Banking and Modern Payments System Security Analysis

Adam Ali.Zare Hudaib *adamhudaib@gmail.com*
Licensed Penetration Tester EC-Council
Certified Ethical Hacker EC-Council
Certified Security Analyst EC-Council
Wireshark Certified Network Analyst (Wireshark University)
CEH , ECSA , LPT , WCNA
Sweden

Abstract

Cyber-criminals have benefited from on-line banking (OB), regardless of the extensive research on financial cyber-security. To better be prepared for what the future might bring, 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 analyzed banking and modern payments system security.

In this research we will review different payment protocols and security methods that are being used to run banking systems. We will 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 will also discuss the weaknesses in the systems that can compromise the customer's trust.

Keywords: Banking Security, Authentication, Chip and PIN, ATM .

1. INTRODUCTION

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 defenses 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 defenses 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.

2. BANKING SECURITY

When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some essential level of security must be established before business on the internet can be reliably conducted. An attack might be in the form of unauthorized access, destruction, corruption or alteration of data or any type of malicious procedure to cause network failure, reboot or hang. Modern security techniques have made cracking very tedious but not impossible. Furthermore, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide array of information regarding security hole and their fixes is freely available on the web.

2.1 Banking Security Architecture

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.

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 [2].

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 [3], 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 [4].

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.

Example of banking security architecture is shown on figure 1.

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].

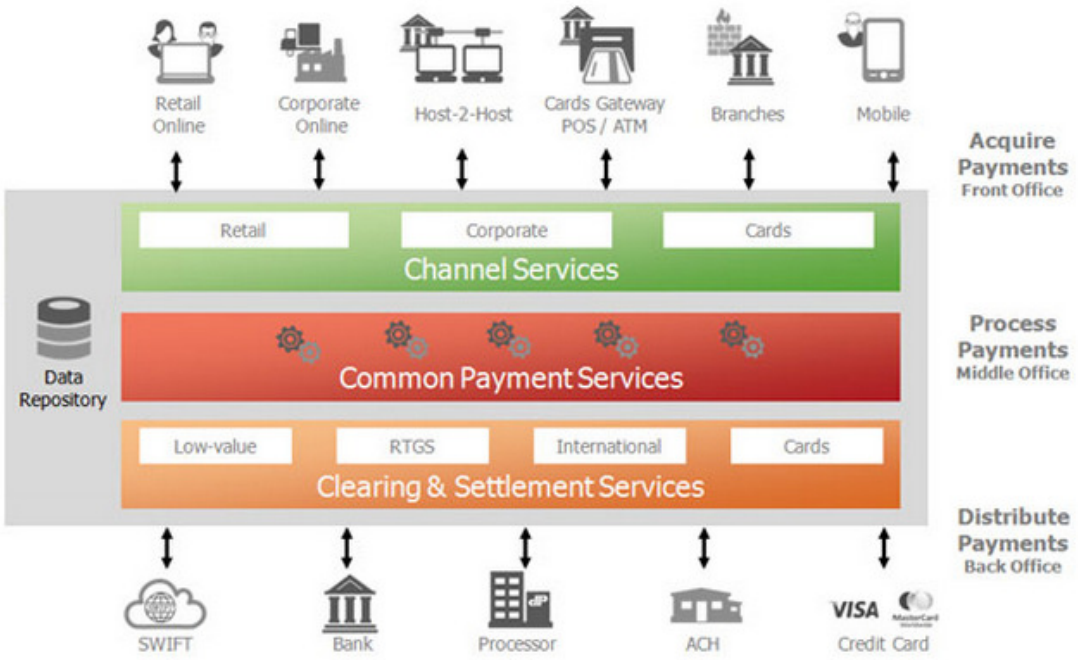

FIGURE 1: Banking Security Architecture.

2.2 Banking Security Attacks and Defense

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].

In order to sidestep this, cyber criminals have taken to using 'money mules'. Mules are often recruited via seemingly legitimate job offers – for instance, the cyber criminals might advertise for

a 'financial manager'. Such services are used because they guarantee anonymity, reducing the likelihood that the cyber criminal will be caught. The remaining funds are the mule's 'commission' – naturally money which has been earned illegally via phishing or financial malware.

When looking at the question of phishing, it's important to have a clear definition of it. This article defines phishing as spoofed messages which allegedly come from a (financial) organization and which are designed to trick the user into giving up confidential information. This is strictly a matter of social engineering, and once malware is involved, the attack can no longer be considered phishing.

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.

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]. In most cases, malware used will capture the information entered by the user in a way similar to that described above. Once the user enters the TAN, the malware will intercept this information and either display a fake error message, or send an incorrect TAN to the financial site. This may result in the user entering another TAN. An organization may require two TANS to complete a transaction – this depends on the organization and the security systems it has decided to implement. If only one TAN is required to make a transaction, the attack describe above could allow a cyber criminal to make two transactions.

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.

More sophisticated malware will use a MitM attack; this not only enables cyber criminals to attack more banks, but also ensures a higher return, as data is processed in real time. A MitM attack uses a malicious server to intercept all traffic between the client and the server i.e. the customer and the financial organization. Although everything will seem normal to the user, when s/he is asked to authorize a transaction, s/he is actually authorizing a transaction created by the cyber criminal. Malware which uses a MiTM attack typically either hides browser notifications about false web site certificates or, more commonly, shows a fake notification. However, depending on the approach used by the malware, it may do neither of these things, simply because it isn't necessary. A lot of the more sophisticated financial malware which uses MitM attacks also makes use of HTML injection [9].

However, there's a clear trend: the increased usage of two-factor authentication by financial organizations has resulted in an increase in malware capable of defeating this type of authentication. This means that the eventual adoption of two-factor authentication will not have any significant long-term effect. It will simply raise the benchmark for financial malware.

Nonetheless, there is a fundamental problem with two-factor authentication, namely that though the session may be secure, whatever happens during that session goes unchecked. In order to increase security, some additional form of communication, such as the use of a cryptographic token or SMS messages (already implemented by some financial institutions) is required. SMS messages could set limits on the lifetime of the TAN, the account numbers being accessed and the maximum permissible transaction amount.

2.3 Internet Banking Authentication and Attacks

The most recent internet banking security threats are listed below:

– Phishing
– Spyware and Adware
– Viruses
– Trojans
– Keyloggers

The attack tree has one root node, representing the final target of the attacker, which is the compromise of the user's bank account. An intruder may use one of the leaf nodes as a means for reaching the target. To categorize Internet banking attacks, each component of the process should be examined: the user terminal/user (UT/U), the communication channel (CC) and the Internet banking server (IBS). The following types of attacks are identified [10]:

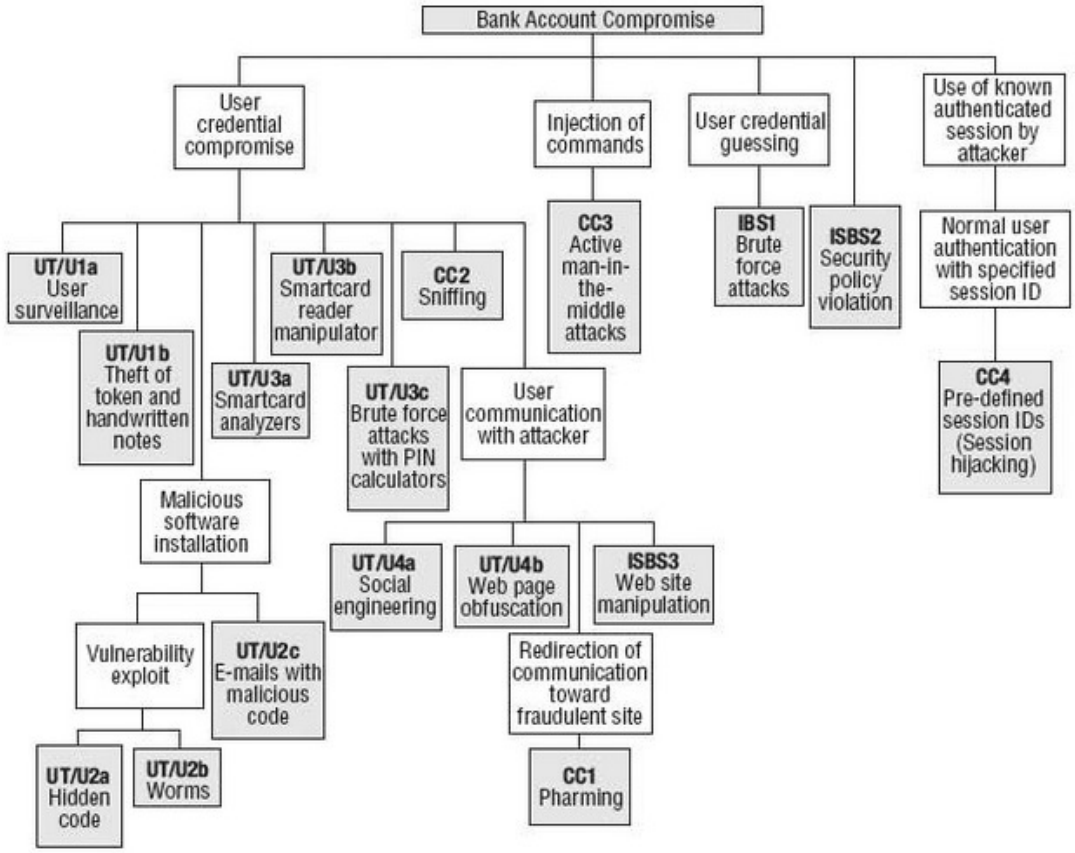

FIGURE 2: Attacks and Threats Models.

Phishing 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.

You can minimize your chances of being a victim of Phishing 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, do not respond and click on any hyperlink. Immediately forward the email to bank [11].

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 [12]. 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.

You can minimize your chances of unintentionally downloading spyware onto your computer, devices.

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.

You can increase your chances of ensuring your computer is free from viruses by:

– 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.

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. You can minimize your chances of unintentionally downloading Trojans [130].

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.

There are ways to prevent this from happening.

– You should not use computers to access accounts which are not trusted (like don't use cybercafe, or other people's computers for accessing Online Banking).
– Keep antivirus software updated every day to protect your system and ensure that your system is virus free.

IBS attacks
These types of attacks are offline attacks against the servers that host the Internet banking application. Examples include:

– IBS1: Brute-force attacks in certain password-based mechanisms are reported to be feasible by sending random usernames and passwords. The attacked mechanisms implement a scheme based on guessable usernames and four-digit passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based calculation. This attack may be combined with username filtering methods for determining the identity of the user. These methods filter the different responses of the server, in the case of valid or invalid usernames.

– IBS2: Bank security policy violation—Violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.

IBS3: Web site manipulation—Exploiting the vulnerabilities of the Internet banking web server may permit the alteration of its contents, such as the links to the Internet banking login page. This may redirect the user to a fraudulent web site where his/her credentials may be captured [14].

3. PAYMENTS SECURITY

3.1 Banking Security Architecture

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. Such devices were foreseen by the EU Electronic Signature Directive which provided for signatures thus created to be admissible as evidence in legal proceedings. However such devices typically cost $100 or more.

The Chip Authentication Programme (CAP) [15]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 [16].

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. Using EMV as the basis for CAP reduced development and deployment costs; using the existing debit card base meant that the CAP devices themselves did not need to be personalized.

The reader requests a list of all the data records stored by a card. These form a hierarchy, with each node being prefixed by a one or two byte tag. In a standard EMV transaction, these would include account number, public key certificates, signatures, and so on. With CAP, only three entries are of interest – the card data object lists (CDOL1 and CDOL2), identified by tags 0x8C and 0x8D respectively, and the CAP bit filter2, identified by the tag 0x9F56. Tag 0x9F55 is also present on cards, with value 0xA0, but its purpose is unclear.

PIN verification. Once the reader has successfully read all available records, it prompts the customer for a 4-digit PIN. This is sent to the card as the payload to the EMV standard VERIFY command. If three consecutive PIN verifications fail, the card will lock itself until taken to an ATM and reset with the correct PIN. While the EMV standard allows for a transaction to continue if the PIN verification fails or is omitted, the CAP reader requires that the card accept the PIN before continuing [17].

Cryptogram generation. Next, the reader requests an application cryptogram from the card, using the GENERATE AC command. The reader first requests an Authorization Request Cryptogram (ARQC), indicating that it wishes to perform an online EMV transaction. The card then responds with an ARQC, indicating that the card is willing to do so. If this was an EMV transaction, the reader would send the ARQC to the bank for verification, but it cannot do so because it is offline. So the reader then requests an Application Authentication Cryptogram (AAC), indicating that it wishes to cancel the transaction.

A similar transaction flow might be seen during a point-of-sale transaction if a shop is only willing to accept online transactions but fails to connect to the bank (e.g. if the phone line is engaged). This protocol may have been designed so that CAP maintains maximum compatibility with EMV smart card applications. While EMV supports offline transactions by requesting a Transaction Certificate (TC) instead of an ARQC, some card risk-management algorithms may lock up if there are too many consecutive offline attempts. Cancelling the transaction should reset the smart card’s risk-management parameters [18].

Reader response formatting. The response to a GENERATE AC call includes a 16- bit application transaction counter (ATC), a Cryptogram Identification Data (CID) type code, Issuer Application Data (IAD) which includes the result of the PIN verification, and an Application Cryptogram (AC) which is a MAC over all this data. The MAC method used to calculate the cryptogram, and the structure of the IAD, are not specified by the EMV standard, as they are proprietary to the card issuer [19].

The basic principle behind CAP – a trusted user interface and secure cryptographic microprocessor – is sound. However the system has been optimized literally to death. Re-using ATM cards for point of sale and CAP saved money but created a vulnerability to relay attack, and increased the risk of violent mugging and murder. Omitting a server-provided nonce removed assurance that responses are freshly generated. Overloading fields introduce a social engineering vulnerability, as it makes the system model too complex for the average user to be expected to visualize.

3.2 Chip and Skim Cloning EMV Cards with Pre Replay Attack

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 [20].

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.

EMV did not cut fraud as its proponents predicted. While using counterfeit and stolen cards did become more difficult, criminals adapted in two ways. First, they moved to “card-not-present" transactions (Internet, mail-order, and phone-based payments) which remained beyond the scope of EMV. Second, they started making magnetic-strip clones of EMV cards. There had always been some ATM “skimming" where crooks put devices on ATM throats to capture card data and record PINs; and now that PINs were demanded everywhere and not just at ATMs, the opportunities for skimming increased hugely. The simultaneous deployment of EMV with magnetic strip meant that fallback and backwards-compatibility features in EMV could be exploited; for several years, all ATMs would still accept mag-strip cards, and even once this started to be phased out in the UK for locally-issued cards, it was still possible to use mag-strip clones of UK cards in ATMs in the USA. This is why, soon after the completion of the UK EMV roll-out in 2005, counterfeit fraud went up. Instead of entering PINs only at ATMs, customers were now entering their PIN in POS terminals, which are much easier to tamper with [21].

Total fraud levels were brought down following 2008 through improvements to back-end fraud detection mechanisms which reject suspicious transactions; by more aggressive tactics towards customers who dispute transactions; and by reducing the number of UK ATMs that accept “fallback" magnetic-strip transactions on EMV-issued cards [22]. Fallback fraud is now hard enough to push the criminal community to more sophisticated smart-card-based attacks.

Prior research showed that it was possible to use a stolen EMV card in a POS device without knowing the PIN. Given a suitable man-in-the-middle device, a crook can trick the terminal into believing that the right PIN was entered, while the card thought it was authorizing a chip-and-signature transaction; criminals have now gone on trial in France for exploiting this “no pin" vulnerability.

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) [23].

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

Malware. There are already numerous cases of malware-infected ATMs operating in Eastern Europe and depending on the internal architecture of the ATM it may be easy for such malware to sabotage the choice of UN. In fact one bank suggested to us that the ATM that kicked of this whole research project may have been infected with malware.

Supply chain attacks. Such attacks have already been seen against POS terminals in the wild, and used to harvest magnetic strip data. So it is feasible that a criminal (or even a state-level adversary) might sabotage the RNG deliberately, either to act predictably all the time, or to enter a predictable mode when triggered via a covert channel. A suitably sabotaged RNG would probably only be detected via reverse engineering or observation of real world attacks.

Collusive merchant. A merchant might maliciously modify their EMV stack to be vulnerable, or inject replayed card data into the authorization/settlement system. He could take a cut from crooks who come to use cloned cards at their store, or just pre-play transactions directly. In the UK, there was a string of card cloning attacks on petrol stations where a gang bribed store managers to look the other way when PIN pads were tampered with and monitoring devices inserted into network connections; exactly what you need to deploy a pre-play attack. Terminal cut-out. A variant is the terminal cut-out or bypass is where the transaction stream between the merchant terminal and the acquirer is hacked to misreport the unpredictable number when triggered by a particular signal (e.g. a particular account number or a known ARQC). This transaction data stream is not normally considered sensitive within the threat model and can be altered at will by merchant software. The attackers' card performing the replay can then use any UN for which it has an ARQC, and the true random UN made up by the terminal will never see the light of day. This is hard to block: there is no provision in currently deployed EMV cards for the terminal to confirm that its choice of UN was correctly included in the cryptographic MAC. The terminal cut-out could be implemented in malware (and there's evidence of bank botnets looking for POS devices), or in a merchant's back-end system (we have evidence of merchants already tampering with transaction data to represent transactions as PIN-verified when they were not, so as to shift liability) [24].

UN modification in the network. A man-in-the-middle device between a POS device and the acquiring bank, perhaps at a network switch, would also be a good way to deploy such an attack. This could be an attractive way to attack merchants that process high- value transactions, such as jewelers or investment firms, who might guard their premises and take care of their POS equipment yet still fall to a targeted attack. A pre-play attack would be much harder to detect than old-fashioned attacks that just convert deny authorization messages into approve messages.

3.3 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).

Ways to improve 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 [25].

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. 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.

3.4 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) [26].
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.

Transaction phases are shown below:

– Authorization
  Terminal reads card. If cardholder enters PIN, terminal calculates a PIN Block inside PED and PIN Block is encrypted under corresponding TPK. Auth message is sent to Acquirer's host. Acquirer processes it and sends to IPS. IPS processes it and sends to Issuer. Issuer approves or rejects it and sends the answer back.

– Clearing
  Consists of: terminal reconciliation; acquirer demands satisfaction from the issuer and sends the clearing presentments through the IPS; IPS processes them and sends them to

the Issuer; issuer may not respond, money transfer is automatically performed at the next stage.

– Settlement;
All parties settle their financial positions through the IPS (consolidated funds transfer).

– Dispute resolution.
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.

3.5 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. This has been partly driven by the sharp increase in online fraud that followed the deployment of EMV smart cards for cardholder-present payments in Europe and else- where. 3-D Secure has so far escaped academic scrutiny; yet it might be a textbook example of how not to design an authentication protocol. It ignores good design principles and has significant vulnerabilities, some of which are already being exploited.

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 [27].

Before 3DS can be used to authenticate transactions, cardholders must register a password with their bank. A reasonably secure method would be to send a password to the customer's registered address, but to save money the typical bank merely solicits a password online the first time the customer shops online with a 3DS enabled card known as activation during shopping (ADS). To confirm that the customer is the authorized cardholder, the ADS form may ask for some weak authenticators (e.g. date of birth), although not all banks do even this. From the customer's perspective, an online shopping website is asking for personal details.

The 3DS specification only covers the communication between the merchant, issuer, acquirer and payment scheme, not how customer verification is performed. This is left to the issuer, and some have made extremely unwise choices. For instance, one bank asks for the cardholder's ATM PIN. It's bad enough that EMV has trained cardholders to enter ATM PINs at terminals in shops; training them to enter PINs at random e-commerce sites is just grossly negligent.

Another issuer-specific choice is how to reset the password when a customer forgets it; here again corners are cut. Some banks respond to one or two failed password attempts by prompting an online password reset using essentially the same mechanisms as ADS. In a number of cases,

the bank requires only the cardholder's date of birth, which is easily available from public records; with one (UK-government-owned) bank, two wrong password attempts simply lead to an invitation to set a new password [28].

A third variable factor is whether the 3DS implementation asks for a whole password or for some subset of its letters. The idea behind asking for a subset is that a single-round keyboard logging attack does not compromise the whole password. However, this compels users to select relatively simple passwords, and probably to write them down.

3.6 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 [29]. In the case of a mechanical imprint, the transaction details are filled in and the customer signs the imprinted slip. In either case, the clerk verifies that the signature matches that on the back of the card to authenticate the transaction. This system has proved to be ineffective, because it has a number of security flaws, including the ability to steal a card in the post, or to learn to forge the signature on the card. More recently, technology has become available on the black market for both reading and writing the magnetic stripes, allowing cards to be easily cloned and used without the owner's knowledge. 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. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. The major disadvantage here is that Finger print authentication cannot be successful if the user has a band aid on his finger. Another disadvantage is fingerprint remains the same even if the person is unconscious or dead. This leads to unauthorized use of a person's fingerprint without his consent. To overcome the limitations of the existing authentication systems of the usage of credit cards, there was proposed a new system of authentication in which authentication is done through two phases. The first phase is verifying the identity of the user using iris recognition and the second phase is the authentication using palm vein technology [30].

Initially the user will be asked to insert his card. The database is checked to verify if such an account exists. If exists, the user will be authenticated using iris recognition. If the user is authenticated in this phase, he will then be asked to stretch out his palm for the vein pattern authentication. This is compared with the stored pattern and if it matches the user is, authenticated.

Users today mostly use textual passwords that follow an encryption algorithm. Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc.

A typical iris recognition system in involves three main modules:

– Image acquisition is to capture a sequence of iris images from the subject using a specifically designed sensor.

– Preprocessing Stage includes determining the boundary of the iris within the eye image, and extracts the iris portion from the image to facilitate its processing. It includes various stages such as: iris segmentation, iris normalization, image enhancement.

– Feature extraction and encoding is the most key component of an iris recognition system and determines the system's performance to a large extent. Iris recognition produces the

correct result by extracting features of the input images and matching these features with known patterns in the feature database.

Users today mostly use textual passwords that follow an encryption algorithm. Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play. Therefore, we use Biometrics in our authentication, which is more customizable and very interesting way of authentication. The vein matching, also called vascular technology is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin. An individual first rests his wrist, on some devices, such that the palm is held centimeters above the device's scanner, which flashes a near- infrared ray on the palm [31].

Unlike the skin, through which near-infrared light passes, deoxygenated hemoglobin in the blood flowing through the veins absorbs near-infrared rays, illuminating the hemoglobin, causing it to be visible to the scanner. Arteries and capillaries, whose blood contains oxygenated hemoglobin, which does not absorb near- infrared light, are invisible to the sensor. The still image captured by the camera, which photographs in the near- infrared range, appears as a black network, reflecting the palm's vein pattern against the lighter background of the palm.

3.7 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 [32].

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.

3.8 Synthetic PIN For Authentication and Authorization

There is a new technology that is used for authenticating users and authorising transactions - the Synthetic PIN. Also, the Synthetic PIN solution may be used as an addition for existing security mechanism that service provider has. This solution consists of four components that are shown on the figure 3: the user’s computer and his phone, and a service provider (for example, a bank) and the SyntPIN server. In addition, the components are connected via networks or sound, drawn as grey cloud shapes in the case of the Internet and the telecom network, and drawn as sound

waves in the case of sound played over the computer's loudspeaker. A network communications channel is shown as a line, with arrowheads showing directions of communication [33].

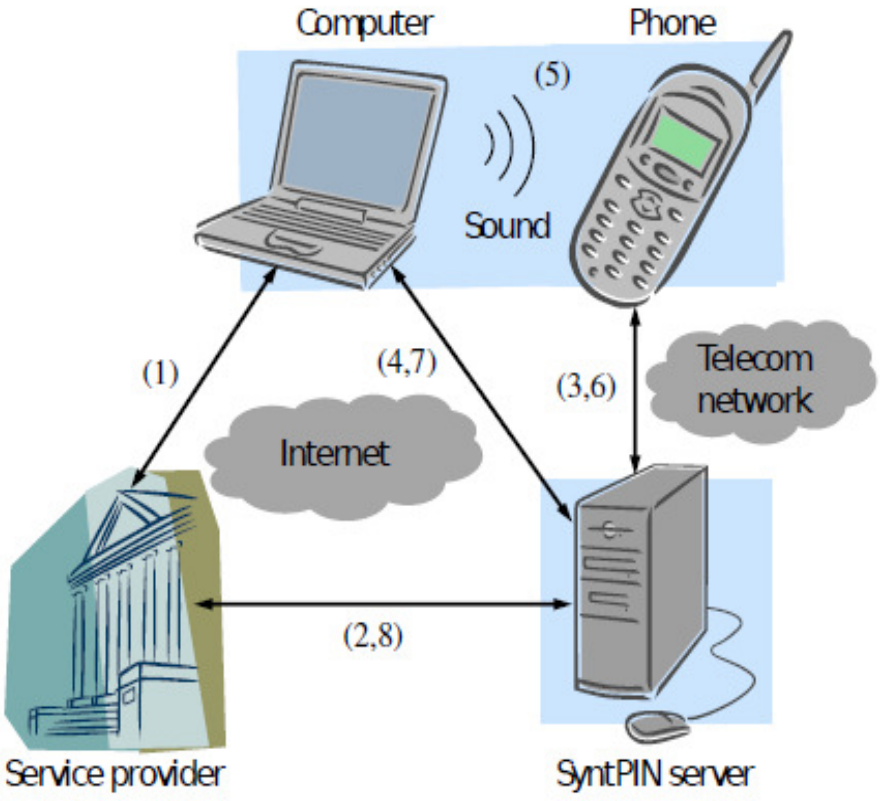

FIGURE 3: Synthetic PIN solution [33].

To perform an authentication or authorisation task the Synthetic PIN solution proceeds as follows. The user is already logged into the service provider's web site, see the channel marked (1) in the diagram. The service provider requests the task by sending a message to the SyntPIN server (2), including the phone number of the relevant user. The SyntPIN server calls the user's phone and waits for the user to answer. Assuming the user answers the call, the server plays a voice message to the user (3). In the case of authentication, SyntPIN server instructs the user to hold the phone up to the loudspeaker of the computer. Then the server sends a unique sound fingerprint4 to the user's computer (4), and the computer starts playing this sound through its loudspeaker (5). This sound is picked up by the phone and transmitted back to the SyntPIN server in the call (6). Once the sound has been received and verified by the SyntPIN server, authentication has succeeded. If the user does not answer the call or hangs up before the sound is transmitted, then the authentication has failed. The SyntPIN server informs the user about authentication success or failure on the user's computer screen (7). Authorisation of a transaction proceeds similarly, the only difference being that the SyntPIN server's call to the user also informs the user about the details of the transaction, using a synthetic voice. Then, the user is instructed to hold the phone up to the loudspeaker of the computer in case he wants to authorise the transaction, or to hang up the call not to authorise it. Last, the SyntPIN server informs the service provider about the result of the authentication or authorisation task, allowing the service provider to take appropriate action (8) [33].

The Synthetic PIN solution has some advantages in compare with the similar security technologies:

1) The PIN code isn't sent to the user. That's why PIN codes couldn't be stolen from unsecure phone, computer or other user's device.
2) SyntPIN server places a call to the user's phone. The user can identify who is calling. And it's hard to divert this call to another number without the knowledge of the user or the SyntPIN server because it requires compromising the telecom network or accessing low level functionality on the phone in order to configure call forwarding. Note that making the user's phone answer a call without the knowledge of the user is hard since to achieve this an attacker must compromise the voice call part of the phone and furthermore the attacker must divert sound from the computer loudspeaker into the answered call. Additional security is ensured if the user's phone is a landline. Mobile phones may be stolen, while landline phones can be protected using traditional physical security measures [33].

3) Also the Synthetic PIN offers to track the position of a user's phone or computer. It can help to thwart attacks: these two units should be in close proximity, otherwise there could be a man-in-the-middle attack in progress. One may also require the user to authorise a transaction by tapping a pre-determined code on the phone's touchscreen or its keyboard. In addition, attacks based on setting up hostile call forwarding may be detected through call forwarding detection mechanisms, depending upon telecom network peering agreements [33].

3.9 The Smart Card Detective

Smart Card Detective (SCD) is a hand-held device, that can protect smartcard users from several attacks, but can also showcase vulnerabilities in the Chip and PIN system. This device contains an ATMEL AVR AT90USB1287 microcontroller that mediates the communication between a smartcard and a terminal, buttons, LEDs and an LCD [36]. The cost of the device has been around $100 (including PCB manufacturing), and in large quantities the expected price is below $20. Using the SCD I developed the Filter Amount application, which was the main goal of the project. This application eavesdrops on a transaction and blocks a payment authorization request until the user verifies the correctness of the transaction. The user is able to check the transaction amount on the LCD and then decide if the transaction should continue or not. Additionally there is a Modify PIN application which replaces the PIN entered on a terminal by a PIN stored in the SCD memory. The main utility of this application is that users do not have to disclose the real PIN and thus can avoid situations where the PIN is seen by criminals looking over the shoulder. Steven Murdoch et al. have recently discovered an important vulnerability in the Chip and PIN system where a PIN transaction can succeed without entering the correct PIN although the receipt will read PIN VERIFIED. It was implemented in SCD. SCD has been successfully tested on a terminal emulator, CAP readers and live terminals [37].

The commercial interest of such device is uncertain. Although such a device can be very useful, carrying yet another gadget every time you go shopping is at least inconvenient. Also the current version of the SCD requires a wired connection between the device itself and the card interface that is inserted into the terminal. However, there are some practical uses of such a device: a user attorney for making high-amount transactions such as buying a car, a research platform for EMV, testing equipment for payment system developers to verify the correct functionality of cards and terminals.

3.10 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 [38].

Therefore a man-in-the-middle device, which can intercept and modify the communications between card and terminal, can trick the terminal into believing that PIN verification succeeded by responding with 0x9000 to Verify, without actually sending the PIN to the card. A dummy PIN must be entered, but the attack allows any PIN to be accepted. The card will then believe that the terminal did not support PIN verification, and has either skipped cardholder verification or used a signature instead. Because the dummy PIN never gets to the card, the PIN retry counter is not altered.

Neither the card nor terminal will spot this subterfuge because the cardholder verification byte of the TVR is only set if PIN verification has been attempted and failed. The terminal believes that PIN verification succeeded (and so generates a zero byte), and the card believes it was not attempted (so will accept the zero byte). The IAD does often indicate whether PIN verification was attempted. However, it is in an issuer-specific proprietary format, and not specified in EMV. Therefore the terminal, which knows the cardholder verification method chosen, cannot decode it. The issuer, which can decode the IAD, does not know which cardholder verification method was used, and so cannot use it to prevent the attack. Because of the ambiguity in the TVR encoding, neither party can identify the inconsistency between the cardholder verification methods they each believe were used. The issuer will thus believe that the terminal was incapable of soliciting a PIN – an entirely plausible yet inaccurate conclusion.

The failure we identify here might be patched in various ways which we will discuss later. But 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. This is because the attack we present does not interfere with either the input or output of transaction authentication, so replacing a transaction MAC with a digital signature will not help. One possible work-around is for the terminal to parse the IAD, which does include the result of PIN verification. This will only be effective for online transactions, and offline transactions where CDA is used, otherwise the man-in-the-middle device could tamper with the IAD as it is returned by the card. It would also be difficult to implement because the IAD was intended only for the issuer, and there are several different formats, without any reliable method to establish which one is used by a particular card. However a solution along these lines would require the acquiring banks and the terminal vendors to act together, which for the incentive reasons discussed above would be both slow and difficult.

3.11 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. This was just not understood in the 1970's; and the need for fair arbitration in particular seems to have been completely ignored.

The second error was probably due to fairly straightforward human factors. 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. Finally, we come to the `consultants': most banks buy their consultancy services from a small number of well known firms, and value an `air of certainty and quality' over technical credentials. Many of these firms pretend to expertise which they do not possess, and cryptology is a field in which it is virtually impossible for an outsider to tell an expert from a charlatan. The author has seen a report on the security of a national ATM network switch, where the inspector (from an eminent firm of chartered accountants) completely failed to understand what encryption was, and under the

heading of communications security remarked that the junction box was well enough locked up to keep vagrants out [40].

4. E–COMMERCE AND MOBILE BANKING

4.1 Banking Security Architecture

Banking fraud cannot be eliminated without a dedicated, trusted security device. Common forms of e-banking fraud is not sufficient to protect against the criminals. avenues of attack are implementable by today's fraudsters. There is a more robust scheme for authentication and authorization of online transactions by using a trusted device to create a very small trusted computing base, enabling secure communication with a bank without relying on the security of any of the intervening computers. This includes the computer which the customer is using to access the e-banking web site. The device forms a trusted path from the bank to the customer. Most solutions at best provide a trusted path to the user's computer (many do not even do this), however, general purpose computers are not themselves trustworthy agents of the user's intentions. This has been seen through the many exploits and Trojans, some of which specifically target Internet banking, to which general purpose computers are subject [41].

The proposed device negates the problems with a compromised computer by providing a trusted, authenticated path to the user over which all transactions are authorized. Because it is guaranteed that each transaction will have the correct details shown to the user the principle on which all of the attacks on online banking are based is removed. Thus, even the most powerful attack, the Trojan, is prevented.

In addition, because the device is the minimum necessary to provide the desired functionality it is possible to audit it for security vulnerabilities. It is also possible to build it with some amount of tamper resistance and hence protect it against attackers with much larger resources than is normally the case. This means that real assurances can be made that the authorization seen by the bank is the same as the one shown to the user, the only way to stop the whole class of attacks [42].

As always no solution is a panacea. There are a number of drawbacks to the proposed system. Firstly interoperability. In the past systems like this have failed because of interoperability issues. The proposal tries to mitigate a number of these, helped by the recent standardization of I/O connections and the emergence of portable languages such as Java. Suggestions for alternative methods of communication have also been made which further ameliorate those problems.

Secondly, there are still some avenues of attack left open. Obviously if an attacker can threaten the customer directly, or deceive them sufficiently, the customer may deliberately authorize a transaction to the attacker. There is only so far that technical solutions can go to prevent such abuses and such attacks are outside the scope of this work. This device also does nothing to keep the transaction log secret. The primary interface for transactions is still the computer, with just transactions being confirmed through the device. Protecting against reading of the

transaction log requires all interaction to be done through the trusted path. This would significantly increase the cost and reduce the ability to audit the device.

4.2 Payment by Mobile

The primary elements of mobile payments technology include NFC, SE, and TSM.
The use of Near Field Communications (NFC) for mobile payments is governed by the ISO 18092 standard and has the following attributes [43]:

– Is limited to a 424 kilobits per second data transfer rate.
– Supports communication ranges up to approximately 0.2 meters.
– Offers no native encryption.

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. The exact implementation of a SE in the mobile device has still not been standardized and there are 3 competing options: 1) build it into a chip on the mobile device; 2) implement it into the existing SIM chip; 3)implement through micro SD cards. 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 [44].

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. Traditional financial service companies (banks, processors, and card

associations) clearly have an advantage from controlling the existing banking and payments infrastructure. The extent to which they can strategically extend their products and services in a way that maintains the customer's trust in their services be key to their success. A foundational element of that trust is the security of the products and services. The wireless carriers are challenged by entering a segment with little financial service experience. Wireless carriers are challenged by being perceived as simply a wireless bandwidth pipe and have struggled with this since the advent of wireless data. Application providers (Google, Apple) within this space clearly hold an edge relative to innovation and speed to market, however, lack of focus on security and privacy will inhibit progress [45]. Additionally, both wireless carriers and application providers are at a clear disadvantage in terms of understanding the regulatory environment faced by current financial service providers.

4.3 Protecting E–Commerce Bank and Credit Card Systems

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.

Consequently, a lot of work was done in the 1990s on beefing up intrusion detection. There are a number of generic systems that do anomaly detection, using techniques such as neural networks, but it's unclear how effective they are. When fraud is down one year, it's hailed as a success for the latest fraud-spotting system; when the figures go up a few years later, the vendors let the matter pass quietly [46].

Credit card numbers are indeed available on the Net, but usually because someone hacked the computer of a merchant who disobeyed the standard bank prohibition against retaining customer credit card numbers after being paid.

Likewise, fraudulent Web-based transactions do occur, but mainly because of poor implementation of the system whereby cardholder addresses are checked during authorization. The real problem facing dot-coms is disputes. It is easy to repudiate a transaction.

The critical importance for online businesses is that, if more than a small percentage of your transactions are challenged by customers, your margins will be eroded; and in extreme cases your bank may withdraw your card acquisition service.

The existing cryptographic protection mechanisms used by the bank card industry— the PINs used at ATMs and some point-of-sale terminals, and the CVVs, which make card forgery more difficult—are largely ineffective online, so new mechanisms were developed. The most widely used is the Secure Sockets Layer protocol (SSL) [47], an encryption system bundled with most Web browsers.

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-business 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.

4.4 Authentication Solutions For Ecommerce and E–Banking

Bank growth and profitability is linked to eBanking. Customers prefer online banking because it is more flexible than high street or phone banking, and it offers banks the opportunity for growth and cost savings. However, eBanking depends on secure authentication and user trust.

X Info Tech is a one-stop shop for complete eBanking security solutions, including hardware, software, consulting and design, training, maintenance and support as well as device customization and fulfillment. With global reach and unique technology [48].

When it comes to remote banking authentication, you need a system than can grow with you. X Info Tech lets you deploy a low-cost, simple system today and still provide an upgrade path for the future.

System supports 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.

The system is completely flexible, allowing you to mix and match users with different devices and authentication schemes. This approach simplifies your backend IT while maximizing flexibility.

For example, System lets you get started with Printed Card or Scratched off Card or simple One Time Password (OTP) Token and, as risks and markets change, seamlessly upgrade to more advanced devices. You can even offer other service providers a multi-issuer authentication service using your authentication system.

The result is a system that lets banks balance the demands of cost, usability and security over time. It is low-risk, scalable, secure, flexible and, above all,future-proof [49].

X Info Tech, as a Two-Factor Authentication, offers protection from all existing kinds of fraud attacks.

Authentication solution includes generation of an OTP – One Time Password. The OTP can be generated on a smart card (presented by a secure device), token, mobile phone or sent by text message.

Benefits using the Token based approach:

– Cost effective devise.
– Provides strong two-factor authentication together with online password.
– Low logistic costs.
– Portability: Token is small and portable - convenient to bring with you at all times.
– A single press on the button generates a One Time Password.
– User-friendly functionality.
– Quick roll-out.
– Smooth personalization, personalize a whole batch in factory or a single device at the bank office.

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) [51].. The Mobile Solution enables PIN protected One Time Passwords (OTP), Signatures, Challenge/Response functionality and other services in strong Two-Factor Authentication schemes [56].

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. We found serious logic flaws in leading online, mobile, e-commerce etc. banking applications. 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.

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. 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.

6. REFERENCES

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

[2] "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].

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

[4] "RedTeam: iTAN online-banking security system". CAN-2005-2779. Internet: http://www.redteam-pentesting.de/advisories/rt-sa-2005-014.txt [Aug, 2005].

[5] "EMVCo, LLC: EMV 4.1". Internet: http://www.emvco.com/ [Aug, 2004].

[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] Jenkins, R. "Brainless thugs get life term". The Times. Internet: http://www.timesonline.co.uk/tol/news/uk/crime/article3850647.ece [May, 2008].

[8] Wong, R.M., Berson, T.A., Feiertag, R.J. "Polonium: an identity authentication system". IEEE Symposium on Security and Privacy, p. 101 [1985].

[9] Drimer, S., Murdoch, S.J. "Keep your enemies close: Distance bounding against smartcard relay attacks". In: USENIX Security Symposium [Aug, 2007].

[10] 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].

[11] Lomas, N. “Government gateway 2.0 looks to fatter future”. Internet: http://www.silicon.com/publicsector/0,3800010403,39168629,00.htm [Oct, 2007].

[12] “Make Card Readers Optional”. Internet: http://www.stopthecardreaders.org/ [2008].

[13] Samuel, H. “Chip and pin scam ‘has netted millions from British shoppers”. Telegraph. Internet: http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3173346%/Chip-and-pin-scam-has-netted-millionsfrom-British-shoppers.html [Oct, 2008].

[14] “Cronto: Products datasheet”. Internet: http://www.cronto.com/download/Cronto_Products_Datasheet.pdf [2010].

[15] Davida, G., Frankel, Y., Tsiounis, Y., Yung, M. “Anonymity control in E-cash systems”. FC 1997. LNCS, vol. 1318, pp. 1–16 [1997].

[16] Kerckhoffs, A. “La cryptographie militaire”. Journal des sciences militaires 9, 5–38 [1983].

[17] Bohm, N., Brown, I., Gladman, B. “Electronic commerce: Who carries the risk of fraud?” The Journal of Information, Law and Technology (3). Internet: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/ [Oct, 2000].

[18] “Banking Code Standards Board”. The banking code. Internet: http://www.bankingcode.org.uk/ [March, 2008].

[19] Drimer, S., Murdoch, S.J., Anderson, R. “Thinking inside the box: system-level failures of tamper proofing”. IEEE Symposiumon Security and Privacy, Oakland, pp. 281–295 [May, 2008].

[20] Burrows, M., Abadi, M., and Needham, R. “A logic of authentication. ACM Transactions on Computer Systems 8”, pp.18-36 [1996].

[21] 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].

[22] “CreditCall”. EMV.LIB Integration Guide. Internet: http://www.level2kernel.com/emvlibfidocumentation.html [June, 2010].

[23] 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].

[24] Drimer, S., and Murdoch, S. J. “Keep your enemies close: Distance bounding against smartcard relay attacks”. USENIX Security Symposium [August, 2007].

[25] Drimer, S., Murdoch, S. J., and Anderson, R. “Thinking inside the box: system-level failures of tamper proofing”. IEEE Symposium on Security and Privacy (Oakland), pp. 281-295 [May, 2008].

[26] “EMVCo. Terminal level 2, test cases”. Type Approval [Nov, 2011].

[27] “EMVCo, LLC. EMV 4.2”. Internet: http://www.emvco.com/ [June, 2004].

[28] Jack, B. “Jackpotting automated teller machines redux”. Presentation at Black Hat USA. Internet: http://blackhat.com/html/bh-us-10/bh-us-10-archives.html [June, 2010].

[29] Kelman, A. “Job v Halifax PLC (not reported) case number 7BQ00307”. Digital Evidence and Electronic Signature Law Review , vol. 6 [2009].

[30] Markettos, A. T., and Moore, S. W. “Frequency injection attack on ringoscillator-based true random number generators”. Workshop on Cryptographic Hardware and Embedded Systems, pp. 317-331 [2009].

[31] Moon, D., Flatley, J., Hoare, J., Green, B., and Murphy, R. “Acquisitive crime and plastic card fraud: Findings from the 2008/09 British crime survey”. Statistical bulletin, Home Ofice, April 2010. Internet: http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs10/hosb0810.pdf [April, 2010].

[32] 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].

[33] Synthetic PIN for Authentication and Authorisation”. Internet:

http://protectoria.com/Secure-Authentication [June, 2014].

[34] Needham, R. M., and Schroeder, M. D. “Using encryption for authentication in large networks of computers”. Commun. ACM 21, pp. 993-999 [Dec. 1978].

[35] “3-D Secure system overview”. Internet: https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=119 [2011].

[36] “RBS Secure Terms of Use”. Internet: https://www.rbssecure.co.uk/rbs/tdsecure/terms_of_use.jsp [Dec, 2009].

[37] “APACS. 2008 fraud figures announced by APACS”. Internet: http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/ [March, 2009].

[38] Nicholas Bohm, Ian Brown, and Brian Gladman. “Electronic commerce: Who carries the risk of fraud?” The Journal of Information, Law and Technology, (3) [Oct, 2000].

[39] “Cronto”. Internet: http://www.cronto.com/download/Cronto_Products_Datasheet.pdf [2012].

[40] Saar Drimer, Steven J. Murdoch, and Ross Anderson. “Optimized to fail: Card readers for online banking”. Financial Cryptography, LNCS 5628. Springer [2009].

[41] “Internet Retailer. Verified by Visa security program used as bait in phishing scams”. Internet: http://www.internetretailer.com/dailyNews.asp?id=13764 [Jan, 2005].

[42] Jon Varco. “Verified by Visa update”. Internet: http://www.barclaycardbusiness.co.uk/information_zone/customer_forum/pdf/1315_jon_varco_visa.pdf. [2012].

[43] Yuhang Ding, Dayan Zhuang and Kejun Wang. “A Study of Hand Vein Recognition Method”, The IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada [July, 2005].

[44] Shi Zhao, Yiding Wang and Yunhong Wang. “Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices”, Fourth International Conference on Image and Graphics [2007].

[45] H. Proença, and A. Alexandre. "Towards noncooperative iris recognition: A classification approach using multiple signatures". IEEE Trans. vol. 29, pp. 607-612 [2007].

[46] Masaki Watanabe, Toshio Endoh,Morito Shiohara, and Shigeru Sasaki. ”Palm vein authentication technology and its applications”, The Biometric Consortium Conference, USA, pp.1-2 [September 19-21, 2005].

[47] Mohamed Shahin, Ahmed Badawi, and Mohamed Kamel. ”Biometric Authentication Using Fast Correlation of Near Infrared Hand Vein Patterns”, International Journal of Biological and Medical Sciences, vol 2,No.1, pp. 141-148 [winter, 2007].

[48] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn. “Image understanding for iris biometrics: A survey”, Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281–307 [2008].

[49] J. Daugman. “Probing the Uniqueness and Randomness of Iris Codes:Results from 200 Billion Iris Pair Comparisons”, Proceedings of the IEEE, vol. 94, no. 11 [2006].

[50] E. M. Newton, P. J. Phillips. “Meta-Analysis of Third-Party Evaluations of Iris Recognition”, IEEE Transactions on Systems, Man, and Cybernetics, vol. 39, no. 1, pp. 4–11 [2009].

[51] J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma. “Robust Face Recognition via Sparse Representation”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 210–227 [2009].

[52] Dan Kaminsky. “DNS rebinding and more packet tricks”. 24th Chaos Communication Congress. Internet: http://events.ccc.de/congress/2007/Fahrplan/track/Hacking/2393.en.html [Dec, 2007].

[53] Jochen Topf. “HTML form protocol attack”. BugTraq posting. Internet: http://www.remote.org/jochen/sec/hfpa/hfpa.pdf [Aug, 2001].

[54] “Obscure. Extended HTML form attack”. Technical report, EyeonSecurity. Internet: http://www.hackerz.ir/e-books/Extended%20HTML%20Form%20Attack.pdf [2002].

[55] Adrian Pastor. “BT home flub: Pwnin the BT home hub - exploiting IGDs remotely via UPnP”. GNUCitizen. Internet: http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub-5/ [Jan, 2008].

[56] Adrian Pastor and Petko D. Petkov. “Hacking the interwebs”. GNUCitizen. Internet: http://www.gnucitizen.org/blog/hacking-the-interwebs/ [Jan, 2008].