Top Online Banking Threats

to Financial Service Providers in 2010
Table of Contents

Introduction.................................................................................................................................................. 3
No Silver Bullet ............................................................................................................................................ 4
Authentication.............................................................................................................................................. 4
The Trade-Off ............................................................................................................................................... 4
Top Threats to Financial Services ........................................................................................................... 5
Solutions for Identity and Data Protection ................................................................................................. 8
SafeNet’s Approach to Identity and Data Protection .................................................................................. 10
Achieving Strong Authentication with SafeNet....................................................................................... 11
Keeping an Eye on the Bottom Line ........................................................................................................ 12
Conclusion .................................................................................................................................................. 12
Introduction

Trust is the foundation of any good relationship. And this has never been truer, or more vital, than with the relationship between financial services providers (FSP) and their customers. Without the confidence that their financial information is protected, consumers will be less likely to use online services. This will directly impact banks initiatives toward cost reduction and efficiency, a key goal around online services. While the consumer must exercise good judgment in how they dispense their personal information, the onus is on the FSP to provide a secure environment in which the customer can conduct their financial transactions.

The financial community is faced with the worst economic conditions in decades. It is vital now more than ever to seek ways to cut costs, retain customers, improve business processes, and demonstrate a positive return on investment to stakeholders. Securing a financial services network environment can be a daunting challenge. At issue is not only meeting the basic business requirement of ensuring that a customer’s financial information remains private and secure, but to do so in accordance with the variety of industry and government regulations. For example, the Federal Financial Institutions Examination Council (FFIEC) issued guidance specifically for banks regarding authentication in Internet banking environments: “For banks offering Internet-based financial services, the guidance describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using the online products and services. Examiners will review this area to determine a financial institution’s progress in complying with this guidance during upcoming examinations.”

Security breaches can have a far-reaching impact to not only a company’s finances, but to their reputation as well. Companies are required to prove their compliance with these regulations and will be held liable for their failure to do so. There is an expectation from customers, employees, and partners—anyone that entrusts a company with their sensitive information—that this information will be protected. Financial organizations must consider all of the potential damage that can be done to their business if sensitive data is lost or stolen—lawsuits, negative publicity, loss of sales and customer confidence, and permanently tarnished reputations.

Studies have shown that the financial services industry has become a primary target of cyber attacks on a global scale. This is not surprising considering the highly valuable information that all FSPs collect and maintain on a daily basis. According to a February 2010 report by Javelin Strategy & Research, total financial losses from identity fraud in 2009 were $54 billion, an increase from $48 billion in 2008. Offering a wider range of online services alone will not be sufficient to reduce customer churn; it must be accompanied by enhanced security features that provide the customer with confidence and, in turn, results in winning their long-term trust and loyalty.

It is, therefore, essential that financial services providers take a proactive approach to identifying potential cyber attack threats and the areas of vulnerability within their own infrastructure. To aid in this process, this paper will provide insight into the top five threats to the online banking in the financial services industry and SafeNet’s recommended solutions for a defense that not only provides a secure transaction environment for customers but also satisfies stringent government and industry compliance regulations.

No Silver Bullet

In the past, most organizations, including those in the financial services industry, were able to make do with a perimeter defense, employing firewalls, intrusion detection, and antivirus software to keep threats at bay and meet compliance requirements. However, not all methods can be used for all threats; therefore, it is advisable to mix the range of solutions to match the threats, usability issues, and the specific requirements of your business in order to achieve a strong authentication and management solution. By making identity and data security an operational cornerstone of their business, FSPs can take an important step towards also ensuring customer confidence.

Authentication

All authentication methods are based on providing the legitimate user with one or more mechanisms for proving their identity. Such “proof” can involve something that only the user knows, such as a password, and something that only the user has access to, such as a physical token or smart card, which is difficult to clone. Unfortunately, most types of authentication proof are rarely infallible—a user’s password may be guessed, or personal information may be easily discovered or disclosed by the user, for example, on social networking sites, such as Facebook or MySpace. Likewise, an external piece of hardware can be temporarily accessed by others, and so on. Thus, multi-factor authentication uses the combination of two or more methods to ensure that, in case of password or token disclosure, the access is still protected since both items are needed for access, thus making impersonation difficult.

In this electronic age, where identity and data theft are becoming commonplace, it is vital that a person’s digital identity be protected at all times. Multi-factor authentication uses two or more factors to validate a user’s identity. Authentication schemes based on multiple factors can be more challenging to compromise and, therefore, serve as an effective solution for high-risk environments, such as online banking. Of course, the effectiveness of a specific method of authentication relies a great deal on the quality of the product/solution selected, as well as implementation and management.

The Trade-Off

It is widely believed that security is a simple trade-off—the higher the security obtained, the greater the cost and user inconvenience. Thus, it suffices to put on one side the expected cost of a successful attack and, on the other side, the cost of greater user inconvenience and the cost of the security mechanism itself. Once these are understood and balanced, it may be assumed that the correct system is easy to choose. However, the fact is that different mechanisms fare differently in the face of incomparable threats. In addition, not all mechanisms can be used for all purposes; for example, not all authentication methods are appropriate for online banking.
Top Threats to Financial Services

Financial services providers are faced with complex challenges that directly affect their bottom line and, potentially, their very survival in a high-churn market. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, should be a core requirement of every company’s security strategy. With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, organizations must focus squarely on their security infrastructure.

According to a 2009 report by the Identity Theft Resource Center, breaches within the business sector rose from 21 percent to 41 percent between 2006 and 2009, far outpacing other sectors. The report also indicated that malicious attacks surpassed human error for the first time in three years. Perhaps the most surprising and unsettling statistic in the study is that, out of 498 reported breaches, “only six reported that they had either encryption or other strong security features protecting the exposed data.”

---

In a study\(^4\) conducted by the Verizon Business RISK Team in 2009, 74 percent of data breaches resulted from external sources, with 91 percent of all compromised records linked to organized criminal groups. The report also determined that a major focus of cyber crime is the financial services sector and the theft of personal identification number (PIN) information, and their associated credit and debit account information.

For financial services organizations, the importance of protecting financial data and assets, and retaining the trust of its customers, employees, and business partners, cannot be overstated. Consider a recent incident in which a Texas bank\(^5\) sued a business customer in order to simply have the court declare that its systems are reasonably secure. The lawsuit was in response to the customer’s demand for repayment of unrecovered funds and their claim that the theft occurred due to the bank’s failure to implement adequate security measures. While an unusual twist to a data breach incident, it represents the importance of security and accountability in the financial services industry.

For over 25 years, SafeNet has led the market in protecting the most sensitive financial transactions for the world’s most important financial services institutions. To achieve this level of respect and success, SafeNet maintains diligence in monitoring the data security landscape, including current technologies, consumer trends, and threat analysis. This section will identify those threats SafeNet considers to be the most prevalent and the most dangerous to the financial services industry.

**Phishing** – Although passwords can also be obtained through less sophisticated means such as eavesdropping, guessing, dumpster diving, and shoulder-surfing, phishing is a common form of cybercrime typically carried out through e-mail or instant messaging, providing links or instructions that direct the recipient to a fraudulent Web site masquerading as a legitimate one. The unsuspecting user enters personal information (such as user names, passwords, Social Security Numbers, and credit card/account numbers), which is then collected by the hacker. Of particular attraction to phishing scams are online banking, payment services, and social networking sites. According to the Gartner survey referenced previously\(^6\), phishing attacks continue to exact financial damage on consumers and financial institutions, with a trend toward higher-volume and lower-value attacks. The survey found that more than five million U.S. consumers lost money to phishing attacks in the 12 months between September 2007 and 2008, a 39.8% increase over the number of victims a year earlier.

---


\(^5\) http://www.computerworld.com/s/article/9149218/Bank_sues_victim_of_800_000_cybertheft


Top Online Banking Threats to Financial Service Providers in 2010
The number of crimeware-spreading sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December 2008, an 827% increase from January of 2008.

*Source: Anti-Phishing Working Group, March 2009*

**Password Database Theft** – Stolen user credentials are a valuable commodity and, often times, cybercrime rings operate solely to obtain this information and sell it to the highest bidder or use it themselves to access user accounts. Hackers steal user data and passwords from one Web site operator to hack other sites. Since many people use the same user ID and password combination for multiple sites, the attacker can hack additional accounts that the user has.

The Sinowal Trojan is a well-known attack developed by a cybercrime group several years ago that is responsible for the theft of login credentials of approximately 300,000 online bank accounts and almost as many credit card accounts. In late 2009, Microsoft Hotmail,7 Google Gmail, Yahoo, and AOL were victims of phishing attacks that exposed thousands of e-mail account user IDs and passwords.

**Man-in-the-Middle (MitM)** – In this type of threat, the attacker can actively inject messages of its own into the traffic between the user’s machine and the authenticating server. One approach for MitM attacks involves pharming, which involves the usage on malicious network infrastructures, such as malicious wireless access points or compromised DNS servers, to redirect users from the legitimate site they are trying to access to a malicious fraudulent Web site that accesses the user credentials and acts on behalf of the user to perform malicious activities.

---


Top Online Banking Threats to Financial Service Providers in 2010
Man-in-the-Browser (MitB) – MitB is a Trojan horse program, a variant of a MitM attack, that infects the user internet browser and inserts itself between the user and the Web browser, modifying and intercepting data sent by the user before it reaches the browser’s security mechanism. A MitB attack has the ability to modify Web pages and transaction content in a method that is undetectable by the user and host application. It operates in a stealth manner with no detectable signs to the user or the host application. Silentbanker is a well-known example of a MitB attack targeted at bank transactions. It uses a Trojan program to intercept and modify the transaction, and then redirect it into the attacker’s account.

Identity Theft – Identity theft refers to all types of crime in which someone illicitly obtains and uses another person’s personal data through deception or fraud, typically for monetary gain. With enough personal information about an individual, a criminal can assume that individual’s identity to carry out a wide range of crimes. Identity theft occurs through a wide range of methods—from very low-tech means, such as check forgery and mail theft to more high-tech schemes, such as computer spyware and social network data mining. The following table illustrates well-known socialWeb sites that have been attacked.

<table>
<thead>
<tr>
<th>Site</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>Fake profiles, SEO poisoning, Malicious links, Malicious document links</td>
</tr>
<tr>
<td>Facebook</td>
<td>Site masking, Twitter and Status malware links</td>
</tr>
<tr>
<td>TinyURL.com</td>
<td>Blogs hosting malware, Blogs linked to malware, Fake SEO links</td>
</tr>
<tr>
<td>bit.ly</td>
<td>Massive fake accounts, Fake SEO links</td>
</tr>
<tr>
<td>Blogger</td>
<td>Infected image links and comment links, Domain typo-spoofing</td>
</tr>
<tr>
<td>Blogster</td>
<td>Videos with malicious links, Links to infected spoofed code</td>
</tr>
<tr>
<td>bebo</td>
<td></td>
</tr>
<tr>
<td>hi5</td>
<td></td>
</tr>
<tr>
<td>digg</td>
<td></td>
</tr>
<tr>
<td>imageShack</td>
<td></td>
</tr>
<tr>
<td>Picasa</td>
<td></td>
</tr>
<tr>
<td>YouTube</td>
<td></td>
</tr>
<tr>
<td>Google video</td>
<td></td>
</tr>
</tbody>
</table>

Solutions for Identity and Data Protection

So what works and what doesn’t? We begin this analysis by describing the properties needed for thwarting the types of attacks that we consider most threatening to the financial services industry.

Phishing - These attacks use social engineering to trap people into giving up their personal information. Users are sent bogus emails that lure users to Internet sites that mimic legitimate sites. Many users, unaware that criminal intent is behind the e-mail, open them, fall into the trap and land up entering personal information into a fraudulent Web site.

---

Password Stealing and Identity Theft - These types of attacks rely on the ability of the attacker to fool users into giving up their personal information and credentials. Since users are typically vulnerable to these types of attacks, any method that relies on a credential that can be disclosed is vulnerable to social engineering attacks. Note, however, that this does not include a physical transfer because users can be rather easily fooled over the phone or via e-mail and the Internet to disclose personal information, but just like the keys to their house or their ATM card, people are less likely to hand someone they don't know their physical smart card or token device.

In contrast, hardware-based secure storage and smart cards are non-transferable and, resist cloning therefore, are less vulnerable to social engineering. The status of software-based secure storage and software-based smart cards is very dependent on the implementation. Many popular implementations enable a user to copy and paste the credential, making it transferable and, therefore, vulnerable. However, it is possible to prevent the user from doing this (without expert hacking skills), in which case, the solution does provide some degree of protection.

Man-in-the-Middle (MitM) Attacks - This type of attack is only successful when the hacker can impersonate each endpoint to the satisfaction of the other. The use of SSL authentication using a mutually trusted certification authority provides strong protection against MitM threats. When the certificate validation relies on the user, the user may fail to correctly validate server certificates and will click through the warning messages. Therefore, when using a certificate-based authentication solution, the onus is usually on the bank itself to ascertain whether the user’s certificate is valid and will not allow a session to be created when the certificate does not match the one in its system.

Although SSL with server authentication makes man-in-the-middle attacks harder to carry out, they are still possible by using phishing or other methods. We do remark that one-time passwords have the advantage that stealing the credential provides the attacker with a single access only (in contrast to stealing a regular password or a credential in secure storage, which provides the attacker with long-term, repeated access). Damage is limited but the vulnerability still exists. The most effective implementation of smart cards/tokens utilize the device along with a user ID and password for secure two-factor authentication).

Man-in-the-Browser (MitB) Attacks - A MitB attack is carried out by infecting a user browser with a browser add-on, or plug-in that performs malicious actions. In principle, as soon as a user’s machine is infected with malware, the attacker can do anything the user can, and can act on their behalf. If a user logs into their bank account while infected, the attacker can make any bank transfer that the user can. By the virtue of being invoked by the browser during Web surfing, that code can take over the session and perform malicious actions without the user’s knowledge.

An effective defense against MitB attacks is through transaction verification utilizing either out-of-band (OOB) technology, in which a user’s identity is verified through a separate channel, such as a telephone. Using a separate channel reduces the risk that both the internet and the additional channel have been compromised. In large financial environments, for example, when a user initiates a transaction, such as a funds transfer, the details of the transaction can be captured and sent back to the user via an automated phone call or SMS message for verification before the transaction is processed. User input is performed either through Interactive Voice Response (IVR) or the keypad. Both of these approaches assume that the user has mobile phone connectivity during the transaction.

Another approach involves the use of a secure portable Web browser that is launched from a bank-issued USB token after the user inserts the device and enters their password. After successful login, the user is taken directly to the issuing bank’s Web site. Utilizing a clean, non-infected browser helps ensure that there is no malware in the browser.
Fraud detection also helps limit the damage an MitB attack can wreak. Although fraud monitoring works after the fact, once a threat has been detected, it can provide useful information to the financial organization as to the types of threats being perpetrated against their infrastructure. User behavior analysis and trend reporting that most fraud detection programs provide can help FSPs determine the risk associated with certain types of transactions. However, fraud detection alone provides little comfort without a formidable defense strategy. When working together with strong user authentication, threats can be captured and contained, while authorized users are allowed secure access to their accounts.

**SafeNet’s Approach to Identity and Data Protection**

Due to the prevalence of malware threats focused on the financial services industry, we do advise incorporating a mix of hardware and software solutions for different user scenarios, depending on the level of security needed for each user. Choosing a solution that enables such a mix also has the advantage that it is possible to first deploy the highest-level of security for some users, and to select other options for other users, based on risk, the users' willingness to use hardware or software-based solutions, and other factors such as TCO.

Because multi-factor authentication requires multiple means of identification at login, it is widely recognized as the most secure methodology for authenticating access to data and applications. SafeNet’s multi-factor authentication solutions allow financial services providers to conduct their Internet-based business operations securely and efficiently, open new market opportunities with secure data access, and protect identities across the business landscape. It is important to note that any malware already present on a computer can carry out malicious operations after the user authenticates because, at this point, it is assumed that any operations originating from the computer are those of the legitimate user. However, the important point is that the damage is limited to this session; once the session is closed, the attacker cannot re-authenticate.

Strong authentication significantly reduces the risk of fraud and data theft, and allows financial organizations to comply with industry and government regulations and standards. SafeNet’s approach allows financial organizations to protect sensitive customer data and transactions at every point in the system—online consumer banking, internal databases, employee laptops, and corporate transactions. Customer care is improved through the higher availability of online services and greater customer confidence in the security of their online assets.

The threat from trusted insiders within the financial organization poses a particularly serious threat. Ease of access to account data, disgruntled employees, and pressures from a down economy have contributed to a rise in this type of crime. Bank employees can also become unwitting participants in bank fraud when their computers are specifically targeted by cybercriminals as a way into the financial network. While authentication cannot prevent an insider breach from occurring, it does create an audit trail of who did what where and when, allowing illegal activity to be more easily traced to its source.

Typically, most organizations will already have a user name and password system in place for network authorization and access; however, deploying a token or smart card solution, including one for consumers or partners that are not part of the internal network, is quickly becoming the method of choice for achieving increased security, and for addressing government and industry requirements for compliance and confidentiality.
Achieving Strong Authentication with SafeNet

Strong authentication is highly effective in combating most forms of cybercrime reviewed in this document. It solves the problem of password stealing, phishing, pharming, and man-in-the-middle attacks by requiring users to access the financial institution’s Web sites with “something they have” – an authentication token, and “something they know” – the token password. Even if criminals know the token password, without the actual token, they are unable to access the Web portal.

Financial organizations, more than ever, need to positively identify employees, contractors, and customers for both physical and logical access. Storing “digital identities” on a secured device, such as a smart card or token, is emerging as a preferred method for assured user identification. These devices can add security and convenience to widely used enterprise applications, such as Windows logon, VPN access, network authentication, digital signatures, and file encryption/boot protection.

MitB attacks are more complex since they are perpetrated from within the computer. One way banks can protect their customers is through strong authentication combined with transaction verification. In this case, the bank sends the details of the transaction to the user via a separate channel, such as SMS. Only after the user enters the details of the transaction and validates it with a passcode, will the bank grant authorization.

Another way to prevent malware from infecting a browser is to provide customers with a “trusted browser” stored on a USB smart card or token with portable memory. When users log on to the secure banking portal, they load a clean, untainted browser from the USB token and use it to access their account.

The typical financial institution supports a variety of access scenarios—local and remote employees, vendors, contractors, and customers—located at points around the world, through wired and wireless connections. With SafeNet, FSP’s can customize authentication solutions to specific risk levels and use cases. From an all-in-one, out-of-the-box one-time password (OTP) authentication solution to readerless smart card certificate-based authenticators, including encrypted flash memory storage, to software-based authenticators that support SMS and OTP delivery to mobile devices, SafeNet has a solution for even the most demanding financial services environment.

SafeNet’s authentication solutions help financial organizations significantly reduce the risk of fraud and data theft, and allow them to comply with strong authentication requirements for online banking as mandated by the FDIC and other industry regulations. SafeNet’s solutions also reduce IT overhead by streamlining all authentication operations, including deployment, provisioning, and ongoing maintenance.

To stay ahead of the relentless barrage of cyber threats, FSPs must take a proactive approach to identity and data security. It is more important than ever to design and implement a comprehensive plan of protection to provide not only the financial organization, but employees, associates, and customers with the assurance that their identity and information are secure.

SafeNet authentication solutions remove the complexities associated with deploying smart cards/tokens and digital identities, enabling FSPs to quickly leverage the benefits offered by these technologies - reduced operational costs, increased profits, and an enhanced customer experience that provides convenient and, most importantly, secure access to their financial information.
Keeping an Eye on the Bottom Line

The change from paper to digital transactions has allowed financial organizations to reduce their operational costs, increase profits, and enhance the overall customer experience by providing convenient and instant access to their financial information. With a concentrated effort towards identity and data protection, financial service providers can apply renewed enthusiasm and vision to their strategies for moving customers to electronic-based business practices. With a properly secured environment, one in which authentication, trust, and accountability are established, financial organizations and customers alike can feel confident in conducting business online.

A design imperative for every SafeNet product is customer return-on-investment. Implementing a security solution must not only solve critical protection and compliance issues, but must also be cost-effective to integrate and maintain. Should a security breach take place that puts the sensitive data of a company and its customers at risk, the officers of the organization may well be directly accountable to not only the company’s Board of Directors, but also to its customers and shareholders.

By implementing a strong authentication system, banks and other financial organizations can secure their digital communication and transaction systems, and increase profitability by lowering operational costs. As consumers perform more electronic transactions, such as credit and debit cards purchases, and online banking and investments, it is increasingly important for financial services providers to institute strict control over how customer information is protected on their networks, both during and after transactions. Having a strong authentication platform is imperative to instilling trust and preserving the financial service brand.

Conclusion

Why should financial services organizations care about strong authentication? The answer brings us full circle—trust. With a strong authentication process in place, the consumer can trust that their financial transactions are private and protected. With greater customer confidence comes lower customer churn and higher transaction volumes, resulting in increased revenue for the FSP.

With a security solution rooted in strong authentication, the financial institution can trust that they are in compliance with industry and government regulations, such as FFIEC, Basel II, PCI DSS, GLBA, and the Identity Theft Act, as well as FDIC and DigSig directives. As threats intensify and regulations increase, a security plan based around robust two-factor authentication places financial organizations in a state of readiness that customers, employees, and shareholders alike can rely upon.

Online financial transactions, payment settlements, and business-to-business exchanges all depend on establishing participant identity and data integrity. Other time-sensitive operations, such as documentation submission, bill calculation, and stock trading, require an auditable trail. Employing multiple, disparate products creates security gaps and heterogeneous environments, which are costly to manage, create compatibility issues, introduce vulnerabilities, and inhibit future growth. Strong authentication is the most direct and cost-effective way to ensure that any user attempting to access sensitive applications and data is an authorized party with the appropriate permissions to view, copy, and modify that data.
SafeNet is the dominant market leader in USB authentication, providing quality, stability, and credibility in an area that requires nothing less. Our solution to identity and data security enables financial organizations to protect sensitive customer data and transactions at every point in the system—internal databases, employee laptops, corporate transactions, and online consumer banking. SafeNet’s authentication solutions have the ability to support the variety of use cases that exist across the financial services landscape, including internal security, compliance, and varying levels of banking customers. The flexibility and scalability of SafeNet’s product offerings provide management and customization options to suite every need and risk level, with the ability to evolve from basic secure access to advanced applications.

It appears inevitable that people are changing the ways they identify themselves to their banks and SafeNet believes we will have an important role to play in the provisioning of these solutions. Customers demand complete assurance that their account information is safeguarded from all possible threats, and where they put their trust, and their money, will be largely based on an FSP’s reputation for providing a safe and secure place to do business. With strong authentication, financial services providers will have one of the core elements to ensure that digital transactions and communications are secure, compliance with regulations is achieved, and that customer privacy and company reputation remain intact.

To find out more about SafeNet authentication solutions go to:
http://www.safenet-inc.com/authentication