IDC TECHNOLOGY SPOTLIGHT

SSH Governance Is Needed to Reduce Risk and Bridge the Trusted Access Gap

July 2016

Adapted from *Security in the 3rd Platform: Marching Toward Proactive Defense* by Christian A. Christiansen and Robert Westervelt, IDC #255791 and *Worldwide Identity and Access Management Forecast, 2015–2019* by Pete Lindstrom, IDC #259561

Sponsored by SSH Communications

Organizations are increasingly addressing weaknesses in Secure Shell (SSH) authentication management, which has suffered from poor governance for years. A recent study conducted by IDC found that the responsibility for provisioning and deprovisioning SSH credentials rests with multiple stakeholders. This fact is known by criminals who take advantage of the lack of governance over SSH to use valid SSH keys in order to bypass security controls and quickly move laterally in the corporate network to sensitive resources. It is essential for organizations to gain visibility into and control over SSH key management as the tally of data breaches stemming from stolen account credentials and hijacked accounts continues to rise. SSH keys help administrators securely manage critical systems remotely and even automate data exchange between applications. But the irony is that poorly implemented policies and monitoring and enforcement mechanisms have resulted in a false sense of security. Today, organizations are swamped with thousands of unchecked SSH keys, some of which have long been abandoned but never revoked. This paper examines recommended risk mitigation practices, explores ways to avoid the complexity issues, and discusses how solutions from SSH Communications Security address the challenges described previously.

Introduction

The SSH protocol is used by system administrators to enable secure access to remote systems. It is rarely managed and almost never assessed for vulnerabilities and configuration weaknesses. This poor management is providing a false sense of security, and digital forensics investigators tell IDC that poorly managed SSH keys are one of the weaknesses being exploited by attackers in breaches. SSH key management has been neglected for so long that organizations assessing the issue for the first time often find thousands of keys used by former employees, contractors, and other individuals who required remote access at one time. In some cases, organizations find SSH keys to privileged accounts that are more than 10 years old.

This growing problem may have reached the breaking point. Forensics investigations into some high-profile data breaches have found evidence that SSH weaknesses may have given attackers an advantage over network and endpoint defenses. New guidelines from the National Institute of Standards and Technology (NIST) shed light on the issue for the first time and provide best practices around provisioning, account management, auditing, and monitoring the issuance of SSH keys.

Understanding SSH

Used for years because of its ease of use and reliability, the SSH authentication protocol enables secure access to remote systems and enables them to execute remote commands, transfer files, and establish automated backups. It is also used to automate IT processes such as machine-to-machine communications. This enables applications to transfer data to internal systems or external business partners. SSH relies on a pair of encryption keys to authenticate administrators to root or administrative and other system accounts.

A version of SSH is shipped with every version of Linux, Unix, and Mac OS X and is available on many mainframe operating environments. While SSH continues to be a highly used protocol for a variety of functions, organizations are only now beginning to gain a better understanding of the risks associated with poorly managed implementations.

Unmanaged SSH Keys Pose Unacceptable Risks

Those interviewed by IDC cited multiple reasons for addressing SSH key management. High-profile data breaches have fueled interest in locking down system access and managing privileged credentials. Negative audit findings are also starting to drive attention to the issue. However, one of the significantly growing drivers is that security-conscious business partners are insisting on tighter security restrictions to maintain the partnership. These partners believe that the following risks are unacceptable:

- **Runaway SSH keys.** Unmanaged keys that are no longer in use are often still functional. IDC interviews with organizations that have deployed solutions to gain visibility into the issue have uncovered SSH keys that have been functional for more than a decade.
- **Unchecked access rights.** High-level access rights are granted to a variety of internal and external users, leaving systems further at risk. Former system administrators and other employees often know that their access rights to critical systems have not been revoked.
- **Poor development processes.** Lack of visibility into SSH use may signal a lack of approvals or coordination when keys are issued for development environments. These environments can be moved into production without revoking the access credentials.
- **Negative audit findings.** Auditors are increasingly requesting documentation proving that SSH key management is being monitored. A negative audit finding impacts the organization and its associated business partners.

SSH keys have no built-in key expiration. This factor, combined with the limited governance that SSH keys receive, has led criminals to view SSH keys as a way to circumvent identity and access management controls. One of the most common tactics used by criminals, after gaining initial access to an organization's systems, is to move laterally on an organization's network to access the sensitive resources they desire. By gaining access to poorly provisioned SSH credentials or leveraging implementation weaknesses, an attacker who compromises one system can often leverage the same credentials to quickly move to other areas of the corporate network. This tactic dramatically increases the ability of an attacker to get in, execute additional malicious code, and exfiltrate sensitive data quickly while easily evading system monitoring solutions and other security controls. By the time an organization identifies the data leakage, the attacker is long gone.

OpenSSH, the widely used open source implementation of the SSH protocol, is not immune to vulnerabilities. An alert issued by the United States Computer Emergency Readiness Team in January 2016 noted critical flaws in the authentication protocol that could be exploited to reveal private data, including the user's private SSH key. A vulnerability addressed in 2015 gave attackers the ability to launch brute-force attacks against a wide variety of servers and products that use the protocol. This critical vulnerability gave attackers almost unlimited attempts to guess (or "brute force") the SSH private key.

New NIST Guidelines Highlight Compliance Requirements

NIST released a report (NISTIR 7966) titled *Security of Interactive and Automated Access Management Using Secure Shell (SSH),* which further highlights the extent of the problem and provides guidance to enable organizations to establish governance over SSH authentication. Most organizations fail to assess and document their SSH key management processes.

The document calls for organizations to assess and gain an understanding of the extent of the problem in their environments and lists recommendations to systematically implement processes to provision, terminate, and monitor SSH keys. At a high level, the document recommends the following:

- Establish policies and procedures where SSH is deployed, including rapidly evolving cloud environments. Apply the principle of least privilege, which promotes restricting user profile privileges to the minimal amount of resources required for individuals to carry out their responsibilities.
- Assess and harden SSH server and client implementations to ensure proper configuration and address known vulnerabilities in previous iterations of the protocol.
- Establish policies and controls over key creation. Create an approval process to restrict the ability of administrators to authorize and install new keys.

NIST also recommends that organizations conduct a thorough inventory to identify untracked identity keys in the environment. The process involves monitoring log data for several months to determine which keys are not being used or which keys are being shared or have been passed on to other individuals.

The guidelines clarify that enterprises should include documenting those responsible for granting access across mission-critical systems. The document also points out that NIST SP 800-53 requires organizations to identify authorized users and their access rights as well as understand and properly authorize connections between information systems.

Careful Planning Overcomes Project Complexity

IDC interviews with IT security architects found that gaining control of this long unmanaged authentication protocol is often mired in complexity. This challenging process requires careful planning, execution, and communication with all impacted employees. While centralizing the key provisioning process and gaining complete visibility and control could take months or even years, risk reduction can happen rapidly, after outdated and rarely used keys are identified and revoked.

An IT security architect at an IT services organization said that interest in SSH key management grew out of more attention placed on hardening system access and insider threats. For years, the large, global organization has been casual about provisioning. The issue poses a significant risk because of the thousands of systems that make up the organization's legacy infrastructure. People are using SSH for critical business use cases, but the IT team hasn't kept track of users who were granted SSH keys and had no centralized way of provisioning them. "If you are using keys, that means you have to manage them, provision them throughout their life cycle, which we were not doing," the IT architect said. "We are looking at millions of trusts and have no idea of the status of what is out there or if anything is being rotated."

Those interviewed by IDC cited multiple reasons for addressing SSH key management. High-profile data breaches have fueled interest in locking down system access and managing privileged credentials. Negative audit findings may drive attention to the issue, but security-conscious business partners that insist on tighter security restrictions to maintain the partnership are one of the biggest drivers.

Those who have led SSH governance projects insist that communication with the various stakeholders involved is essential in ensuring the least amount of disruption possible. Management also needs to be educated about the risks and to express their support for establishing SSH governance policies and processes. Achieving full and continual SSH key governance takes time, with systematic rollout of oversight processes to avoid significant disruption to business operations. After management buy-in, organizations are learning to take a systematic approach, identifying critical resources that need attention first and then advancing to less critical systems in a second or third phase of the project.

Considering SSH Communications Universal SSH Key Manager

SSH Communications Security is a key encryption software provider with solutions and innovations deployed globally across many company Web servers, datacenters, and network infrastructures. The company has a strong focus on understanding and managing SSH keys and providing best-in-class privileged access solutions for the IT security industry.

Universal SSH Key Manager (UKM) is an enterprise-grade SSH user key management solution. UKM takes a nondisruptive approach that enables enterprises to gain and retain control of the SSH infrastructure without interfering with operations in production systems. The idea is that there should be no need to rip and replace how users get their work done or change the hundreds of automated processes that are the lifeblood of ongoing business. UKM's nondisruptive approach is based on four principles:

- **Discover.** Discover all SSH keys, map trust relationships, and identify policy violations.
- **Monitor.** Track key usage to determine which keys can be safely removed without affecting operations.
- **Remediate.** Remove keys that should be revoked and bring valid keys under policy compliance.
- **Manage.** Eliminate manual processes, centralize control, enforce compliance, and audit all activity.

UKM enables the delegation of key remediation actions to the users who are ultimately responsible for the applications and the users to whom the keys belong. In addition, a user portal provides a simple way to request and provision SSH-based access from a central point in line with security policies and with a full audit trail from start to finish.

According to the company, the Universal SSH Key Manager solution has been successfully deployed in extremely large and demanding customer environments in the banking, finance, energy, and government markets, saving a typical Fortune 1000 organization on average $1 million to $3 million per year in overhead costs while reducing the risk of serious security breaches and resolving open compliance issues.

SSH Communications Security provides cybersecurity solutions that monitor, control, and automate trusted access to critical data. Managing enterprise identities and their access is fundamental to security, and while most identity access management solutions address traditional end users, they tend to ignore higher-level trusted access. SSH Communications Security software and services are designed to bridge the trusted access security gap for customers in all industries and verticals. The company understands that identity and access are vitally important to information security. Many solutions address the security issues for end users but fall short in addressing trusted access provided by SSH keys — including automated and privileged access for system administrators, developers, outsourcing partners, and other privileged users.

Therefore, SSH Communications Security estimates that 80% of all privileged access credentials in large networks lie outside the control of present identity and access governance solutions. This lack of control is problematic for enterprises and government agencies alike. Appropriate management of trusted access for critical infrastructure requires organizations to have visibility into and control of SSH keys so that they can manage the unforeseen risks and adhere to varied regulatory mandates.

Challenges

SSH Communications Security established its niche in the management of SSH keys. This unique differentiator makes the company a pioneer in addressing this long-standing issue. However, a variety of other vendors are realizing the importance and challenges of SSH user key–based access and are extending their platforms to address SSH key management.

Some standalone tools are available for smaller, targeted enterprise implementations; such tools can be deployed more quickly but may be limited in capabilities and SSH versions supported. SSH Communications Security is currently working toward a unified technology platform; however, to date, SSH key management, privilege account management, and PKI management are offered as separate solutions. The company is also developing a centralized platform that will be able to support other use cases such as management of keys on network devices. Opportunity exists for being the key security enabler for DevOps strategies, securing virtual environments and providing management and oversight of privileged credentials and remote management of big data analytic environments.

Conclusion

The SSH protocol was originally designed to provide an encrypted tunnel that could secure remote log-ins, remote command executions, and file transfers. Its popularity is due, in part, to the ease of key provisioning for system and application administrators to generate and store new keys for access. Administrators also typically implement the open source OpenSSH protocol, which is freely available and included in Linux and Unix operating systems, without the understanding of what is needed to manage and maintain the access provided by the SSH keys, which have been generated for years across their IT infrastructure.

SSH governance is a growing requirement and being increasingly examined by business partners and scrutinized by auditors. Organizations should be proactive in taking inventory of their network to determine the extent of authorized SSH keys and user identities. Few proprietary solutions exist that are designed to directly address the problem. Organizations that try to implement a custom solution to restrict and rotate private keys find that the process also gets bogged down in complexity and expense.

It is generally accepted that centralizing key management returns control of the provisioning and deprovisioning of SSH keys to the enterprise. SSH key management products can overcome some of those issues and mitigate the risk associated with poorly governed SSH access procedures. To the extent that SSH Communications Security can address the challenges described in this paper, IDC believes that the company's key management solution set is well positioned for success.
