SSH User Key Management Draft & Meeting Summary

Tatu Ylonen

SSH Communications Security

ylo@ssh.com

The Problem We Try to Address

- SSH user keys very widely used for automated machine-to-machine access (and interactive access by sysadmins)
- Large organizations often have 8-200 authorized keys per server
- It is about managing access (rather than keys)
- Risks from unmanaged automated access:
  - Virus spread risk
  - Backdoors bypassing privileged access auditing
  - Leaked keys may allow access to production systems
  - No control of who can access what and no proper termination of access
- Problem not limited to key-based access; similar risks with certificates and Kerberos authentication
- Need reasonable compromise between security and practical implementability in a large enterprise

Main Elements of Solution

- Remediating legacy environment
  - Document and justify existing trust relationships
  - Remove orphan and unused keys
  - Add command restrictions
- Establishing proper processes
  - Approval, setup, removal of trust relationships
- Continuous operation and monitoring
  - Ensuring things remain under control, documented, audited
- All operations can be performed manually (and via audits)
- Requirements depend on system risk/impact classification

Next Steps

- Available internet-draft: draft-ylonen-sshkeybcp-00.txt
- Created mailing list: sshmgmt@ietf.org
- Please send comments to the draft to the list or to me (ylo@ssh.com) as soon as possible
- Planning next revision around end of March