SSH KEYS:
Security Asset or Liability for Healthcare?

Securing access to network systems is an ongoing healthcare IT priority, driven by the need to protect patient safety and comply with privacy rules such as HIPAA. This effort will only become more challenging over time, given that the demand for computer networks is expected to reach nearly 50 billion connected devices and more than 275 billion applications by 2025. Relying on more machines means there will be more machine-to-machine connections requiring protection.

Consumers, patients and physicians use web applications and clinical systems, which are protected by secure login protocols in the healthcare industry. However, when computer servers and medical devices are exchanging data on the network, they do not validate their identities with usernames and passwords. Instead, they use machine-to-machine authentication, such as Transport Layer Security (TLS) certificates or Secure Shell (SSH) keys. While the computer industry spends an estimated $10 billion annually to protect human identities, healthcare organizations invest comparatively little on protecting machine identities.

Produced in partnership with
HIMSS Media

> ***"The ability to connect without a password, or anything interactive, makes SSH keys so important and useful in automation. Obviously, if you are automating a process, you don't want someone to have to enter a password in the middle of that."***
>
> **Mike Dodson** | Vice President of Worldwide Customer Security Strategy & Solutions | Venafi

"The ability to connect without a password, or anything interactive, makes SSH keys so important and useful in automation," noted Mike Dodson, vice president of worldwide customer security strategy & solutions at Venafi, a global leader in machine identity protection. "Obviously, if you are automating a process, you don't want someone to have to enter a password in the middle of that."

Healthcare IT administrators and application owners who work behind the scenes need deeper access to network servers to conduct maintenance and support, which is almost always controlled by SSH keys. While Privileged Access Management (PAM) solutions are focused on protecting against risks associated with that activity, SSH is also used to automate file exchanges between servers and other devices on the network. This is where the risk of exposing electronic Protected Health Information (ePHI) is most vulnerable.

Risky SSH behavior

"SSH keys are both widely used and misused as machine identities," said Dodson. "On every network there are two actors: people and machines. We need to protect both."

SSH keys routinely control administrative access to servers and machine-to-machine automation. And because SSH implementation is included for free with major operating systems, executive ownership typically does not exist, which makes it easy for IT administrators to overlook its importance. However, if SSH keys are left unprotected and unaccounted for, entire healthcare enterprises are left defenseless against breaches by bad actors. To deliver safe and effective patient care, healthcare IT leaders need to be vigilant and secure their networks, as well as the business and clinical systems and medical devices that rely on them.

A potential vulnerability occurs whenever an administrator creates SSH keys for routine server connections instead of relying on the authorized account username and password. The administrator's client computer and target server trade private and public keys to identify and authenticate transactions. This ability to establish such passive interactions makes SSH keys useful in process automation. However, as the number of servers grows, the demand for automated file exchanges between them increases. At the same time, the number of public and private keys generated between the administrator and multiple servers on the network proliferates, creating unintended risks—especially if the keys are weak and easy to guess.

Another potential liability involves backdoor keys. Some administrators have read-and-write permissions to create SSH keys and place them into their authorized keys file folder without managerial oversight. Subsequently, broad system access can be granted without the approval of a business owner or responsible party. The associated risk is not necessarily caused by an untrustworthy authorized user, although such behavior should not be ruled out. More importantly, the lack of proper controls leaves the system vulnerable to backdoor keys being created during a phishing or malware breach and then, if left undetected, the intruder can later regain network access.

One of the most serious risks associated with SSH is "port forwarding," which is the ability to circumvent the firewall-protected network segmentation that controls access and traffic. It's common practice to assign ports and open encrypted tunnels through firewalls for legitimate business needs by following a stringent request process. However, if safeguards are not established, an administrator with approved tunnel access can open other ports on the client computer, giving an unauthorized user—or a bad actor operating on the same network segment—access to an indirect connection through the host system and into the encrypted firewall tunnel.

"Many of our healthcare customers have thousands or tens of thousands of SSH servers in their environments. Each server is administered, controlled and configured individually by the person responsible for that machine. There is no central policy, practice or enforcement for how this should be done."

Mike Dodson

You can't protect what you don't know about

In a recently commissioned study, Venafi asked IT and security professionals with in-depth SSH knowledge from more than 100 healthcare institutions in the U.S., U.K. and Germany about their use of SSH keys and their readiness to protect them against attackers. The results indicate that most healthcare organizations are underprepared to protect against broad SSH-based attacks. In fact, 47 percent of those surveyed responded that SSH management is delegated to the IT administrators for the systems they control rather than centrally managed.

"Many of our healthcare customers have thousands or tens of thousands of SSH servers in their environments," said Dodson. "Each server is administered, controlled and configured individually by the person responsible for that machine. There is no central policy, practice or enforcement for how this should be done."

More striking, fewer than 10 percent of respondents admitted to having a complete and accurate inventory of SSH keys. Only 41 percent indicated they control who can write authorized key files. Improper control of SSH environments, which can be used to bypass security mechanisms, was another important finding: 40 percent don't prohibit port forwarding, and almost as many (37 percent) put no limits on source location.

Additional study findings show that 70 percent don't rotate administrator SSH keys regularly—less often than usernames and passwords—even though SSH keys have higher access privileges. Thirty-nine percent of those surveyed don't remove the SSH keys of administrators who were reassigned, terminated or left their jobs, which is concerning. Finally, the study found that 58 percent of respondents don't rotate SSH keys used by automated processes where administrators had access to them.

The state of SSH in healthcare

Based on the results of the study, one can conclude several important challenges remain with current SSH implementations in our healthcare institutions. Control mechanisms cannot accurately inventory administrator keys. Machine-to-machine keys that are automatically generated are not regularly rotated. Additionally, administrator keys could be weak, and former employees might still have access to their keys. The potential remains for backdoor keys to exist. Finally, lax SSH policies could encourage port forwarding through firewalls and open pivoting opportunities for attackers.

"A Privileged Access Management solution does not safeguard you from these risks; its focus is on protecting against the interactive risk of humans who have privileged access. This type of solution does not protect against the risks of SSH keys that are used by automated processes," added Dodson. "The use of SSH keys should be centrally controlled and enforced by policy."

Five practices to mitigate SSH risks

SSH environments provide privileged access to some of the most sensitive data for healthcare enterprises, including billing transactions and ePHI. The use of SSH keys should be centrally controlled through policies that limit both access and entitlements to vulnerable patient data and medical devices. Hygiene policies that are analogous to user identities must be established and enforced. Without taking such precautions, healthcare IT professionals increase their risk of a network system breach, as well as noncompliance with patient privacy laws, such as HIPAA.

HEALTHCARE IT PROFESSIONALS CAN FOCUS ON THE FOLLOWING FIVE PRACTICES TO IMMEDIATELY MITIGATE SSH RISKS IN THEIR ENVIRONMENTS:

1. Discover and maintain an accurate inventory of all SSH keys and server configurations.
2. Establish and enforce policy-driven controls on permission to create and access authorized SSH key files and ensure they are root-owned.
3. Take adequate steps to prevent unauthorized port forwarding and require IP source control for SSH keys.
4. Rotate SSH keys and review entitlements on a regular basis.
5. Audit frequently for compliance with all SSH policies.

"You have to start with education, and you're going to have to start at a high level in the organization," Dodson explained. "We've had a lot of success helping customers start with the chief information security officer or similar function. There's typically no single owner for SSH, but there is usually a single owner for info security."

Secure SSH keys and the machines they connect.
Turn to Venafi.

VENAFI®

About Venafi:
Venafi is the cybersecurity market leader in machine identity protection, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile and SSH. Venafi provides global visibility of machine identities and the risks associated with them for the extended enterprise – on premises, mobile, virtual, cloud and IoT – at machine speed and scale. Venafi puts this intelligence into action with automated remediation that reduces the security and availability risks connected with weak or compromised machine identities while safeguarding the flow of information to trusted machines and preventing communication with machines that are not trusted. For more information, visit: www.venafi.com.

Produced by HIMSS Media | www.himssmedia.com | © 2019