SECURITY ISSUES AND SOLUTIONS IN E-PAYMENT SYSTEMS

Bogdan-Alexandru URS*

Abstract

Nowadays e-Payment systems have become increasingly popular due to the widespread use of the internet based shopping and banking. The number of private and corporate transactions that are done electronically is growing rapidly. Malicious applications targeting online banking transactions have also increased dramatically in past few years. Worms, Trojans, viruses, phishing, pharming, spoofing, man-in the middle, denial of service attack, transaction poisoning and spamming are the most common threats. All this malicious activity has lead to unauthorized access, theft and fraud. Information security is an essential requirement for any efficient and effective e-Payment system. In Romania, specific legislation has been created in order to protect the e-Payment system and fight cyber-crime.

Key Words: *e-Payment, malware, solutions, biometrics.*

1. Introduction

Generally a payment is a transfer of an item of value from one party to another in exchange for the provision of goods, services or both, or to fulfill a legal obligation[1]. Over the course of history the payment system has evolved significantly, from the simplest and oldest form of payment, which is the exchange of one good or service for another to present day E-money and the Electronic payment system. In the modern world, common means of payment by an individual can include money, cheque, debit, credit, bank transfer and Internet payments[2].

Typically we think of the electronic payments as referring to online transactions on the internet, there are actually many forms of electronic payments. As technology develops, the range of devices and processes to transact electronically continues to increase while the percentage of cash and check transactions continues to decrease[3].

Today, many users make payments electronically, instead of using cash or a check, in person or by mail. Hundreds of electronic payment systems have been developed to provide secure Internet transactions. In order to secure these transactions two cryptographic methods are used in electronic payment systems which includes a

* Lawyer, Baroul Cluj, Romania.

[1] See at http://en.wikipedia.org/wiki/Payment, accesed on April 21th 2015.

[2] See at http://insta-change.com/en/wiki.php, accesed on April 21th 2015.

[3] See at http://www1.american.edu/initeb/sm4801a/epayment1.htm, consulted accesed on April 22th 2015.

secret key (used to encrypt and decrypt the initial transmission to the recipient) and the public key (which uses both a private and a public key)[4].

2. Types of e-Payment

Nowadays most used electronic payment systems are the following: Smart card-based e-payment system, Online payment system, Mobile phone based payment system, E-Wallet Payment System and the E-Cheque Payment System. New payment types are continuously discovered and there are additional methods that exist or are being developed continuously each year[5].

Smart card-based electronic payment system

The Smart card uses a plastic card with an embedded integrated circuit chip providing users with mobility and data portability. It combines plastic and magnetic cards used for different identification purposes in to one card, which can access multiple services, networks and the Internet allowing it to be used for multiple functions and applications[6] .

The smart card payment system provides three-factor authentication security mechanism for the verification and authentication of a given user. These are personal identification number (PIN), digital signature, and fingerprint biometric. This mechanism increases the security level of this payment system[7]. Credit cards, debit cards and prepaid cards currently represent the most common form of electronic payments.

Online payment system

Online payments are based on Internet Banking and involve transferring money or making a purchase online via the Internet. Consumers can transfer money to third parties from their bank account, or they can use credit, debit and prepaid cards to make purchases online.

The Online payment system allows customers of a financial institution to conduct financial transactions on a secured website operated by the institution, which can be a retail bank, virtual bank, credit union or building society[8]. To access a financial institution's online banking facility, a customer using his Internet connection must have a registered account for verification. This allows the customer to link his costumer number to several accounts which he controls, which may be cheque,

---

[4] J L. Camenisch, J. M. Piveteau, M. A. Stadler, *Security in Electronic Payment Systems*, Information Technology Laboratory of SBG. Retrieved 21 apr. 2015 from http://www.ubilab.org/ Publications/print_versions/pdf/piv94b.pdf.

[5] See at http://www1.american.edu/initeb/sm4801a/epayment1.htm, accesed on April 22th 2015.

[6] Singh Sumanjeet, *Emergence of Payment Systems in the age of Electronic Commerce: The State of Art, Asia Pacific Journal of Finance and Banking Research Vol. 3. No. 3. 2009. Retrieved apr. 21 from* http://globip.com/articles/asiapacific-vol3-article2.pdf.

[7] P. Aigbe, J. Akpojaro, *Analysis of Security Issues in Electronic Payment Systems*, International Journal of Computer Applications Volume 108 – No. 10, December 2014. Retrieved 25 apr. 2015 from http://ijcaonline.org/archives/volume108/number10/18946-9993.

[8] S. Sumanjeet, *Emergence of Payment Systems in the age of Electronic Commerce: The State of Art, Asia Pacific Journal of Finance and Banking Research.*

savings, loan, credit card and other accounts.[9]

Mobile phone based payment system

This system allows consumers to use their mobile phone in order to pay for transactions in several ways. Consumers can send an SMS message, transmit a PIN number, use WAP to make online payments, or perform other segments of their transaction with the phone. As phones develop further, consumers are likely to be able to use infrared, Bluetooth, NFC and other to transmit full account data in order to make payments securely and easily from their phone.

Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to the mobile network and allow payments to be made. Mobile payments can become be an alternative to paper money, cheques, credit cards and debit cards. It can also be used for payment of bills, electronic funds transfer, Internet banking payments, direct debit and electronic bill presentment[10]. SMS banking is a service that is offered from banks to its customers, permitting them to operate selected banking services over their mobile phones using SMS messaging[11].

Electronic Wallet Payment System

The electronic wallet (e-wallet) provides all of the functions of today's wallet on one convenient smart card eliminating the need for several cads. The e-Wallet will also provide numerous security features not available to regular wallet carriers[12].

The most common example of e-wallet Paypal. PayPal allows payments and money transfers to be made through the Internet. It is a fast way to pay and get paid online. With Paypal money is sent without sharing financial information. People also have the flexibility to pay using their account balances, bank accounts, and credit cards.[13].

Another popular example of an e-wallet on the market that can be used for micro-payments is Windows Phone Wallet developed by Microsoft. This e-wallet eliminates the reentering of personal information on the forms, resulting in higher speed and efficiency for online shoppers[14].

A new emerging e-wallet is Google Wallet, which has a similar function as PayPal to facilitate payments and money transfers online. It also features a security that has not been cracked to date, and the ability to send payments as attachments via email. Google Wallet allows an easier way to pay in stores, online or to anyone in the US with a Gmail address. It works with any debit or credit card, on every mobile carrier. Functions like "Tap and pay" are key elements that allows users to pay in store at millions of locations[15].

---

[9] M. S. Uddin, A. Y. Akhi, *E-Wallet System for Bangladesh an Electronic Payment System*, International Journal of Modeling and Optimization, Vol. 4, No. 3, June 2014. Retrieved 22 apr. 2015 from *http://www.ijmo.org/papers/376-A1015.pdf.*

[10] V. Goyal, Dr. U.S. Pandey, S. Batra, *Mobile Banking in India: Practices, Challenges and Security Issues, International Journal of Advanced Trends in Computer Science and Engineering, 2012.* Retrieved 23 apr. 2015 from www.warse.org/pdfs/ijatcse03122012.pdf.

[11] M. S. Uddin, A. Y. Akhi, *E-Wallet System for Bangladesh an Electronic Payment System.*

[12] M. S. Uddin, A. Y. Akhi, *E-Wallet System for Bangladesh an Electronic Payment System.*

[13] See at https://www.paypal-media.com/about, accesed on April 23th 2015.

[14] See at http://www.windowsphone.com/en-us/how-to/wp8/apps/wallet, accesed on April 23th 2015.

[15] See at https://www.google.com/wallet/, accesed on April 23th 2015.

Electronic Cheque (eCheque) Payment System

Electronic cheques are the equivalent of paper-based cheques. The electronic cheques are initiated during an on-screen dialog and the funds are transferred over a computer network at the time of the transaction. Authorized users are assigned a portable electronic cheque book which is an amalgam of a secure hardware device and specialized software[16].

The payer writes the e-Cheque on a computer, cryptographically signs it, and e-mails it via the Internet. The payer signs the e-Cheque using the secure hardware device, and includes its authenticating certificate, signed by the issuing bank. The payee receives the e-Cheque, verifies the payer's signature on the e-Cheque, endorses it, writes a deposit slip, and signs the deposit slip[17].

3. Security issues that threaten the e-payment systems

Today the security issues that threaten Electronic payment systems are changing constantly, and often extremely quickly. The most common threats include viruses, worms and Trojan horses. Viruses are spread via email or by downloading infected files. Viruses are a nuisance threat that can be categorized as a Denial of Service (DoS) tool due to the fact that they only disrupt electronic communications[18].

Nowadays there are thousands of different types of computer viruses and internet malicious programs. Malicious software can easily attack the mobile banking payment system by taking up passwords on the web browser or any cached information on operating system. For example the Zeus Trojan was used to target mobile bank users by inflicting defect SMS banking[19].

Worms can be categorized as special viruses that spread using direct Internet connections. They are standalone programs that do not require a host program for activation and spread themselves independently from computer to computer by exploiting security vulnerabilities or configuration errors in operating systems or applications[20].

Trojan horse programs launched against client systems pose the greatest threat to the e-Payment systems because they can bypass or subvert most of the authentication and authorization mechanisms used in an electronic transaction. The Trojan horses aim to spy on sensitive data (e.g. passwords, confidential data, etc.) and send it back to their owners to gain access to third-party computers and thus take

---

[16] See at http://www.theengineer.co.uk/more-sectors/electronics/news/electronic-chequebook-could- assist-internet-transactions/1011700.article, consulted at 24/04/2015.

[17] P. Aigbe, J. Akpojaro, *Analysis of Security Issues in Electronic Payment Systems.*

[18] M. Niranjanamurthy, DR. Dharmendra Chahar , *The study of E-Commerce Security Issues and Solutions, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.* Retrieved 22 apr. from http://www.ijarcce.com/Upload/2013/july/69-o-Niranjanamurthy%20The%20study%20of%20ECommerce%20Security%20Issues%20and%20Solutions .pdf.

[19] V. Goyal, Dr.U.S.Pandey, S. Batra, *Mobile Banking in India: Practices, Challenges and Security Issues.*

[20] M. Vrîncianu, L. A. Popa, *Consideration Regarding the Security and Protection of E-Banking Services Consumers' Interests*, Academy of Economic Studies, 2010, Bucharest, Romania. Retrieved 27 apr. 2015 from http://core.ac.uk/download/pdf/6492899.pdf.

control of them remotely[21]. Trojans are normally disguised as applications that are useful to users of the computers they infect. These programs can be installed on a remote computer by the simplest of means, for example an email attachment or when users visit certain websites and download a so called "harmless" program[22]. As they do this, a key logger program that has bound to the downloaded program is also installed on their computer without their knowledge. When the users log into their bank's website, the information keyed during the session will be captured and sent to the attacker. This is one of the most effective ways of stealing information because it captures everything the user is doing on his device. The key loggers or spyware, as they are also known are particularly dangerous because they can trace any kind of activity a user performs on his computer system[23].

Another common method that is used to disrupt the security of the e-payment system is a denial-of-service attack (DoS) or a distributed denial-of-service attack (DDoS) that involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. By doing this they attempt to make computer resources unavailable to its intended users (for example "flooding" a network in order to prevent access to a service or a particular device by disrupting the service and not allowing access to a specific device). The DoS attacks typically target sites or services hosted on web servers such as banks or credit card payment gateways. The illegitimate use involves the use of information by unauthorized persons or for unauthorized purposes[24].

Phishing and Pharming are methods used to solicit personal information by posing as a trustworthy organization. In recent years both pharming and phishing have been used for online identity theft information. Phishing attacks use email or malicious websites to solicit personal information. Usually the attacker sends an email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts[25]. Pharming is a type of fraud that involves diverting the client Internet connection to a counterfeit website, so that even when he enters the correct address into his browser, he ends up on the forged site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software[26].

---

[21] M. Lutovac, H. Berisha, M. Gardasevic, T. Milya, *Computer abuse and the protection against cyber terrorism,* The international conference - The Rule of Law in the Digital Era, Accent Publishing House, page 56, Cluj-Napoca, 2015.

[22] M. Niranjanamurthy, DR. Dharmendra Chahar, *The study of E-Commerce Security Issues and Solutions,* International Journal of Advanced Research in Computer and Communication Engineering.

[23] I. Vasiu, L. Vasiu, *A Framework for Secure Electronic Payments,* The international conference - The Rule of Law in the Digital Era, Accent Publishing House, pp. 73, Cluj-Napoca, 2015.

[24] M. Vrîncianu, L. A. Popa, *Consideration Regarding the Security and Protection of E-Banking Services Consumers' Interests.*

[25] M. Vrîncianu, L. A. Popa, *Consideration Regarding the Security and Protection of E-Banking Services Consumers' Interests.*

[26] A. Fatima, *E-Banking Security Issues – Is There A Solution in Biometrics?,* Journal of Internet Banking and Commerce, August 2011, vol. 16, no. 2. Retrieved 25 apr. from http://www.arraydev.com/commerce/JIBC/2011-08/Fatima.pdf.

Recent developments in e-payment has led to the creation of new kind of attacks. Intrusive methods that have a high degree of aggression are more and more used. Man-In-The-Middle is one of those methods that involves a type of attack where attackers intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data[27]. Man-In-The-Middle can be combined with Spamming or E-mail bombing that is caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Sending unsolicited commercial emails to individuals is also achieved placing software agents into a third-party system and setting it off to send requests to an intended target[28].

Drive-by downloads are malware infections that represent a major threat to e-payment. Users get infected with such malware simply by visiting a particular website. These websites often contain legitimate content, but have been contaminated by harmful programs that smuggle malicious codes into the site[29].

A Masquerading or a spoofing attack as it is also known is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. A common method of Masquerading is consists in sending a message that appears to be from someone else[30]. The impersonator is typically another user that has changed the username or the IP levels by changing the source and/or destination IP of the address of packets in the network[31].

4. Solutions

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all e-payment based products and services. No single control or security device can adequately protect a system connected to a public network. The method and system can be augmented by requesting for different security credentials such as PIN, cryptographic key, digital signature, biometrics, etc, to establish multiple layers of authentication[32].

The electronic payment system with a higher number of authentication factors may have higher secure level. This means that an electronic payment system with higher authentication factors will have a stronger security level which lowers or

[27] A. Fatima, *E-Banking Security Issues – Is There A Solution in Biometrics?*.

[28] M. Niranjanamurthy, DR. Dharmendra Chahar, *The study of E-Commerce Security Issues and Solutions*, International Journal of Advanced Research in Computer and Communication Engineering.

[29] M. Vrîncianu, L. A. Popa, *Consideration Regarding the Security and Protection of E-Banking Services Consumers' Interests*.

[30] V. Goyal, Dr.U.S. Pandey, S. Batra, *Mobile Banking in India: Practices, Challenges and Security Issues.*

[31] M. Niranjanamurthy, DR. Dharmendra Chahar, *The study of E-Commerce Security Issues and Solutions*, International Journal of Advanced Research in Computer and Communication Engineering.

[32] A. Fatima, *E-Banking Security Issues – Is There A Solution in Biometrics?*.

reduces the fraud vulnerability of the electronic payment system, and this eventually boost users confidence[33].

In order to properly protect the e-payment system both technical and legal solutions must be found. In Romania, specific legislation has been created by the development of Government Ordinance no. 130/2000 on the regime of distance contracts [34], Law no. 455/2001 on Electronic Signatures [35], the Government Emergency Ordinance no. 193/2002 concerning the introduction of modern means of payment[36], Law no. 677/2001 on the protection of the processing of personal data and free movement of such data, with subsequent amendments[37],
Regulations of National Bank of Romania no. 4/2002 concerning transactions by electronic payment instruments and the relationship between participants in these transactions[38], the Law no. 365/2002 on electronic commerce[39] and the Order of the Ministry of Communications and Information Technology no. 389/27.06.2007 regarding the approval procedure of payment instruments with remote access applications such as Internet banking, home-banking or mobile banking[40].

Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy that are expected in the future years. Biometrics can become a possible solution that allows the automatic identification of a person based on her physiological or behavioral characteristics. It provides a better solution for the increased security requirements of our information society. As biometric sensors continue to become less expensive, the public will realizes that biometrics is actually an effective strategy in case of fraud, making this technology more likely to be used in every transaction needing authentication[41].

5. Conclusion

One of the technological innovations in banking, finance and commerce is the Electronic Payments. Electronic Payments enables us to perform financial transactions electronically fast and easily. Although it provides a number of benefits

[33] Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler, *Security in Electronic Payment Systems*.

[34] Government Ordinance no. 130/2000 on the regime of distance contracts, published in the Official Journal of Romania, Part I, no. 431 of 9 february 2000.

[35] Law no. 455/2001 on Electronic Signatures, published in the Official Journal of Romania, Part I, no. 429 of 31st July 2001.

[36] Government Emergency Ordinance no. 193/2002 concerning the introduction of modern means of payment, published in the Official Journal of Romania, Part I, no. 942 of 23 December 2002.

[37] Law no. 677/2001 on the protection of the processing of personal data and free movement of such data, published in the Official Journal of Romania, Part I, no. 790 of 12 December 2001.

[38] Regulations of National Bank of Romania no. 4/2002 concerning transactions by electronic payment instruments and the relationship between participants in these transactions, published in the Official Journal of Romania, Part I, no. 503 of 12 July 2002.

[39] Law no. 365/2002, published in the Official Journal of Romania, Part I, no. 279 of 21st April 2003.

[40] Order of the Ministry of Communications and Information Technology no. 389/27.06.2007 regarding the approval procedure of payment instruments with remote access applications such as Internet banking, home-banking or mobile banking, published in the Official Journal of Romania, Part I, no. 485 of 19 July 2007.

[41] A. Fatima, *E-Banking Security Issues – Is There A Solution in Biometrics?*.

for customers and business opportunities, it comes with risks, especially security issues. E-payments systems should have reliable and secure methods to authenticate their customers thus reducing the inherent risks. The level of authentication used should be appropriate to the risks associated with them.

References

1. P. Aigbe, J. Akpojaro, *Analysis of Security Issues in Electronic Payment Systems*, International Journal of Computer Applications Volume 108 – No. 10, December 2014;
2. I. Vasiu, L. Vasiu, *A Framework for Secure Electronic Payments*, The international conference - The Rule of Law in the Digital Era, Accent Publishing House, page 73, Cluj-Napoca, 2015;
3. Singh Sumanjeet, *Emergence of Payment Systems in the age of Electronic Commerce: The State of Art, Asia Pacific Journal of Finance and Banking Research Vol. 3. No. 3. 2009;*
4. M. Vrîncianu, L. A. Popa, *Consideration Regarding the Security and Protection of E-Banking Services Consumers' Interests*, Academy of Economic Studies, 2010, Bucharest, Romania;
5. V. Goyal, Dr.U.S.Pandey, S. Batra, *Mobile Banking in India: Practices, Challenges and Security Issues, International Journal of Advanced Trends in Computer Science and Engineering, 2012;*
6. Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler, *Security in Electronic Payment Systems,* Information Technology Laboratory of SBG;
7. M. S. Uddin, A. Y. Akhi, *E-Wallet System for Bangladesh an Electronic Payment System*, International Journal of Modeling and Optimization, Vol. 4, No. 3, June 2014;
8. M. Lutovac, H. Berisha, M. Gardasevic, T. Milya, *Computer abuse and the protection against cyber terrorism*, The international conference - The Rule of Law in the Digital Era, Accent Publishing House, page 56, Cluj-Napoca, 2015;
9. M. Niranjanamurthy, DR. Dharmendra Chahar, *The study of E-Commerce Security Issues and Solutions, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013;*
10. A. Fatima, *E-Banking Security Issues – Is There A Solution in Biometrics?*, Journal of Internet Banking and Commerce, August 2011, vol. 16, no. 2.