IJCSN International Journal of Computer Science and Network, Volume 3, Issue 4, August 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.274

Banks & E–Commerce Network Security Threats and Best Policies in Practice

Adam Ali.Zare Hudaib

Licensed Penetration Tester, CEH , ECSA , LPT , WCNA,
"2.MAS" Poland . Lublin 20-032

Abstract - This increase in e–commerce has driven the need to create an online payment system. Unfortunately, there are a lot of flaws and internet frauds. Cyber–criminals have benefited from on–line banking (OB). We try to predict how hacking tools might evolve. We briefly survey the state–of–the–art tools developed by black–hat hackers and conclude that they could be automated dramatically. To demonstrate the feasibility of our predictions and prove that many two–factor authentication schemes can be bypassed, we have analysed banking and modern payments system security. In this research we review different payment protocols and security methods that are being used to run banking systems. We survey some of the popular systems that are being used today, with a deeper focus on the chips, cards, NFC, authentication etc. In addition, we also discuss the weaknesses in the systems that can compromise the customer's trust.

Keywords - *Banking security, authentication, chip and PIN , e–payment , security protocol , bitcoin , NFC.*

1. Introduction

Progress in web technologies has led to rapid growth of hybrid web applications that combine the Application Programming Interfaces (APIs) of multiple web services (e.g., search APIs, map APIs, payment APIs, etc.) into integrated services like personal financial data aggregations and online shopping websites. The pervasiveness of these applications, however, brings in new security concerns. The web programming paradigm is already under threat from malicious web clients that exploit logic flaws caused by improper distribution of the application functionality between the client and the server (e.g., relying on client logic to validate user privileges). Cryptology, the science of code and cipher systems, is used by governments, banks and other organisations to keep information secure. It is a complex subject, and its national security overtones may invest it with a certain amount of glamour, but we should never forget that information security is at heart an engineering problem. The hardware and software products which are designed to solve it should in principle be judged in the same way as any other products: by their cost and effectiveness. However, the practice of cryptology differs from, say, that of aeronautical engineering in a rather striking way: there is almost no public feedback about how cryptographic systems fail. Most of the development of online financial services has been reactive, doing the minimum amount of work to try and frustrate the attacks which are observed. It has also been quite piecemeal and uncoordinated. Almost all of the defences have a simple attacker model which only considers those attacks which their prospective target has experienced in the wild. Some of these systems manage to achieve their (fairly limited) goals, but many of them are only partially effective at best [1].

In reaction to the defensive schemes developed by the targets of attacks, many criminals have started to become more sophisticated. This is still lost in the noise of the remarkably successful but simple attacks, which explains why very few people are working on more robust systems. Nevertheless, these new attacks prove that the criminals can adapt to break the defences which are currently being rolled out.

This thesis is a discussion of the attack and defence landscape surrounding online banking and how these high profile targets and their users can best be protected. We will review different payment protocols and security methods that are being used to run online payment systems.

2. Threats and Attacks on E–commerce and Banking Network Systems

2.1 Banking Security

In Internet banking as with traditional banking methods, security is a primary concern. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the systems.

For statistics: in three waves of attacks since September 2013, consumers have reported inability to conduct online transactions at more than a dozen banks, including Wells Fargo & Co (WFC.N), Citigroup Inc (C.N), JPMorgan Chase & Co (JPM.N) and Bank of America Corp (BAC.N). Banks have spent millions of dollars to fend off the hackers and restore service. In DDoS attacks, thousands of computers all try to contact

a target website at the same time, overwhelming it with meaningless connections until it is rendered inaccessible. The banks have said little about their frantic efforts behind the scenes to restore websites, and industry groups have generally played down the impact and severity of the attacks [2].

The security of the average Internet banking application is addressed at three levels. The first concern is the security of client information as it is sent from the customer's PC, mobile phones, corporate clients etc. to the Web server. The second area concerns the security of the environment in which the Internet banking server and client information database reside. Finally, security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web systems [3].

Data security between the client browser and Web server usually is handled through a security protocol called Secure Sockets Layer (SSL). SSL provides data encryption [4], server authentication, and message integrity for a Internet connection. In addition, SSL provides a security "handshake" that is used to initiate the connection. This handshake results in the client and server agreeing on the level of security they will use and fulfills any authentication requirements for the connection.

Also online banking application supports data encryption. Requests for online banking information are passed on from the Web server to the Internet banking server. The Internet banking application is designed using a three–tiered architecture. The three–tiered architecture provides a double firewall, completely isolating the Web server from the client information SQL database.

The World Wide Web interface receives SSL input and sends requests through a firewall over a dedicated private network to the Internet banking server. The World Wide Web interface is the only process capable of communicating through the firewall to the Internet banking server. Therefore, only authenticated requests communicate with the Internet banking server.

The client information database is housed on a database server, which implements security algorithm in addition to the firewall technology. The client database is usually stored on a RAID–5 drive array, which provides uninterruptible data access, even in the event of a hard drive failure [5].

A security analyzer constantly monitors login attempts and recognizes failures that could indicate a possible unauthorized attempt to log into an account. When such trends are observed, steps will be taken automatically to prevent that account from being used. Implementation of the SSL security protocol on the Web server and client browser ensures authenticated data has been received from the client. The three–tiered approach of the Internet banking application creates a double firewall which performs information requests over dedicated networks designed to handle specific functions. Placing all business logic and event logging within the Internet banking server creates a controlled environment which allows quick incorporation of Internet security technologies as they evolve. Finally, the security analyzer monitors login attempts in order to prevent unauthorized logins.

The Open Payment Framework is built entirely on a Service Oriented Architecture (SOA) delivering common, reusable services consisting of a comprehensive data model, choreographed payment business processes and configurable services including parsing, validation, cost based routing, warehousing security, auditing and many more [5].

2.2 Banking Security Attacks

Notwithstanding an increased number of attacks, the percentage of financial malware detected each month is dropping. The reasons for this are detailed below:

- Malware authors constantly change their programs in order to evade detection by antivirus solutions. However, if the changes made are minor, AV vendors will still be able to detect new malware samples using signatures created for previous variants.
- Banking attacks are usually a multi–step process: social engineering, phishing, and the use of Trojan–Downloaders which then download the financial malware. It's easier for the criminals to modify the Trojan–Downloader programs (which are usually smaller in size, and generally less complex) than the financial malware itself.

Banks have responded to the increased number of attacks by investing more time, money and effort into developing mechanisms for detecting fraud and illegal activity. One safeguard is for an alert to be triggered if a large amount of money is transferred to a 'suspicious' region of the world [6].

Given that phishing continues to be widespread, it is obviously a successful method of attack. Phishing attacks work on all major operating systems. However, there's one major downside from the cyber criminal's point of view: the user has the choice whether or not to click on a link contained in an email, and is then able to choose whether or not to enter his/ her credentials.

This element of choice is inherent in all social engineering approaches. A technical approach involving the use of malware removes this element of choice, making those users who didn't fall for a phishing scam are still a viable target.

Financial malware comes in all shapes and sizes, and will often be tailored to target a single organization. There's no requirement for the cyber criminals to spend time creating unnecessarily complex malware [7]. There are several methods which malware authors can use to get around banking security and harvest user information. For instance, if a bank uses single–factor authentication with a static username and passwords, it's a simple matter of capturing keystrokes. Alternatively, some banks have created dynamic keypads so that the user needs to click a 'random' pattern in order to enter his password. Malware authors use two different methods to circumvent this type of security – they can either create screen dumps when the user visits a specific site or simply gather the information being sent to the site by grabbing the form. In both cases, the stolen data is processed later. Another method used by cyber criminals is to redirect traffic. Additionally, although the traffic is redirected, it may not be processed in real time, which gives the victim the chance to contact his/ her bank to stop the transaction. The most recent internet banking security threats are listed below.

Phishing. It is a scam where fraudsters 'fish' for your personal details by using hoax emails claiming to be from financial institutions. This method continues to be favored by online thieves.

Hoax emails claiming to be from banks are often generated overseas, and are sent in bulk asking recipient to provide sensitive information such as their username, password, Customer Registration Number or Debit Cards / Credit Cards numbers and PINs by providing a link leading to a fake website, enabling thieves to gather the details for later fraudulent use.

Spyware and Adware. Spyware is a type of software that secretively collects user information while on the Internet. Adware is a type of spyware used by marketers to track Internet user's habits and interests for the purpose of customizing future advertising material[11]. The information is then used to customize future advertisements directed to the user, or can be sold to a third party for the same purpose.

Viruses. A computer virus is software that affixes itself to another program like a spreadsheet or word document. While active, the virus attempts to reproduce and attach itself to other programs. This can tie up resources such as disk space and memory, causing problems on any home computer. An email virus is the latest type of computer virus that is transported through email messages and usually replicates by automatically distributing itself out to all contacts on the victims email address book.

Trojans. A Trojan is a destructive program that poses as a harmless application. Unlike viruses, Trojans do no replicate themselves and do not need a host program to attach to. Some Trojans will claim to rid the computer of viruses or other harmful applications, but instead introduce viruses and leave it vulnerable to attacks by hackers and intruders.

Keyloggers. If fraudster installs a software called "keylogger" on the computer or the device on which the customer is accessing Online Banking, the software copies to a file, every keystroke typed on that pc. This sensitive information gets captured that the fraudster can later use for fraudulent purposes and illegitimate access to your account.

IBS attacks. These types of attacks are offline attacks against the servers that host the Internet banking application. Examples include: brute–force attacks in certain password–based mechanisms are reported to be feasible by sending random usernames and passwords, bank security policy violation, web site manipulation — exploiting the vulnerabilities of the Internet banking web server may permit the alteration of its contents [12].

2.3 Payments Security

Authentication attack can be resisted by cryptographically binding the one–time code to the data of the transaction being attempted – transaction authentication. A robust way to do this is to provide the customer with an electronic signature device with a trustworthy display on which she could verify the transaction data, a trusted path to authorise a digital signature, and a tamper–resistant store for the signing key. The Chip Authentication Programme (CAP) [13] is a lower–cost implementation of this general approach. Individual countries have adopted different variants of CAP based on the original specification. Usually it uses the deployed "Chip & PIN" smart card infrastructure. Participating banks have sent out handheld smart card readers with keypads and displays which, with a customer's card and PIN, generate one–time passwords. Even though Chip & PIN is based on the public EMV standard, the CAP standard is secret and so not subject to scrutiny, despite being a critical security component the public must rely on for banking transactions.

CAP operates in three modes – identify, respond, and sign. These differ in the information a user is asked to enter before a response code is generated. For all three modes a PIN is required first. Thereafter, identify just returns a onetime code; for respond a numerical challenge is required; and for sign an account number and a value are needed. The numerical response code is a compressed version of a MAC computed by the card under its key; it is calculated over the information entered by the customer, a transaction counter, and a flag showing whether the PIN matches the one stored on the card [14].

The implementation of the CAP system is heavily based on the EMV smart card protocol being introduced

throughout Europe for credit and debit card point−of−sale transactions. In the UK, EMV is known under the "Chip & PIN" brand.

EMV is now the leading scheme worldwide for debit and credit card payments, as well as for cash withdrawals at ATMs, with more than 1.34 billion cards in use worldwide. US banks were late adopters, but are now in starting to issue EMV cards to their customers. EMV cards contain a smart card chip, and are more difficult to clone than the magnetic−strip cards that preceded them. EMV was rolled out in Europe over the last ten years, with the UK being one of the early adopters. After it was deployed, the banks started to be more aggressive towards customers who complained of fraud, and a cycle established itself. Victims would be denied compensation; they would Google for technical information on card fraud, and find one or other of the academic groups with research papers on the subject; the researchers would look into their case history; and quite often a new vulnerability would be discovered [5].

We wondered whether, if the "unpredictable number" generated by an ATM is in fact predictable, this might create the opportunity for an attack in which a criminal with temporary access to a card can compute the authorization codes needed to draw cash from that ATM at some time in the future for which the value of the UN can be predicted. We term this scenario the "pre−play" attack. We discovered that several ATMs generate poor random numbers, and that attacks are indeed possible.

The specifications and conformance testing procedures simply require that four consecutive transactions performed by the terminal should have unique unpredictable numbers. Thus a rational implementer who does not have the time to think through the consequences will probably prefer to use a counter rather than a cryptographic random number generator (RNG); the latter would have a higher probability of failing conformance testing (because of the birthday paradox) [15].

Even if the UN generation algorithms are patched, a number of powerful attack variants may make pre−play attacks viable for years to come.

Chip secrets. There are chip attack methods:

Non−invasive attacks observe or manipulate with the chip without any physical harm to it; low−cost: require relatively simple equipment and basic knowledge; time consuming and not always successful. AES is attacked by side−channel attacks such as SPA, DPA, CPA, EMA, DEMA (takes 1 second/1 day); poor signal−to−noise ratio of about −15dB due to low−power operation and multiple sources of noise (clocks, pumps, acquisition).

Invasive attacks almost unlimited capabilities in extracting information and understanding chip functionality; expensive, requires a very sophisticated equipment and knowledge; less time consuming and straightforward for many devices. AES is attacked by partial reverse engineering followed by microprobing (takes 1 day).

Semi−invasive attacks fill the gap between non−invasive and invasive types: direct access to the chip's surface is required but without any physical harm to it; moderate cost: some equipment can be easily built; higher success rate compared to non−invasive attacks; some are easily repeatable and relatively quick to set up. AES is attacked by optical fault injection attack (1 hour) and optical emission analysis (1 week/1 hour).

Bumping attacks are dangerous and can compromise the security in chips – evaluation and protection is necessary. Backside approach helps in modern chips, it is simple to do and does not require expensive optics and precise positioning. Bumping attacks can be used for partial reverse engineering to understand internal data paths and chip structure.

Modern payments security: EMV, NFC etc. The total number of purchases on all major worldwide card issuers (American Express, Diners Club, JCB, MasterCard, UnionPay and Visa) increased to a total of 135.33 billion, up 12.1 percent from 2010 on an additional 14.56 billion transactions, the Nilson Report, 2011 report said. Some statistics: as of early 2011, 1.2 billion EMV cards were deployed across the globe along with 18.7 million EMV terminals (via IBID). Over a billion smartphones sold by 2012. By 2014, 44% of smartphones will be NFC−compatible (via). Payment card users in Russia: Spring 2011 to Spring 2012: from 49% to 56% (via GfK Rus).

There are Notable IPS (International Payment Systems):

- Visa.
- MasterCard (MC).
- Japan Credit Bureau (JCB).
- Diners Club (DC).
- American Express (AMEX).
- China Union Pay (CUP).

Usually they have security methods: plastic (holograms, watermarks) and cryptography (DES, 3DES, mode: EDE, 2 keys: ABA, cardholder authentication, card authentication, encryption) [5].

Processing cycle begins with cardholder. He receives a card and sign it manually, opens PIN envelope, reads it and burn it. Then issuer (personalization, embossing, encoding, authorization processing, presentment processing). The card is just a static read−only piece of plastic. The acquirer manages terminals and provides services to merchants. Acquirer's host software provides

authorization and presentment processing. The terminal reads card and talks to acquirer's host.

Terminals usually talk to acquirer's host in their special protocols: ATM, POS, SSD. But some are built over ISO8583.

NFC system uses devices: tags, smart cards, readers, mobile devices. Ans secures them by NFC Ready and NFC Secure; secure element; authentication; encryption. The secure element (SE) is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications (e.g., American Express, Discover, MasterCard, Visa and other payment applications). SEs can also support other types of secure transactions, such as transit payment and ticketing, building access, or secure identification.

Verified by Visa and MasterCard secure code. Banks worldwide are starting to authenticate online card transactions using the `3–D Secure' protocol, which is branded as Verified by Visa and MasterCard Secure Code. The primary purpose of 3DS is to allow a merchant to establish whether a customer controls a particular card number. It is essentially a single–sign on system, operated by Visa and MasterCard, and it differs in two main ways from existing schemes such as OpenID or InfoCard. First, its use is encouraged by contractual terms on liability: merchants who adopt 3DS have reduced liability for disputed transactions. Previous single sign–on schemes lacked liability agreements, which hampered their take–up. Few organizations are willing to trust a third–party service provider to authenticate users when they have no recourse in the event of error or attack. (In any case, security economics teaches that you're unlikely to get a secure system if Alice guards it while Bob pays the cost of failure.) Second, in other respects 3DS does not adopt the lessons learned from single–sign on, and breaks many established security rules [5].

Security vulnerabilities of chip and PIN. Chip and PIN is the brand name adopted by the banking industries in the United Kingdom and Ireland for the rollout of the EMV smart card payment system for credit, debit and ATM cards. The word "chip" refers to a computer chip embedded in the smartcard; the word PIN refers to a personal identification number that must be supplied by the customer. "Chip and PIN" is also used in a generic sense to mean any EMV smart card technology which relies on an embedded chip and a PIN.

The Chip and PIN implementation was criticized as designed to reduce the liability of banks in cases of claimed card fraud by requiring the customer to prove that they had acted "with reasonable care" to protect their PIN and card, rather than on the bank having to prove that the signature matched. Before Chip and PIN, if a customer's signature was forged, the banks were legally liable and had to reimburse the customer. Until 1 November 2009 there was no such law protecting consumers from fraudulent use of their Chip and PIN transactions, only the voluntary Banking Code. While this code stated that the burden of proof is on the bank to prove negligence or fraud rather than the cardholder having to prove innocence, there were many reports that banks refused to reimburse victims of fraudulent card use, claiming that their systems could not fail under the circumstances reported, despite several documented successful large–scale attacks[18].

Chip and PIN cards are not foolproof; several vulnerabilities have been found and demonstrated, and there have been large–scale instances of fraudulent exploitation. In many cases banks have been reluctant to accept that their systems could be at fault and have refused to refund victims of what is arguably fraud, although legislation introduced in November 2009 has improved victims' rights and put the onus on the banks to prove negligence or fraud by the cardholder. Vulnerabilities and fraud are discussed in depth in the main article.

Chip and PIN are broken. The central flaw in the protocol is that the PIN verification step is never explicitly authenticated. Whilst the authenticated data sent to the bank contains two fields which incorporate information about the result of the cardholder verification – the Terminal Verification Results (TVR) and the Issuer Application Data (IAD), they do not together provide an unambiguous encoding of the events which took place during the protocol run. The TVR mainly enumerates various possible failure conditions for the authentication, and in the event of success does not indicate which particular method was used [5].

At heart there is a protocol design error in EMV: it compartmentalizes the issuer specific MAC protocol too distinctly from the negotiation of the cardholder verification method. Both of the parties who rely on transaction authentication – the merchant and the issuing bank – need to have a full and trustworthy view of the method used to verify the cardholder; and because the relevant data cannot be collected neatly by either party, the framework itself is flawed [39].

A major contributing factor to the fact that these protocol flaws remained undiscovered is the size and complexity of the specification, and its poor structure.

Core protocol failures are difficult to fix. None of the security improvements already planned by banks will help: moving from SDA to DDA will not have any effect, as these are both methods for card authentication, which occurs before the cardholder verification stage. Neither will a further proposed enhancement – CDA (combined data authentication) – in which the

transaction authorization stage additionally has a digital signature under a private key held by the card.

Why cryptosystems fails in ATM. Nowadays, however, it is clear that ATM security involves a number of goals, including controlling internal fraud, preventing external fraud, and arbitrating disputes fairly, even when the customer's home bank and the ATM raising the debit are in different countries. Many organisations have no computer security team at all, and those that do have a hard time finding it a home within the administrative structure. The internal audit department, for example, will resist being given any line management tasks, while the programming staff dislike anyone whose role seems to be making their job more difficult.

Corporate politics can have an even worse effect, as we saw above: even where technical staff are aware of a security problem, they often keep quiet for fear of causing a powerful colleague to lose face [5].

2.4 E–commerce and Mobile Banking

The primary elements of mobile payments technology include NFC, SE, and TSM.

Under the typical scenario, NFC communications are established automatically when two compatible devices are brought within range of each other; however, the NFC technology in mobile computing and other devices used for mobile wallet transactions is typically tuned for a much shorter range, on the order of a few millimeters.

Since NFC offers no native encryption, mobile payments using NFC must be coupled with a Secure Element (SE) which is a cryptographic module in the mobile device. ISIS and MasterCard are leveraging the SIM approach while Google wallet is using phone that have built in modules. A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services [18].

The security risks associated with mobile devices are very similar to any other computing device with a few key exceptions:

- Mobile devices have a smaller form factor and therefore are more susceptible to loss or theft.
- Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way.
- Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life.

The key risks to the mobile device include:

- Malware.
- Malicious applications.
- Privacy violations relative to application collection and distribution of data.
- Wireless carrier infrastructure.
- Payments infrastructure/ecosystem.
- SMS vulnerabilities.
- Hardware and Operating System vulnerabilities.
- Complex supply chain and new entrants into the mobile ecosystem.
- Lack of maturity of Fraud tools and controls.

The mobile banking and payments ecosystem is complex and dynamic. It is not clear who will emerge as the winner(s) in the growing space from a financial services, application provider or technology perspective. Security and the perception of security will clearly play a role in who ends up dominating.
The protection of electronic commerce systems pulls together a lot of the topics. Failures come from misconfigured access control, implementation blunders, theft of network services, inappropriate use of cryptology—you name it.

3. Threats on E–payment Systems

3.1 Payment Systems

There is payment by instruction type of systems, when a payer basically orders the bank to move a sum of money from her account into a payee's account. Examples in this category are credit and debit cards as well as many forms of cheques. The moment at which the money is actually moved from the payer's account into the payee's account depends on the system, but at all times banks and credit card companies will try to prevent discrepancies between accounts. The central security aspect in these systems is to ensure that only legitimate account holders are able to issue payment instructions. Of course, digital signatures are the solution for doing this over a large, open network such as the Internet. Since digital signatures only make sense if there is an infrastructure for certifying public keys, a lot of effort is devoted to just this. See, for instance, the SET (Secure Electronic Transaction) proposal, a joint effort by MasterCard, VISA, and other influential partners, which specifies a hierarchy of certification authorities on top of the payment protocols [20]. Prepaid systems are conceptually close to electronic equivalents of cash. Telephone cards, smart card based systems, as well as

e–cash fall into this category. The user's account is debited as soon as the card or device is reloaded with electronic cash. During payments the electronic cash is released again, and only then the payee's account will be credited. In the meantime the issuer keeps a float corresponding to the outstanding cash. The central security aspect in this type of system is to ensure that cards or representations of cash cannot be forged. When forgery happens, the float will ultimately be insufficient to credit all of the payees' accounts for received payments. Of course, it should also be ensured that only legitimate account holders can reload cash from their accounts. However, this security aspect is now limited to the infrequent withdrawal protocol, and is no part anymore of the more frequent payment protocol.

Although the payment protocol is functionally a protocol between two parties (payer and payee) many payment systems require that the payee contacts a third party (e.g., the bank or the credit–card company acting as an acquirer) before accepting a payment. If that is the case, the system is called an on–line payment system; the communication between a payee and its acquirer may be using any communication medium (not necessarily the Internet). If such a contact with a third party is not required during the payment protocol, the system is called off–line. In an off–line system payees are required to contact their acquirer on a regular basis for clearing all received payments.

A basic requirement of a payment protocol is that it allows a payee to receive payments from any payer. A payment can be seen as some sort of authentication of the payer towards the payee (to show that the payment is authentic). Authentication can be based on secret key cryptography or on public key cryptography. In the latter case, the payee only needs to have a public key available in order to verify incoming payments. Although the costs of equipping smart cards with crypto co–processors are expected to become marginal, it is important to note that the property of public verifiability can be obtained using simple smart cards only, provided one applies a method of what we call signature transport. In such a system, signatures are created by the issuer only, and later endorsed by the payer during the payment protocol, depending on a challenge from the payee. The trick is to achieve that sufficiently many payments can be made between successive reloads, which requires optimal use of the limited amount of EEPROM available on simple smart cards. The added advantage is that the secret key for creating signatures is only used by the issuer. In case authentication is based on secret key (symmetric) cryptography, how– ever, the payer and payee must have a shared secret key available in order to complete a payment. A straightforward solution is to give all users the same secret key, but this is generally considered insecure, as this would mean that breaking a single smart card (i.e., extracting its secret key) will suffice to break the complete system. The standard solution is therefore to break the symmetry between payers and payees by equipping the merchants with a highly secure tamper–proof box called a SAM that contains a master key. The payers' keys are derived from this master key in a process called diversification by applying a cryptographic hash (e.g., SHA–1) to the concatenation of the master key and the payer's card number. The idea is that the SAM is more difficult to break than a smart card, and also that it is possible to routinely check (as part of the maintenance) if the SAMs have not been tampered with. In the EMV standard (developed by Europay, MasterCard, and Visa) a first step is made toward including public key authentication. To prevent frauds in which cards with fake card numbers are introduced, each card carries a fixed RSA certificate that shows the validity of the card number. At the start of each payment, the certificate can be verified against the public key stored in the POS terminal. The remainder of the payment protocol again relies on a secret master key stored in the SAM of the POS terminal. Checkout based on using electronic payment system consists of some typical steps. For example, if using PayPal, it starts when the button "Check out with PayPal" on page of the merchant website is clicked. Then user is directed to page on PayPal, where he can click the "Pay Now" button to pay. Then, the shopper's browser is redirected back to the merchant's website to finish the order, which usually does not require the shopper's actions. Finally, the shopper gets the confirmation page. The checkout process is arranged in this way to ensure that all three parties – the shopper, the e–payment system, and the merchant, stay consistent despite their different locations across the Internet.

Dynamic web are invoked through HTTP requests: the client sends an HTTP request through a URL with a list of arguments and receives an HTTP response (often a web page) dynamically constructed by the server as the outcome of the call. These responses serve as the building blocks for the workflows of various checkout solutions offered by different payment systems service providers (Amazon, PayPal, and Google). Some of the solutions, such as PayPal Standard and Amazon Simple Pay, are entirely based upon HTML, while the others, like PayPal Express and Checkout By Amazon, implement SOAP and NVP APIs. Also e–payment systems websites communicate exclusively over HTTPS to guarantee end–to–end security [21].

3.2 Technologies Used for Online Payment Security

There are a few different protocols that are used for online security today. The most common security mechanism is SSL. Some of the others include TLS, and SET.

Secure Sockets Layer, more commonly known as SSL, is a protocol that is used to maintain client and server

authentication. A site is easily identified as using SSL if it has the small yellow padlock at the bottom of the browser.

In SSL, communication between the server and the client is encrypted using their certificates. This encryption creates virtual information that is not hackable by others.

The purpose of SSL is to provide a means to allow secure communication between two parties. However, one party must have a certificate trusted by the other in order to help prevent man in the middle attacks. SSL also supports authentication, encryption and key exchange.

SSL uses a handshake protocol. Suppose a client wants to make a purchase from a website server, but this server does not know anything about the client.

SSL uses a key size of 40–bits for the RC4 stream encryption algorithm. This is considered a sufficient degree of encryption for commercial exchange. Both HTTPS and SSL support the use of X.509 digital certificates from the server. This way, the user can authenticate the sender if needed [23].

One of SSL's strengths is its ability to help prevent some common attacks. SSL is strong against the brute force attack because it uses 128 bits. The dictionary attack which tends to be more efficient than a brute force attack is where an attack tries every word in a dictionary as a possible password for an encrypted message. This attack is also avoidable because SSL has very large key spaces. The replay attack which reruns messages that were sent earlier is prevented since SSL uses 128–bit nonce value to indicate a unique connection. And as mentioned earlier, the Man–In–the–Middle Attack is prevented by using signed certificates to authenticate the server's public key.

Despite the fact that SSL has the ability to prevent some common attacks, it still has some weaknesses. One of the weaknesses found in SSL is the brute force attack against weak ciphers. This weakness was forced by the US export on Netscape. This weakness still remains one of the most obvious weaknesses of the SSL protocol and it has broken many times [20].

Another weakness in SSL is the renegotiation of the master key. It is known that after a connection has been established, the same master key gets used all the way through the connection. This could be a serious security flaw if SSL are layered underneath a long running connection. One possible solution for this flaw is to force renegotiation of the master key at different times. This way, the difficulty and the cost of the any brute force attack will be multiplied by the number of times that the master key has changed [20].

The Transaction Layer Security protocol, commonly known as TLS, is based on SSL and will soon become its successor. TLS has some changes in its MAC, has clearer and more precise specifications, cleaner handling because of not having a client certificate, and more flexibility.

Secure Electronic Transaction, SET, provides a way for the client's credit card number to be sent to authorizing banks. However, there was not enough market acceptance of SET to make it commonplace.

3.3 Bitcoin

Bitcoin is a peer–to–peer payment network and digital currency based on an open source protocol, which makes use of a public transaction log. Bitcoin was introduced in 2009 by pseudonymous developer "Satoshi Nakamoto". It is called a cryptocurrency because it uses public–key cryptography. When paying with bitcoin, no actual monetary exchange takes place between buyer and seller. Instead, the buyer requests an update to a public transaction log, the blockchain. This master list of all transactions shows who owns what bitcoins currently and in the past and is maintained by a decentralized network that verifies and timestamps payments using a proof–of–work system. The operators of this network, known as "miners", are rewarded with transaction fees and newly minted bitcoins [20].

In order to make a payment, a user requests an update to the master transaction list, the blockchain, and the transaction is validated by the network. Although transactions can be validated instantly, it takes bitcoin miners approximately 10 minutes to record the payment within the blockchain and confirm it was not spent twice. In addition, transactions that pay a fee may be processed more quickly [25].

Bitcoin functions using public–key cryptography, in which a user generates a pair of cryptographic keys: one public and one private. Only the private key can decode information encrypted with the public key; therefore the keys' owner can distribute the public key openly without fear that anyone will be able to use it to gain access to the encrypted information. An example public wallet (owned by the FBI) demonstrates its structure, a string of 34 numbers and letters (the private key, however, must be kept secret and secure) [15]. The public key can be used as an "address" to which other users can send bitcoins. Anyone wishing to use Bitcoin can create one or more Bitcoin addresses, which are collected and tracked in "wallets". Anyone can send bitcoins to the public address provided by the owner of the wallet, while the private key must be entered by the wallet owner to send bitcoins. Securing and protecting the private key is the essence of wallet security. If the private key for an address is not kept secret, the bitcoins may be stolen; theft has been documented on numerous

occasions, and the practical day–to–day security of Bitcoin wallets remains an on–going concern.

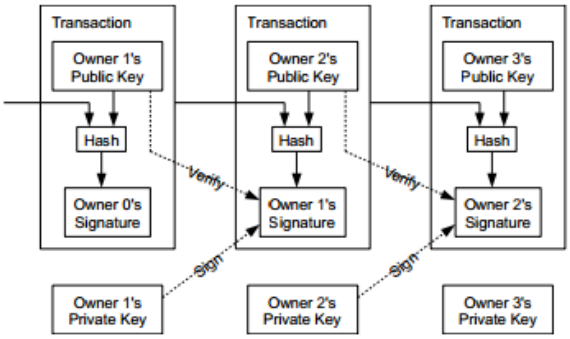

Fig. 1. Bitcoin payment processing (Source: http://en.wikipedia.org/wiki/Bitcoin)

3.4 NFC

Near field communication (NFC) is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than a few inches.

Near Field Communication is used mostly in paying for purchases made in physical stores or transportation services. A consumer using a special mobile phone equipped with a smartcard waves his/her phone near a reader module. Most transactions do not require authentication, but some require authentication using PIN, before transaction is completed. The payment could be deducted from a pre–paid account or charged to a mobile or bank account directly [26].

Mobile payment method via NFC faces significant challenges for wide and fast adoption, due to lack of supporting infrastructure, complex ecosystem of stakeholders, and standards. Some phone manufacturers and banks, however, are enthusiastic.

Losing the NFC RFID card or the mobile phone will open access to any finder and act as a single–factor authenticating entity. Mobile phones protected by a PIN code acts as a single authenticating factor. Lawfully opened access to a secure NFC function or data is protected by time–out closing after a period of inactivity. Attacks may happen despite provisions to shut down access to NFC after the bearer has become inactive. Additional features to cover such an attack scenario dynamically shall make use of a second wireless authentication factor that remains with the bearer in case of the lost NFC communicator. Relevant approaches are described as an electronic leash or its equivalent, a wireless key.

3.5 Heartbleed & Internet Explorer Vulnerability

The U.S. Department of Homeland Security is advising Americans not to use the Internet Explorer web browser until a fix is made for a serious security flaw that has been discovered. The flaw allows malicious hackers to get around security protections in the Windows operating system through a corrupted Adobe Flash file. Users can avoid the attack by turning off Adobe Flash through the Internet Explorer Setting or using other web browsers[32].

Also you may have seen recent news reports about a major security flaw discovered in "OpenSSL" – a commonly used Internet security technology. OpenSSL is used by many websites for encrypting personal data, communications and transactions. This security flaw was recently exploited by a software bug called "Heartbleed." Experts believe that Heartbleed has the capability to acquire user ID's, passwords and other personal information from websites using Open SSL. It is not yet known who's personal information may have been compromised or how much information was stolen[33].

4. Best Practices and Policies

4.1 Protecting E–commerce Bank and Credit Card Systems

The use of Transaction Authorisation Numbers (TAN) for signing transactions makes gaining access to accounts somewhat more complex. The TAN may come from a physical list issued to the account holder by the financial organisation or it may be sent via SMS. In either case, the cyber criminal does not have access to the TAN [8].

You can minimize your chances of being a victim of scams by:

- Typing actual web–site address into your Internet browser to log on to Internet Banking.
- Treating all emails requesting personal log on information such as username, password or PIN with extreme caution. Authentic BankMuscat emails will not request personal details or log on information.
- Immediately deleting emails of unknown origins, no matter how innocent or provocative the subject headings sound.
- Changing your Internet Banking password on a regular basis.
- If you receive an email requesting you to register or enter sensitive details, not responding and click on any hyperlink. Immediately forward the email to bank [10].
- Not using computers to access accounts which are not trusted (like don't use cybercafe, or other people's computers for accessing Online Banking).

- Keeping antivirus software updated every day to protect your system and ensure that your system is virus free.
- Not downloading spyware onto your computer, devices.
- Installing anti−virus software, and keeping it updated with the latest virus definitions.
- Downloading and installing security patches for your operating system as soon as they become available.
- Not accepting attachments from emails of unknown sources.
- Installing software from trusted sources only[5] .

Ways to improve chup security:

- turn some ROM areas into reprogrammable Flash areas;
- reprogram low−level features;
- access shadow areas;
- access hidden JTAG registers;
- find the JTAG registers responsible for controlling read sense;
- amplifiers, such that VREF can be adjusted [16].

The hardware security protection in Actel ProASIC3 FPGAs is under serious threat due to unforeseen problems in the corporate security strategy of the management team. Access path to shadow hardware features brings capability of making ProASIC3 chips more robust and serve security critical applications for the next few years. Embedded memory is more secure than encrypted external memory storage, and encrypted bitstream is even less secure.

Credit card duplication and crime prevention using biometrics. Until the introduction of Chip and PIN, all face−to−face credit or debit card transactions used a magnetic stripe or mechanical imprint to read and record account data, and a signature for verification. Under this system, the customer hands their card to the clerk at the point of sale, who either "swipes" the card through a magnetic reader or makes an imprint from the raised text of the card. In the former case, the account details are verified and a slip for the customer to sign is printed [5]. In the case of a mechanical imprint, the transaction details are filled in and the customer signs the imprinted slip. Fingerprints are one of many techniques used to identify individuals and verify their identify. Matching algorithms used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. Pattern based algorithms compare the basic fingerprint patterns (arch, whole, and loop) between a previously stored template and a candidate fingerprint [17].

4.2 Authentication Solutions for E−commerce and E−banking

There is a wide variety of Two−Factor Authentication solutions, including:

- One Time Password (OTP).
- Double Authentication.
- Challenge−response.
- Sign−What−You−See.
- Secure Domain Separation.
- Dynamic Signatures.
- Electronic Signatures.

For example, the Mobile Solution is a set of different technologies allowing authentication to be performed through already existing infrastructures. As part of the secure devices family they emphasize different capabilities with respect to security, usability and the look & feel experience. The set of media utilized offer different solutions in terms of service activation – all easy and cost effective, ranging from self−activation to Over The Air activation (OTA) [5].. The Mobile Solution enables PIN protected One Time Passwords (OTP), Signatures, Challenge/Response functionality and other services in strong Two−Factor Authentication schemes [5].

4.3 Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q−R Code

While implementing online banking system, secure data transfer need can be fulfilled by using https data transfer and database encryption techniques for secure storage of sensitive information. To eliminate threat of phishing and to confirm user it's proposed to use concept of QR−code with android application. QR−code which would be scanned by user mobile device which overcome the weakness of traditional password based system. The security was improved by using one time password (OTP) which hides inside QRcode [34]. But the importance of security and ease of use is like two side of a coin. It cannot be provided considering that show up on one side. Therefore, we should always seek for safety devices to meet all ease and security of electronic financial services.

4.4 Multi−Factor Authentication for Era of Zero Trust

But knocking just as insistently are hordes of cybercriminals who build lucrative businesses out of nothing more than illicit access to your data, transactions and information. The largest U.S. bank websites are faltering under sustained attacks and regulators have recently warned institutions to "undertake a complete overhaul of their security infrastructure" because of the newly discovered "Heartbleed" bug. Even when the wire room's computers recognize PINs and passwords, they say nothing about the person entering them, and the FBI warnings are about stolen credentials. As a result, banks are increasingly turning to passive authentication methods over which the user has no control or even awareness of being subjected to, such as biometrics that

recognize the user's keystroke cadence, pressure, and latency.

Security officials may have "zero trust" but obviously that's not what you want to convey to your best customers! As wealth management customers increasingly lobby to perform much of their work online and on mobile, their large transactions will make them attractive cybercrime targets. That means striking a fine balance on the trust meter. First, show the customer that you care about their security – that they can trust you to keep their funds safe. Conspicuous authentication does that. Then they want you to show that you trust them by making sure their self–authentication is not too onerous but still effective. And finally there is the need to make both shows of trust rapid and convenient. Reliable security does more than protect. It lets banks enrich the customer experience. For example, imagine if, when your affluent customer visits the branch, your facial recognition technology authenticated him immediately, with the system then prompting your customer service rep to quickly research questions that customer normally asks, pull up the customer's accounts, and be fully prepared for the customer by the time he reaches her office. To make customers comfortable with such methods, you can offer these kinds of services as perks and obtain their informed consent in advance [35].

4.5 New Recommendations and Solutions from PayPal

PayPal welcomes the opportunity to share its experience gained from 15 years of successful activity in the payments business. PayPal is the world's largest PSP to never suffer a major breach of customer information. PayPal records best–of–class fraud losses while simultaneously setting the industry standard for growth/market adoption through an efficient customer security experience. PayPal is therefore eager to share these insights with the ECB to identify and discourage fraudulent transactions and would like to provide alternative suggestions for an effective and innovative regulatory framework for the ECB to consider as the basis for a review of its recommendations. PayPal strongly encourage the ECB to promote the use of back–end risk–based authentication capabilities. These capabilities allow PSPs to dynamically select the most effective authentication challenge for any given authentication context. Risk–based authentication capabilities are not the same as standard fraud monitoring. Most anti–fraud monitoring capabilities are initiated after an authentication event. Risk–based authentication is the ability to leverage a variety of factors, including but not limited to device recognition, in a combinatorial scheme that is spoof–resistant and highly effective when combined with one or more shared secrets. PayPal also suggest making use of innovative authentication factors to better achieve the ECB's objective of strong customer authentication.

Leveraging instead of back–end risk–based capabilities, such as recognition of the consumer computer (one of many assessment tools for establishing a trust score for the authentication context), along with occasional use of SMS authentication when users enrol a new computer as a strongly authenticated trusted device, will significantly improve protection and reliability as the end user is successfully recognised as long as she either has access to either the same computer or phone as previously used. This approach also simplifies user experience and permits the addition of other user–facing security measures. PayPal would therefore like to present an alternative, forward–looking framework for a harmonised minimum level of security best practice that will reduce the risk of information and financial loss for PSP customers.

One core element of such an innovative framework is an alternative definition of strong customer authentication, based on the ability to empirically protect the customer from harm. Another central feature is the fourth authentication factor which leverages current and emerging technologies to assess "something consistently associated with the user" (aka "something you do"). This requires back–end risk–based authentication capabilities to make dynamic decisions concerning the most effective authentication techniques in any particular authentication context. It also highlights the need for PSPs to invest in innovation as regards authentication challenges so as to fend off organised crime.

As the ECB considers single–factor authentication, as only control mechanism, inadequate for transactions involving access to customer information or movement of funds to other parties, PSPs should use effective methods to authenticate the identity of the customers using their products and services. The authentication techniques employed by the financial institution must be appropriate to the associated risks of harm to the customers. Financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

A regular risk–assessment update is of utmost importance given the speed of technological progress. In addition, the strong authentication procedure should be designed so as to mitigate the risks related to the confidentiality of the authentication data. This must be in combination with back–end risk–based authentication capabilities which enable a dynamic selection of the appropriate authentication challenge, based on a dynamic risk assessment of the respective authentication context [36].

5. Conclusions

Assessing the security of Internet banking applications requires specialized knowledge on vulnerabilities,

attacks and countermeasures, to gain an understanding of the threats, how they are realized and how to address them. The case study in this article demonstrated that the use of the attack tree should facilitate the work of auditors, security consultants or security officers who wish to conduct a security assessment of an Internet banking authentication mechanism.

We presented our analysis of banking and modern payments system security, E–payment, as an example of security challenges in third–party service integration. We found serious logic flaws in leading online, mobile, e–commerce etc. banking applications, leading merchant applications, popular online stores and payment providers (i.e., PayPal). We discussed the weaknesses in the systems that can compromise the customer's trust. Although, we showed and analyzed ways of defense from security threats.

Most of the problems facing online businesses are no different from those facing other organizations, and the network security risks are not much different from those facing traditional businesses. The real increased risks to an e–banking have to do with ways in which traditional risk management mechanisms don't scale properly from a world of local physical transactions to one of worldwide, dematerialized ones. Credit card transaction repudiation is the main example at present. There are also significant risks to rapidly growing companies that have hired a lot of new staff but that don't have the traditional internal controls in place.

Web applications increasingly integrate third–party services. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet. Online payments through are relatively safe because they use SSL technology which is the safest mechanism being used today or another secure methods (for example, using public–key cryptography). But the problem is the SSL protocol is not flawless, and users who see the yellow padlock at the bottom of the browser may get a false sense of security. Also there are always some flaws in security methods. But in reality, the security of online payment also depends on the customer himself. He should gain knowledge in how to use the internet so that he can be more aware of email scams and website URLs that may not be from payment system website. For example for PayPal users, the lack of knowledge and common sense appears to have caused more problems than insecurity. However, there probably is no best way to be fully secured other than to just avoid online purchases altogether. We believe that our study takes some steps in the banking security problem. We analyzed payments security, found problems, analyzed existing security solutions and proposed new ways to solve payments security. They are more effective and up–to–date. In future work we are considering the security challenges that come with new banking payment systems, web service integrations in other scenarios, e.g., social networks and web authentication services, cancel, return flows.. Fundamentally, we believe that the variety and changes of banking systems demands new security approaches and research efforts on ensuring the security quality of the systems it produces.

References

[1] Anderson, R.J., Needham, R.M. Robustness principles for public key protocols. CRYPTO 1995. LNCS, vol. 963, pp. 236–247 (1995).

[2] Cyber attacks against banks more severe than most realize. Internet: http://www.reuters.com/article/2013/05/18/us–cyber–summit–banks–idUSBRE94G0ZP20130518 (2014).

[3] APACS: Online banking usage amongst over 55s up fourfold in five years. Internet: http://www.apacs.org.uk/media_centre/press/08_24_07.html (Aug, 2007).

[4] APACS announces latest fraud figures. Internet: http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm (Sep, 2008).

[5] Adam Ali.Zare Hudaib. Banking and modern payments system security analysis. International Journal of Computer Science and Security (IJCSS), vol. 8, issue 2 (2014).

[6] Taylor, M. Police think French pair tortured for pin details. The Guardian. Internet: http://www.guardian.co.uk/uk/2008/jul/05/knifecrime.ukcrime (Jun, 2008).

[7] Finn, C. MTN not budging on fraud issue. IOL technology. Internet: http://www.ioltechnology.co.za/article.page.php?iSectionId=2885&iArticl%eId=4402087 (May, 2008).

[8] Make Card Readers Optiona. Internet: http://www.stopthecardreaders.org/ (2008).

[9] Cronto: Products datasheet. Internet: http://www.cronto.com/download/Cronto_Products_Datasheet.pdf (2010).

[10] Choudary, O. The smart card detective: a hand–held EMV interceptor. Master's thesis, University of Cambridge. Internet: http://www.cl.cam.ac.uk/~osc22/scd/ (June 2010).

[11] CreditCall. EMV.LIB Integration Guide. Internet: http://www.level2kernel.com/emvlibfidocumentation.html (June, 2010).

[12] de Ruiter, J., and Poll, E. Formal analysis of the EMV protocol suite. Theory of Security and Applications (TOSCA 2011), vol. 6693 of LNCS, Springer, pp. 113–129 (March, 2011).

[13] EMVCo. Terminal level 2, test cases. Type Approval (Nov, 2011).

[14] Murdoch, S. J. Reliability of chip & PIN evidence in banking disputes. Digital Evidence and Electronic Signature Law Review, vol. 6, Pario Communications, pp. 98–115 (Nov, 2010).

[15] Murdoch, S. J., Drimer, S., Anderson, R., and Bond, M. Chip and PIN is broken. IEEE Symposium on Security and Privacy (Oakland) (May, 2010).

[16] Needham, R. M., and Schroeder, M. D. Using encryption for authentication in large networks of computers. Commun. ACM 21, pp. 993–999 (Dec. 1978).

[17] 3–D Secure system overview. Internet: https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=119 (2011).

[18] RBS Secure Terms of Use. Internet: https://www.rbssecure.co.uk/rbs/tdsecure/terms_of_use.jsp (Dec, 2009).

[19] Cronto. Internet: http://www.cronto.com/download/Cronto_Products_Datasheet.pdf (2012).

[20] Adam Ali.Zare Hudaib. E–payment Security Analysis In Depth. International Journal of Computer Science and Security (IJCSS), vol. 8, issue 1 (2014).

[21] S. Murdoch and R. Anderson. Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication. Financial Cryptography and Data Security, Jan. 2010, pp. 42–45.

[22] PayPal. PayPal – Data Security and Encryption. Internet: http://www.paypal.com/cgi–bin/webscr?cmd=p/gen/security–outside (Dec, 2013).

[23] Rui Wang, Shuo Chen, XiaoFeng Wang, Shaz Qadeer. How to Shop for Free Online Security Analysis of Cashier–as–a–Service Based Web Stores. Internet: http://research.microsoft.com/pubs/145858/caas–oakland–final.pdf (Dec, 2013).

[24] The Secure Sockets Layer Protocol. Internet: http://www.cs.bris.ac.uk/~bradley/publish/SSLP/chapter4.html (Nov, 2013).

[25] SearchSecurity.com. Internet: http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci214006%2C00.html (Dec, 2013).

[26] Alex Hern. Bitcoin me: How to make your own digital currency. Internet: http://www.theguardian.com/technology/2014/jan/07/bitcoin–me–how–to–make–your–own–digital–currency (Dec, 2013).

[27] Bitcoin. Internet: http://en.wikipedia.org/wiki/Bitcoin.html (Dec, 2013).

[28] Bitcoins. Internet: http://www.weusecoins.com/en/ (Dec, 2013).

[29] Near field communication. Internet: http://en.wikipedia.org/wiki/Near_field_communication (Dec, 2013).

[30] Mike Clark. Inside Secure adds sales agents. Internet: http://www.nfcworld.com/2012/12/05/321436/inside–secure–adds–sales–agents (Dec, 2013).

[31] NFC and Contactless Technologies. Internet: http://nfc–forum.org/what–is–nfc/about–the–technology/ (Dec, 2013).

[32] Important Information Regarding Use of the Microsoft Internet Explorer Web Browser. Internet: http://www.consumer.ftc.gov/articles/0155–free–credit–reports (2014).

[33] Heartbleed. Internet: http://heartbleed.com (2014).

[34] Abhishek Gandhi. Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q–R Code. International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, pp. 1327–1329.

[35] Terry Hartmann. Multi–Factor Authentication for Era of Zero Trust. Internet: http://www.bai.org/bankingstrategies/Risk–Management–and–Fraud/Security/Fraud/Multi–Factor–Authentication–for–Era–of–Zero–Trust (Apr, 2014).

[36] Response to the European Central Bank – Recommendations for the Security of Internet Payments. Internet: ttp://www.ecb.europa.eu/paym/pol/activ/instr/shared/files/PayPal.pdf (2014).