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 ona 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 fiures 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.

DOI : 10.5121/ijcsit.2011.3113

Plaid Ex1007
Page 1 of 12

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.

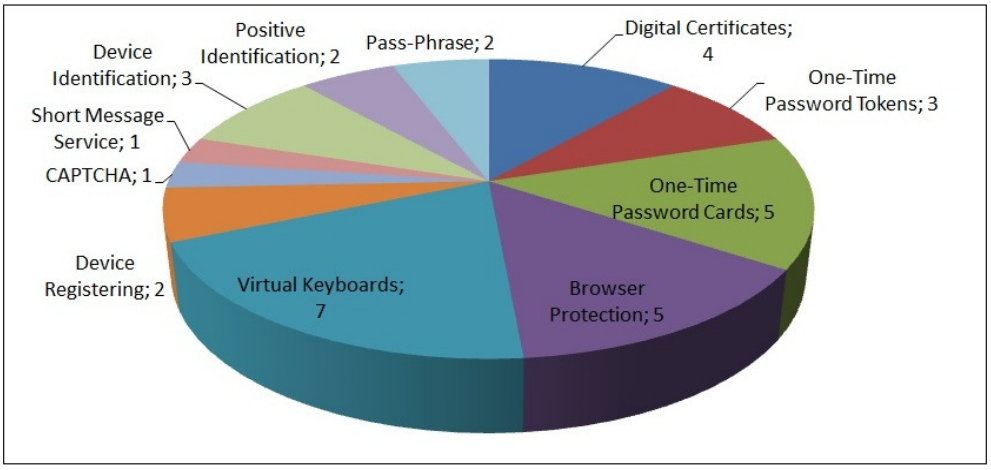

Figure 1: Internet Banking Security Models

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.

Plaid Ex1007
Page 4 of 12

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 atthe 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 util 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).

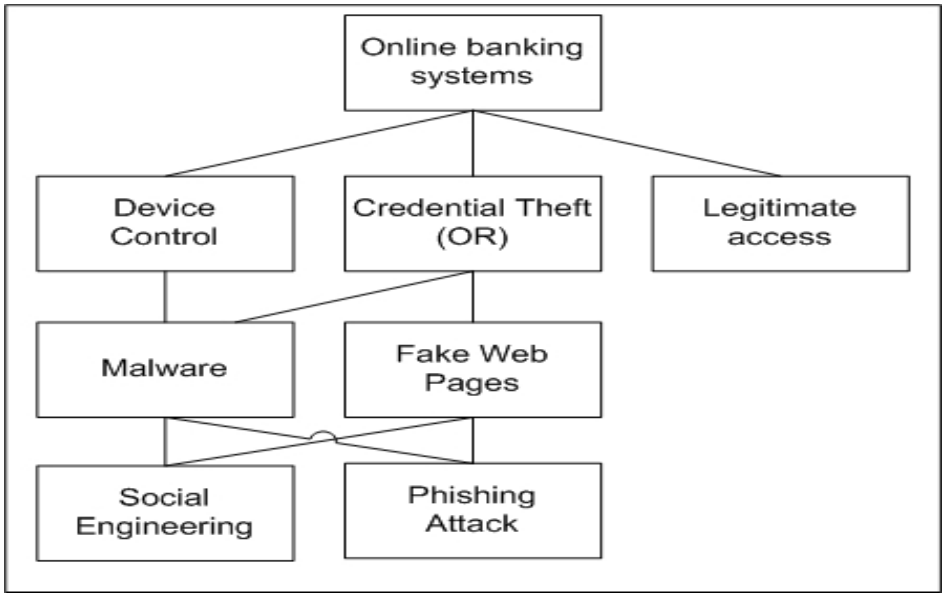

Figure 2: Attack Tree model

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).

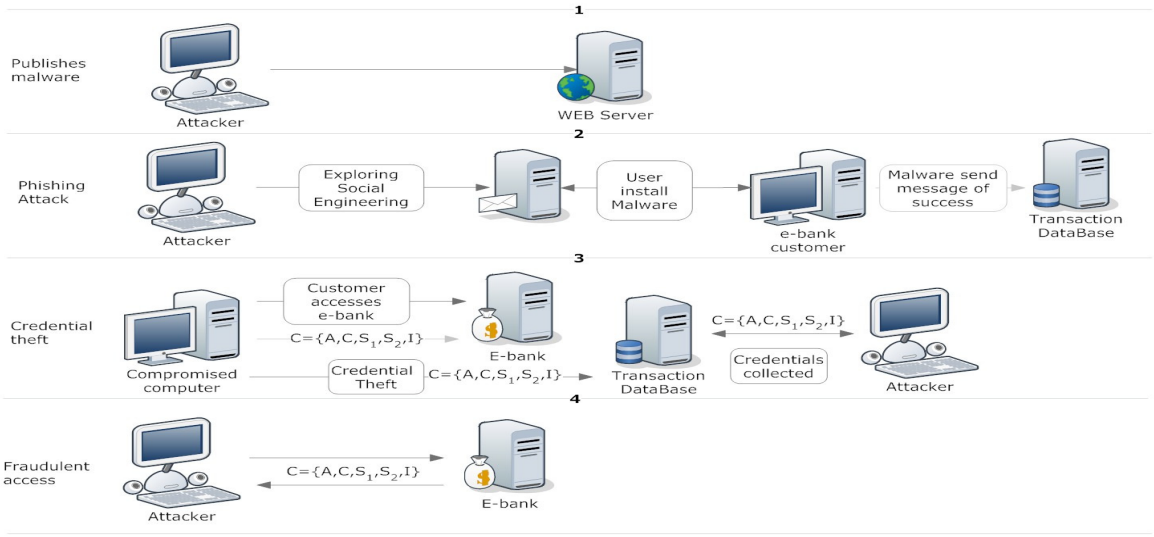

Figure 3: Credential Theft

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.

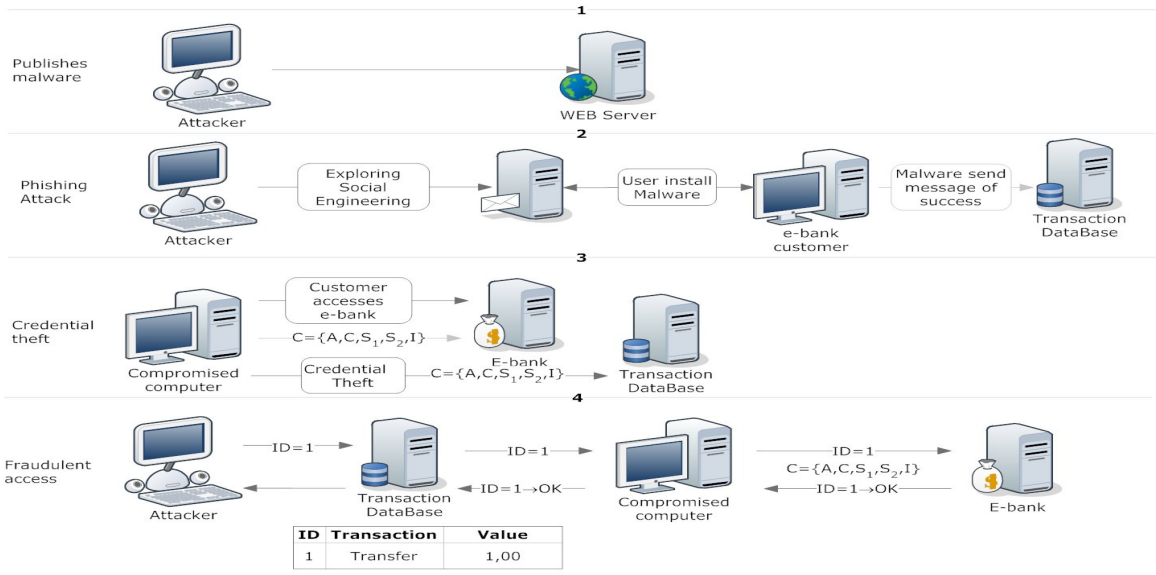

Figure 4: Device Control

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," Procedings 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. Wordshop 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