A Compliance White Paper

What CISOs Need to Know About The New NIST Guidelines for Secure Shell

ssh®

TABLE OF CONTENTS:

About SSH Communications Security:

Founded in 1995, SSH Communications Security is the company that invented the SSH protocol - the gold standard protocol for data-in-transit security solutions. Today, over 3,000 customers across the globe, including 7 of the Fortune 10, trust our Information Assurance Platform to secure the path to their information assets. Our platform enables businesses of all types and sizes to protect their information assets by providing the gold standard data-in-transit security solutions that prevents data loss in both internal and external environments, hardened perimeter security through our multi-channel two-factor authentication and internal security control management solutions that enables organizations to more easily manage user keys and monitor administrator traffic across your networks.

Introduction

The National Institute of Standards and Technology (NIST) is the US government agency responsible for promoting U.S. innovation and industrial competitiveness. One area of NIST responsibility is the establishment of cybersecurity standards and guidelines for US Federal government agencies. This responsibility was mandated by the Federal Information Security Management Act of 2002 (FISMA). A corner stone of these standards is NIST Special Publication 800-53. NIST 800-53 specifies the management, operational and technical safeguards for protecting the confidentiality, integrity, and availability of IT systems and electronic information. In short, it describes the IT security controls federal agencies must implement as required by the FISMA act of 2002.

On August 20, 2014, The Computer Security Division of NIST released Interagency Report 7966 (NISTIR 7966). This report provides guidelines for the security of automated access management using Secure Shell (SSH). The report explains how those guidelines map directly to the security controls mandated in NIST 800-53 and the President's Cyber Security Framework

These new developments within NIST have great significance for CISOs and other executives responsible for IT security. This white paper explains why NIST has taken these steps and what it means for IT security management not only within federal government agencies but also within the commercial sector.

Why NIST is Focusing on Secure Shell

Secure Shell is a protocol and software suite used for securely transmitting data, application tunneling and remote systems administration. It comes preinstalled on Unix, Linux, IBM Mainframes and is available on Windows. It is deployed on millions of servers and is used in approximately 90% of data center environments. Privileged users such as systems administrators and application developers use Secure Shell for interactive access. Secure Shell is even more widely used for automated system to system processes including backups, data base updates, system health monitoring applications and automated systems management. In short, Secure Shell performs a critical role in the functioning of the modern, highly automated data center.

However, Secure Shell is often viewed as "part of the plumbing" and often does not get much attention as a potential operational risk. In the words of NIST "The security of SSH-based automated access has been largely ignored to date.". This blind spot has contributed to numerous costly data breaches. As a result, the Computer Security Division (CSD) of NIST concluded that poor Secure Shell access controls within IT environments constitute a major operational risk. In order to address this, NIST has developed a comprehensive set of guidelines and controls that federal agencies and commercial enterprises should adopt.

Hidden Risks of Poorly Managed Secure Shell Identities

At its core, Secure Shell is used for logging into application and service accounts on remote servers. Secure Shell supports authentication methods such as passwords, tokens, digital certificates and public key. With public key authentication, a public key is configured on a server as an authorized key and the private key is stored on a client machine (which in itself is often a server computer) in a small file as an identity key. Private key files can be encrypted using a passphrase. However, private keys used for automation typically are not passphrase protected as the passphrase itself would need to be stored in a file or hardcoded in a script to enable automated execution of a process.

Public/Private key based authentication is inherently more secure than other forms such as passwords. That is why NIST recommends public key, especially in support of process automation. And in fact, within both government and commercial sectors, key based authentication is very widely used. Unfortunately, there is a downside. When improperly managed, Secure Shell keys can be used by attackers to penetrate the IT infrastructure. The compromise of just one private key can be leveraged to configure hard-to-notice backdoors, to bypass privileged access control solutions and to perpetrate large scale attacks and data breaches.

NIST has identified the following vulnerabilities that organizations are most often exposed to and should evaluate within the scope of their security assessments:

- Vulnerable SSH implementation (insecure versions, configuration weaknesses)
- Stolen, leaked, and unterminated SSH user keys (Lack of visibility and process controls over key lifecycle management)
- Backdoors (unaudited user keys)
- Unintended usage of user keys (Lack of separation of duties, unintended privilege escalation)
- Incorrect user key location (Lack of access controls to key files).

These vulnerabilities result in the risks listed in Table 1.

Contractors and employees who left years ago still have access to critical systems. This exposes the enterprise to data loss or other malicious activity.
Unneeded keys remain authorized on system, application and user accounts. Each public key based authorization creates an exposure in the event that the corresponding private key is compromised.
Unauthorized copies of private keys in circulation. In general, the holder of a private key can make copies, even if this violates company policy. Central monitoring and controls can reduce or even eliminate the potential for unauthorized copies being used.
Private keys not passphrase protected. Lack of policy enforcement over private key protection increases the risk of credentials being compromised.
Keys not rotated regularly or at all. Key rotation is a basic requirement for protecting credentials, just as most organizations require end users to regularly change their passwords.
Unintended escalation of access. Secure Shell configuration controls are needed to prevent users from escalating privileges or gaining access to other accounts.
Breakdown of separation of duties. This is a common issue in financial services – often caused by lack of controls over key authorizations that get propagated from development to production servers.
Unintended access between test and production environments.
Lack of visibility of trust relationships.
Inability to meet audit requirements. This can extend to basics such as reporting on all trust relationships and activity logging.
Human errors in manual key setup and removal process. This can result in unintended access being granted, or failure to remove authorizations when required.
Misconfigured Secure Shell software. This can allow users to violate policies such as prohibitions on VPN access in or out of the network.
Number of individuals authorized to create permanent trust relationships, resulting in breakdown of access controls.

Table 1: Primary Risk Exposures

Best Practices

In recognition of the seriousness of these risks, NIST IR 7966 provides a set of recommended best practices for managing Secure Shell identities (public and private keys). These best practices map to NIST 800-53 Security Controls and the President's Cyber Security Framework. These best practices are summarized as follows:

1. Standardize the key configuration across the environment.
2. Authorized key file should not allow end user write access.
3. Centralized key provisioning (no more "self service provisioning). Key provisioning should be centralized and limited to a much smaller number of root level administrators.
4. Cipher configuration – allow only strong ciphers and specified key lengths.
5. Require password protection for private keys.
6. Require logging of Secure Shell activity.
7. Ensure Secure Shell server will not execute if authorized keys file and home directory are insecure.
8. Prevent privilege escalation by process spawning.
9. Segregate system accounts from person accounts.
10. Use controls to limit Secure Shell access to specific commands and source addresses.
11. Rotate keys.
12. Remove unneeded User Keys.
13. Document key usage
14. Regular audits.

CISO Takeaways

These recommendations from the Computer Security Division of NIST are a direct call to action for CISOs within the US Federal government. This is also a call to action for commercial sector CISOs. NIST 800-53 and associated Interagency Reports are widely accepted industry standard best practices, even for commercial entities that are not doing business with the Federal government.

The good news is the first steps in dealing with these issues are not difficult or costly. The first steps are simple: Find out to what extent your organization is exposed to the risks NIST has identified. Skilled personnel with the right tools can accomplish this within a matter of days. If these resources are lacking internally, there are well qualified third parties that can work with your internal staff to get the job done quickly and efficiently. CISOs should require the following from their staff:

1. A current state evaluation, benchmarked against the recommended NIST 800-53 controls
2. An assessment of risk
3. A set of recommendations

Working from this basic foundation, your staff can develop an action plan to address significant risk and compliance issues.

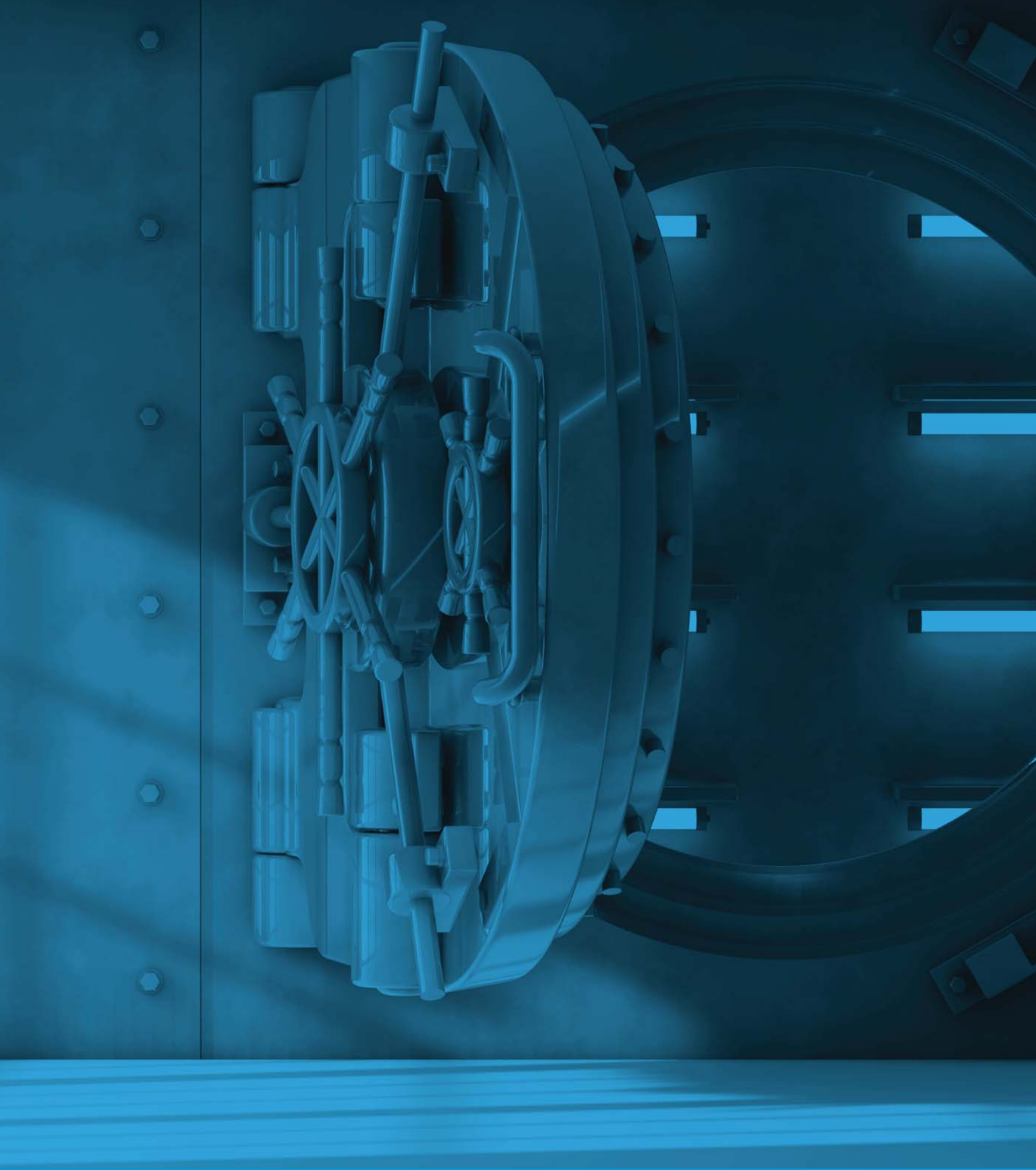
SSH Communications Security offers training, services and products that help organizations address the issues NIST has raised. Working together with your staff, we can provide a comprehensive evaluation of your current environment and recommend effective approaches for remediation.

Further Reading and Resources

>> NISTIR 7966

>> NIST 800-53

Please contact us at www.ssh.com if you would like more information.



ssh®

www.ssh.com