



Security of Interactive and Automated Access Management Using Secure Shell (SSH)

Users and hosts must be able to access other hosts in an interactive or automated fashion, often with very high privileges. This is necessary for a variety of reasons, including file transfers, disaster recovery, privileged access management, software and patch management, and dynamic cloud provisioning. Accessing other hosts is often accomplished using the Secure Shell (SSH) protocol.

The SSH protocol supports several mechanisms for interactive and automated authentication. Management of this access requires proper provisioning, termination, and monitoring processes. However, the security of SSH key-based access has been largely ignored to date. This publication assists organizations in understanding the basics of SSH interactive and automated access management in an enterprise, focusing on the management of SSH user keys.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- NIST.IR.7966.pdf