How to Prevent Data Loss and Monitor Your Encrypted Networks

Samuli Siltanen
VP, EMEA
SSH Communications Security
samuli.siltanen@ssh.com
What we will cover today...

• About SSH Communications Security

• What are the problems in encrypted environments

• What are the business drivers to act?

• Introducing CryptoAuditor
Quick Facts

• We are the inventors of the SSH protocol
• Listed in NASDAQ OMX Helsinki (SSH1V)
• 50+ patents in various countries
• One of the most widely used protocols in the world with millions of deployments worldwide
• Over 3,000 customers worldwide including 7 of the Fortune 10
Why SSH?

• We know SSH:
  – Many of world’s largest enterprises depend on our 24x7 support.
  – Manageability for large environments with tens of thousands of SSH Servers & Clients.
  – z/OS, Solaris, Windows, Unix, Oracle, Linux, etc., for us: one SSH
  – Enterprise features: x509 support, group & policy based SSH connection control, …
Some of Our Customers

Energy & Utilities
- AGCO
- FirstEnergy
- GenOn
- ExxonMobil
- DTE Energy

Government
- Department of Defense
- United States Courts
- DISA
- NASA

Financial
- Barclaycard
- CapitalOne
- LCH.Clearnet
- ABN-AMRO
- BNP Paribas
- HSBC

Retail
- Stockman
- Ross
- Staples
- Harris Teeter

Healthcare
- Highmark Blue Shield
- Standard Life
THE CHALLENGE
Key customer and market challenges

How to ensure compliance with regulations and security standards, such as PCI-DSS?

How to audit and control internal and external privileged users’ activities?

How to enable visibility, auditing, alerts, and intrusion and data loss prevention also for encrypted connections?

How to enable external users’ access (contractors, outsourced IT, maintenance providers) with proper and efficient auditing and control?
Encryption vs. Visibility Paradox

- Typical enterprise data flows:
  - Internal to Internal
  - Internal to External
  - External to Internal

- Encryption means losing visibility to the content of the traffic!

- How to trace and audit users’ commands and activities?
- How to inspect and analyze incoming and outgoing data flows?
PCI-DSS req. 10

- Track and monitor all access to network resources and cardholder data

SOX section 404, req. 1.1

- Monitoring database access by privileged users

ISO 27001, A.10.10

- Monitoring objective: To detect unauthorized information processing activities.

HIPAA 164-312:

- Record and examine activity in information systems that contain or use EPHI
7.3 Incident and Security Incident Management

7.3.10 FIs should perform a root cause and impact analysis for major incidents which result in severe disruption of IT services

9.1 Data Loss Prevention

9.1.2 The FI should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information: Data at endpoint, Data in Motion, Data at rest

9.6 Security Monitoring

9.6.1 To facilitate prompt detection of unauthorized or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.

9.6.4 The FI should perform real-time monitoring of security events for critical systems and applications

11.1 User Access Management

11.1.2 Personnel from vendors, service providers or consulting firms: FI should subject these external employees to close supervision, monitoring and access restrictions similar to those expected of its own staff.

11.2 Privileged Access Management

11.2.3 The FI should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed
SSH CryptoAuditor - Privileged user access control and audit ”on-the-wire”:

→ No sign-in portals
→ No client or hosts agents to control access or gather audit trail

• Optical Character Recognition (OCR) to index and inspect session activities
• Audiovisual audit trail of administrative sessions
• On-the-fly (invisible) access control
• Inline, agentless, on-the-fly and invisible secure shell DLP and audit capabilities
• Centralized visibility for remote systems access
• Integration into existing DLP, IDS, SIEM

• Centralized key importation capabilities – enabling invisible user operation
• No changes to user experience or need to operate through a bastion server
Record entire session and all identities, from peer to target hosts.

<table>
<thead>
<tr>
<th>Real AD user identity</th>
<th>Destination server identity</th>
<th>Intermediate host</th>
<th>Target host</th>
<th>Video playback of session</th>
</tr>
</thead>
<tbody>
<tr>
<td>mattmak-ext root</td>
<td>ssh</td>
<td>session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>joukli-ext root</td>
<td>ssh</td>
<td>session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>deepafet-ext root</td>
<td>ssh</td>
<td>sftp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>alktsa-ext root</td>
<td>ssh</td>
<td>session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prist-ext root</td>
<td>ssh</td>
<td>session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>georgad-ext Administrator rdp</td>
<td>desktop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>georgad-ext Administrator rdp</td>
<td>clipboard</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Inspect session manually or run periodic scans and reports.

Look in all reported sessions (with Optical Character Recognition) for:

"Login*" OR "restart" OR "660001*"
Create periodically run scans and reports.

Session playback opens a timeline with timestamps of found occurrences.

Results can be downloaded as CSV, or saved as a periodically run scan and results emailed as CSV or displayed as a graph.

Keyword 660001* found in RDP session, within a clipboard copy command == data i.e. copied from hel-ts01.ncsd.corp host to client desktop.
Data Loss Prevention systems cannot inspect SFTP or SSH traffic.

Stop data loss in real time with transparent CryptoAuditor deployment and seamless integration to DLP system.

CryptoAuditor Hound sends unencrypted traffic to DLP server via standard ICAP protocol for further inspection.

It depends on the DLP server what will be done to the inspected packets/connections:
- Close the connection
- Raise alerts...

Diagram:
- Client
- SSH or SFTP
- Hound
- Unencrypted (over ICAP)
- Response
- Trails
- DLP (ICAP) server
- Vault
- Server
- DLP (ICAP) server
- Vault
- Hound

Table:

<table>
<thead>
<tr>
<th>DLP: DLP-example</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFTP preview size</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Maximum chunk size</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ICAP:

- Server name(s): icap.example.com
- Server port: 1344
- Minimum inspectable size: 6
- Uri: icap://localhost/echo
- Reject on internal failure: [ ]

Extra headers:

Possible X-prefix headers passed in each ICAP request. In these $USER will be replaced with the user name, $CLIENTADDR with the name or IP number of the client computer, $ORIGINADOR with the name or IP number of the server, $CHANNEL with the name of the SSH-protected channel, such as sftp, x11, or shell.
Replay Administrator Activity

- Ability to view the audit trail as a video stream, both terminal and graphical connections
- No need for additional applications, video streams directly through web-browser
Thank You!

Samuli Siltanen
VP, EMEA
SSH Communications Security
samuli.siltanen@ssh.com