inherent vulnerabilities. In section 5, attack modelling is introduced and we describe efficient attacks against currently adopted solutions. In section 6, the countermeasures necessary to thwart the presented attacks are introduced. Finally, in section 7, we conclude with suggestions for future works.

2. RELATED WORKS

Current research is directed towards attacks and malicious activities identification in online banking systems. In [14] the authors introduce attack techniques focused on vulnerabilities which are present in a specific internet banking system, presenting attack implementation results. In [16] the authors propose a protocol for legitimate user identification based on transaction profile pattern matching and dynamic keys and groups. However, a model solely based on legitimate user identification is not computationally efficient due to the constantly growing number of online banking systems users. The same authors propose a smartcard based identification protocol in [10].

Several security models aiming at phishing mitigation have been proposed [24] [25]. Basically, both solutions are limited to identifying users through the analysis of currently adopted processes and security models, being inefficient when applied to new internet banking systems. The results in [29] show that any device operating in a compromised environment becomes equally compromised as the environment could alter and tamper communication messages sent and received by the device. The authors suggest that a device authentication model would effectively secure the banking system against such compromised situations.

Most of the proposed solutions are limited to identifying adversaries through pattern matching algorithms which detect suspect behavior patterns among transaction history data. Due to the sheer number of internet banking transactions such methods do not efficiently identify attackers before they perform a significant amount of illegitimate transactions and fraud.

3. INTERNET BANKING SECURITY MODELS

Online banking systems require efficient security models capable of identifying users and authorizing transactions, thus mitigating fraud. However, current models are focused on fraud identification instead of fraud prevention, which means that actions are taken only after a fraud occurs instead of performing a series of preventive procedures.

Analysing the security devices implemented by the ten largest banks in Brazil it is observed that several security layers and methods are concurrently adopted (Figure 1). Virtual keyboards are clearly one of the most used models, being adopted in 8 different banks. However, banking trojans continue to successfully operate, directing security to reactive fraud identification rather than prevention.

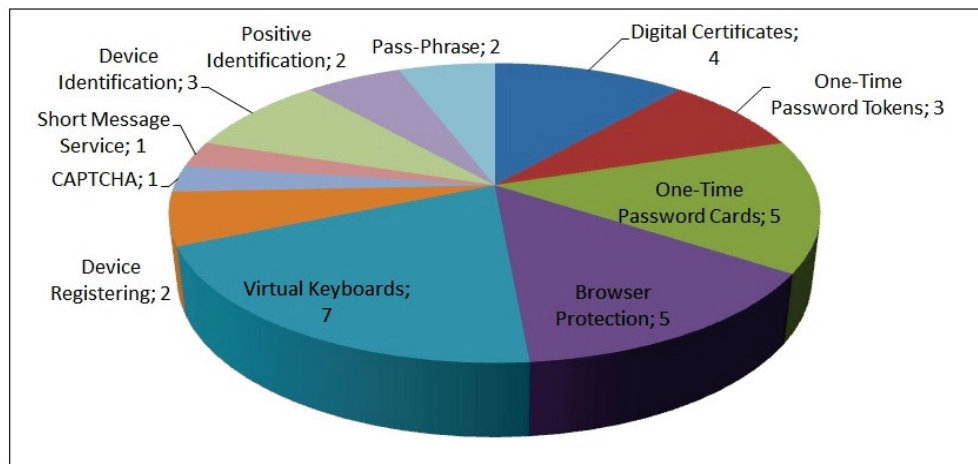


Figure 1: Internet Banking Security Models

In this analysis, SSL (Secure Sockets Layer) was not considered because it is adopted in all online banking systems. Moreover, SSL only provides security from the network layer downwards but is not capable of guaranteeing protection against attacks based on the application layer, where data is captured or modified before encryption.

Basically, banking systems need to accurately identify the user and authorize his access to banking transactions. The identification schemes are based on two main factors: unique secret information previously shared by the user and the bank (such as passwords) and unique characteristics of the device which is being used to access the service (device fingerprinting). However, if any of the media through which these informations are collected (including the user's device) is compromised, the security system is compromised as a whole because it would allow an adversary to insert and capture information at a point of the system. It is important to understand how banking systems employ security mechanisms and why they do not efficiently mitigate system subversion and consequent frauds.

4. CURRENTLY ADOPTED SECURITY MODELS

The models currently adopted in online banking systems are based on several security layers, consisting on diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing identification, authentication and authorization.

- **Digital Certificates:** Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity. In Brazil, banking systems use A1 and A3 certificates issued and signed by ICP-Brasil [12].
- **One-Time Password Tokens:** One-Time Password devices [18] are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.
- **One-Time Password Cards:** One-Time Password Cards constitute a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.
- **Browser Protection:** In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.
- **Virtual Keyboards:** Virtual keyboards were developed to thwart the efficient use of keyloggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between

different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

- **Device Registering:** This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.
- **CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans Apart [28], is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.
- **Short Message Service (SMS):** This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to informed in order to authorize and process the transaction through the online banking system.
- **Device Identification:** Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.
- **Positive Identification:** Positive identification is a model where the user is required to input some secret information only known to him in order to identify himself. It is applied as a second authentication method.
- **Pass-Phrase:** It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involve money movement.
- **Transaction Monitoring:** Even though this method is not thoroughly analyzed in the present work, it is currently applied in all online banking systems, each of them using different techniques. Artificial intelligence [27], transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

5. VULNERABILITIES IN ONLINE BANKING SYSTEMS

Table 1 presents known vulnerabilities which affect each security model discussed in this paper. It does not present all the vulnerabilities which may exist in such models but shows that those models are currently vulnerable to several attacks. The correct identification of the threats faced by current Internet banking systems [1] is essential for designing more efficient models which provide a higher level of security.

Table 1: Vulnerabilities in Internet Banking Systems

Security Models	Vulnerabilities
Digital Certificates	It is possible to export A1 certificates and remotely utilize them; A3 certificates can be used by more than one user at the same time, allowing adversaries to use stolen certificates.
OTP Token	The generated password may be captured and used in real-time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering.
OTP Card	Malware may collect passwords or lure the user into informing them.
Browser Protection	New malware remain active until they are identified by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data (such as passwords) in an unsafe environment.
Virtual Keyboard	Known tools such as Screenloggers or mouseloggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied. [14].
Device Registering	Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device.
CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software.
Short Message Service	The attacker may alter the cellular phone number to which the authorization messages are sent.
Device Identification	Characteristics thought to be unique to the user's device may be reproduced.
Positive Identification	Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information.
Pass-Phrase	Tools such as screenloggers, keyloggers or mouseloggers can be used to capture the secret information; Decryption techniques may be applied.[14].
Transaction Monitoring	Recent malwares are creating behavior profiles which enable them to impersonate the user profile. [17].

6. ATTACK MODELLING AND TYPICAL SCENARIOS

The attack tree model [15] for common attacks against online banking systems is presented in Figure 2. This model represents the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (engineering social and phishing) then to gain control of device (malware) and credential theft legitimate user (fake Web pages and malware).

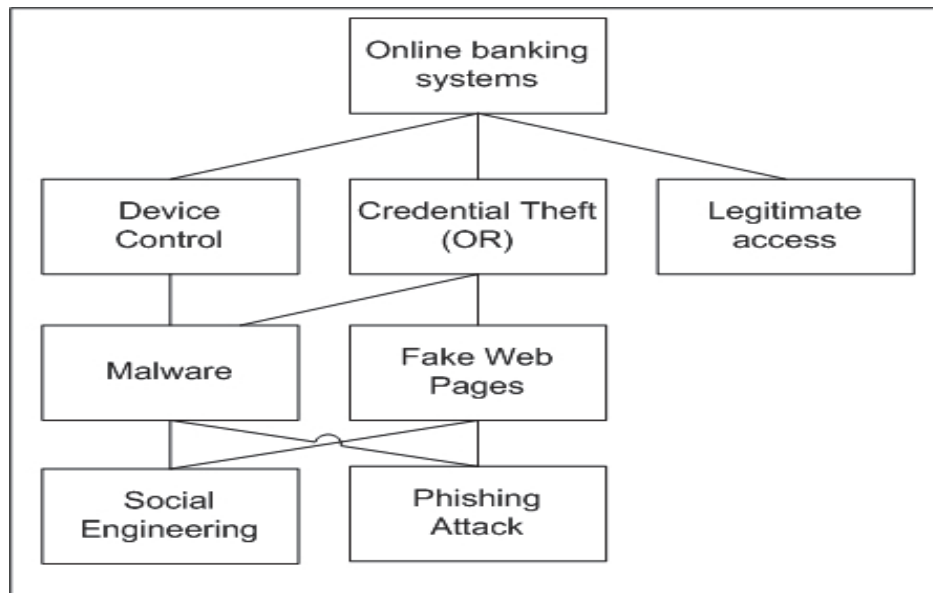


Figure 2: Attack Tree model

The attacks description in this section are based on current trends observed in malware specifically focused on banking. It has been observed that such attacks are efficient against the authorization and authentication schemes currently adopted in online banking systems. Each attack is present along with a description of the security mechanisms they target.

6.1 CREDENTIAL THEFT

This kind of attack is the simplest and most commonly performed against banking systems. It basically consists in obtaining the necessary credentials and user data in order to access the system as a legitimate user, providing information normally known only to legitimate users (Figure 3).

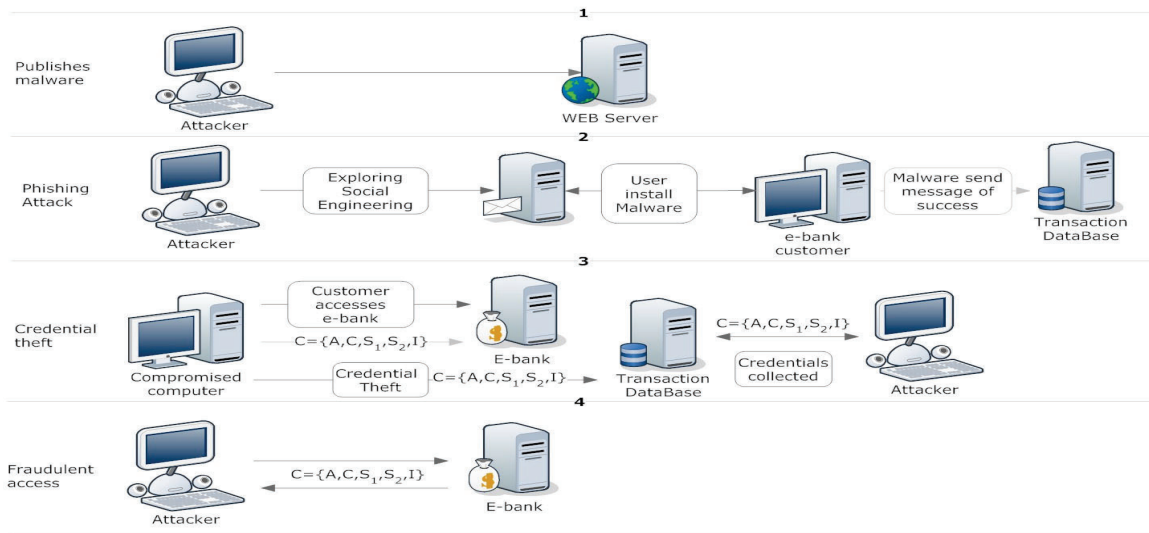


Figure 3: Credential Theft

This attacks is effective against the following security mechanisms: **OTP Token; OTP Card; Browser Protection; Virtual Keyboard; CAPTCHA; SMS; Positive Identification; Pass-Phrase.**

The attacker must capture all information needed to reproduce a legitimate access, therefore you must have the credentials to $C = \{A, C, S_1, S_2, I\}$, to:

- A - Bank Identifier;
- C - Customer unique identifier;
- S_1 - Access password;
- S_2 - Authorization password;
- I - Device Identification information.

Credential theft is summarized in the following steps:

1. The attacker publishes specially crafted malware or counterfeit banking system web pages.
2. Exploiting vulnerabilities in applications such as browsers or applying social engineering the attacker manages to install malware in the device through which the honest user access online banking services.
3. When the legitimate user accesses the service, the authentication data informed by him is captured by the malware or counterfeit web page which the attacker controls.
4. After the malicious artefact obtains the information necessary for accessing the Internet banking system, the user is transparently redirected to the legitimate

service. No error message is issued but generally the user has to re-inform the authentication data.

5. The attacker verifies which information was captured.
6. Having obtained the necessary data, the attacker performs the authentication process, accessing the system as a legitimate user. In order to perform the authentication process the attacker fully impersonates the legitimate user, also providing information about the legitimate user's device physical characteristics, which is commonly used as an authentication factor.

6.2 DEVICE CONTROL

The device control attack is presented in Figure 4 and its objective is to obtain full control of the user's device instead of only stealing data used in the authentication process. The user's device itself is then used by the attacker to access the banking service and perform frauds. This attack is more complex than credential theft (Figure 3) and tracing its origin is much more difficult because the attacker never directly accesses the online banking service.

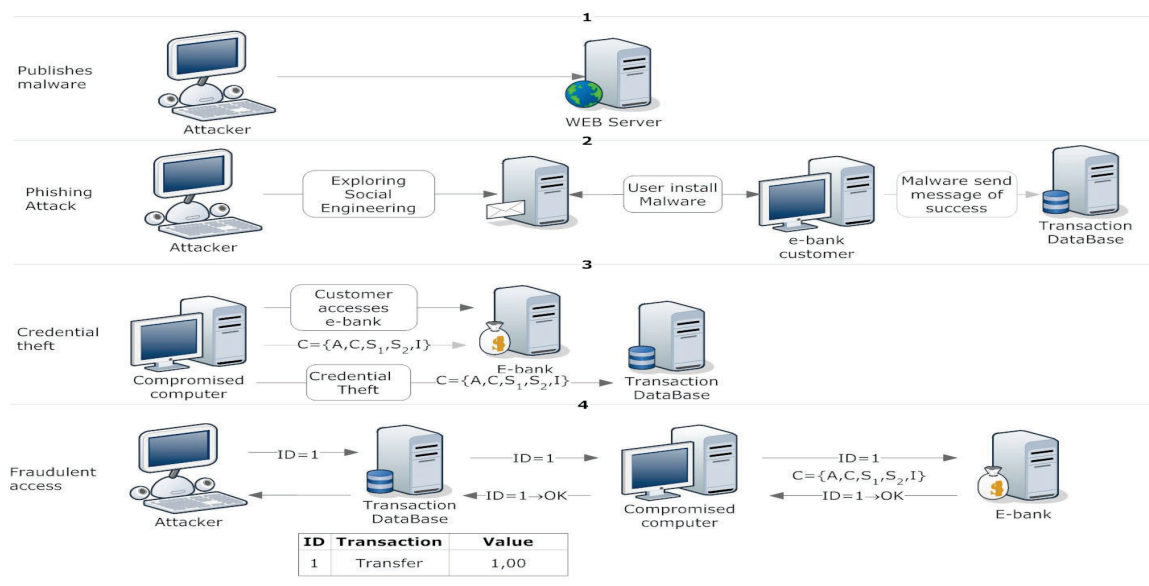


Figure 4: Device Control

This attacks is effective against the following security mechanisms: **Digital Certificates; Device Registering; Device Identification; Transaction Monitoring.**

Device control is summarized in the following steps:

1. The attacker publishes specially crafted malware or counterfeit web pages.

2. Exploiting vulnerabilities in applications such as browsers or applying social engineering the attacker manages to install malware in the device through which the honest user access online banking services.
3. The malware then captures the information necessary for accessing the service.
4. After the malicious artefact obtains the information necessary for accessing the Internet banking system through the legitimate user's device, it downloads a list of transactions to be performed previously stored by the attacker in a remote repository.
5. Having obtained the necessary data, the malware automatically accesses the online banking system as a legitimate user through the user's device and performs the transactions specified by the attacker.
6. While the malware remains active, it suppresses information about the transactions it performed from the banking system's interface, preventing the user from detecting the attacks.
7. The attacker updates the repository containing transactions to be performed by the malware.

7 POTENTIAL COUNTERMEASURES

Due to the inherent complexity and flexibility of the presented attacks it seems unlikely that a single centralized security solution would successfully solve the security issues on which they are based, effectively mitigating those attacks. The main problem relies on the weakest link in the security chain, generally the user (or his access device), and its role in the whole authentication and authorization process. In most cases, the security of the authentication and authorization process in online banking systems is based on secret information supposedly known only by legitimate users and the bank, depending on the user for maintaining the secrecy of such information. However, as it was described in the previous sections, an attacker can easily obtain this secret information through the use of social engineering techniques and malware, compromising the system as a whole. In face of these issues, new authentication and identification models should be as independent from the user or the security of his device as possible, relying on more than one source for authentication and identification data.

A identification and authentication model potentially resilient to the attacks presented in 6.1 and 6.2 should be based on independent secure channels for authentication/authorization data and transaction data. In this model, security is guaranteed even if an attacker compromises one of the channels. The separate authentication/authorization channel is to be chosen in such a way that the user has little or no influence on its security, being based on devices which the user does not control or administer, and not on the user's internet access device (used for transactions) which may be easily compromised by remote attackers.

Taking into consideration that any device associated or dependent on a compromised environment (such as compromised network or host) is also considered compromised, a

potentially secure authentication and identification model for online banking systems should fit the following requisites:

- The authentication data channel is independent from the transaction data channel.
- The identification model is independent from user provided information.
- Perform mutual authentication, where both the user and the service provider must prove their identities.
- Verify and confirm all the information obtained from the user in order to detect patterns and irregularities which may indicate a fraud.
- Maintain a history database for each user containing information which form a user transaction profile associated with reputation and trust models used to detect fraud and malicious tendencies.

A authentication and identification model with these characteristics would be secure against the attacks presented in section 6.

8 CONCLUSION

The security models for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods, which are also the components where most Internet banking systems' vulnerabilities are found. The aforementioned methods depend on the user's knowledge of secret authentication information and the user's ability for maintaining both this information and the device used to access internet banking services secure. If the user's platform (i.e. computing devices, operating systems and applications) is compromised, the banking system is compromised as a whole, allowing the execution of fraudulent transactions. As result of these issues, most of the online banking systems currently in operation may be compromised and subverted. Two attacks which efficiently render current security models ineffective are presented, demonstrating how vulnerable internet banking systems are.

Most of the attacks directed at online banking systems target the user (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authentication data. This fact indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related informations leaks and security issues affecting the system and leading to fraud.

In face of the current security issues and the growing number of attacks and consequent frauds, new internet banking systems should be designed as to provide better authentication and identification methods which are less dependent on the user. The basic characteristics of such methods are introduced based on the analysis the methods currently employed. A internet banking systems with those characteristics will render the presented attacks (and other attacks) ineffective, significantly decreasing the number of observed frauds.

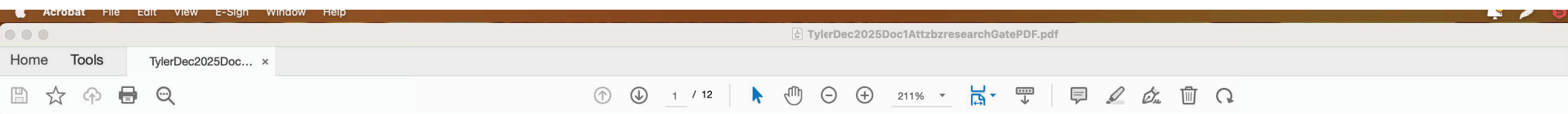
As a future work, a new internet banking system could be developed along with a new security model which provide the security requisites introduced in this paper. Furthermore, efficient techniques for real-time fraud and attacks detections could be proposed based on efficient data mining and pattern recognition methods.

REFERENCES

- [1] ISO/IEC 27002 Code of practice for information security management. 2. ed. Rio de Janeiro: ABNT, 2007.
- [2] ISO/IEC. 27001 Information security management systems Requirement. Rio de Janeiro: ABNT, 2007.
- [3] CAVUSOGLU, Hasan e Cavusoglu, Huseyin. Emerging Issues in Responsible Vulnerability Disclosure. Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain, 2004.
- [4] GOGUEN, Alice; Feringa, Alexis; Stoneburner, Gary. Risk Management Guide for Information Technology Systems [Report]. Computer Security Division Information Technology Laboratory ; National Institute of Standards and Technology Gaithersburg. Nist Special Publication 800, Julho 2002.
- [5] KOSSEW, David. State of the Art Security in Internet Banking [Peridico]. 1997.
- [6] MARSH, Stephen P. Formalising Trus as a Computational Concept. Tese (Doutorado). University of Stirling. - Scotland, UK, 1994. - p. 198.
- [7] MICROSOFT, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008 [Report]. Security Intelligence Report, January through June 2008.
- [8] PEOTTA, Laerte; Amaral, Dino. Estudo de taxonomia de ataques e atacantes em um honeypot de alta interao. Proceedings of the First International Conference on Forensic Computer Science Investigation, Braslia, pp. 38-42, ISSN 1980-1114, 2007.
- [9] WEEKS, Stephen. Understanding Trust Management Systems. IEEE Symposium on Security and Privacy. 2001.
- [10] O. Dandash, P. Dung Le, and B. Srinivasan, Internet banking payment protocol with fraud prevention, 2007 22nd International International Symposium on Computer and Information Sciences, Nov. 2007, pp. 1-6.
- [11] YAHALOM, R.; Klein, B. ; Beth, T. Trust Relationships in Secure Systems-A Distributed Authentication Perspective. IEEE Symposium on Security and Privacy. Washington, DC : IEEE Computer Society, May 24-26, 1993.
- [12] V. Bertol, R.T. Jr, and L.P. Melo, "Um Modelo Para As Normas Sobre Certificacao Digital No Brasil," Proceedings of the Four International Conference on Forensic Computer Science Investigation (ICoFCS'2009), 2009.
- [13] L. Granville, L. Tarouco, and R.R. Barcelos, "Taxonomia de Malwares : Uma Avaliacao dos Malwares Automaticamente Propagados na Rede," Sbseg 2009, Campinas - So Paulo: 2009, pp. 43-56.
- [14] CORREIA, M. A. S. et al. Segurana em Internet Banking. XIII Simposio Brasileiro em Seguranca da Informacao e Sistemas Computacionais (SBseg), Gramado - RS, 2008. 291-299.
- [15] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing Attack Trees using Generalized Stochastic Petri Nets," 2006 IEEE Information Assurance Workshop, 2006, pp. 116-123.
- [16] DANDASH, O.; DUNG, P. ; SRINIVASAN, B. Security Analysis for Internet Banking Models. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. [S.l.]: [s.n.]. 2007. p. 1141 - 1146.
- [17] FINJAN MALICIOUS CODE RESEARCH CENTER. Cybercrime Intelligence: Cybercriminals use Trojans & Money Mules to rob online banking accounts. [S.l.]. 2009.
- [18] HALLER, N. A One-Time Password System (RFC 2289). Internet Engineering Task Force. [S.l.]. 1998.
- [19] MICROSOFT. An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008. [S.l.]. 2008. January through June.

- [20] NAMI, M. R. E-Banking: Issues and Challenges. 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. 263-267.
- [21] NILSSON, M. A. A.; HERD, S. Building Security and Trust in Online Banking. Conference for human-computer interaction. Portland - Oregon - USA: [s.n.]. 2005.
- [22] SYMANTEC. Relatorio Sobre Ameacas de Seguranca na Internet. Symantec - America Latina. [S.l.]. 2010.
- [23] T. T. et al. Modeling Internet Attacks. Workshop on Information Assurance and Security. NY: IEEE. 2001.
- [24] A.S. Martino and X. Perramon, A Model for Securing E-Banking Authentication Process: Antiphishing Approach, 2008 IEEE Congress on Services - Part I, Jul. 2008, pp. 251-254.
- [25] A.S. Martino and X. Perramon, Defending E-Banking Services: Antiphishing Approach, 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Aug. 2008, pp. 93-98.
- [26] WANG, H.; HUANG, X.; DODDA, R. G. Ticket-based mobile commerce system and its implementation. Q2SWinet '06: Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks. Terromolinos, Spain: ACM. 2006. p. 119--122.
- [27] WEIMING, G. et al. Falcon: on-line monitoring and steering of large-scale parallel programs. FRONTIERS '95: Proceedings of the Fifth Symposium on the Frontiers of Massively Parallel Computation (Frontiers'95). Washington, DC, USA: IEEE Computer Society. 1995. p. 422.
- [28] YAN, J.; EL, A.; SALAH., Usability of CAPTCHAs or usability issues in CAPTCHA design. SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security. New York, NY, USA: ACM. 2008. p. 44--52.
- [29] M. JOHNSON, A new approach to Internet banking. University Cambridge. (PhD) 2008, p. 113.
- [30] Carneiro, B. and Sousa, R. T., Identifying Bank Frauds Using Crisp-DM And Decision Trees, International Journal of Computer Science & Information Technology . October, vol. 2, 2010, pp. 162-169

ATTACHMENT C



International Journal of Computer Science

, No 1, Feb 2011

A FORMAL CLASSIFICATION OF ATTACKS AND VULNERABILITIES IN INTERNET BANKING SYSTEMS

NET
TIES

Laerte Peotta, Marcelo D. Holtz

Deus, Rafael

Electrical Engineering
Campus Universitario Darcy Ribeiro

nB)
a, DF -- Brazil
ab.br

{peotta, holtz,

Document Properties

Description Security Fonts Initial View Custom Advanced

Description

File: TylerDec2025Doc1AttzbzresearchGatePDF.pdf

Title: Microsoft Word - 13

Author: Admin

Subject:

Keywords:

Created: 2/22/11, 6:39:10 AM Additional Metadata...

Modified: 2/22/11, 6:39:10 AM

Application: PScript5.dll Version 5.2.2

Advanced

PDF Producer: GPL Ghostscript 8.15

PDF Version: 1.4 (Acrobat 5.x)

Location: /Users/Mary/Downloads/

File Size: 637.70 KB (653,009 Bytes)

Page Size: 8.50 x 11.00 in Number of Pages: 12

Tagged PDF: No Fast Web View: No

Help Cancel OK

Abstract

A formal classification of attacks and vulnerabilities that affect current internet banking systems is presented along with two attacks which demonstrate the insecurity of such systems. Based on a thorough analysis of current security models, we propose a guidelines for designing secure internet banking systems which are not affected by the presented attacks and vulnerabilities.

ATTACHMENT D



Peer-reviewed

A Formal Classification of Internet Banking Attacks and Vulnerabilities

Authors: [Laerte Peotta](#), [Marcelo D. Holtz](#), [Bernardo M. David](#), [Flavio G. Deus](#), [Rafael Timoteo de Sousa](#)

Article, 2011

Edition: [View all formats and editions](#)

Publication:

International Journal of Computer Science and Information Technology, 3, 20110228, 186

ISSN:

0975-4660

DOI:

[10.5121/ijcsit.2011.3113](https://doi.org/10.5121/ijcsit.2011.3113)

OCLC Number / Unique Identifier:

4795335283

More Information:

[dx.doi.org](https://dx.doi.org/10.5121/ijcsit.2011.3113)

University of Chicago Library

[356 miles](#) from your current location.

1100 E. 57th Street, Chicago, IL, 60637, United States

Emporia State University

William Allen White Library

[476 miles](#) from your current location.

William Allen White Library, 1 Kellogg Circle, Emporia, KS, 66801-5092, United States

Anderson University

Robert A Nicholson University Library

[509 miles](#) from your current location.

1030 University Blvd, Anderson, IN, 46012, United States

University of Regina

[649 miles](#) from your current location.

Dr John Archer Libr, 3737 Wascana Pkwy, Regina, SK, S4S 0A2, Canada

Syracuse University

[858 miles](#) from your current location.

222 Waverly Avenue, Suite 219 - Administration, Syracuse, NY, 13244-2010, United States

University of Georgia

University of Georgia, Main Library

[921 miles](#) from your current location.

UGA Main Library, 320 S. Jackson St., Athens, GA, 30602-1641, United States

Florida Atlantic University

Boca Raton Campus, S.E. Wimberly Library

[1,476 miles](#) from your current location.

777 Glades Rd, LY-3 / 214, Boca Raton, FL, 33431-6496, United States

Stanford University

Cecil H. Green Library

[1,582 miles](#) from your current location.

557 Escondido Mall, Arguello Way, Stanford, CA, 94305-6004, United States

Memorial University of Newfoundland- QEII Library

MUN

[1,920 miles](#) from your current location.

Queen Elizabeth II Library, 234 Elizabeth Avenue, St Johns, NL, A1B 3Y1, Canada

Glasgow Caledonian University

[3,711 miles](#) from your current location.

The Saltire Centre, Glasgow Caledonian University, Cowcaddens Road, Glasgow, G4 0BA, United Kingdom

Are you ready to unleash a world of knowledge and discovery?

Sign in to WorldCat and unlock a treasure trove of library holdings, favorite your go-to libraries, and curate lists that fuel your curiosity.

Sign in

ATTACHMENT E

[Home](#)[Editorial](#)[Submission](#)[Indexing](#)[Special Issue](#)[Contacts](#)[AIRCC](#)[2011, Volume 3, Number 6](#)[2011, Volume 3, Number 5](#)[2011, Volume 3, Number 4](#)[2011, Volume 3, Number 3](#)[2011, Volume 3, Number 2](#)[2011, Volume 3, Number 1](#)[Archives](#)

From 3D Model Data to Semantics
 My Abdellah Kassimi and Omar El beqqali, Sidi Mohamed Ben Abdellah University, Morocco

[Full Text](#)

Recycling of Bandwidth in Metropolitan Area Networks(MAN)
 Bhargava Devana¹, Sudharshana Kristipati¹, Raghava Nirati², ¹JNTU - India and ²JITS, India

[Full Text](#)

Adaptation AC to Improve Wireless Access Network Dependability
 Olfa Ben Ahmed and Zied Choukair, University of Carthage, Tunisia

[Full Text](#)

A Comparative Study To Find A Suitable Method For Text Document Clustering
 S.C.Punitha¹ and M.Punithavalli², ¹P.S.G.R. Krishnammal College for women, India and ²Sri Ramakrishna College of engineering, India

[Full Text](#)

Recognizing Bangla Grammar Using Predictive Parser
 K.M. Azharul Hasan, Al-Mahmud, Amit Mondal and Amit Saha, Khulna University of Engineering and Technology, Bangladesh

[Full Text](#)

Hybrid GPS-GSM Localization of Automobile Tracking System
 Mohammad A. Al-Khedher, Balqa Applied University, Jordan

[Full Text](#)

Network Intrusion Detection Using Data Mining and Network Behaviour Analysis
 Ahmed Youssef and Ahmed Emam, King Saud University, KSA

[Full Text](#)

Technical Analysis of Remote 3D Visualization on Mobile Devices
 U.S. Junghare¹, V.M. Thakare², R.V.Dharaskar³ and S.S. Sherekar², ¹Brijlal Biyani Science College, India, ²SGB Amravati University, India ³M.P.G.I. Nanded, India

[Full Text](#)

Integrated Environment for Developing E-Learning Lectures
 Vladimir Bondarev¹, Alexander Ossyka² and Afif Mghawish¹, ¹Kharkov National University of Radio Electronics, Ukraine and ²Al-Zaytoonah Private University, Jordan

[Full Text](#)

Analysis of Different Privacy Preserving Cloud Storage Frameworks
 Rajeev Bedi¹, Mohit Marwaha¹, Tajinder Singh², Harwinder Singh³ and Amritpal Singh¹, ¹Beant College of Engineering and Technology, India, ²Global Institute of Engineering and Technology, India and ³SSCET, India

[Full Text](#)

Investigating the Awareness of Applying the Important Web Application Development and Measurement Practices in Small Software Firms
 Faudziah Ahmad, Fauziah Baharom and Moath Husni, Universiti Utara Malaysia, Malaysia

[Full Text](#)

Flooding Attacks to Internet Threat Monitors(ITM): Modeling and Counter Measures Using Botnet and Honeypots
 K.Munivara Prasad¹, A.Rama Mohan Reddy² and M.Ganesh Karthik³, ¹Rayalaseema University, India ²SV University, India and ³Sree vidyanikethan Engg.College, India

[Full Text](#)

Mobile Geographic Information Systems: A Case Study on Mansoura University, Egypt
 Asmaa Ahmed Hussein¹, Elkhedr Hassan Eibrahim² and Aziza Asem¹, ¹Mansoura University, Egypt and ²King Saud University, KSA

[Full Text](#)

An Improved Neural Image Compression Approach With Cluster Based Pre-Processing
 Ashanta Ranjan Routray and Munesh Chandra Adhikary, Fakir Mohan University, India

[Full Text](#)

From Learning Style of Webpage Content to Learner's Learning Style Mohamed.G. Darwesh¹, Magdy. Z. Rashad² and Abdelaziz. K. Hamada², ¹Cairo University, Egypt and ²Mansoura University, Egypt	Full Text
Image Labeling and Segmentation using Hierarchical Conditional Random Field Model Manoj K.Vairalkar and Sonali.Nimbhorkar, RTMN University - Nagpur, India	Full Text
Multi-Resolution Analysis For Medical Image Compression Mohammed Alhanjouri, Islamic University of Gaza, Palestine	Full Text
Introduction Of Knowledge Management Architecture Using Multi Agent Sheikh Amanur Rahman¹, Anamika Bhardwaj¹, Mukul Pathak¹ and Shobhit Singh Rathore², ¹Galgotias College of Engineering & Technology, India and ²SDG Software India Pvt. Ltd, India	Full Text
Optimal Fuzzy Model Construction With Statistical Information Using Genetic Algorithm Md. Amjad Hossain¹, Pintu Chandra Shill², Bishnu Sarker¹ and Kazuyuki Murase², ¹KUET, Bangladesh and ²University of Fukui, Japan	Full Text
Edge Detection Techniques For Image Segmentation Muthukrishnan.R and M.Radha, Bharathiar University, India	Full Text

--	--

It Security Issues Within the Video Game Industry Stephen Mohr¹ and Syed (Shawon) Rahman^{1,2}, ¹Capella University, USA and ²University of Hawaii-Hilo, USA	Full Text
Adaptive Beamforming Algorithm for Interference Suppression in GNSS Receivers Zhao hongwei¹, Lian Baowang¹ and Feng Juan^{1,2}, ¹Northwestern Polytechnical University, China, ²KIT- Karlsruhe Institute of Technology, Germany	Full Text
Minimize the False Positive Rate in a Database Intrusion Detection System A. Rezk, H. Ali, M. El-Mikkawy and S. Barakat, Mansoura University, Egypt	Full Text
Design Pattern Management System: A Support Tool Based on Design Patterns Applicability Zakaria Moudam, Radouan Belhissi and Nouredine Chenfour, University Sidi Mohammed Ben Abdellah Fez, Morocco	Full Text
Genetic Algorithm (GA) In Feature Selection For CRF Based Manipuri Multiword Expression (MWE) Identification Kishorjit Nongmeikapam¹ and Sivaji Bandyopadhyay², ¹Manipur University, India and ²Jadavpur University, India	Full Text
IRIS Recognition Based On LBP and Combined LVQ Classifier M. Z. Rashad, M. Y. Shams, O. Nomir and R. M. El-Awady, Mansoura University, Egypt	Full Text
An IR-based Pedestrian Detection System Implemented with Matlab-Equipped Laptop and Low-Cost Microcontroller Erwin Thomas Gilmore, Chukwunweike Ugboeme and Charles Kim, Howard University, USA	Full Text
New Method for 3D Shape Retrieval Abdelghni Lakehal and Omar El Beqqali, Sidi Mohamed Ben AbdEllah University, Morocco	Full Text
Research Review for Digital Image Segmentation Techniques Ashraf A. Aly¹, Safaai Bin Deris¹ and Nazar Zaki², ¹Universiti Teknologi Malaysia and ²UAE University, UAE	Full Text
Stable Filtering for Artificial Pheromone Potential Field Constructed By Mobile Robots and Passive RFID Tags Piljae Kim and Daisuke Kurabayashi, Tokyo Institute of Technology, Japan	Full Text
Evaluate the Performance of Optical Cross Connect Based on Fiber Bragg Grating Under Different Bit Rate Bobby Barua, Ahsanullah University of Science and Technology, Bangladesh	Full Text
Optimized Fuzzy Logic Application for MRI Brain Images Segmentation Indah Soesanti¹, Adhi Susanto¹, Thomas Sri Widodo¹, Maesadji Tjokronagoro², ¹Gadjah Mada University, Indonesia and ¹Gadjah Mada University, Indonesia	Full Text

Robust seed selection algorithm for k-means type algorithms K. Karteeka Pavan ¹ , Allam Appa Rao ² , A. V. Dattatreya Rao ³ and G. R. Sridhar ⁴ , ¹ Jagarlamudi Chadramouli College of Engineering, India, ² Jawaharlal Nehru Technological University, India, ³ Acharya Nagarjuna University, India and ⁴ Endocrine and Diabetes Centre, India	Full Text
Knowledge Based Methods for Video Data Retrieval S.Thanga Ramya and P.Rangarajan, RMD Engineering College, India	Full Text
Analysis and Design Complex and Large Data Base using MySQL Workbench Dedi Iskandar Inan and Ratna Juita, Papua State University, Indonesia	Full Text
Direct Manipulation of Web Browsing History Gholam H. Khaksari, Pennsylvania State University, USA	Full Text
A Semantically Enriched Web Usage Based Recommendation Model C.Ramesh ¹ , K. V. Chalapati Rao ¹ and A.Goverdhan ² , ¹ CVR College of Engineering, India and ² JNTUH College of Engineering, India	Full Text
Enhancing Confidentiality of Private Communication through Dual Compression Kristipati Sudharshana Reddy, Munwar Sk and Rajesh Bhakthavatsalam, SVEC - JNTU, India	Full Text
Optimum Partition Parameter of Divide-And-Conquer Algorithm for Solving Closest-Pair Problem Mohammad Zaidul Karim and Nargis Akter, Daffodil International University, Bangladesh	Full Text
Monitoring Software Reliability using Statistical Process Control: An MMLE Approach R Satya Prasad ¹ , Bandla Sreenivasa Rao ² and R.R. L. Kantham ¹ , ¹ Acharya Nagarjuna University, India and ² VRS & YRN College, India	Full Text

--	--

Automatic Application Level Set Approach In Detection Calcifications In Mammographic Image Atef Boujelben ¹ , Hedi Tmar ² , Jameleddine Mnif ¹ and Mohamed Abid ² , ¹ National School of Medicine of Sfax, Tunisia and ¹ National School of Engineers of Sfax, Tunisia	Full Text
A Robust Steganography Model Using Wavelet-Based Block-Partition Modification Sherin Youssef, Ahmed Abu Elfarag and Reta Raouf, Arab Academy for Science & Tech - Alx., Egypt	Full Text
Cultural Influences on Explicit and Implicit Knowledge Sharing Behaviour in Virtual Teams Xi Zhang, Chinese Academy of Sciences, P. R. China	Full Text
A Fuzzy Framework For Segmentation, Feature Matching And Retrieval Of Brain MR Images Archana.S and Sridhar.S, College of Engineering - Guindy, India	Full Text
MDA-Based ATL Transformation To Generate MVC 2 Web Models Mhamed Rahmouni and Samir Mbarki, Ibn Tofail University, Morocco	Full Text
Comprehensive Measurement Framework for Enterprise Architectures Mahesh R. Dube ¹ and Shantanu K. Dixit ² , ¹ VIT - Pune, India and ² WIT - Solapur, India	Full Text
Plants Images Classification Based on Textural Features using Combined Classifier M.Z. Rashad, B.S.el-Desouky and Manal S .Khawasik, Mansoura University, Egypt	Full Text
Design and FPGA Implementation of DDR3 SDRAM Controller for High Performance Shabana Aqueel and Kavita Khare, M.A.N.I.T - Bhopal, India	Full Text
Self-Adaptation Mechanism to Control the Diversity of the Population in Genetic Algorithm Chaiwat Jassadapakorn and Prabhas Chongstitvatana, Chulalongkorn University - Bangkok, Thailand	Full Text
Packet Scheduling Of Two Classes Flow Rabie Barhoun and Abdelwahed Namir, University Hassan II, Morocco	Full Text

Reduction Of Blocking Probability In Shared Protected Optical Network Nirmala L Devi ¹ and V M Pandharipande ² , ¹ Osmania University, India and ² Dr. Babasaheb Ambedkar Marathwada University, India	Full Text
DNA Lossless Differential Compression Alogorithm Based on Similarity of Genomic Sequence Database Heba Afify, Muhammad Islam and Manal Abdel Wahed, Cairo University, Egypt	Full Text
Performance Analysis Of Various Data Mining Classification Techniques On Healthcare Data Shelly Gupta ¹ , Dharminder Kumar ² and Anand Sharma ² , ¹ Banasthali University, India and ² GJUS&T - Hisar, India	Full Text
Towards A Model Of Maturity For Is Risk Management Mina Elmaallam and Abdelaziz Kriouile, ENSIAS - Rabat, MOROCCO	Full Text
A Fuzzy Approach For Clustering Gene Expression Time Series Data Sadiq Hussain and G.C. Hazarika, Dibrugarh University - Assam, India	Full Text
Novel Apporach for Speech Recognition by Using Self - Organized Maps R.L.K.Venkateswarlu ¹ , R. Vasantha Kumari ² and A.K.V.Nagayya ¹ , ¹ Sasi Institute of Technology and Engineering, India and ² Perunthalaivar Kamarajar Arts College, India	Full Text
Special Issue on "ICCSEA - 2011"	
A New Trusted Third-Party Billing For Mobile Networks Supriya Chakraborty ¹ and Nabendu Chaki ² , ¹ JIS College of engineering - West Bengal, India and ² University of Calcutta, India	Full Text
Performance Evaluation And Impact Of Weighting Factors On An Energy And Delay Aware Dynamic Source Routing Protocol Jihen Drira Rekik, Leila Baccouche and Henda Ben Ghezala, Manouba University, Manouba, Tunisia	Full Text
Indian Languages IR using Latent Semantic Indexing A.P.SivaKumar ¹ , P.Premchand ² and A.Govardhan ¹ , ¹ JNTUACE, India and ² Osmania University - Hyderabad, India	Full Text
Active Controller Design For Global Choas Anti-Synchronization Of Li and Tigan Chaotic Systems Sundarapandian Vaidyanathan ¹ and Karthikeyan Rajagopal ² , ¹ Vel Tech Dr. RR & Dr. SR Technical University, India and ² Singhania University Rajasthan, India	Full Text

--	--

Information Security Plan for Flight Simulator Applications Jason Slaughter ¹ and Syed (Shawon) M. Rahman ^{1,2} , ¹ Capella University, USA and ² University of Hawaii-Hilo, USA	Full Text
Common Phases of Computer Forensics Investigation Models Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, Universiti Tenaga Nasional, Malaysia	Full Text
Comparison and Analysis of Watermarking Algorithms in Color Images - Image Security Paradigm D. Biswas ¹ , S. Biswas ² , P.P. Sarkar ² , D. Sarkar ² , S. Banerjee ¹ and A. Pal ¹ , ¹ Academy of Technology - Hoogly, India and ² University of Kalyani, India	Full Text
Evolutionary Neural Networks algorithm for the Dynamic Frequency Assignment Problem Jamal Elhachmi and Zouhair Guennoun, Mohammadia School of Engineers (EMI), Morocco	Full Text
Optimal Self Correcting Fault Free Error Coding Technique in Memory Operation Harikishore .Kakarla ¹ , Madhavi Latha .M ² and Habibulla Khan ¹ , ¹ KL University, India and ² JNTUH - Hyderabad, India	Full Text
Ubiquitous Mobile Health Monitoring System for Elderly (UMHMSE) Abderrahim BOURUIS ¹ , Mohamed FEHAM ¹ and Abdelhamid BOUCHACHIA ² , ¹ Abou-bekr BELKAID University, Algeria and ² University of Klagenfurt, Austria	Full Text
A Review on Elliptic Curve Cryptography for Embedded Systems Rahat Afreen ¹ and S.C. Mehrotra ² , ¹ Tom Patrick Institute of Computer & I.T - Rauza Bagh, India and ² Dr. B.A.M. University,	Full Text

India	
Statistical Analysis on Software Metrics Affecting Modularity in Open Source Software Andi Wahyu Rahardjo Emanuel¹, Retantyo Wardoyo², Jazi Eko Istiyanto² and Khabib Mustofa², ¹Maranatha Christian University, Indonesia and ²Gadjah Mada University, Indonesia	Full Text
Proposed Information Sharing Security Approach for Security Personnels, Vertical Integration, Semantic Interoperability Architecture and Framework for Digital Government Md.Headayetullah, G.K. Pradhan, Sanjay Biswas and B. Puthal, SOAU - Bhubaneswar, India	Full Text
Hybrid of Particle Swarm Optimization with Evolutionary Operators to Fragile Image Watermarking Based DCT Sawsan Morkos Gharghory, Electronics Research Institute - Cairo, Egypt	Full Text
Image Retrieval using Bit-plane Pixel Distribution N S T Sai¹ and R C Patil², ¹Tech Mahindra Limited - Mumbai, India and ²NMIMS University, India	Full Text
Detection of Masses in Digital Mammogram Using Second Order Statistics and Artificial Neural Network Al Mutaz M. Abdalla¹, Safaai Dress¹ and Nazar Zaki², ¹Universiti Teknologi - Malaysia, India and ²UAE University, UAE	Full Text
Effective Independent Quality Assessment using IV&V Pathanjali Sastri Akella¹ and K. Nageswara Rao², ¹V. R. Siddhartha Engineering College, India and ²P. V. P. Siddhartha Institute of Technology, India	Full Text
E-Learning personalization based on Dynamic learners' preference Essaid El Bachari, El Hassan Abelwahed and Mohammed El Adnani, University Cadi Ayyad, Morocco	Full Text
An LMS Based Blind Source Separation Algorithm Using A Fast Nonlinear Autocorrelation Method Behzad Mozaffari Tazehkand, University of Tabriz, Iran	Full Text
A Novel Technique for Back-Link Extraction and Relevance Evaluation Pooja Gupta¹, A.K. Sharma² and Divakar Yadav³, ¹MAIT - New Delhi, India, ²YMCA University of Science and Technology, India and ³JUITU - Noida, India	Full Text
Electronic Commerce in Web 3.0: The Evidence from Emerging Economics Xi Zhang¹ and Doug Vogel², ¹Chinese Academy of Sciences, China and ²City University of Hong Kong, China	Full Text
A Comparative Experiment of Several Shape Methods in Recognizing Plants A. Kadir, L.E. Nugroho, A. Susanto and P.I. Santosa, Gadjah Mada University, Indonesia	Full Text
RCause - A Root Cause Analysis Model to Identify the Root Causes of Software Reengineering Problems Er. Anand Rajavat¹ and Vrinda Tokekar², ¹Shri Vaishnav Institute of Technology and Science Indore, India and ²Institute of Engineering and Technology (DAVV) Indore, India	Full Text
Unsupervised horizontal collaboration based in SOM Nadia Mesghouni Khaled Ghedira and Moncef Temani, University of Tunis Laboratory LI3 ISG Tunis, Tunisie	Full Text

--	--

Clustering Posts in Online Discussion Forum Threads Dina Said¹ and Nayer Wanas², ¹University of Calgary, Canada and ²Electronics Research Institute - Giza, Egypt	Full Text
The Development of Electronic Payment System for Universities in Indonesia: On Resolving Key Success Factors Veronica S. Moertini, Asdi A. Athuri, Hery M. Kemit and Nico Saputro, Parahyangan Catholic University, Indonesia	Full Text
Brightness Factor Matching for Gesture Recognition System Using Scaled Normalization Mokhtar M. Hasan and Pramoud K. Misra, Banaras Hindu University, India	Full Text
Behavior Analysis in a learning Environment to Identify the Suitable Learning Style Abdelaziz. K. Hamada¹, Magdy. Z. Rashad¹ and Mohamed.G. Darwesh², ¹Mansoura University, Egypt and ²Ahram Canadian University, Egypt	Full Text

An Object-Oriented Modeling and Implementation of Spatio-Temporal Knowledge Discovery System K.Venkateswara Rao¹, A.Govardhan² and K.V.Chalapathi Rao¹, ¹CVR College of Engineering, India and ²JNTUH College of Engineering, India	Full Text
An Effective CBVR System Based on Motion, Quantized Color and Edge Density Features Kalpna Thakre¹, Archana Rajurkar² and Ramchandra Manthalkar³, ¹Sinhgad College of Engineering, India, ²MGM College of Engineering, India and ³SGGSIE&T - Nanded, India	Full Text
Model Based System Engineering Approach of a Lightweight Embedded TCP/IP M. Z. Rashed, Ahmed E. Hassan and Ahmed I. Sharaf, Mansoura University, Egypt	Full Text
Model-Based Factors to Extract Quality Indications in Software Lines of Code Mohammed Abdullah H. Al-Hagery, Qassim University, KSA	Full Text
Wavelet Based Spectrum Sensing Techniques for Cognitive Radio - A Survey Karthik Divakaran, Naveen Manikandan P and Shri Hari R R, Amrita Vishwa Vidyapeetham, India	Full Text
Ontology Alignment Using Machine Learning Techniques Azadeh Haratian Nejhad, Bitā Shadgar and Alireza Osareh, Shahid Chamran University, Iran	Full Text
A Novel Parallel Algorithm for Clustering Documents Based on the Hierarchical Agglomerative Approach Amal Elsayed Aboutabl¹ and Mohamed Nour Elsayed², ¹Helwan University, Cairo, Egypt and ²Princess Noura University, Kingdom of Saudi Arabia	Full Text
Adaptive Team-Based Multi-Agent Organizational Model: A Case in Rescue Systems Afsaneh Fatemi, Kamran Zamanifar and Naser Nematbakhsh, University of Isfahan, Iran	Full Text
A Descriptive Model for Developing a Hydraulic Geodatabase by Using the GIS Softwares El khamlichi Ahmed Mortada¹, Kadiri Mohamed¹, El mahboul Abdellah² and Merzouki Abderrahmane³, ¹University Abdelmalek Essaadi, Morocco, ²Hydraulic basin Agency of Oum Er Rabii, Morocco and ³University of Granada, Spain	Full Text
Application of PUF-Enabled RFID Tags in Electronic Banking Saeed Mehmandoust and Reza Ebrahimi Atani, The University of Guilan, Iran	Full Text
Energy Efficient Task Scheduling of Send-Receive Task Graphs on Distributed Multi-Core Processors with Software Controlled Dynamic Voltage Scaling Abhishek Mishra and Anil Kumar Tripathi, Banaras Hindu University, India	Full Text
Special Issue on "CCSIT - 2011"	
A Design of a Computer-Aided Diagnostic Tool For Chest X-Ray Analysis Kim Le, University of Canberra, Australia	Full Text
Characterization and Validation of Requirements Management Measures Using Correlation and Regression Model S. Arun Kumar and T.Arun Kumar, VIT University, India	Full Text
An Automated Size Recognition Technique for Acetabular Implant in Total Hip Replacement A. Shapi'i, R. Sulaiman, M.K. Hasan and A.Y.M. Kassim, Universiti Kebangsaan Malaysia, Malaysia	Full Text
PHP Framework for Database Management Based on MVC Pattern Chanchai Supaartagorn, Ubon Ratchathani University, Thailand	Full Text
Importance of Data Collection and Validation for Systematic Software Development Process Mala.V.Patil¹ and A.M.Nageswara Yogi², ¹Anna University - Coimbatore, India and ²Defence Research and Development Organization - Bangalore, India	Full Text
Affine Invariant Descriptors of 3D Object Using Multiple Regression Model M. Elhachloufi¹, A. El Oirrak¹, D. Aboutajdine² and M.N. Kaddioui¹, ¹Caddy Ayyad University, Morocco and ²LEESA-GSCM, Morocco	Full Text

Use-Case, Runtime and Deployment Views for Developing Subsidies Mobile Wallet Dina Darwish, International Academy for Engineering and Media Science, Egypt	Full Text
Diagonal Based Feature Extraction for Handwritten Alphabets Recognition System Using Neural Network J.Pradeep, E.Srinivasan and S.Himavathi, Pondicherry College Engineering, India	Full Text
Electre Methods in Solving Group Decision Support System Bioinformatics on Gene Mutation Detection Simulation Ermatita ¹ , Sri Hartati ² , Retantyo Wardoyo ² and Agus Harjoko ² , ¹ Sriwijaya University, Indonesia and ² Gadjah Mada University, Indonesia	Full Text
A Novel Super Resolution Reconstruction of Low Resolution Images Progressively Using DCT and Zonal Filter Based Denoising Liyakathunisa and C.N .Ravi Kumar, Sri Jayachamrajendra College of Engineering, India	Full Text
Mining Target-Oriented Fuzzy Correlation Rules to Optimize Telecom Service Management Hao-En Chueh, Yuanpei University, Taiwan	Full Text
Improving the Character Recognition Efficiency of Feed Forward BP Neural Network Amit Choudhary ¹ and Rahul Rishi ² , ¹ Maharaja Surajmal Institute, India and ² TITS - Bhiwani, India	Full Text
Initial Classification Through Back Propagation In a Neural Network Following Optimization Through GA to Evaluate the Fitness of an Algorithm Amit Ganatra, Y P Kosta, Gaurang Panchal and Chintan Gajjar, Charotar University of Science and Technology, India	Full Text
Adaptive Fuzzy Filtering for Artifact Reduction in Compressed images and videos P.Ramakrishna Rao ¹ , B.Addai ¹ , G.Ramakrishna ¹ and T.PanduRanga Vital ² , ¹ Dr.B.R.Ambedkar University, India and ² Gayathri College of Science and Management, India	Full Text
Channel Allocation for Direct Sequence Spread Spectrum Using Vertex Merge Algorithm Handrizal, A.Noraziah and Ahmed N Abd.Alla, University Malaysia Pahang, Malaysia	Full Text
Combining Speedup Techniques based on Landmarks and Containers with parallelised preprocessing in Random and Planar Graphs R. Kalpana ¹ and P. Thambidurai ² , ¹ Pondicherry Engineering College, India and ² Perunthalaivar Kamarajar Institute of Engineering & Technology, India	Full Text
Machine Learning Methods for Spam E-Mail Classification W.A. Awad ¹ and S.M. ELseuofi ² , ¹ Port Said University, Egypt and ² Ras El Bar High inst., Egypt	Full Text
A Formal Classification of Internet Banking Attacks and Vulnerabilities Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus and Rafael Timoteo de Sousa Jr., University of Brasilia (UnB), Brazil	Full Text
Characterization of Tumor Region Using SOM and Neuro Fuzzy Techniques in Digital Mammography Anamika Ahirwar and R.S. Jadon, Madhav Institute of Technology & Science, India	Full Text
Search-Based Software Test Data Generation Using Evolutionary Computation P. Maragathavalli, Pondicherry Engineering College, India	Full Text

ATTACHMENT F

A FORMAL CLASSIFICATION OF INTERNET BANKING ATTACKS AND VULNERABILITIES

Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo de Sousa Jr.

Electrical Engineering Department, University of Brasilia (UnB)
Campus Universitario Darcy Ribeiro -- Asa Norte -- 70910-900 -- Brasília, DF -- Brazil
{peotta,holtz,bernardo.david,desousa}@redes.unb.br

Abstract

A formal classification of attacks and vulnerabilities that affect current internet banking systems is presented along with two attacks which demonstrate the insecurity of such systems. Based on a thorough analysis of current security models, we propose a guidelines for designing secure internet banking systems which are not affected by the presented attacks and vulnerabilities.

KEYWORDS

Internet banking, e-bank, online bank, identification, authentication, authorization.

1. INTRODUCTION

Currently there is a clear need for efficient security models by banks which offer online access to their banking systems [20]. In face of the growing number of transactions processed through online banking systems, several new security technologies and models which aim at providing authenticated secure communications through known insecure channels have been introduced in current literature [16].

The number of malware and exploits focused on online banking systems vulnerabilities has been steadily growing during past years [19]. Recent reports [22] indicate that banking trojans were among the 50 main security threats in 2009, while Brazil figures as the source and destination of most of those attacks performed in Latin America[30].

In order to propose security models and solutions in general it is first necessary to understand and properly classify the existing attack techniques and the vulnerabilities on which they are based. Such characterization must be conducted taking into consideration the external factors that affect security and the intrinsic trust relation between users and providers of online banking services. Furthermore, it must be considered the responsibility for maintaining security is always transferred to the weakest link in the security chain, which means, in most cases, the final user. In this paper we present a formal analysis and classification of the several vulnerabilities and attacks that affect online banking systems.

The rest of this paper is organized as follows: the current security models for online banking are discussed in sections 2 and 3. In section 4, we present a comparative analysis of the solutions currently adopted by banking institutions and their inherent vulnerabilities. In section 5, attack modelling is introduced and we describe efficient attacks against currently adopted solutions. In section 6, the countermeasures necessary to thwart the presented attacks are introduced. Finally, in section 7, we conclude with suggestions for future works.

2. RELATED WORKS

Current research is directed towards attacks and malicious activities identification in online banking systems. In [14] the authors introduce attack techniques focused on vulnerabilities which are present in a specific internet banking system, presenting attack implementation results. In [16] the authors propose a protocol for legitimate user identification based on transaction profile pattern matching and dynamic keys and groups. However, a model solely based on legitimate user identification is not computationally efficient due to the constantly growing number of online banking systems users. The same authors propose a smartcard based identification protocol in [10].

Several security models aiming at phishing mitigation have been proposed [24] [25]. Basically, both solutions are limited to identifying users through the analysis of currently adopted processes and security models, being inefficient when applied to new internet banking systems. The results in [29] show that any device operating in a compromised environment becomes equally compromised as the environment could alter and tamper communication messages sent and received by the device. The authors suggest that a device authentication model would effectively secure the banking system against such compromised situations.

Most of the proposed solutions are limited to identifying adversaries through pattern matching algorithms which detect suspect behavior patterns among transaction history data. Due to the sheer number of internet banking transactions such methods do not efficiently identify attackers before they perform a significant amount of illegitimate transactions and fraud.

3. INTERNET BANKING SECURITY MODELS

Online banking systems require efficient security models capable of identifying users and authorizing transactions, thus mitigating fraud. However, current models are focused on fraud identification instead of fraud prevention, which means that actions are taken only after a fraud occurs instead of performing a series of preventive procedures.

Analysing the security devices implemented by the ten largest banks in Brazil it is observed that several security layers and methods are concurrently adopted (Figure 1). Virtual keyboards are clearly one of the most used models, being adopted in 8 different banks. However, banking trojans continue to successfully operate, directing security to reactive fraud identification rather than prevention.

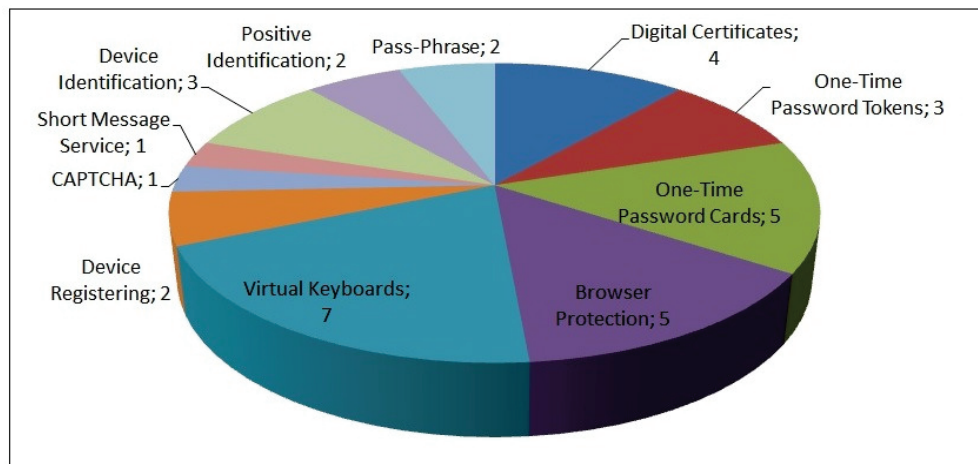


Figure 1: Internet Banking Security Models

In this analysis, SSL (Secure Sockets Layer) was not considered because it is adopted in all online banking systems. Moreover, SSL only provides security from the network layer downwards but is not capable of guaranteeing protection against attacks based on the application layer, where data is captured or modified before encryption.

Basically, banking systems need to accurately identify the user and authorize his access to banking transactions. The identification schemes are based on two main factors: unique secret information previously shared by the user and the bank (such as passwords) and unique characteristics of the device which is being used to access the service (device fingerprinting). However, if any of the media through which these informations are collected (including the user's device) is compromised, the security system is compromised as a whole because it would allow an adversary to insert and capture information at a point of the system. It is important to understand how banking systems employ security mechanisms and why they do not efficiently mitigate system subversion and consequent frauds.

4. CURRENTLY ADOPTED SECURITY MODELS

The models currently adopted in online banking systems are based on several security layers, consisting on diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing identification, authentication and authorization.

- **Digital Certificates:** Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity. In Brazil, banking systems use A1 and A3 certificates issued and signed by ICP-Brasil [12].
- **One-Time Password Tokens:** One-Time Password devices [18] are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.
- **One-Time Password Cards:** One-Time Password Cards constitute a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.
- **Browser Protection:** In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.
- **Virtual Keyboards:** Virtual keyboards were developed to thwart the efficient use of keyloggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between

different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

- **Device Registering:** This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.
- **CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans Apart [28], is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.
- **Short Message Service (SMS):** This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to be informed in order to authorize and process the transaction through the online banking system.
- **Device Identification:** Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.
- **Positive Identification:** Positive identification is a model where the user is required to input some secret information only known to him in order to identify himself. It is applied as a second authentication method.
- **Pass-Phrase:** It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involve money movement.
- **Transaction Monitoring:** Even though this method is not thoroughly analyzed in the present work, it is currently applied in all online banking systems, each of them using different techniques. Artificial intelligence [27], transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

5. VULNERABILITIES IN ONLINE BANKING SYSTEMS

Table 1 presents known vulnerabilities which affect each security model discussed in this paper. It does not present all the vulnerabilities which may exist in such models but shows that those models are currently vulnerable to several attacks. The correct identification of the threats faced by current Internet banking systems [1] is essential for designing more efficient models which provide a higher level of security.

Table 1: Vulnerabilities in Internet Banking Systems

Security Models	Vulnerabilities
Digital Certificates	It is possible to export A1 certificates and remotely utilize them; A3 certificates can be used by more than one user at the same time, allowing adversaries to use stolen certificates.
OTP Token	The generated password may be captured and used in real-time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering.
OTP Card	Malware may collect passwords or lure the user into informing them.
Browser Protection	New malware remain active until they are identified by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data (such as passwords) in an unsafe environment.
Virtual Keyboard	Known tools such as Screenloggers or mouseloggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied. [14].
Device Registering	Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device.
CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software.
Short Message Service	The attacker may alter the cellular phone number to which the authorization messages are sent.
Device Identification	Characteristics thought to be unique to the user's device may be reproduced.
Positive Identification	Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information.
Pass-Phrase	Tools such as screenloggers, keyloggers or mouseloggers can be used to capture the secret information; Decryption techniques may be applied.[14].
Transaction Monitoring	Recent malwares are creating behavior profiles which enable them to impersonate the user profile. [17].

6. ATTACK MODELLING AND TYPICAL SCENARIOS

The attack tree model [15] for common attacks against online banking systems is presented in Figure 2. This model represents the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (engineering social and phishing) then to gain control of device (malware) and credential theft legitimate user (fake Web pages and malware).

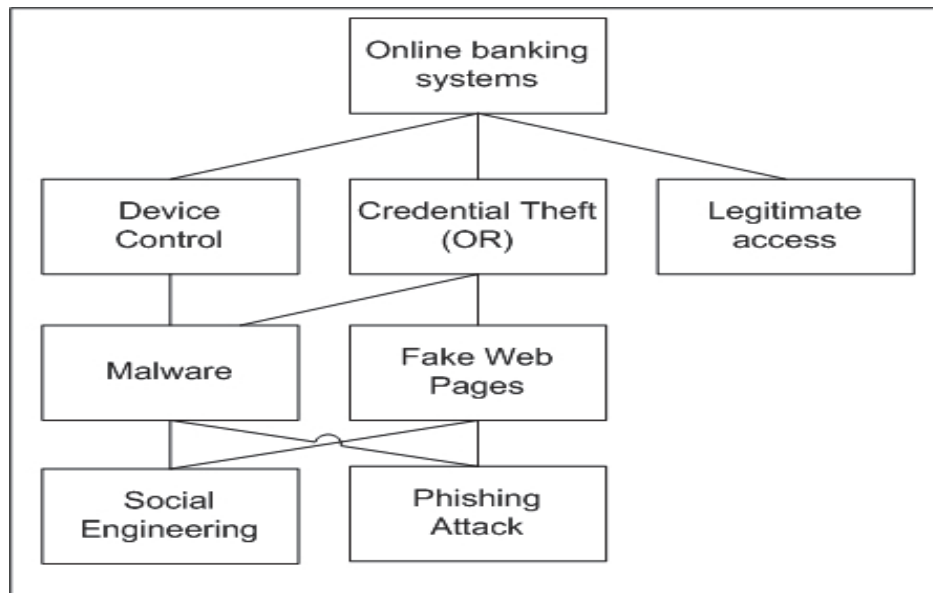


Figure 2: Attack Tree model

The attacks description in this section are based on current trends observed in malware specifically focused on banking. It has been observed that such attacks are efficient against the authorization and authentication schemes currently adopted in online banking systems. Each attack is present along with a description of the security mechanisms they target.

6.1 CREDENTIAL THEFT

This kind of attack is the simplest and most commonly performed against banking systems. It basically consists in obtaining the necessary credentials and user data in order to access the system as a legitimate user, providing information normally known only to legitimate users (Figure 3).

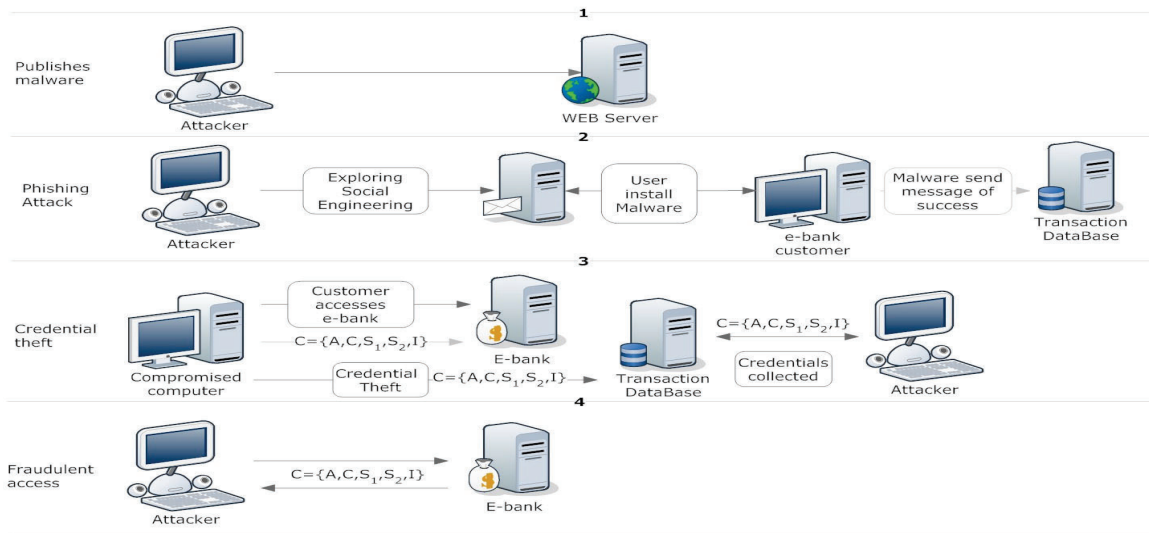


Figure 3: Credential Theft

This attacks is effective against the following security mechanisms: **OTP Token; OTP Card; Browser Protection; Virtual Keyboard; CAPTCHA; SMS; Positive Identification; Pass-Phrase.**

The attacker must capture all information needed to reproduce a legitimate access, therefore you must have the credentials to $C = \{A, C, S_1, S_2, I\}$, to:

- A - Bank Identifier;
- C - Customer unique identifier;
- S_1 - Access password;
- S_2 - Authorization password;
- I - Device Identification information.

Credential theft is summarized in the following steps:

1. The attacker publishes specially crafted malware or counterfeit banking system web pages.
2. Exploiting vulnerabilities in applications such as browsers or applying social engineering the attacker manages to install malware in the device through which the honest user access online banking services.
3. When the legitimate user accesses the service, the authentication data informed by him is captured by the malware or counterfeit web page which the attacker controls.
4. After the malicious artefact obtains the information necessary for accessing the Internet banking system, the user is transparently redirected to the legitimate

service. No error message is issued but generally the user has to re-inform the authentication data.

5. The attacker verifies which information was captured.
6. Having obtained the necessary data, the attacker performs the authentication process, accessing the system as a legitimate user. In order to perform the authentication process the attacker fully impersonates the legitimate user, also providing information about the legitimate user's device physical characteristics, which is commonly used as an authentication factor.

6.2 DEVICE CONTROL

The device control attack is presented in Figure 4 and its objective is to obtain full control of the user's device instead of only stealing data used in the authentication process. The user's device itself is then used by the attacker to access the banking service and perform frauds. This attack is more complex than credential theft (Figure 3) and tracing its origin is much more difficult because the attacker never directly accesses the online banking service.

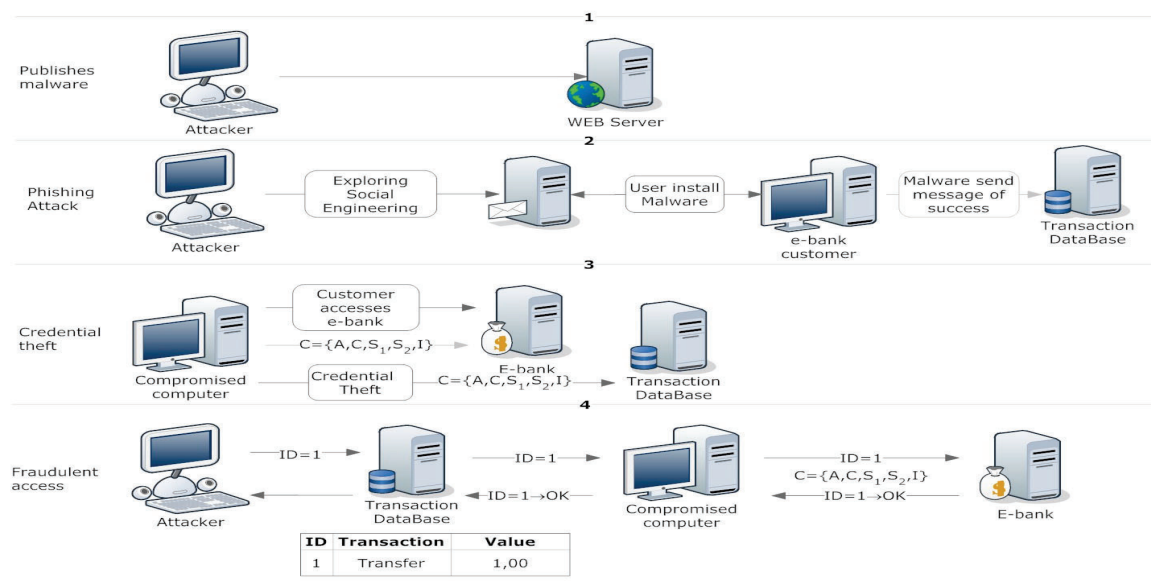


Figure 4: Device Control

This attacks is effective against the following security mechanisms: **Digital Certificates; Device Registering; Device Identification; Transaction Monitoring.**

Device control is summarized in the following steps:

1. The attacker publishes specially crafted malware or counterfeit web pages.

2. Exploiting vulnerabilities in applications such as browsers or applying social engineering the attacker manages to install malware in the device through which the honest user access online banking services.
3. The malware then captures the information necessary for accessing the service.
4. After the malicious artefact obtains the information necessary for accessing the Internet banking system through the legitimate user's device, it downloads a list of transactions to be performed previously stored by the attacker in a remote repository.
5. Having obtained the necessary data, the malware automatically accesses the online banking system as a legitimate user through the user's device and performs the transactions specified by the attacker.
6. While the malware remains active, it suppresses information about the transactions it performed from the banking system's interface, preventing the user from detecting the attacks.
7. The attacker updates the repository containing transactions to be performed by the malware.

7 POTENTIAL COUNTERMEASURES

Due to the inherent complexity and flexibility of the presented attacks it seems unlikely that a single centralized security solution would successfully solve the security issues on which they are based, effectively mitigating those attacks. The main problem relies on the weakest link in the security chain, generally the user (or his access device), and its role in the whole authentication and authorization process. In most cases, the security of the authentication and authorization process in online banking systems is based on secret information supposedly known only by legitimate users and the bank, depending on the user for maintaining the secrecy of such information. However, as it was described in the previous sections, an attacker can easily obtain this secret information through the use of social engineering techniques and malware, compromising the system as a whole. In face of these issues, new authentication and identification models should be as independent from the user or the security of his device as possible, relying on more than one source for authentication and identification data.

A identification and authentication model potentially resilient to the attacks presented in 6.1 and 6.2 should be based on independent secure channels for authentication/authorization data and transaction data. In this model, security is guaranteed even if an attacker compromises one of the channels. The separate authentication/authorization channel is to be chosen in such a way that the user has little or no influence on its security, being based on devices which the user does not control or administer, and not on the user's internet access device (used for transactions) which may be easily compromised by remote attackers.

Taking into consideration that any device associated or dependent on a compromised environment (such as compromised network or host) is also considered compromised, a

potentially secure authentication and identification model for online banking systems should fit the following requisites:

- The authentication data channel is independent from the transaction data channel.
- The identification model is independent from user provided information.
- Perform mutual authentication, where both the user and the service provider must prove their identities.
- Verify and confirm all the information obtained from the user in order to detect patterns and irregularities which may indicate a fraud.
- Maintain a history database for each user containing information which form a user transaction profile associated with reputation and trust models used to detect fraud and malicious tendencies.

A authentication and identification model with these characteristics would be secure against the attacks presented in section 6.

8 CONCLUSION

The security models for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods, which are also the components where most Internet banking systems' vulnerabilities are found. The aforementioned methods depend on the user's knowledge of secret authentication information and the user's ability for maintaining both this information and the device used to access internet banking services secure. If the user's platform (i.e. computing devices, operating systems and applications) is compromised, the banking system is compromised as a whole, allowing the execution of fraudulent transactions. As result of these issues, most of the online banking systems currently in operation may be compromised and subverted. Two attacks which efficiently render current security models ineffective are presented, demonstrating how vulnerable internet banking systems are.

Most of the attacks directed at online banking systems target the user (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authentication data. This fact indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related informations leaks and security issues affecting the system and leading to fraud.

In face of the current security issues and the growing number of attacks and consequent frauds, new internet banking systems should be designed as to provide better authentication and identification methods which are less dependent on the user. The basic characteristics of such methods are introduced based on the analysis the methods currently employed. A internet banking systems with those characteristics will render the presented attacks (and other attacks) ineffective, significantly decreasing the number of observed frauds.

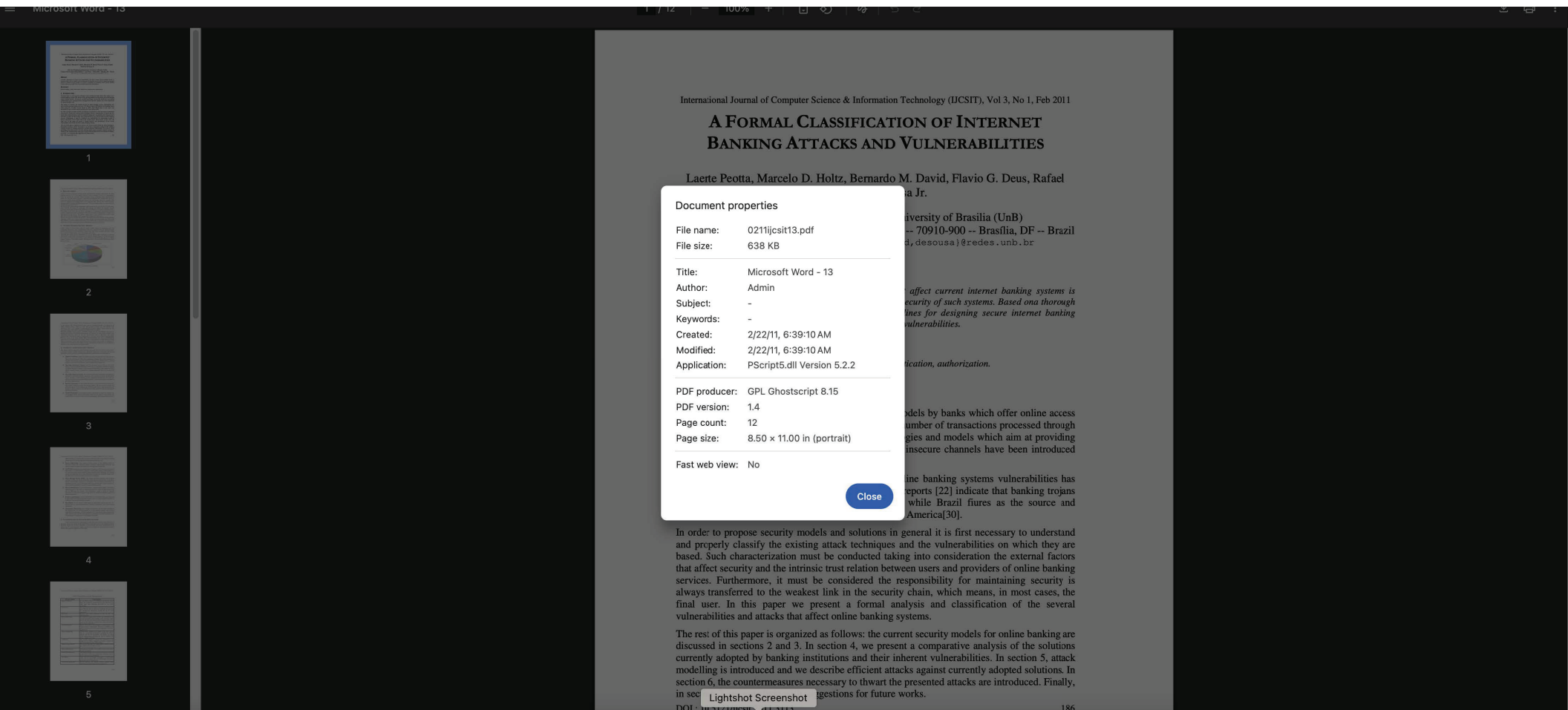
As a future work, a new internet banking system could be developed along with a new security model which provide the security requisites introduced in this paper. Furthermore, efficient techniques for real-time fraud and attacks detections could be proposed based on efficient data mining and pattern recognition methods.

REFERENCES

- [1] ISO/IEC 27002 Code of practice for information security management. 2. ed. Rio de Janeiro: ABNT, 2007.
- [2] ISO/IEC. 27001 Information security management systems Requirement. Rio de Janeiro: ABNT, 2007.
- [3] CAVUSOGLU, Hasan e Cavusoglu, Huseyin. Emerging Issues in Responsible Vulnerability Disclosure. Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain, 2004.
- [4] GOGUEN, Alice; Feringa, Alexis; Stoneburner, Gary. Risk Management Guide for Information Technology Systems [Report]. Computer Security Division Information Technology Laboratory ; National Institute of Standards and Technology Gaithersburg. Nist Special Publication 800, Julho 2002.
- [5] KOSSEW, David. State of the Art Security in Internet Banking [Peridico]. 1997.
- [6] MARSH, Stephen P. Formalising Trus as a Computational Concept. Tese (Doutorado). University of Stirling. - Scotland, UK, 1994. - p. 198.
- [7] MICROSOFT, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008 [Report]. Security Intelligence Report, January through June 2008.
- [8] PEOTTA, Laerte; Amaral, Dino. Estudo de taxonomia de ataques e atacantes em um honeypot de alta interao. Proceedings of the First International Conference on Forensic Computer Science Investigation, Braslia, pp. 38-42, ISSN 1980-1114, 2007.
- [9] WEEKS, Stephen. Understanding Trust Management Systems. IEEE Symposium on Security and Privacy. 2001.
- [10] O. Dandash, P. Dung Le, and B. Srinivasan, Internet banking payment protocol with fraud prevention, 2007 22nd International International Symposium on Computer and Information Sciences, Nov. 2007, pp. 1-6.
- [11] YAHALOM, R.; Klein, B. ; Beth, T. Trust Relationships in Secure Systems-A Distributed Authentication Perspective. IEEE Symposium on Security and Privacy. Washington, DC : IEEE Computer Society, May 24-26, 1993.
- [12] V. Bertol, R.T. Jr, and L.P. Melo, "Um Modelo Para As Normas Sobre Certificacao Digital No Brasil," Proceedings of the Four International Conference on Forensic Computer Science Investigation (ICoFCS'2009), 2009.
- [13] L. Granville, L. Tarouco, and R.R. Barcelos, "Taxonomia de Malwares : Uma Avaliacao dos Malwares Automaticamente Propagados na Rede," Sbseg 2009, Campinas - So Paulo: 2009, pp. 43-56.
- [14] CORREIA, M. A. S. et al. Segurana em Internet Banking. XIII Simposio Brasileiro em Seguranca da Informacao e Sistemas Computacionais (SBseg), Gramado - RS, 2008. 291-299.
- [15] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing Attack Trees using Generalized Stochastic Petri Nets," 2006 IEEE Information Assurance Workshop, 2006, pp. 116-123.
- [16] DANDASH, O.; DUNG, P. ; SRINIVASAN, B. Security Analysis for Internet Banking Models. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. [S.l.]: [s.n.]. 2007. p. 1141 - 1146.
- [17] FINJAN MALICIOUS CODE RESEARCH CENTER. Cybercrime Intelligence: Cybercriminals use Trojans & Money Mules to rob online banking accounts. [S.l.]. 2009.
- [18] HALLER, N. A One-Time Password System (RFC 2289). Internet Engineering Task Force. [S.l.]. 1998.
- [19] MICROSOFT. An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008. [S.l.]. 2008. January through June.

- [20] NAMI, M. R. E-Banking: Issues and Challenges. 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. 263-267.
- [21] NILSSON, M. A. A.; HERD, S. Building Security and Trust in Online Banking. Conference for human-computer interaction. Portland - Oregon - USA: [s.n.]. 2005.
- [22] SYMANTEC. Relatorio Sobre Ameacas de Seguranca na Internet. Symantec - America Latina. [S.l.]. 2010.
- [23] T. T. et al. Modeling Internet Attacks. Workshop on Information Assurance and Security. NY: IEEE. 2001.
- [24] A.S. Martino and X. Perramon, A Model for Securing E-Banking Authentication Process: Antiphishing Approach, 2008 IEEE Congress on Services - Part I, Jul. 2008, pp. 251-254.
- [25] A.S. Martino and X. Perramon, Defending E-Banking Services: Antiphishing Approach, 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Aug. 2008, pp. 93-98.
- [26] WANG, H.; HUANG, X.; DODDA, R. G. Ticket-based mobile commerce system and its implementation. Q2SWinet '06: Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks. Terromolinos, Spain: ACM. 2006. p. 119--122.
- [27] WEIMING, G. et al. Falcon: on-line monitoring and steering of large-scale parallel programs. FRONTIERS '95: Proceedings of the Fifth Symposium on the Frontiers of Massively Parallel Computation (Frontiers'95). Washington, DC, USA: IEEE Computer Society. 1995. p. 422.
- [28] YAN, J.; EL, A.; SALAH., Usability of CAPTCHAs or usability issues in CAPTCHA design. SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security. New York, NY, USA: ACM. 2008. p. 44--52.
- [29] M. JOHNSON, A new approach to Internet banking. University Cambridge. (PhD) 2008, p. 113.
- [30] Carneiro, B. and Sousa, R. T., Identifying Bank Frauds Using Crisp-DM And Decision Trees, International Journal of Computer Science & Information Technology . October, vol. 2, 2010, pp. 162-169

ATTACHMENT G



ATTACHMENT H

The Wayback Machine - <https://web.archive.org/web/20110302081810/http://airccse.org:80/journal/ijcsit...>



Journal Home

IJNSA

IJCNC

IJWMN

IJCSIT

IJMA

GRAPH-HOC

IJMIT

IJDMS

IJNGN

IJSEA

IJAIA

IJSIP

AIRCC Home

February 2011, Volume 3, Number 1

Affine Invariant Descriptors of 3D Object Using Multiple Regression Model [\[pdf\]](#)

M. Elhachloufi¹, A. El Oirak¹, D. Aboutajdine² and M.N. Kaddioui¹,
¹Caddy Ayyad University, Morocco and ²LEESA-GSCM, Morocco

Use-Case, Runtime and Deployment Views for Developing Subsidies Mobile Wallet [\[pdf\]](#)
 Dina Darwish, International Academy for Engineering and Media Science, Egypt

Diagonal Based Feature Extraction for Handwritten Alphabets Recognition System Using Neural Network [\[pdf\]](#)
 J.Pradeep, E.Srinivasan and S.Himavathi, Pondicherry College Engineering, India

Electre Methods in Solving Group Decision Support System Bioinformatics on Gene Mutation Detection Simulation [\[pdf\]](#)
 Ermatita¹, Sri Hartati², Retantyo Wardoyo² and Agus Harjoko²,
¹Sriwijaya University, Indonesia and ²Gadjah Mada University, Indonesia

A Novel Super Resolution Reconstruction of Low Resolution Images Progressively Using DCT and Zonal Filter Based Denoising [\[pdf\]](#)
 Liyakathunisa and C.N .Ravi Kumar, Sri Jayachamrajendra College of Engineering, India

Home

ForthComing Papers

Archives

2011 Volume 3, Number 5

2011 Volume 3, Number 4

2011 Volume 3, Number 3

2011 Volume 3, Number 2

2011 Volume 3, Number 1

2010 Volume 2

2009 Volume 1



Mining Target-Oriented Fuzzy Correlation Rules to Optimize Telecom Service Management [[pdf](#)]

Hao-En Chueh, Yuanpei University, Taiwan

Improving the Character Recognition Efficiency of Feed Forward BP Neural Network [[pdf](#)]

Amit Choudhary¹ and Rahul Rishi², ¹Maharaja Surajmal Institute, India and ²TITS - Bhiwani, India

Initial Classification Through Back Propagation In a Neural Network Following Optimization Through GA to Evaluate the Fitness of an Algorithm [[pdf](#)]

Amit Ganatra, Y P Kosta, Gaurang Panchal and Chintan Gajjar, Charotar University of Science and Technology, India

Adaptive Fuzzy Filtering for Artifact Reduction in Compressed images and videos [[pdf](#)]

P.Ramakrishna Rao¹, B.Addai¹, G.Ramakrishna¹ and T.Panduranga Vital², ¹Dr.B.R.Ambedkar University, India and ²Gayathri College of Science and Management, India

Channel Allocation for Direct Sequence Spread Spectrum Using Vertex Merge Algorithm [[pdf](#)]

Handrizal, A.Noraziah and Ahmed N Abd.Alla, University Malaysia Pahang, Malaysia

Combining Speedup Techniques based on Landmarks and Containers with parallelised preprocessing in Random and Planar Graphs [[pdf](#)]

R. Kalpana¹ and P. Thambidurai², ¹Pondicherry Engineering College, India and ²Perunthalaivar Kamarajar Institute of Engineering & Technology, India

Machine Learning Methods for Spam E-Mail Classification [[pdf](#)]

W.A. Awad¹ and S.M. ELseuofi², ¹Port Said University, Egypt and ²Ras El Bar High inst., Egypt

A Formal Classification of Internet Banking Attacks and Vulnerabilities [[pdf](#)]

Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus and Rafael Timóteo de Sousa Jr., University of Brasilia (UnB), Brazil

Characterization of Tumor Region Using SOM and Neuro Fuzzy Techniques in Digital Mammography [[pdf](#)]

Anamika Ahirwar and R.S. Jadon, Madhav Institute of Technology & Science, India

Search-Based Software Test Data Generation Using Evolutionary Computation [[pdf](#)]

P. Maragathavalli, Pondicherry Engineering College, India



ATTACHMENT I



International Journal
of Computer Science
& Information
Technology (IJCSIT)

A Formal Classification of Internet Banking Attacks and Vulnerabilities

Authors Flavio G. Deus and Rafael Timoteo de Sousa Jr Laerte Peotta, Marcelo D. Holtz, Bernardo M. David

Publication date 2011/2

Journal International Journal of Computer Science & Information Technology (IJCSIT)

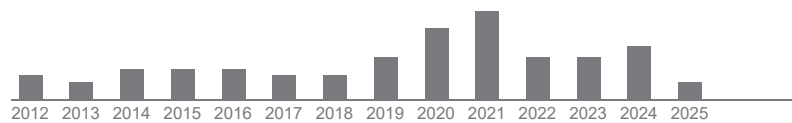
Volume 3

Issue 01

Pages 186-194

Publisher AIRCC Publication

Total citations [Cited by 93](#)



Scholar articles [A formal classification of internet banking attacks and vulnerabilities *](#)
L Peotta, MD Holtz, BM David, FG Deus, RT De Sousa - International Journal of
Computer Science & ..., 2011
[Cited by 93](#) [Related articles](#) [All 7 versions](#)

ATTACHMENT J

The Wayback Machine - https://web.archive.org/web/20110917052615/http://airccse.org:80/journal/jcsit_index.html

Indexing:

Abstracting & Indexing Services:

The articles of IJCSIT are indexed/abstracted in the following index services.



The Elektronische Zeitschriftenbibliothek EZB

Genamics JournalSeek

EBSCO



Scribd



Bibliographic Information

ISSN : 0975 - 4660
e-ISSN : 0975 - 3826
doi : 10.5121/ijcsit



