Pragma Systems
Using SSH for PCI Compliance

A WHITE PAPER

Objective :

The objective of this document is to examine the federal and industry regulatory environment and to analyze the benefits of utilizing Secure Shell (SSH) in achieving PCI compliance. In addition, to review the role Pragma Systems, Inc. and its FortressSSH product can play in a robust, secure computing environment.

Executive Summary

In the wake of the first Sept. 30, 2007, Payment Card Industry (PCI) deadline for locking down networks and customer data, it's clear many companies – and more than half of smaller organizations – still fall short of prescribed security standards. As a result, the majority of Telnet-dependent companies are now scrambling to find cost-effective solutions for effecting full compliance with PCI Data Security Standards (PCI DSS).

And that's just PCI. Beyond the credit-card industry security initiative, state, federal and international regulators are driving the need for increased network security and full regulator audit compliance for companies of all sizes. From HIPAA (the Health Insurance Portability and Accountability Act) to GLBA (the Graham-Leach-Bliley Act), PIPEDA (the Personal Information Protection and Electronic Documents Act) to the technology tenets of Basel II, US companies face an alphabet soup of interwoven – and competing – requirements for protecting sensitive consumer information.

In a complex regulatory environment that's constantly changing, the only thing companies can be sure about is that, for all their simplicity and ease of use, Telnet and FTP do not provide the secure foundation companies require to effect a comprehensive compliance solution. Secure Shell (SSH) and its bundled file transfer component SFTP (Secure File Transfer Protocol) are exponentially more secure than Telnet and FTP respectively.

These days, the natural tension between the demands of day-to-day business and the need for greater system security is prompting many companies to migrate from the straightforward simplicity of Telnet to the heightened level of security provided by SSH. As they do, Pragma Systems' FortressSSH offerings are becoming their platform of choice.

Pragma Systems is the leading provider of end-to-end, enterprise-class SSH technology, facilitating secure remote access for all Microsoft Windows platforms. Pragma's end-to-end solutions provide highly secure access to corporate supply chain, CRM, distribution and warehouse applications over wireless, Bluetooth, LAN, WAN and mobile networks.

Pragma's extremely fast, scalable and feature rich FortressSSH product suites fundamentally address the security challenges associated with remote management, file transfer, and application delivery – providing the best possible platform for a comprehensive program to ensure compliance with the requirements of PCI DSS.

PCI Compliance Today: Too Little, Too Late

Over the last decade, credit-card identity theft has been responsible for tens of millions in financial losses for consumers, merchants and financial institutions. As a result, the world's major card issuers have collaborated to develop a set of universal data-protection protocol – the PCI DSS – in a bid to protect cardholder privacy and personal information. The PCI protocol requires all organizations handling card-based transactions to comply with 12 major security components, ranging from periodic vulnerability scanning to a comprehensive review of user entitlements.

Organizations failing to comply with PCI will soon face stiff financial penalties and the loss of capabilities to process card transactions – the lifeblood for many small to medium-sized businesses as well as major corporations. Adding to the complexity, companies working to satisfy PCI requirements must implement these guidelines across their entire environment, in many cases necessitating significant changes across all of their network infrastructure.

A recent ebiz.com report states that as many as 50 percent of Level 1 (see definition of levels below) merchants were not in compliance with PCI when the initial Sept. 30, 2007, deadline for Level 1 compliance passed – and an even larger percentage of smaller, Level 2 merchants are now scrambling to put in place the security measures they need to pass their first round of pending PCI audits. In a separate report, VeriSign, Inc. finds that 53 percent of all companies still fall short of meeting PCI data-security standards and, therefore, are not sufficiently protecting sensitive consumer information.

Analysts at Gartner, Inc., underscore these findings. "To live up to the trust of their customers, companies in the payment card industry need to implement enterprise-wide security processes and controls to protect card data and other sensitive customer information," writes John Pescatore, vice president, Gartner, Inc., in a recent published report. "The key to making PCI DSS compliance less cumbersome and less complex is to build security into ongoing operations."

Similarly, the Burton Group and its analysts continue to be inundated with small to mid-sized companies behind the eight ball on the PCI compliance front. "We've been fielding many questions from entities who are trying to achieve PCI compliance," states Diana Kelley, vice-president and senior analyst for the Burton Group, in a November 2007 story by the Associated Press. "Requirement 6, to 'Develop and maintain secure systems and applications,' is one area where customers are particularly confused about how to comply. "

As confusing as effecting compliance may be, though, not doing so can carry with it dire consequences. Companies failing to comply with PCI standards will soon face financial penalties or lose the ability to process credit card transactions. More important, the bad publicity that may stem from failing to comply could result in serious, lasting damage to a company's brand equity and corporate goodwill.

PCI DSS: The View from 50,000 Feet

To summarize, the PCI DSS requires merchants and member service providers (MSPs) who store, process or transmit cardholder data to:

- Build and maintain a secure IT network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks; and
- Maintain an information security policy

Compliance requirements depend on each organization's specific activity level. The PCI classifies companies into four levels, based on the annual number of credit/debit card transactions they process.

Level 1: Merchants with more than 6 million transactions p.a., or whose data has previously been compromised

- Must undergo annual onsite security audits and quarterly network security scans.

Level 2: Merchants with 150,000 to 6 million transactions a year

- Must complete annual self-assessment questionnaires; and
- Must undergo quarterly scans by an approved PCI scanning vendor.

Level 3: Merchants with 20,000 to 150,000 transactions a year

- Are required to undergo quarterly scans by an approved scanning vendor; and
- Must complete an annual self-assessment questionnaire.

Level 4: Merchants with less than 20,000 transactions

- Are not required to report compliance but the company must, nevertheless, achieve and maintain proven compliance.

PCI Compliance: Is Your Company Ready?

In the very near term, any business that processes, transmits or stores credit-card information, regardless of their level, will be required to begin demonstrating compliance with PCI DSS in the form of quarterly and annual audits by independent third-party providers. In fact, while the publicity surrounding security breaches has recently been focused on larger companies, Visa recently reported that the majority of data breaches are occurring at smaller businesses within the Level 3 and 4 tiers.

The PCI DSS defines a security framework that applies to all members, merchants, and service providers that store, process or transmit cardholder data. PCI DSS specifically requires that cardholder data and sensitive information be encrypted when transmitted across public networks.

In line with this, many mid-sized and smaller companies find themselves faced with the need to implement a comprehensive, effective, and cost-effective compliance program that meets the following 12 requirements:

1. Installs and maintains a firewall configuration to protect data
2. Eliminates vendor-supplied defaults for system passwords and other security parameters
3. Protects stored data
4. Encrypts transmission of cardholder data and sensitive information across public networks
5. Uses and regularly updates anti-virus software
6. Develops and maintains secure systems and applications
7. Restricts access to data by business need-to-know
8. Assigns a unique ID to each person with computer access.
9. Restricts physical access to cardholder data
10. Tracks and monitors all access to network resources and cardholder data
11. Regularly tests security systems and processes; and
12. Maintains a policy that addresses information security

When it comes to addressing all 12 of these requirements, no one product or approach fits the bill. For organizations now reliant upon Telnet and other unencrypted Internet connections, though, it's clear that effecting PCI compliance necessarily must begin with a shift to a system – likely SSH and SFTP– that provides secure connections for all Internet transactions.

PRAGMA SYSTEMS

FortressSSH: Jumpstart Your PCI Compliance

Without question, unencrypted internet connections such as Telnet and FTP can be intercepted and read by malicious hackers – and are, therefore, by definition unable to pass a third-party audit. Making the shift to SSH and SFTP are, then, the foundation most companies need to effect a robust compliance program – and Pragma Systems and its FortressSSH product suites stand alone in helping companies begin meeting the strictures of PCI DSS Requirements 4 and 10.

Most important, PCI DDS Requirement 4 calls for the encryption of cardholder data across open, public networks – the core ability of the FortressSSH Suite's functionality. Beyond this, PCI DDS Requirement 6 calls for companies to develop and maintain secure systems and applications – and FortressSSH gives developers the platform organizations need to create secure systems and applications. Finally, PCI DDS Requirement 10 calls for companies to track and monitor all access to network resources and cardholder data. Since FortressSSH logs authentication, its logging functionality affords companies a great start for putting in place a comprehensive program for tracking access to secure information.

Specifically, FortressSSH's protection measures effect compliance with the following tenets and subsections of Requirements 4 and 10:

Requirement 4.1-4.1.1:

Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL)/ trans port layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive card holder data during transmission over open, public networks.

4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely ex clusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use only in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.

When reviewing Sections 4.1 and 4.1.1, it is important to note that SSH (including FortressSSH) uses the same encryption mechanisms as SSL/TLS and IPSEC – and then goes one step further, actually providing additional security features. SSL is an older version of TLS: TLS 1.0 is the equivalent of SSL 3.0. SSH was invented to provide secure remote access and secure file transfer (via SFTP) similar to how SSL/TLS's origin was to secure web e-commerce and IPSEC's use is in to build VPN access. SSH and SFTP has become IEEE Draft standard and is widely deployed and adopted in the industry.

The Request for Comments (RFC) Overview Notes for the Internet lists two basic properties of the TLS Record protocol:

1. **The connection is private.** Symmetric cryptography is used for data encryption (e.g., DES [DES], RC4 [RC4], etc.) The keys for this symmetric encryption are generated uniquely for each connection, and are based on a secret negotiated by another protocol such as the TLS Handshake Protocol. The Record Protocol can also be used without encryption.

2.**The connection is reliable.** Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g. SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

In brief, TLS provides a mechanism to keep people from seeing data being transferred (connection and is private) and a mechanism to verify that the data being received was the data being sent (connection is reliable). That second feature may seem like a basic error-checking capability, but it is, actually, intended to prevent a hacker from modifying the data in route.

Moreover, IPSEC is defined in RFC 4301-4309. In Section 2.1, "Goals/Objectives/ Requirements/ Problem Description," it states that "IPSEC is designed to provide interoperable, high quality, cryptographically based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself). In fact, IPSEC provides a superset of SSL/TLS functionality." From this, it seems clear that encryption and message integrity are paramount to effecting compliance with PCI-DSS.

Pragma Systems' FortressSSH security features closely resemble IPSEC, utilizing the same algorithms for encryption: message authentication code (MAC) processing and key exchanges. Moving beyond the encryption function, however, SSH affords companies the perfect balance of security and ease-of-use. FortressSSH provides more flexibility in authentication than either SSL/TLS or IPSEC, it's easier to use, and it's as secure as SSL/TLS or IPSEC. Simply put, SSH offers an effective, elegant approach to meeting the mandate of PCI DDS Requirement 4.

Requirement 10.2.4-10.2.5:
Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.2.4 Invalid logical access attempts

10.2.5 Use of identification and authentication mechanisms

Pragma's FortressSSH Suite directly addresses the tenets of PCI DDS 10.2.4-10.2.5, providing robust authentication including password, public key, and Kerberos authentication mechanisms. FortressSSH also readily facilitates tracking and logging invalid logging attempts and valid connections.

International Organic Grocer, Pragma & PCI: Food for Thought

Like other Level 1 merchants, the world's leading retailer of natural and organic foods – with more than 250 retail outlets in North America and the United Kingdom – was faced in early 2007 with effecting compliance with the PCI DSS. The grocer, supported by nine distribution centers, nine regional bakehouses and five commissaries, is headquartered in the southern US and employs 54,000. The organization also owns four subsidiaries, comprising a coffee company, two seafood processing facilities, and a produce field-inspection office.

With the initial Sept. 1, 2007, deadline for Level 1 compliance with the PCI DSS looming, the grocery concern urgently required a system that could work seamlessly with the IBM point-of-sale system the company had already put in place to effectively secure its network connections.

Their key requirements: A way to remotely establish secure connections with its 265 stores, facilitating the secure transfer of files between all levels of its operations. To fully comply with PCI, the grocer's technology team knew it needed to migrate its more than 300 users in seven regions toward a secure SSH and SFTP environment.

Making matters more complex, the global grocer's technology systems comprised remote users at its world headquarters, regional offices and individual store levels in two countries.

The retailing giant turned to Pragma's market-leading FortressSSH ClientSuite, which gives organizations the ability to secure networks comprising desktop, laptop, industry-standard mobile and handheld devices. That's because Pragma is able to offer end-to-end, innovative, cost-effective secured computing solutions. With nearly 20 years of experience in securing networks and remote communications, Pragma Systems was uniquely positioned to help the company kick off the tough process of PCI compliance.

Secure Connectivity…
Done Right

"Once we met with Pragma, our choice was clear," explains a company manager. "After reviewing our options, we knew Pragma Systems, with its Fortress suite, its deep experience in helping companies effect secured communications, and its ability to integrate seamlessly with our existing technology, would be the quickest path toward helping us meet the stringent requirements of the PCI DDS."

Working in lockstep with the global retailer's IT team, Pragma put in place its enterprise-grade FortressCL and FortressFX clients, installing across the approximately 300 laptop and desktop computers currently running WindowsXP and IBM's 4690 Supermarket Application.

The end result? Extremely secure, reliable connections, office to office, level to level, country to country. "Problem solved," the manager asserts. "Pragma's FortressSSH allowed us to effect complete compliance with the PCI. After submitting evidence of our FortressSSH installations to external auditors, we were deemed to be PCI compliant."

As Pragma Systems Vice President Andrew Tull points out, the more secure and most flexible connectivity solutions work within a company's existing technology environment – in this case, the grocer's IBM point-of-sale network – and support today's toughest standards: 802.11i, WPA2, AES encryption, RFID, and more. "We've designed our Pragma solution specifically to help companies of all types and sizes effect compliance with PCI and other mandatory security standards in the most secure, reliable way possible," explains Tull. "Our Pragma servers and clients give you the cost-effective tools you need to achieve audit-proof secured connections across your entire enterprise."

Why Pragma Systems?

Simply put, Pragma Systems delivers. Helping companies make the move to a comprehensive program of compliance with PCI and other regulatory requirements is the reason so many organizations have come to rely on Pragma's outstanding performance, superior customer service and across-the-board reliability.

Call Pragma today, and learn how we can help your company by providing:

- **Reliable, proven enterprise-grade secure connectivity software** for all Windows® environments (Servers, Desktops and Windows Mobile):
- That's highly-secure – even offering a protocol for secure remote login and other secure net work services over an insecure network;
- Facilitates **data and system management**;
- Allows **secure file transfers**; and
- Provides consistent, **reliable application delivery**
- **A powerful, convenient** approach to protecting communications on a computer network
- **Superior and responsive customer service** – both throughout the sales process and dur ing lifetime of usage
- **Peace of mind**

Appendix:

Helpful Links/Reference Materials

1. Guide for PCI Compliance: http://www.pcicomplianceguide.org/

2. Download the PCI DSS:
https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

3. PCI Security Standards Council's "Self Assessment Questionnaire":
https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf

4. PCI Compliance News: http://www.pcicomplianceguide.org/pcicompliancenews.html

5. The IT Audit Checklist Series: http://www.itcinstitute.com/display.aspx?id=2499

6. CIO Magazine's "A Guide to Practical PCI Compliance": http://www.cio.com/article/153751

7. IT Compliance Institute White Paper Library:
http://www.itcinstitute.com/wp/logWprequest.aspx?productId=168

8. PCI Compliance Overview: http://en.wikipedia.org/wiki/PCI_DSS

9. eWeek's "10 Things You Should Know About PCI Compliance":
http://www.eweek.com/slideshow/0,1206,a=217455,00.asp

10. Pragma Systems, Inc.: www.pragmasys.com

To Contact Pragma Systems

Pragma Systems, Inc.
13809 Research Blvd.
Suite 675
Austin, Texas 78750
Corporate: 512.219.7270
Sales: 800.224.1675
FAX: 512.219.7110

sales@pragmasys.com or orders@pragmasys.com

www.pragmasys.com