A COMPLIANCE PAPER

WHAT YOU NEED TO KNOW ABOUT NIST GUIDELINES FOR SECURE SHELL (NISTIR 7966)

ssh communications security

TABLE OF CONTENTS:

ssh communications security

ABOUT SSH COMMUNICATIONS SECURITY

As the inventor of the SSH protocol, we have a twenty-year history of leading the market in developing advanced security solutions that enable, monitor, and manage encrypted networks. Over 3,000 customers across the globe trust the company's encryption, access control and encrypted channel monitoring solutions to meet complex compliance requirements, improve their security posture and save on operational costs. SSH Communications Security is headquartered in Helsinki and has offices in the Americas, Europe and Asia. The company's shares (SSH1V) are quoted on the NASDAQ OMX Helsinki. For more information, visit www.ssh.com

INTRODUCTION

The National Institute of Standards and Technology (NIST) is the US government agency responsible for promoting U.S. innovation and industrial competitiveness across all verticals and industries. One area of NIST responsibility is the establishment of cybersecurity standards and guidelines for US Federal government agencies and the private sector needs to always be prepared for regulatory and standards bodies to follow suit. This responsibility was mandated by the Federal Information Security Modernization Act (FISMA) of 2014. NIST Special Publication 800-53describes 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 2014.

On October 30th, 2015, the Computer Security Division of NIST released the final version of Interagency Report 7966 (NISTIR 7966), "Security of Interactive and Automated Access Management Using Secure Shell (SSH)." The purpose of this document is to assist organizations in understanding the basics of SSH and SSH access management in an enterprise, focusing on the management of SSH user keys. It describes the primary categories of vulnerabilities in SSH user key management and recommends practices for planning and implementing SSH access management based on (SP) 800-53 and the President's Cybersecurity Framework.

This white paper explains the driver behind NISTIR 7966 and its importance to all layers of management. NISTIR 7966 details everything an individual needs to know about the SSH protocol and the security of interactive and automated access management using SSH. It is critical to educate the masses about SSH key management, its wide usage and how to manage the deployments based on industry best practices.

WHY IS NIST FOCUSING ON SSH?

SSH is a protocol and software suite used for securely transmitting data, application tunneling and remote systems administration. The SSH protocol ships standard with every UNIX, Linux, and Mac system, as well as IBM mainframes. It is also widely used on Windows (Microsoft announced plans to make it a standard component of Windows). SSH is deployed on millions of servers and is used in approximately 90% of data center environments. Privileged users, such as system administrators and application developers, use SSH for secure interactive and remote access. SSH is even more widely used for automated machine-to-machine processes including backups, database updates, system health monitoring applications and automated systems management. In short, SSH performs a critical role in the functioning of the modern, highly automated digital networks found in every business or data center.

The use of SSH grew in a grassroots fashion from system administration, and its deployment never got much management attention or planning in most organizations. It was a standard component requiring no purchasing decision. It is the "Invisible Plumbing" that runs in nearly all systems and is most often seen as being owned by the "IT department".

As a result, the Computer Security Division of NIST concluded that poor SSH access controls within Information Technology (IT) environments constitute a major operational and security risk that could be best addressed by publishing IR 7966.

HIDDEN RISKS OF POORLY MANAGED SSH IDENTITIES

At its core, SSH is used for logging into application and service accounts on remote servers. SSH 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 hard-coded in a script to enable automated execution of a process.

Public key 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 widely used for both human and machine-to-machine privileged access. Improperly managed SSH keys can be leveraged by attackers to penetrate the IT infrastructure and move freely across a network without detection. 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 categories of vulnerabilities that organizations are most often exposed to and should evaluate within the scope of their security assessments:

- Vulnerable SSH implementation - could have vulnerabilities that allow it to be exploited in order to gain unauthorized access to communications or systems.
- Improperly configured access controls - In its role of enabling administration of systems via elevated privileges—including root—SSH is highly susceptible to enabling unauthorized access due to improperly configured access controls.
- Stolen, leaked, derived, and unterminated SSH user keys - pose a similar problem to stolen, leaked, derived, and unterminated interactive user account credentials.
- Backdoors (unaudited user keys) - Many organizations mandate that all privileged access to their servers take place through a privileged access management system that records all actions performed. Unfortunately, SSH public key authentication can be used to create a "backdoor" that bypasses the privileged access management system.

- Unintended usage of user keys - Users may, intentionally or unintentionally, use identity keys for purposes for which they were not intended.
- Pivoting - Malware can be engineered to use SSH keys to spread when automated access is allowed.
- Lack of knowledge and human errors - One of the greatest ongoing challenges to the security of SSH-based systems is the potential for human error due to the complexity of SSH management and the lack of knowledge many administrators have regarding secure SSH configuration and management.

Below is a list of some of the potential **risks** that are introduced as a result of the above vulnerabilities:

- Employees (full-time, contractors or temporary) who may have left or transferred out of an organization, may have leftover unauthorized access to production.
- Lack of segregation of duties where individuals have unauthorized access to production systems from non-production environments (test, development, implementation, etc.).
- 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.
- Private keys without passphrase protection. 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.
- Ineffective access controls resulting in audit findings and exceptions. Depending on how wide of an access control gap it is, and the fact that access controls are considered key controls, this may lead to a material weakness.
- Human errors in manual key setup and removal process. This can result in unintended access being granted, or failure to remove authorizations when required.
- Lack of visibility of trust relationships or the number of individuals authorized to create permanent trust relationships, resulting in breakdown of access controls.

ADOPT BEST PRACTICES FOR SSH KEY MANAGEMENT

NISTIR 7966 provides a set of recommended best practices for managing SSH identities (public and private keys). These best practices map to NIST 800-53 Security Controls and the Cybersecurity Framework. These best practices are summarized as follows:

- SSH Security Policies and Procedures - The definition of policies should clearly spell out roles and responsibilities in order to prevent misunderstandings that result in security lapses and to ensure accountability.
- Secure SSH Implementation
  - Only enable SSH server functionality where required.
  - Keep SSH server and client implementations fully up to date.
  - Harden SSH server and client implementations.
  - Enforce least privileged access.
- SSH Identity and Authorized Keys
  - Enforce minimum key length and approved algorithms.
  - Cryptoperiods – Maximum time a key may be used before replacement.
  - Identity key access control – Restrict access to which they have been as signed.
  - Identity key passphrases – Interactive user keys should be protected by a passphrase.
  - Identity key duplication – Identity keys should not be duplicated.
  - Authorized key access controls – Non-superusers cannot install authorized keys.
  - Authorized key command restrictions – Command restrictions for automated processes.
  - Authorized key source restrictions – Restrict automated process keys by IP addresses.
  - Replace on compromise or reassignment – SSH keys should be changed when compromise is suspected.
  - Usage logging – Log key fingerprints for access based on SSH authorized keys.
  - Pivot prevention – Accounts should not be configured with both incoming and outgoing identity key-based trust relationships.
  - No environment crossing – Keys should not cross environments.
- SSH Key-based Access Provisioning, Life cycle and Termination Processes
  - Formal process defined for requesting key-based access.
  - Approvals defined and required for all SSH key-based access.
  - Only authorized individuals may provision SSH key-based access.
  - SSH key-based access usage should be logged.
  - SSH key-based access should be reviewed regularly for appropriateness.
  - Terminate SSH key-based access for decommissioned processes and terminated or transferred users.
- Establish Continuous Monitoring and Audit Processes
- Inventory and Remediate Existing SSH Servers, Keys, and Trust Relationships
  - Map all trust relationships.
  - Add command and source restrictions.
  - Identify and remove any orphaned and duplicate authorized keys.
  - Ensure passphrase protection, key length and algorithms.
  - Enforce the provisioning process.
  - Assign ownership of all access granting keys.
  - Monitor and analyze key-based access usage.
  - Onboard all relevant hosts into a system for managing keys.
- Automate Inventory of All SSH Identities - Review key-based access, provisioning of SSH user keys, monitoring and auditing.
- Educate Executive Management.

NISTIR 7966 MAPPING TO INDUSTRY BEST PRACTICE CONTROLS

The NISTIR 7966 provides the following lists to assist organizations in implementing SSH security measures:

- NIST Special Publication (SP) 800-53 Revision 4 security controls that are most pertinent for securing SSH-based interactive and automated access management;
- Selected Cybersecurity Framework subcategories with their implications to SSH-based interactive and automated access management; and
- Criteria for selecting SSH key management tools.

The tables below highlight some of these controls. Please refer to the NISTIR 7966 appendices for the complete mapping:

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations":

NIST SP 800-53	SSH Implications
Account Management	• SSH user keys authorize access. • Enhanced auditing is SSH enabled to provide audit trails. • Valid authorization before installing keys. • SSH keys monitored periodically. • Ensure timely rotation of SSH private keys.
Access Enforcement	• Approvals for key-based access should be enforced. • Prevent users from propagating access through new private keys.
Least Privilege	• Command restrictions configured for SSH keys. • SSH keys for privileged accounts configured only if non-privileged account cannot do the task. • No unauthorized access to private keys that grant privileged access.
Remote Access	• Enforce policies when allowing SSH key-based remote access. • Host key management should be required for preventing man-in-the-middle attacks.
Continuous Monitoring	• SSH-based access should be regularly analyzed.

Cybersecurity Framework subcategory:

Cybersecurity framework subcategory	SSH Implications
Organizational communication and data flows are mapped	SSH user keys define permanent trust relationships.
Identities and credentials are managed for authorized devices and users	SSH user keys authorize access to the information system and specify privileges for access.
Data in transit is protected	SSH connections using key-based authentication protect the confidentiality and integrity of data in transit.
Access to systems and assets is controlled, incorporating the principle of least functionality	SSH user keys define permanent trust relationships that interconnect information systems.
Monitoring for unauthorized personnel, connections, devices, and software is performed	SSH-based access should be regularly analyzed as part of a continuous monitoring program to detect unapproved authorized keys.

CONCLUSION

The new guideline NISTIR 7966 from the Computer Security Division of NIST is a direct call to action for organizations regardless of industry and is a mandate for the US Federal government. 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.

NISTIR 7966 explains the vulnerabilities associated with poor management of interactive and automated SSH access, as well as the potential impact of misuse or compromise of SSH keys used for client authentication.

The good news is that the initial steps in dealing with these issues are not difficult or costly. Initially organizations must find out to what extent their environments are exposed to the risks identified. Skilled personnel with the right tools can accomplish these initial steps within a matter of days.

Organizations that acquire and use automated SSH key management products should be able to significantly decrease their risks related to SSH access with a reasonable amount of effort. Without automation, most organizations will struggle to remediate the existing SSH environment and to properly secure new SSH usage.

Auditors must start including the assessment and evaluation of SSH keys in their audit checklists. Start addressing this “dark side” of compliance immediately by becoming aware and addressing accordingly.

Government entities must be ready for regulators knocking on their doors inquiring about SSH keys management per NISTIR 7966.

Management at all levels should adhere to the best practices listed above to ensure timely and total risk reduction or elimination. This means boards, CEOs, CTOs and CISOs must include SSH key management in their organizations' risk management strategy as the potential issue is an equivalent if not a higher risk as compared to critical business risks. Organizations should not let the "forgotten credentials" (SSH keys) cause them issues, audit exceptions or worst of all a security breach.

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.

For information on SSH Communications Security, please visit www.ssh.com

FURTHER READING

- Federal Information Security Modernization Act (FISMA) of 2014
- National Institute of Standards and Technology - NIST
- NIST Internal/Interagency Reports (NISTIR)
- NISTIR 7966
- NIST Special Publication (NISTSP) 800-53 Revision 4
- Cybersecurity Framework

ssh communications security