Artaker.at COMPUTERSYSTEME

sms|passcode

Whitepaper

MODERN THREATS DRIVE DEMAND FOR NEW GENERATION MULTI-FACTOR AUTHENTICATION

A SURVEY SHOWS THAT 90% OF ALL COMPANIES HAD BEEN BREACHED IN THE LAST 12 MONTHS. THIS PAIRED WITH THE FACT THAT THREATS LIKE ZEUS AND HACKING HAVE COMPROMISED THE MORE THAN 20 YEAR OLD TWO-FACTOR AUTHENTICATION TOKEN, CREATES THE CASE FOR A NEW GENERATION OF MORE SECURE REAL-TIME MULTI-FACTOR AUTHENTICATION SOLUTIONS.

→

INTRODUCTION

The use of online services has exploded in the last decade as remote access has become a default way to access enterprise systems and to conduct business. Initially designed for employee access, today remote access is an integral component of the way we live and work – for employees and consumers alike.

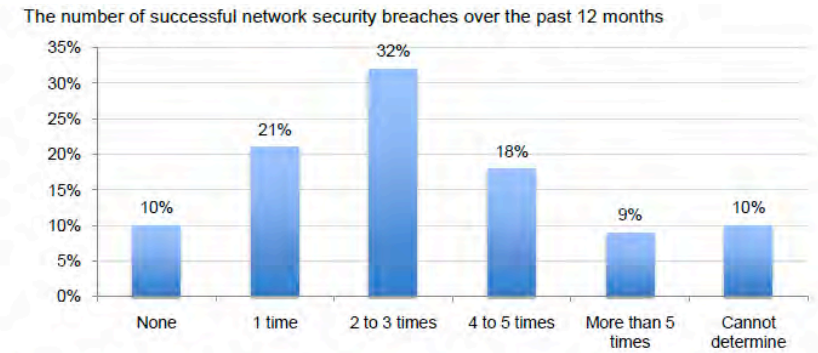
With the development of this pervasive use of online access to conduct business, the threat of identity theft has increased with a speed and complexity not seen before.

According to some researchers, online identity theft schemes will surpass all other forms of financial crime within just a few years. Clearly attacks against companies like Adobe, New York Times, Citibank, Lockheed Martin, and Sony gives a clear illustration of how criminals are targeting both employee and consumer identity theft.

A survey of more than 500 corporations by Ponemon Research revealed that 90% had been successfully hacked in the last 12 months. This research demonstrates the need for all corporations to adopt two-factor authentication as a means to protect against breaches.

Consequently, modern mobile phone based multi-factor authen¬tication is in high demand.

SMS PASSCODE is the leading technology in this fast growing space, delivering protection of online identities in a highly secure and convenient way.



© Ponemon Research, 2011. Source: http://www.ponemon.org

GI forecasts that by 2014 the market for mobile phone-based 2FA products and services will account for 61 percent of the total OTP 2FA market

THE BASICS OF HACKING

Just as the remote access industry has evolved, so have the threats and their complexity. Back in the early days when only user name and password were used, hackers simply used 'brute force' user name and password guessing or dictionary attacks to assume a user's identity. This is essentially a computer or a hacker that simply continues various combinations of the password until success is achieved.

As systems became immune to this method by blocking the account after a few faulty attempts, new techniques such as key loggers were invented. A key logger is a piece of software running as a background service that captures a user's key strokes during login and sends it back to the source of the attack.

Today the most widely used attacks are pharming and phishing or a combination of the two. This is a technology and method by which a user is led to a fake website that is identical to the original. This tricks the user into entering their user name and password. Once the credentials have been captured, the user is often presented with a 'down for maintenance' message or something similar to buy the hacker some time. Some of the more advanced attacks send the information via a small instant message program in real time to the hacker essentially compromising the widely adopted two-factor authentication tokens. One such example, Zeus malware, captures a user's credentials including the most advanced time based token codes and sends the information to the hacker.

Therefore, in today's IT landscape even the most secure traditional two-factor authentication token devices can no longer ensure the identity of a user. The fact that so many organizations are unaware that traditional tokens can be compromised poses a significant security risk.

Recently, newer more sophisticated methods of intercepting a user's interaction with a given system have emerged such as man-in-the-browser, man-in-the-middle and session hijacking. Common to these threats is that as the threat-technology matures and becomes mainstream, the adoption of that technology grows exponentially. These sophisticated schemes are still less common and far overshadowed by phishing and pharming attacks.

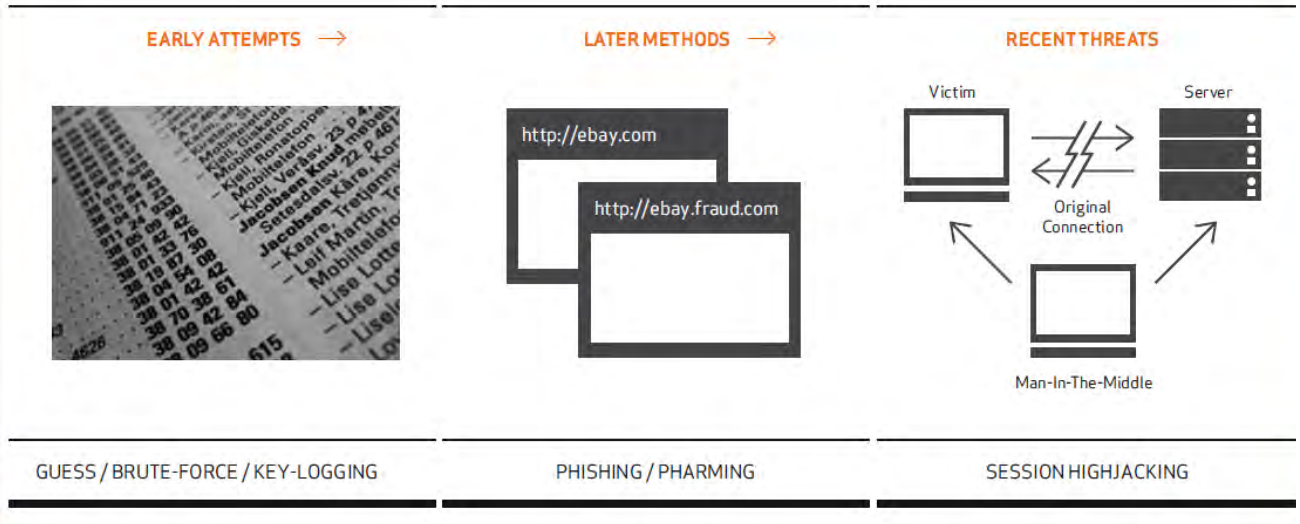


Figure 1) It has become a never ending cat-and-mouse game, where the industry continues to try and outpace the criminals. For corporations offering business services, the trade-off between the threat risk level and the costs and investments required to protect against them is a continuous process.

THE RIGHT LEVEL OF PROTECTION

As the complexity of the access protection increases, so does the complexity of the threats. This is a never-ending battle where organizations constantly need to evaluate what is the right level of investment – and protection – for the business. Often, the best possible protection is out of reach for many organizations and thus a trade-off has to be made.

To protect against these employee and customer identity theft schemes within budgetary constraints, organizations have embarked on different technologies such as certificates, biometric scanning, identity cards and hard- and software tokens, with the latter being the most dominant technology.

Certificates are often viewed as the ideal solution connecting two devices with a secure identifiable connection. The main issue is the deployment and administration of these certificates and the risks that these are copied without the user knowing it. Biometric scanning is also viewed as a very secure alternative. However, the assumption that you always have a functioning finger or iris scanner handy has proven impractical plus the fact that the scan represents a digital file that can be compromised.

Identity cards have also been viewed as a good solution but like the biometric scanners, it has proven to be impractical, especially in a world that calls for **B**ring **Y**our **O**wn **D**evice, consequently where users demand access from an ever changing variety of devices..

This leaves the field to two-factor authentication tokens. Two-factor authentication means that a login uses two factors, something you know: the user name and password, and something you have: a "hardware token" (a small device with a display where a code is shown) or a “soft token” app (a program installed on a mobile phone showing a code on the phone’s display). This code is entered along with user name and password to gain access.

This is a more complicated protection mechanism with an administrative burden and for the software token with limited phone brand support. The assumption is that the token protects users against phishing and the likes easier than any of the alternatives above.

In reality however, the token approach, which may have been seen as providing the best protection with the highest ROI in the past, have been cumbersome to administer and have now been surpassed by malware such as the Zeus. Zeus and the likes can do this as they take advantage of the weakness that a user enters the code together with user name and password. Furthermore, a simple web search will provide "cook-books" on methods for compromising token-based security systems. This family of solutions is called *Pre-issued passcode based solutions”* and have all the same weakness. Moreover, this is regardless of whether the passcode is delivered via a hardware- or software token or even if it is shipped using an SMS. A new more secure approach is needed.

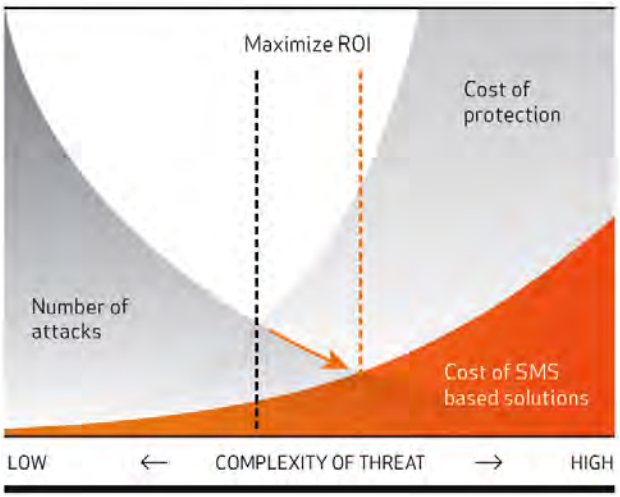


Figure 2) as illustrated above, the number of attacks decline dramatically as the access system complexity and protection mechanism grows. However, protection against the modern threats results in exponentially growing costs. With a real-time multi-factor authentication solution based on SMS, this trend is broken as the costs are driven down while at the same time the security increases. This is driven by the global adoption of the mobile phone that eliminates the need to manage physical user devices. The new generation of real-time multi-factor authentication solutions based on SMS provides a higher level of protection at a lower cost than the comparable alternatives.

DIFFERENT APPROACHES - DIFFERENT OUTCOMES

To address the demand for more security and to be able to address the modern threats, while meeting the users need for easier and more flexible solutions, a new generation of multi-factor authentication based on the mobile networks has emerged.

The main driver for this new generation of solutions is that many organizations, including organizations who traditionally did not focus on a high level of security, now due to the present threat landscape need increased security and that is without having to take on the cost and administrative burden of maintaining hard- or software based tokens. Additionally the present threat landscape now includes many tools that compromises the traditional solutions. Consequently, the ability to have a device that is connected in real time and at the same time is unique to that particular individual all over the world. To truly take advantage of this, the solution needs to operate in real-time generating the code for a particular login session and not on a "valid until" time or "Valid until used" basis. As a matter of fact, most of the current sms based solutions have been implemented so they fundamentally work like a token where the code is valid for a period of time or until used and not specific to the login session. The only real difference being that the code is passed to the user via a mobile phone display via SMS. Thus it is still a code valid for a period of time and therefore it can be compromised just like a regular token. The notion that you have a token code that is pre-calculated or known in advance and not created in real-time was the reason behind the attacks against the leading token technology in the world.

Thus a regular token via SMS is not necessarily safeguarding against the modern threats. To do so, a new generation modernized approach needs to be designed to operate efficiently in a message based environment like the mobile networks and it must be built on a set of key parameters:

▶ Increased Security: The solution must leverage the network connected benefits providing the ability to tie the login identity to a personalized unique device – the phone – and to send a code to that device that is tied to the specific user login attempt (also known as login session). Hence preventing the code from being easily compromised by even simple phishing like it is the case with tokens or any pre-issued passcode based solutions.

▶ Easy infrastructure: To ease the burden on the ever increasing infrastructure complexity, the solution must automatically plug into the different login scenarios such as Citrix, VMware, Cisco, Microsoft, SSL VPNs, IPsec VPNs and web logins and provide these logins in an integrated, session based architecture.

▶ Fault tolerance: As the system moves to a real-time delivery of the code, the architecture needs to be robust and redundant on the server side as well as supporting multiple delivery mechanism regardless of geographic location. Furthermore, this needs to be supported for both small/midsize companies as well as large enterprises.

▶ Management: It must be installed and managed easily within the existing user management infrastructure.

2011 was the year of catastrophic hacks.

RECOGNIZED TECHNOLOGY LEADER

The SMS PASSCODE solution delivers a new generation of login security based on multi-factor authentication via the mobile phone SMS network.

To successfully protect an employee or consumer account from being accessed using these new advanced identity theft schemes, SMS PASSCODE can use multiple factors; ex. something you know (a user name and password), and something you have (a mobile phone), and even the specific session the users is logging on from. SMS PASSCODE can also use the network the user is logging in from and even the country as a factor. Therefore SMS PASSCODE can create a security policy that only allows logins from certain users, accessing from certain countries, which radically limits the hacker's possibilities to compromise the login systems.

Essentially, a user first enters the user name and password. Once this is validated, the solution generates and sends in real-time a one-time passcode to the user's mobile phone via SMS, voice call or via a secure e-mail. The passcode has to match up against the initial login attempt, as it is only valid for that particular login session. This is also referred to as a "session specific code".

This subtle, yet dramatically different approach makes SMS PASSCODE a more secure new generation solution designed for today's threat landscape.

SMS PASSCODE offers a number of major advantages compared with other SMS based solutions, software and hardware tokens alike as it provides a more secure and intuitive login process, plug-and-play integration, and highly scalable and fault tolerant implementation.

▶ More secure login process: SMS PASSCODE represents a new level of security with session based and location aware login security, where the one-time passcode is tied to and generated based upon a successful user challenge validation (name and password match) and where the SMS code can contain location information notifying a user of a potential advanced hacker attack.

▶ Plug-and-Play integration: SMS PASSCODE installs in a very simple and fast process and protect all the major login scenarios like Citrix, VMware, Cisco, SSL VPNs, IPsec, VPNs, Outlook Web Access, and other Cloud based systems. The Installation process even handles Active Directory integration with a single click, as it requires no changes to the Active Directory.

▶ Maximum scalability and reliability: SMS PASSCODE uses the same solution to implement a 5 user installation and a 50,000 user installation. The architecture is built from the ground up to be fault tolerant and scalable as all components are coupled in a message based framework.

▶ High flexibility: SMS PASSCODE's unique policy driven engine can handle many diverse needs from individuals to groups, making the solution very user friendly even if the organization has many different kinds of needs.

▶ Lower costs: SMS PASSCODE delivers this higher level of security at a lower cost than any alternative solution, and with higher user convenience.

It is the combination of a new generation more secure solution that is easy to implement at much lower costs even in complex environments that has paved the way for the significant user adoption of SMS PASSCODE.

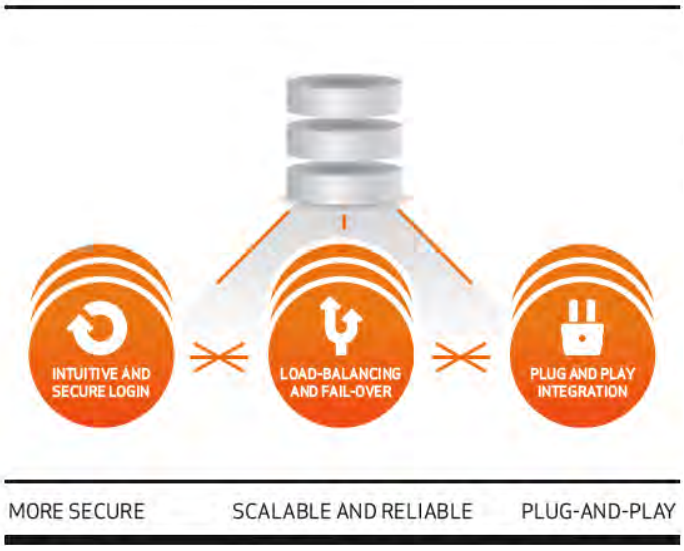


Figure 3) SMS PASSCODE offers a number of major advantages compared with other SMS based solutions, software and hardware tokens alike as it provides a more secure and intuitive login process, plug-and-play integration, and highly flexible, scalable and fault tolerant implementation.

SUMMARY

The threats on the internet have rapidly surpassed the current defenses. The result is that identity theft by some is said to be the most profitable financial crime today. To protect against this, many companies have relied on the more than 20 year old token two-factor authentication technology. However, malware like Zeus or even simple phishing has successfully developed threats that can capture token codes and compromise the user account.

Protection against this new generation of threats calls for a new generation multi-factor authentication solution. In essence a solution that can deliver a session and location specific code to the users mobile phone in real-time, ensuring that the code is generated subsequent to a user name and password challenge, after which the code is entered to complete a closed loop login process.

The benefits of using a real-time network connected solution are many including increased security, ease of user adoption, and lower costs. SMS PASSCODE has been recognized by major industry illuminators like Red Herring, Secure Computing Magazine and Info Security Magazine as the technology leader in this new generation of network connected solutions.

To learn more, and to take a "test drive", please visit: www.smspasscode.com.

About SMS PASSCODE

SMS PASSCODE is the leading technology in multi-factor authentication using your mobile phone. To protect against the rise in internet based identity theft hitting both consumers and corporate employees, SMS PASSCODE offers a stronger authentication via the mobile phone SMS service compared to traditional alternatives.

SMS PASSCODE installs in minutes and is much easier to implement and administer with the added benefit that users find it an intuitively smart way to gain better protection. The solution offers out-of-the-box protection of the standard login systems such as Citrix, Cisco, Microsoft, Juniper, VMWare and other IPsec and SSL VPN systems as well as websites. Installed at thousands of sites, this is a proven patent pending technology.

SMS PASSCODE has been awarded twice with the prestigious Red Herring 100 most interesting tech companies list, Gartner Group Magic Quadrant in User Authentication, a Secure Computing Magazine Top 5 Security Innovator, InfoSecurity Guide Best two-factor authentication, a Citrix Solution of the Year Finalist, White Bull top 30 EMEA companies, a Gazelle 2010 and 2011, 2012 Fast Growth firm and a ComOn most promising IT company Award.

Artaker Computersysteme GmbH
www.artaker.at | office@artaker.at | 1040 Wien, Heumühlgasse 11
Wien: +43-1/588 52-180 | Linz: +43-732/907 602 | Graz: +43-316/908 701

www.smspasscode.com