WHITEPAPER
Two-Factor Authentication:
An essential guide in the fight against Internet fraud

Document Number
GP_WP_2W

Issue Status
1.0

Issue Date
02 February 2006

Prepared by

GPayments Pty Ltd
A member of the NEUROCOM Group
Suite 201 Fujitsu House
14 Rodborough Road
Frenchs Forest NSW 2086
PO Box 6151
Frenchs Forest DC NSW 2086
Australia
Tel: +61 2 9453 5411
Fax: +61 2 9453 5433
Email: info@gpayments.com

Contents

1 Abstract

Implementing a two-factor solution for authentication of online users plays an important role in the fight against online fraud. Two-factor authentication reduces the window of opportunity for fraudsters and can eliminate, contain or mitigate online attacks. There is a myriad of two-factor devices and methodologies in the market today, which have varying degrees of effectiveness, cost and usability. Implementing and rolling out a two-factor authentication solution to a large user base involves a significant investment. As such, it is important to have a good understanding of the benefits and limitations of two-factor authentication technologies and the relative strengths and weaknesses of devices and solutions, before making a decision.

In this paper we will classify credential theft related attacks into two broad categories: active and passive. We will examine different technologies for online authentication and analyse their strengths and weaknesses. In particular we will look at two-factor authentication methods and provide an empirical comparison of these methods. We will recommend a number of inexpensive and simple procedural changes that can protect users and reduce fraudsters' interest in an organization and its users.

Two-factor authentication is an emerging market where new devices and authentication methods are continuously being introduced by the vendors. As such it is important for organizations to choose a vendor agnostic two-factor platform based on open standards in order to ensure flexibility in choosing devices from different vendors and avoid being locked to a vendor's propriety product or solution.

Two-factor authentication is an effective solution for a real problem today. Although essential, two-factor authentication by itself will not be able to stop all kinds of online fraud. Securing user terminals and educating users also plays an important role.

1.1 Audience

The paper is designed for those who require a better understanding of two-factor authentication concepts and products. Chapters 2, 3 and 4 are targeted at business personnel who are responsible for the decision making process regarding the authentication strategy of an organization. Chapter 5 provides an overview of different two-factor authentication technologies and chapter 6 provides a quick comparison. Chapters 5 and 6 are more targeted at technical personnel.

Although this paper explores the concept and implementation of two-factor authentication from the financial industry's point of view, readers from outside the financial sector may also find it very relevant to their particular industry.

2 Introduction

Passwords as a means of authentication have long reached their expiry date. Gartner predicts that by 2007, 80 percent of organizations will reach the 'password breaking point' and will need to strengthen the user authentication with alternative security methods [1]. In this paper we will look at stronger alternatives for online authentication, commonly known as two-factor authentication. We use the word 'stronger' because nothing is absolute. Two-factor authentication is an important step in safe-guarding online accounts, which combined with securing user terminals and intrusion detection and confinement technologies, can dramatically reduce online fraud.

Many organizations, particularly in the financial sector, have realized the importance of two-factor authentication and are either deploying it or they are in the process of evaluating the various solutions available. It is important to understand what can and cannot be achieved by two-factor authentication in general and with vendor solutions in particular and use complementary methods to address any shortcomings.

The device manufacturing market still lacks openness and is dominated by products that are based on proprietary algorithms. Lack of transparency and a closed market has hindered the adoption of two-factor authentication and has kept the price of devices and implementations high; in a market where paying royalties for verification software as well as hardware is commonplace. Fortunately, the market is adjusting, as more companies produce products based on open standards such as OATH[1], MasterCard CAP[2] and Visa DPA[3], which helps to create downward pressure on prices. An organization, which intends to implement a two-factor authentication solution, will benefit from adopting a device agnostic platform, based on open standards, and avoiding being locked into a proprietary product.

In this paper we will classify credential theft related attacks into two broad categories: active and passive. We will examine the different technologies available for online authentication and analyse their relative strengths and weaknesses. In particular, we will look at two-factor authentication methods and provide an empirical comparison of these methods. We will recommend a number of inexpensive and simple procedural changes that can protect users and reduce fraudsters' interest in an organization and its users.

Simply using a second factor of authentication does not guarantee strong authentication nor does it necessarily prevent online fraud. However, two-factor authentication is an important element in reducing online fraud. Using the right two-factor solution not only protects users against direct offline and passive online attacks, but also can contain active attacks. We will define the different types of credentials theft attacks in the following section.

[1] Open Authentication
[2] Chip Authentication Program
[3] Dynamic Passcode Authentication

2.1 Credential Theft Attacks

Credential theft attacks are attempts by fraudsters to steal user credentials to gain access to a user's private or sensitive information, for financial gain or otherwise.

In order to evaluate the effectiveness of two-factor authentication techniques, we first define two broad classes of attacks: *passive* and *active*. Passive attacks can be further broken down into online and offline attacks.

2.1.1 Passive Attacks

Passive attacks are the class of attacks where stolen credentials are stored and processed at a later time. Passive attacks can be offline or online.

Offline attacks are selective and targeted thefts of credentials by fraudsters who have direct access to a user's assets. An individual with access to the victim's computer can easily install a key logger or a malware application to collect data from the unsuspecting user.

- Offline attacks have a limited scope and are low-yield.
- Offline attacks are the simplest form of credential theft. They do not require any technical expertise nor do they incur any cost.

Users can fall victim to such an attack simply because they write down their passwords or store them unencrypted in some conspicuously named file on a local hard disk. Recent study suggests that in 50% of identify theft cases where the perpetrator is known, the fraud is committed by someone close to the victim [2]. In other words, a large portion of fraud is committed by people with direct access to their victims' assets.

Online attacks are random theft of credentials. The attacker targets a large number of users over the Internet, in the hope of exploiting vulnerable systems or taking advantage of naïve users, to steal credentials.

- This type of attack is comparatively high-yield; returns of up to 3% have been reported [3]. The most common type of an online attack is phishing.
- There is a cost associated with staging an online attack for acquiring email lists, personal data, list of vulnerable computers for hosting counterfeit sites and even custom development of crimeware[4].
- Depending on sophistication of an online attack, the fraudster requires medium to high technical expertise.

Phishing, a method commonly used by fraudsters in recent years, is an example of a passive attack. The combination 'ph' is a common substitute for 'f' in hacking circles. The term phishing comes from the analogy that hackers fish for user credentials [4] on the Internet by putting bait in front of users to lure them into a trap. The bait is usually an innocent looking email with a cover story to convince users to visit a counterfeit website, to divulge credentials and personal information. To date, phishing scams have been passive, largely due to the fact that harvested data can be used at a later time. This may change in the future as two-factor authentication becomes more prevalent and the window of opportunity for exploiting harvested data shrinks.

[4] Crimeware is software specifically designed or used for unlawful activities such as stealing personal information

2.1.2 Active Attacks

Active attacks are sophisticated attempts by fraudsters to steal and then use stolen credentials in real-time.

- Active attacks are more expensive to orchestrate
- Active attacks require a high level of technical expertise
- Active attacks may require custom development of crimeware that is capable of stealing information and that can actively use harvested information to its immediate benefit.

The more recently publicized 'man-in-the-middle' attack is an example of an active attack. There is no evidence of such an attack at the time of writing for credential theft, simply because far easier methods with higher returns are still available.

Man in the middle (MIM) is a term borrowed from cryptography where an attacker gains access to the secret key used for encrypting data between a sender and a receiver. The attacker can then eavesdrop between the two parties while passing the information at the same time. In the context of credential theft, this is a counterfeit website that interacts with the user on behalf of the real site and passes the information behind the scenes between the two parties. MIM is an example of an active attack. Some security analysts have used the hypothetical example of MIM attack to question the case for implementing two-factor authentication technology. While it is true that simply using a second factor authentication for user logins cannot prevent an MIM attack, a proper implementation of two-factor authentication across sensitive resources in tandem with complementary preventative technologies can neutralize or at least contain MIM attacks.

Active attacks are not a security problem today but they will be in the near future. There will be a two-phase shift in credential theft trends as more organizations improve their authentication security by implementing two-factor. At first, the criminals will shift their attention to soft targets, those left behind in their implementation of two-factor. Once two-factor becomes main-stream and passive attacks unviable, the criminals will resort to more sophisticated active attacks. Organizations, especially financial institutions, should use this window to prepare their users for the second wave.

The best defence against an active attack is by securing user terminals. Making sure that:

- The operating systems and all applications are fully patched
- Malware and virus definitions are up to date.
- A firewall is used for Internet connections
- Anti-spyware and anti-adware are used to ensure that the system is free from any unnecessary applications that could possibly compromise the user terminal.

An anti-phishing filter will also reduce the chance of users being mislead to fraudulent sites. A compromised system is not only a threat to the owner but also a potential threat to other Internet users. Educating users will play an important role in improving the security of individuals as well as businesses on the Internet.

3 Two-Factor Authentication Benefits

Two-factor authentication is based on something that a user has (a physical device) and something that a user knows (a PIN number or password). A common application of two-factor authentication in everyday life is withdrawing money from an ATM. The user is required to enter their card in the ATM (something they have) and then type their PIN (something they know). By using something a user knows with something a user has, the same level of authentication can be brought to the online world.

3.1 Reducing the Window of Opportunity

Phishing attacks with the aim of collecting user credentials are viable today because the data collected from users can be used for an extended period of time. The window of opportunity is wide and open with static passwords. A second factor of authentication can narrow down this window of opportunity and render any collected data useless.

3.2 Eliminating Passive Attacks

Passive attacks are semi-automatic at best. The data may be automatically collected, but will be processed manually by a fraudster. Implementing a two-factor authentication method, which minimizes the window of opportunity, can eliminate passive attacks as the stolen credentials are only valid for a short period of time. Another benefit of two-factor authentication is that stolen data is only valid for single use and cannot be used for repeated access.

3.3 Mitigating the Risk of Active Attacks

Using the right two-factor authentication solution cannot only eliminate passive attacks, but it can also contain and limit the damage from an active attack. It is true that an attacker that compromises a user's system or uses MIM can let the user pass the security checks and then exploit their account. However, two-factor authentication with signing capability can prevent the attacker from achieving any financial benefit, since the transaction amounts and destinations can be digitally signed and will be of no use to the attacker.

3.4 Increasing the Cost to Implement Fraud

Most criminals are in the business of maximizing gains while minimizing cost; increase their cost and minimize their gain and they will suddenly lose interest in your assets. Implementing two-factor authentication will make it harder for fraudsters as they will have to shift to more expensive active attacks. Two-factor also reduces their gain as it shrinks the window of opportunity.

4 Additional Security Measures

In addition to implementing two-factor authentication, there are a number of simple methods and inexpensive changes that can be made to existing systems to improve the overall security and limit the damage that an attacker can cause when a user is compromised.

4.1 Identify Areas of Vulnerability

The first step in securing a system is to understand its weaknesses and where it is most vulnerable. Organizations need to constantly evaluate and monitor their security processes.

4.2 Compliance to Standards

Organization must ensure that they comply with the established standards and industry's best practices such as PCI, Visa AIS, 3-D Secure, MasterCard SDP, etc for storage and handling of sensitive information.

4.3 Removing Unneccesary Information

Review your website and remove unnecessary information. Do not share information that is already known to the user and is unlikely to change. Welcoming a user with their name, while warm and hospitable, adds no real value but exposes the user by linking their account with a real name. While an organization might have to store a user's date of birth, mother's maiden name, social security number or driver license details, there is no reason why they have to make them accessible via their website. The real user already knows this information and there is no benefit in displaying it to them.

4.4 Masking Credit Card Numbers

Many organizations are targeted because they keep credit card information. Access to credit card data is also a key element in identity theft. Credit card numbers are popular targets as they can be widely and easily used for making unauthorized purchases. This could be a major reason why an organization, which stores credit card information is targeted (e.g. 40 million credit card records were stolen from Card Systems in June 2005 [5]).

Organizations should mask account numbers, particularly credit cards and display a few digits only. This is an inexpensive yet effective tactic. There is no reason why the full credit card numbers need to be shown in an online statement or in the list of accounts. The authorized user can always look check the full credit card number on the card itself.

4.5 Authentication of Credit Card Transactions

While masking credit card numbers is an effective and simple way of eliminating credential theft targeted at credit cards, organizations may still be subject to traditional internal and external hacking of their systems in an attempt to retrieve card numbers. Users can also be targeted by crimeware such as key loggers, which focus on intercepting credit card information. Credit card numbers are valuable because they can be used on the Internet without further authentication. Visa international has introduced the 3-D Secure initiative to address the problem with credit card authentication, the standard has also been adopted by MasterCard and JCB. Mass roll out of 3-D Secure can play an important role in combating online/card not present fraud and can reduce theft of credentials aimed at collecting card numbers as they can no longer be used for making easy purchases on the Internet.

In its vanilla form, 3-D Secure for credit card authentication is based on static passwords and as such subject to their problems. Financial institutions should adopt a two-factor strategy that can address both their access control (e.g. user login) and transactional authentication needs (such as authentication of credit card transactions and money transfers).

4.6 Authentication of Transactions

Phishing has been used to retrieve random numbers on TAN[5] lists [6]. Other forms of two-factor authentication could be vulnerable depending on the life span of tokens generated by the device.

To improve security, transactions should be authenticated and carry a digital signature. A two-factor authentication system with support for signatures can prevent or contain the damage of an active attack.

Details of a transaction cannot be predicted by the attacker beforehand and as such using a two-factor device with signing capability provides a clear advantage. Ideally all transaction details should be signed, but entering all transaction details on an authentication device is practically prohibitive. Instead the device is usually given a numeric challenge with a few digits and then produces a signed response. Using a complex challenge that users cannot easily infer from transaction data is a bad security decision. It makes users vulnerable to an MIM attack where the attacker replaces the challenge with data suitable for a fraudulent transaction while showing the legitimate transaction details. Using simple criteria such as the last four digits of the destination account as the ‘challenge’ is much more viable than more complicated methods such as signing the hashing of transaction details.

4.7 Delayed Transactions and Notifications

Delaying money transfers, especially to overseas accounts, is an inexpensive method that can allow users that frequently check their online accounts to detect fraudulent transactions. A more effective solution is to send notification to users. For example sending SMS notification for high value transactions, combined with delayed payment is an effective way of containing the financial damage caused in a compromised account.

[5] See section 5.4 for more information on TAN lists

4.8 User Education

Protecting user terminals from being compromised by malicious software is the key to neutralizing active attacks. User awareness plays an important role in protecting user terminals. User education may not be a direct responsibility of an organization that provides services on the Internet but money spent on educating the user may pay off as users are less likely to be compromised or taken advantage of and therefore less prone to financial loss.

5 Two-Factor Authentication Devices

A multitude of devices and technologies, from various vendors, are available for two-factor authentication. Not all two-factor authentication solutions are created equal; they differ in security, convenience and cost.

In addition to hardware devices, an organization needs to implement server side software for verification of tokens. Some vendors provide an SDK or an API, which needs to be integrated with the organization's website. Others provide an authentication server that can be used for verification, management and administration of tokens and devices. Some authentication servers only support a vendor's own hardware tokens while there are device agnostic platforms that support tokens from different vendors. These software platforms provide an organization with more flexibility in selecting a hardware solution or migrating between different vendors.

There are two broad categories of two-factor devices: connected and unconnected.

- Connected devices interact directly with the authentication engine by transferring data via a physical link (e.g. USB, Bluetooth), minimizing user interaction.
- Unconnected devices require users to be the medium between the device and the authentication system to transfer information.

In the following subsections we will further categorize two-factor authentication devices and compare their features.

5.1 Hardware One Time Password Generators

Hardware one time password generators also known as OTP devices are perhaps the most widely used two-factor authentication device, today. They are relatively cheap to implement[6] and easy to use.

Based on the password generation algorithm there are two broad types of OTP devices: time-synchronous and counter based.

A time-synchronous OTP creates an unpredictable number based on an internal clock. The authentication server can verify the generated number as long as the OTP's internal clock is sufficiently synchronized with the authentication server. Since the OTP's internal clock drifts, a perfect synchronization is not possible and the authentication server has to accept tokens generated within an acceptable window. It is important to minimize the synchronization window in order to reduce the window of opportunity for a potential attacker. Most OTP vendors also implement a time offset mechanism to counter the effect of accumulative drift. The offset is adjusted with each successful verification. A time-synchronous OTP may have to be recalibrated if not used for a long time.

A counter based OTP increments an internal counter every time a new token is generated. The authentication server can verify the generated number as long as the OTP's internal counter is sufficiently synchronized with the authentication server. The OTP's counter is incremented every time a token is generated while the server's counter is adjusted with each successful verification. The authentication server has

[6] Compared to Chip cards, USB , Biometric and Chip enabled USB devices

to implement a look-ahead window to ensure usability. With this type of device, the OTP generator and authentication server can easily go out-of-sync.

Compared to a time-synchronous device, a counter based OTP generator provides less protection against an offline or online passive attack. It is easy to launch a phishing attack and collect as many tokens as required to be used at a later time or someone with access to the device can create as many tokens as needed without having to act upon the collected tokens immediately. Some counter based devices are PIN protected. This protects against an opportunistic offline attack but is exposed to an online attack.

OTP devices are battery driven and need to be replaced every couple of years. Each OTP device is uniquely seeded with a cryptographic key and as such users usually need to repeat the enrolment process every time an OTP device is replaced.

Some OTP devices can produce digital signatures making them an effective tool against active attacks.

5.2 Software Based One Time Password Generators

Software based OTPs emulate the concept of a hardware token. The security of a software based OTP is directly related to security of the cryptographic key or seed which is used in generating the unpredictable sequence.

Software OTPs are subject to duplication. Users can lose control of their software tokens without knowing that they have been compromised. The effectiveness of a software-based OTP is inversely proportional to the ease with which their deployment platform can be accessed by an attacker. For example implementing a software token for a personal computer is not a good security decision while on a PDA or a mobile phone, which is less accessible, it can be an effective yet inexpensive solution (at least until mobile phones become as accessible as personal computers and everyone has to install firewall, antivirus, spam filer, etc on their mobile phones as well).

A software-based OTP for a mobile handset protected by an additional PIN comes close to a hardware-based OTP. While there are no direct delivery and hardware costs with mobile tokens, in a mass rollout the challenge for an organization would be supporting customers with deployment and operation of the software on an ever growing list of mobile phones. An organization that chooses a mobile based OTP solution must also consider that a number of users, however small, may not have a compatible mobile phone or a mobile phone at all.

5.3 Terminal Profiling

A class of two-factor solutions register characteristics of the user's terminal (PC, PDA, mobile phone, etc) as the second factor of authentication. During the enrolment process, certain characteristics of the user terminal such as hardware configuration, operating system, network ID, IP address and browser type are registered alongside the user's account. For subsequent logins, user access is limited to a previously profiled terminal associated with the user account.

Some vendors use virtual, transparent or even fingerprinting to describe their solution. Unlike human fingerprints, these so called terminal fingerprints are neither unique nor irreproducible. The solution also has to tolerate a certain amount of change in the profiled data for usability and allow users to register multiple terminals

or register their primary terminal in case variations in system configuration invalidate the stored profile. An attacker can either try to replicate a user's profile or use phishing to get the user to register the attacker's terminal with their account.

The main problem with terminal profiling is that it does not limit the window of opportunity and from this perspective, is not very different to static password authentication. However it can be a practical and inexpensive back-up mechanism in case the primary authentication device is not available. For example, an organization that uses OTP devices, can benefit from terminal profiling as a back-up mechanism to provide customers who have lost their tokens with an alternative access mechanism for a limited time and until they receive a replacement device.

5.4 TAN Lists

TAN is an acronym for "Transaction Authentication Number". A TAN list, one of the first two-factor authentication methods, is a list of unpredictable numbers printed on a piece of paper.

TAN lists are inexpensive, easy to use, portable and easy to distribute. In their simplest form, the user enters the next number in sequence from the list, in addition to a static password in order to access a protected resource. A simple TAN list is subject to passive attacks such as phishing where a user can be tricked to enter the next number on a phishing website or can be copied or viewed by a person with direct access to user's TAN card. There are stronger variations that can provide better security such as scratch TAN lists, which are tamper evident and TAN matrices that provide better protection against phishing.

The main problem with a TAN list is that it is meant to last for a relatively long period of time (a month or more) and if compromised leaves a relatively large window of opportunity for an attacker.

In terms of security, a TAN matrix provides a better protection against passive attacks as the selection of the unpredictable number is random.

5.5 SMS Tokens

SMS can be used as the medium for delivery of an unpredictable number as a second factor of authentication.

There are two types of SMS tokens: instant SMS tokens and batch SMS tokens

- With instant SMS, the message is sent immediately following a successful authentication of the user. The user needs to wait to receive the unpredictable number before they can complete the second factor of authentication. Instant SMS is often criticized for the lack of service guarantee and its recurring cost per token. SMS protocol does not guarantee delivery or timely delivery of messages. This may reduce the usability of a two-factor authentication based on SMS.
- With batch SMS on the other hand, the user receives a list of unpredictable numbers similar to a TAN list before they login. Each unpredictable number is associated with a letter of alphabet or a row number. The user needs to enter the unpredictable number associated with a requested row as the second factor of authentication. Batch SMS can greatly reduce the recurring cost of SMS and works around the serviceability issues of the SMS protocol as the list is sent to users

before they actually need them. The downside to using batch SMS though, is that the window of opportunity is substantially larger than an instant SMS.

5.6 Smartcards and Chip Readers

Smartcards are the more secure replacement for magnetic stripe cards. With today's technology magnetic cards can be easily duplicated, by fraudsters, in a process known as card skimming. Many banks (especially in Europe and Asia Pacific) have already made or are making the investment to upgrade their magnetic card base to chip protected smartcards. Others are ultimately expected to follow suite due to practical and compliance related considerations.

A side benefit of rolling out smartcards is the ability to use them for online authentication. This requires the end user to have a smartcard reader. With the ability to store certificates and produce signature for transactions, smartcards are considered to be the ultimate two-factor authentication device. While many financial institutions may finally switch to smartcards for authentication, the cost of implementing an EMV infrastructure plus the additional cost of providing users for card readers can be prohibitive at first. However a smart choice would be to select a platform that supports chip authentication and offers an easy and inexpensive upgrade path from any two-factor authentication device to smartcard authentication.

The principal of authentication with a smartcard is to sign an unpredictable challenge generated by the authenticating party. The signature is calculated securely by the chip on the smartcard. The cryptographic key never leaves the secure confines of the smartcard and as such provides the highest level of security. Access to smartcard functions can be further protected with a PIN.

There are two types of smartcard readers: connected and unconnected.

- As the name suggests, a connected reader can directly interface with the user terminal (via USB, Bluetooth, etc) in order to exchange the challenge and the signed cryptogram. Connected readers require installation of software on the user terminal, which facilitate the exchange of data between the reader and the authentication server.
- The unconnected version, however, does not have a direct interface with the user's terminal; the user has to mediate the information between the authenticating party and the reader. The user enters the challenge on the reader via a keypad. The smartcard application then produces the reduced cryptogram, which is normally a 6-11 digit code and displays the result to the user.

Creating cryptograms involves an application transaction counter or ATC. ATC is incremented with generation of each cryptogram. For successful verification of a cryptogram, the authentication server needs to know the exact ATC. Authentication servers use ATC synchronization algorithms and tolerate out of sync ATC's to some extent. Organizations who intend to implement smartcard authentication need to be aware of this limitation and rollout chip cards with at least two smartcard applications each with their own ATC: one for the authentication purposes and the other for the authorization of credit card purchases at merchant terminals to avoid potential problems with ATC synchronization.

5.7 Chip Enabled USB

USB devices are easy to use and come in small form factors. A number of two-factor device manufacturers produce devices that can perform cryptographic operations when connected via USB. From a functional perspective, a chip enabled USB is equivalent to a smartcard plus the smartcard reader.

Like connected chip card readers, users need to install software for the chip enabled USB device to work.

Some USB devices can be PIN protected or use some other form of user authentication such as fingerprint scanning to further protect access to the USB device.

5.8 Biometrics

Most of the devices that we have discussed so far can be combined with a biometric scanner such as a fingerprint scanner or an iris scanner. Use of biometrics authenticates the user to the device rather than the authentication server. A positive biometric identification unlocks the device's functionality; the device still needs to generate some form of a cryptogram to prove the identity to the server. For example a standard chip card reader comes with a numeric keypad which allows users to enter a PIN and authenticate themselves to the chip card before a cryptogram is generated. The PIN pad can be replaced with a more user friendly fingerprint scanner.

While easy to use, futuristic and fashionable, biometric sensors are still relatively expensive and increase the cost of a two-factor authentication device.

5.9 Virtual Keypads

While not a two-factor device or technology, virtual keypads have been increasingly used as an intermediate solution to improve the security of static passwords.

Virtual keypad is also known as dynamic keypad, online keypad or scramble pad. A virtual keypad is a software implementation of a keyboard, which is used to protect users from key loggers. Some virtual keypads dynamically arrange the symbols on a keyboard to further complicate detection of keys for a logger. Compared to a normal keyboard, using a virtual keypad is inconvenient especially when the symbols on the keypad are dynamically repositioned each time.

According to APWG an organization that among other things, monitors online fraud patterns on the Internet, the use of key loggers to capture user credentials rose by 125% in July 2005 compared to the April period. It was also reported that in the same period more sophisticated screen scraping techniques where becoming popular among key loggers. This shift was in response to roll out of virtual keypads by more financial institutions. The key logger waits for the user to visit the sign-in page and takes a screen capture with every mouse click, hence revealing the sequence of characters entered by the user.

Virtual keypads do not provide much value and may even increase the risk of exposing user credentials. Most virtual keypads make it much easier for an onlooker to read a password, while each letter is being clicked by the user.

6 Comparison of Two-Factor Devices

The following table provides a comparison of two-factor devices from a security, cost and usability perspective. Given the versatility of two-factor devices and differences in implementation within each category, the comparison should be regarded as a general guide.

	Protection Against Passive Attacks	Protection Against Active Attacks	Initial Cost	Device Cost	Maintenance Cost	Support Cost	Per Transaction Cost	Ease of Use	Portability	Client Software
Random Number Generators 	High	Low to Medium	Medium	Medium	Medium	Low	None	Medium	High	No
Unconnected Chip Card Reader 	High	Medium	High	Medium	Medium	Low	None	Medium	Medium	No
Connected Chip Card Reader 	High	Medium	High	Medium	Low	Low	None	High	Low	Yes
CHIP Enabled USB 	High	Medium	Medium	High	Low	Low	None	High	High	Yes
TAN Lists 	Low to Medium	Low	Low	Low	Low	Low	None	Medium	High	No
Mobile Phone Using SMS 	Medium to High	Low	Low	None	None	Low	Medium to High	Medium	High	No
Mobile Phone Using Applet 	Medium	Medium	Low	None	None	Medium to High	None	Medium	High	Yes
Software Only (PC based)	Low to Medium	Low	Low	None	None	Medium	None	Medium to High	High	Yes
Terminal Profiling	Low	Low	Low	None	None	Low	None	Medium	Medium	No

7 Conclusion

In this paper we categorized and studied credential theft attacks and discussed several methods and technologies that can be used for stronger authentication of users and transactions. The benefits, weaknesses and limitations of each method were discussed. We argued that two-factor authentication needs to be an integral part of an organization's security strategy but we also argued that two-factor authentication alone is not the silver bullet and cannot completely eliminate online fraud, securing user terminals is also crucial and needs to be encouraged by better user education.

Two-factor authentication is still an emerging market, and as such one would expect that over time, more economical and more secure solutions will become available. In such an environment, organizations which plan to invest in such infrastructure should adopt an extensible solution based on open standards that provides them with flexibility and should avoid being locked into expensive, proprietary, patent-pending and vendor specific solutions to ensure that they can benefit from future technological enhancements and reduction of unit prices without having to write off their existing investment.

8 References

[1] Computer Weekly, http://www.computerweekly.com/Articles/2005/09/13/211737/Plannowtobeat2007password'breakdown'%2cGartneradvises.htm

[2] http://www.bbbonline.org/idtheft/safetyquiz.asp

[3] Computer World, http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,92948,00.html

[4] http://www.phishspot.com/

[5] CNet, http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html

[6] http://www.finextra.com/fullstory.asp?id=14384