



A White Paper

Common Attacks That Jeopardize Financial Service Companies

How revolutionary two-factor authentication and strong traffic encryption protects systems from common attacks, policy weakness, and information theft—and plays a critical role in attaining regulatory compliance

**Authored by
George V. Hulme**

**KoolSpan, Inc.
11134 Stephalee Lane
North Bethesda, MD 20852
+1 (301) 468-9434
www.koolspan.com**

EXECUTIVE SUMMARY

The word is printed on our money. It can vanish forever from a single mistake. Yet, it's the cornerstone of every company that operates within the financial services sector. We're talking about trust. And few—if any—other industries appreciate the value of information integrity, or the risk of losing trust, more than financial services companies.

But a quick glance at news headlines shows that the cases of identity theft and the hacked systems that expose personally identifiable and financial account information, credit card, and social security numbers are all eroding trust. And the threats against the vulnerabilities of financial services business-technology systems are rising. Spyware writers are growing cleverer at lifting confidential information from systems and networks. Hackers are quicker to exploit the dozens of weekly-announced vulnerabilities that place systems at risk to attack and data theft. The Internet and business-technology systems have made it possible to work from anywhere and whirl both information and currency around the globe. This speed and availability of information, along with the complexity and inherent vulnerabilities of modern IT systems, enables attackers and malicious insiders to gain unauthorized access to information, whether they're sitting in an office cubicle in New York or at an Internet café thousands of miles away in Kazakhstan.

There are no greater threats to organizations than those that originate on the inside. In recent years, federal agents have arrested financial service employees for illegally obtaining and selling customer account information and accessing customer account information – without authorization and with the intent to commit fraud. A landmark study published by the CERT Coordination Center and the U.S. Secret Service in August 2004 examined 23 incidents conducted by 26 financial services employees between 1996 through 2002. The report highlights employees who altered customers' historical information for payment, conducted sabotage against IT systems, or misused or exceeded their authorized access levels to commit fraud. The study found that the incidents conducted by insiders required little technical sophistication. In fact, in 87 percent of the cases, insiders used simple, legitimate user commands to conduct their crimes. The attacks typically involved the abuse of organizational business rules and policies, rather than sophisticated hacker attacks. In about 30 percent of cases, the financial impact to the victim company exceeded \$500,000.

It's certainly not only criminally-intent insiders from whom financial services firms need to protect their internal networks, applications, and customer information; hackers and organized criminal rings are determined to infiltrate systems that hold either customer account information or information that could be used to conduct identity theft. They're using keystroke loggers to steal usernames and passwords. They try to trick unsuspecting bank employees into revealing their log-on credentials, and they rely on software and network vulnerabilities to infiltrate financial services systems. And, as larger financial institutions increase their security, hackers and organize crime are expected to increasingly target smaller, regional financial institutions, which are seen as easier targets.

Concerns about the availability, integrity, and confidentiality of financial information have led to an unprecedented number of state and federal laws and regulations in recent

years—from Gramm-Leach-Bliley and Sarbanes-Oxley, which aim to ensure the integrity, security, and confidentiality of financial information, to California SB 1386, which requires institutions to inform California residents when certain types of financial account information could have been accessed by an unauthorized party. All of these regulations seek to ensure that companies have the proper levels of security and access controls in place to manage regulated financial information. But it's clear that many firms don't have the adequate technical controls and policies to successfully protect their systems and information. There can be no other explanation for ongoing headlines of financial services firms—large and small—announcing that personally identifiable financial information may have been compromised.

The stakes are high. All that a criminally intent hacker has to find is a single mistake—a configuration error within a server, an application that wasn't timely patched, a guessed or stolen credential, such as a password. One of the clear weaknesses in today's commonly deployed security defenses is how openly proprietary and regulated information travels “in the clear” within the corporate LAN. Most of the security defenses in place today—intrusion detection systems, firewalls, anti-virus programs, vulnerability scanning—are deployed to defend and harden the perimeter of the LAN. As a result, when employees and other trusted insiders access applications within the LAN, the information they access is sent across the network as unencrypted, plainly readable information, available to any malicious insider or crafty attacker. To compound the problem, the vast majority of security defenses in place today only protect against known threats and require constant updates and tuning, such as firewall configuration changes, anti-virus, and IDS threat signature updates, to be able to protect against exploits and other attacks *only after they appear*. This leaves serious lag times—a window of opportunity—for attackers who operate one step ahead of most security vendors.

This paper will detail the common attacks used to infiltrate financial services systems and their networks, and provide insight into a revolutionary authentication and encryption solution that defeats all of them. Financial services firms need a way to protect their most valuable applications and data with traffic encryption that there's no known way to compromise, and with authentication credentials that can't be stolen.

COMMON ATTACKS THAT TARGET FINANCIAL SERVICE APPLICATIONS AND NETWORKS

Packet Sniffing Attacks

A packet sniffer is one of the oldest tools that can be used by attackers to capture as it's transmitted within the network. Any traffic transmitted without encryption—which can include usernames/passwords, personally identifiable information, and regulated financial information—is at risk of capture. Packet sniffers, which can be placed at various points along a network, are easy to install, yet very difficult to detect. One of the best ways to mitigate the risks posed by packet sniffers is to encrypt the internal traffic that transmits regulated and valuable information.

Man in the Middle Attacks

A man-in-the-middle attack is another common form of eavesdropping and data manipulation in which the attacker compromises network communications between two end points, often snooping an otherwise normal authentication process. For this class of attack, which can affect IPsec and SSL encrypted connections, wireless, and wired

networks alike, the attacker can capture, read, and even insert information into network traffic. Strong authentication and traffic encryption mitigate man-in-the middle attacks.

IP Spoofing Attacks

It's possible for attackers to try to "impersonate" one of the end points of a connection in order to "hijack" the connection. The attacker, in essence, tricks the server into thinking that the attacking system is actually a trusted client. This type of attack also can be performed in the opposite direction: the client can be fooled into thinking it's accessing a trusted server. This is a sophisticated attack, and there are countermeasures that can reduce the likelihood of successful IP Spoofing-style attacks. These include rejected packets that claim to be local but originate from the Internet, avoiding the use of source address authentication, and requiring two-factor authentication (that can't itself be spoofed or forged) to access applications.

Social Engineering Attacks

These occur when attackers attempt to trick employees into providing their usernames and passwords. Common social engineering ploys include emergency phone calls from "IT support" and phishing e-mails that target the log-on credentials for employees or anyone else who may have access into the systems of the targeted firm. Security awareness training and strong authentication are a couple of ways to mitigate this form of attack.

Password Attacks

Troubling, passwords still remain widely used when it comes to authentication and

Two-Factor Authentication Best Practices

Even the most air-tight security systems need to be carefully architected, deployed, and managed. The following best practices help organizations get the most from their strong authentication deployments:

1. Regularly review your organization's authentication policy. Determine who needs to have access to what networks and specific applications.
2. Establish organizational workflow: how will new employees be granted access to the necessary applications and networks? For current employees, how will access rights be modified as job responsibilities change? What supervisory sign-offs will be required? How will the change request be communicated and fulfilled by the IT department? How will employees be deprovisioned when they leave the organization?
3. Based on information value and regulatory risks, determine what applications require strong authentication and traffic encryption. Consider strong authentication for remote access, regulated systems, and the most valuable systems and applications.
4. Employees commonly forget their passwords, and at times authenticators will be misplaced or otherwise unavailable. To ensure employees have access to the systems and information they need, create a process that reliably confirms their identity before granting access.

access control. The danger is that passwords are easily guessed, jotted down on sticky notes, or quickly hacked through dictionary and other brute-force attacks from readily available tools on the Internet. Passwords and usernames also are stolen through Trojan horses, keystroke loggers, and packet sniffers that capture all network traffic. Criminally-inclined insiders, who know the organization and its people, find it especially easy to steal the usernames and passwords of their coworkers to gain access to applications and information they're not authorized to see. Password security can be increased somewhat by requiring the use of passwords that are eight or more characters in length, and consist of numbers, letters, and other characters. Users also should be required to change their passwords frequently. Two-factor authentication is the most effective way to mitigate password attacks.

Attacks Against System Vulnerabilities

Security vulnerabilities in applications and within the software that runs servers and network gear make it much easier for attackers to gain access to internal networks. Such flaws make it possible for attackers to infiltrate trusted systems within networks, install Trojans or packet sniffers, and launch other forms of attack that affect the availability, integrity, and confidentiality of systems and information. Timely application of security patches is the best way to reduce the risks associated with known application and network security flaws.

MITIGATING ATTACKS THAT TARGET THE CONFIDENTIALITY AND SECURITY OF YOUR SYSTEMS

The best approach to mitigate the attacks that commonly target financial services firms is through the consistent application of defense-in-depth. That is, the ongoing use of security policy, best practices, and the deployment of multiple layers of defensive technologies, such as properly configured firewalls, intrusion-detection systems, anti-virus programs, the encryption of critical data held within databases and financial applications, employee awareness training, and the regular updating of business systems with software patches. One of the most significant steps that financial services firms can take to protect against both network layer attacks and those that target the weaknesses associated with passwords is to have granular access control policies enforced through strong authentication and powerful traffic encryption. This greatly mitigates the risk from attacks that attempt to steal network traffic, pilfer passwords, and gain unauthorized access.

The Role of Two-Factor Authentication and Traffic Encryption to Boost Security and Help Attain Compliance

Two-factor, or strong, authentication, is typically authentication that verifies users' identity based on something that they "know," such as a password or a PIN, and something that they have, such as a token or a Smart Card. Strong authentication provides a much more secure way to authenticate entry to networks, applications and databases that hold business-critical and heavily-regulated financial information. Strong authentication also helps to ensure enforceable and auditable access to regulated information. The combination of two-factor authentication with the strong encryption of network traffic is, in conjunction with a defense-in-depth security program, the best way to protect against hackers, malicious insiders, or anyone not authorized to view or

access information as it whirls within the corporate LAN or is accessed by remote workers.

Conventional security measures have proven troublesome. In an attempt to increase security, especially for remote workers, most companies (if they allow remote access at all) rely on the use of encryption through virtual private networks and passwords. Highly security-conscious financial services firms added USB-tokens, smart cards, and one-time passwords (OTP) to the mix. The infrastructure costs associated with these technologies are high. First, there is the expense of the authentication/synchronization clocks on multiple servers; the dependency on an expensive VPN infrastructure to operate; and the ongoing overhead, whether outsourced or handled in-house, associated with managing a PKI infrastructure. The VPN infrastructure alone is not easy to manage, as help-desk calls concerning password resets and VPN-client software functionality often are excessively high. And, typically, VPNs do nothing to encrypt traffic for local workers accessing applications within the LAN. That leaves internal traffic wide open for snoops to steal information right off the wire through the use of tools such as packet sniffers. Also, traditional LCD devices that display OTPs often prove inconvenient. Their batteries die at inopportune moments and their display screens increasingly become unreadable over time through normal wear and tear.

For years, financial services firms have considered deploying strong authentication for internal access to applications and networks, but the hardware and integration costs associated with smart-cards, biometric devices, USB tokens, and OTP devices have proven prohibitive. The security gains often were determined not to be worth the required financial investment. But the risk reward equation for strong authentication and encrypted access to sensitive and regulated financial information has changed as regulatory compliance complexity and pressures have increased, as has the concerns surrounding data breaches and identity theft. That's why financial services firms increasingly seek an easy-to-deploy and manage, as well as a cost-effective, way

Two-Factor Authentication and Regulatory Compliance

While legislators and regulators have not established the types of technology that must be used to adequately provide for the confidentiality, integrity, and availability of regulated financial information, one of the cornerstones of compliance is to make certain that only authorized personnel have access to view or manipulate financial data. Passwords alone are no longer getting the job done.

For instance, in October 2005, the Financial Institutions Examination Council (FFIEC) issued new online banking standards that will require stronger authentication capabilities than simple usernames and passwords to conduct Internet transactions. The FFIEC wrote that more secure authentication methods will be needed "to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions." The same logic is true for both internal transactions and remote workers accessing regulated and proprietary information. In fact, in December 2004, the research firm Gartner declared that the effective use of passwords is near the breaking point. It said: "Mitigating authentication weaknesses by increasing password length and complexity will reduce security if passwords are pushed beyond the peak of their effectiveness. They are approaching this point now."

Passwords are on life-support, and it's just a matter of time before they're declared dead.

Regulated companies must provide reasonable precautions when allowing remote workers, customers, business partners, and suppliers to have access to applications and networks that contain regulated information. Two-factor authentication and strong network traffic encryption is one of the critical defenses to put into place to ensure that only authorized identities can access regulated information. That's why financial-services companies must now seriously consider strong authentication for access to regulated systems, enforce granular access controls to these applications and networks, and encrypt network traffic to protect against internal snoops and hackers.

to provide their organization both strong authentication to protect access to valuable and regulated information and powerful traffic encryption within their corporate networks.

THE KOOLSPAN SOLUTION

KoolSpan Inc. provides such a solution. KoolSpan has devised a unique approach that provides network traffic security and strong authentication that doesn't require modification to the applications or networks it protects. The efficient KoolSpan platform comprises three components: a Lock, access Keys, and a management application. KoolSpan's cryptographic keys are generated and stored within hardware, and never are transmitted during the authentication process. Also, every packet of network traffic is encrypted with the strongest commercially available encryption, 256-bit AES, that doesn't affect performance. KoolSpan has developed a secure, extremely proficient, and cost-effective way for large and small financial services firms to grant users access to applications through strong authentication and the highest levels of network traffic security available.

The KoolSpan solution uses the metaphor of a Lock and Key. The Lock, a small network-based device, authenticates and bridges users onto the network. Multiple Locks can be used to securely connect multiple networks. For secure authentication and access to applications, end users are provided small USB Keys that enable PCs to bridge onto the network. There are no servers or other costly infrastructure required.

It's this simplicity of the KoolSpan solution that makes a clear ROI attainable. Compare KoolSpan with the cost of a two-factor VPN and internal LAN security deployment. The design, installation, equipment, and management costs for just the VPN are estimated to total more than 60 percent of a similarly sized KoolSpan installation. And the same KoolSpan deployment, if also used for internal LAN security, greatly reduces the complexity and expense of securing the network. In this scenario, the estimated TCO SAVINGS is greater than 165 percent.

The KoolSpan solution provides these immediate benefits:

- "Wake-up Secure" Smart Card capability leaves nothing exposed during authentication
- Simple, yet robust Lock and Key Architecture
- 256-bit AES encryption – the strongest commercially available
- Complete End-to-End Layer 2 protection
- Per-packet network traffic keying
- No need for certificate server or manager
- Compatible with all Ethernet-based networking equipment
- No need to alter existing applications or networking gear

How It Works

KoolSpan has accomplished this highly secure, yet deceptively simple solution through the company's distinctive, inventive use of Smart Card technology embedded within its network Lock and USB Keys. The authentication process is applied at both ends of a connection to provide an extremely secure communications link. KoolSpan provides

Layer 2, on-chip Ethernet encryption. The two Smart Cards independently authenticate with each other and securely compute the 256-bit AES session keys used to protect all network communications. The session key is changed with each network packet. This Layer 2 implementation provides actual bridging and transparent operation to all higher layer protocols, including IP and applications.

Network and Key Management

Unlike most other implementations that utilize digital credentials and cryptographic keys, which require complex servers or extensively managed PKI root authorities, KoolSpan is managed through its Enterprise Management application and a “Master Key” Smart Card. At setup, the Master Key is initialized and generates a set of unique network keys. The entire process takes place within the secured Smart Card. End user keys, which are “cloned” from the Master Key, are protected the same way. The secret keys of trusted users are enciphered and securely transmitted to the network-based Locks. Once this setup is complete, the Enterprise Management application need only be run when a change is required, such as adding and removing user Keys. The network Keys can’t be read directly, and are even unknown to the system administrator, who has complete control of the system. Through KoolSpan’s approach, enterprises essentially run their own turnkey “root authority.”

Layer-2 Operation

KoolSpan operates at Layer 2 of the OSI model. This is true whether operating within the enterprise LAN, a home Internet connection, or a Wi-Fi hotspot. The system doesn’t proxy users (typical of VPNs); rather it creates a secure Ethernet bridge for trusted users. This architecture is why KoolSpan can operate transparently to the network, devices, applications, and other assets it protects. This is accomplished by the Key and Lock securely authenticating at Layer 3; then the KoolSpan driver establishes a virtual Ethernet adapter that is encrypted at Layer 2 and tunneled at Layer 3. All of this complexity is hidden from the end users—they’re simply provided secure, authenticated access to the network and applications where the Lock resides.

Bi-Directional Authentication Without Key Exchange

KoolSpan achieves two-factor authentication without forcing the end users to type their one-time password. When the users insert the KoolSpan Key, they’re prompted for their user-defined eight-character password that identifies the user to the Smart Card within their Key. Without further user interaction, the Smart Card generates the OTP that is sent to the network Lock; the Lock replies with its own OTP enabling the user’s Key to authenticate the network. Network keys are never transmitted. The OTP generation process occurs entirely within the Smart Cards. This provides not only convenience for the end user, but allows mutual authentication to be established without exposing the OTPs to anyone. It’s impossible for the user, or anyone else, to access the OTP. It can’t be phished, hacked, guessed, stolen, or socially engineered from the end user—a weakness that plagues passwords and certain types of tokens. Also, the KoolSpan Key doesn’t require batteries that lose power at inopportune moments or LCDs that crack or grow difficult to read through normal use.

What Separates KoolSpan from Competing Strong Authentication and Traffic Encryption Solutions

Unlike traditional VPNs, KoolSpan doesn’t require any client application, certificates, or user-specific applications to be installed—just a simple client-side driver. All user-specific information is stored securely within the KoolSpan Key Smart Card. It’s through

this simplicity that KoolSpan slashes help-desk calls common with user names and passwords, as well as VPN-client software troubleshooting.

The entire authentication and traffic encryption process is hidden from end users and attackers—which greatly reduces the risk of attacks that target weaknesses in passwords and the network. KoolSpan’s solution greatly extends simple user authentication, but combines strong user authentication and highly-secure access to networks and applications in a single key that provides users a simple, consolidated, consistent way to access multiple networks and applications.

And the magic with KoolSpan is the way it lifts operational security and compliance without any need to overhaul existing applications or alter network infrastructure. The KoolSpan Platform operates transparently to the network and applications it protects, whether accessed from the internal LAN, remote, or wireless connection. Financial services firms now can more easily and cost-effectively bring a high level of trust, fortification, and compliance to their high-value business-technology systems, and protect regulated and highly sensitive information.

Financial services firms that implement KoolSpan will benefit from its simple, robust, and secure architecture:

- Instantly protect all network assets
- Powerful 256-bit AES internal LAN traffic encryption
- Remote users are directly connected to protected assets
- No impact on network or application performance
- Consistent user experience
- Secure wire-line, wireless, and VoIP applications
- Secure remote access across public networks
- Secure branch office connectivity

GEORGE V. HULME BIO

George V. Hulme is an internationally recognized information security journalist. For more than 20 years Hulme has written about business, technology, and IT security topics. From March 2000 through March 2005, as senior editor at InformationWeek magazine, he covered the IT security and homeland security beats. His work has appeared in CNN.com, Government Computer News, Nation’s Business, Network World, San Francisco Examiner, The Industry Standard, VARBusiness, and dozens of other technology publications.