The Pitfalls of Encrypted Networks in Banking Operations – Compliance Success in two industry cases

Elba Horta
Regional Sales Manager, Southern Europe
SSH Communications Security
elba.horta@ssh.com

ENABLE, MONITOR & MANAGE
ENCRYPTED NETWORKS

SSH Communications Security

WE ENABLE, MONITOR & MANAGE ENCRYPTED NETWORKS

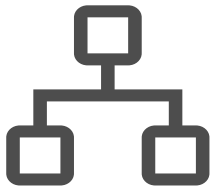
Quick Facts:

- Inventors of the SSH protocol
- Finnish Listed Company: NASDAQ OMX Helsinki (SSH1V)
- 3,000 customers including 7 of the Fortune 10

What We Do:

- Secure Shell Access Controls & Key Management
- Privileged Access Management
- Data-in-Transit Encryption

ENABLE	MONITOR	MANAGE
Tectia™ SSH	**CryptoAuditor™**	**Universal SSH Key Manager™**

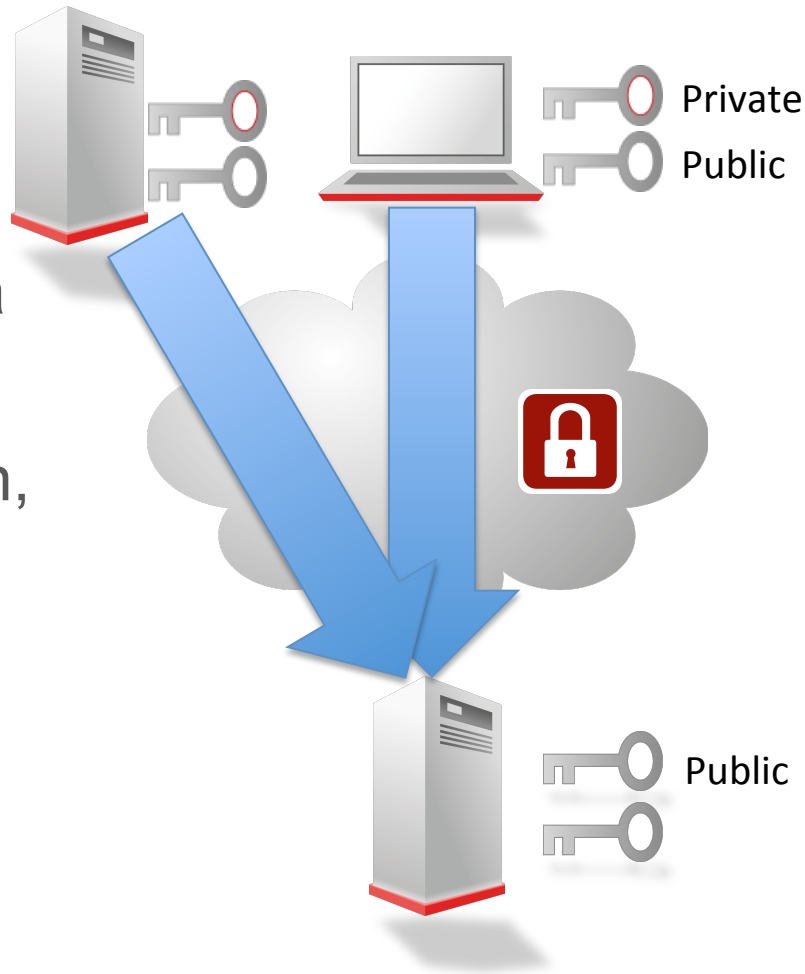


Our Customers

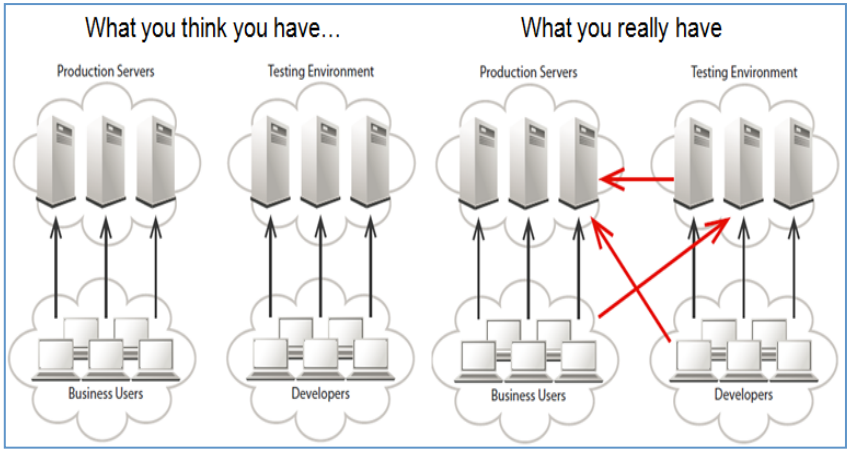
FINANCIALS	RETAIL	GOVERNMENT	UTILITIES & TRANSPORT	G2000/ ENTERPRISE
Deutsche Bank	Walmart	U.S. ARMY	FedEx	The Washington Post
citi	TJX THE TJX COMPANIES, INC.	U.S. AIR FORCE	eurostar	SAP
HSBC	STAPLES	U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849	FirstEnergy	EMC²
BNP PARIBAS	LOWE'S	DEPARTMENT OF THE NAVY UNITED STATES MARINE CORPS	BNSF	hp
euroclear	Harris Teeter	IRS	Burlington Northern Santa Fe Railway	Mercedes-Benz
barclaycard	BJ's		conEdison, inc.	Disney
CapitalOne				GM

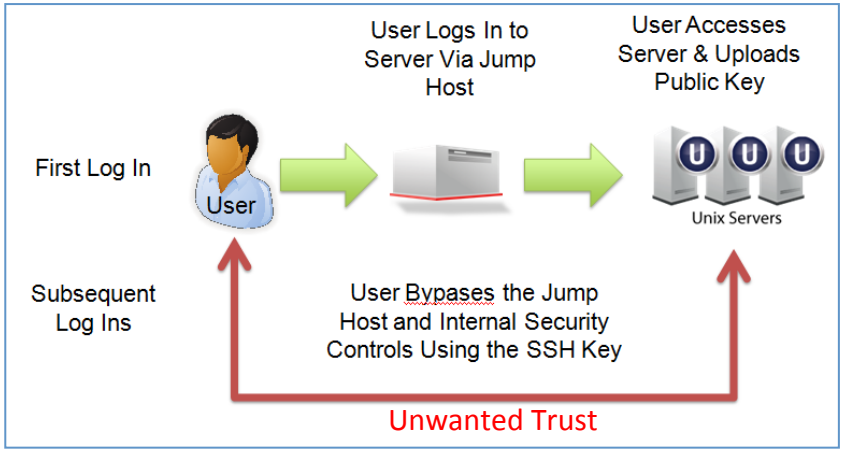
20 years of unmanaged SSH?

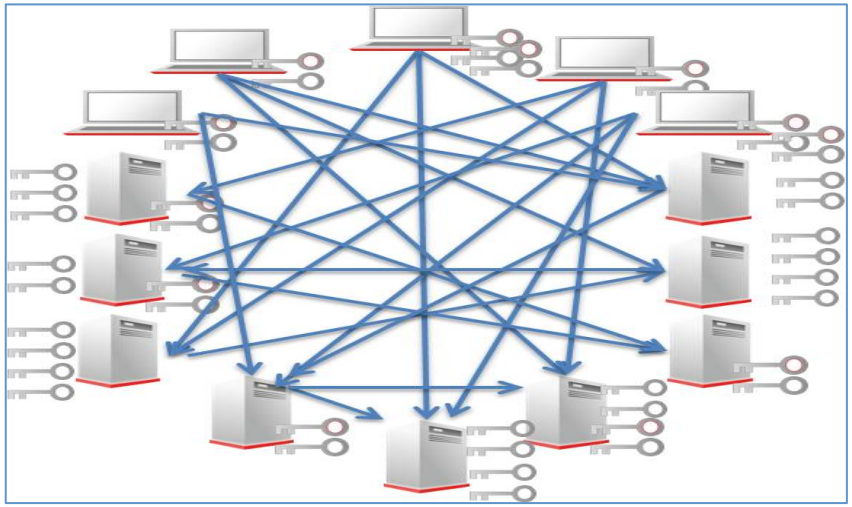
- No user key restrictions!
  - move or copy private keys
  - No expiration date
- No explicit association between a private key and an identity
- What governance? – key creation, tracking and removal



The SSH Key Management Challenges





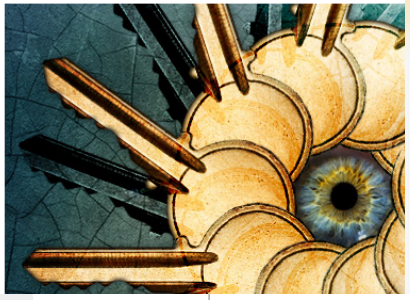


The risks are real

Former Hostgator employee arrested, charged with rooting 2,700 servers

Prosecutors: Backdoor and digital key gave him near u

by Dan Goodin - Apr 19 2013, 7:51pm FLEDT



COMPUTERWORLD

White Papers Webcasts

Topics | News | In Depth | Reviews | Blogs

Security | Application Security | Cybercrime and Hacking | Cybe | Malware and Vulnerabilities | Mobile Security | Privacy

Home > Security

News

Hackers break into two FreeBSD Proj servers using stolen SSH keys

ages distributed b
achines

EXPOSED ROOT SSH KEY WAS SHIPPING WITH EMERGENCY ALERT SYSTEM DEVICES

by Michael Mimoso Follow @mike_mimoso July 8, 2013 , 5:18 pm

SECURITY

Linux backdoor squirts code into SSH to keep its badness buried

Fokirtor! It LOOKED like legitimate traffic...

News | Sport | Comment | Culture | Business | Money | Life & style

News > Technology > Software

GitHub users warned over security risk

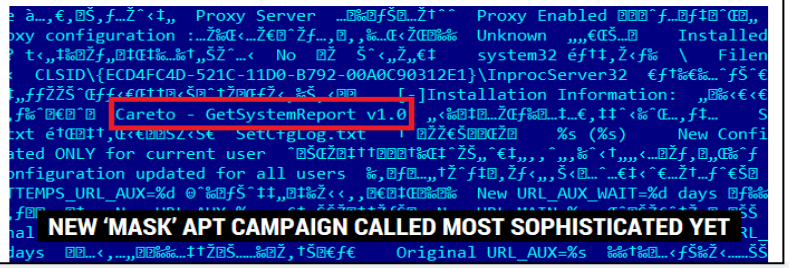
Search tool on programming site turns up SSH keys, which could allow attackers to hack sites or alter programs silently

SECURITY ANALYST SUMMIT 2014

9-13 FEB 2014 HARD ROCK HOTEL, PUNTA CANA, DOMINICAN REPUBLIC

threatpost | CATEGORIES | FEATURED | PODCASTS | VIDEOS

Welcome > Blog Home > Government > New 'Mask' APT Campaign Called Most Sophisticated Yet



NEW 'MASK' APT CAMPAIGN CALLED MOST SOPHISTICATED YET

Compliance Mandates and Regulations

- PCI-DSS
- Sarbanes-Oxley
- ISO 27001
- NIST
- National Regulations

Industry Case 1: Top 5 Global Bank

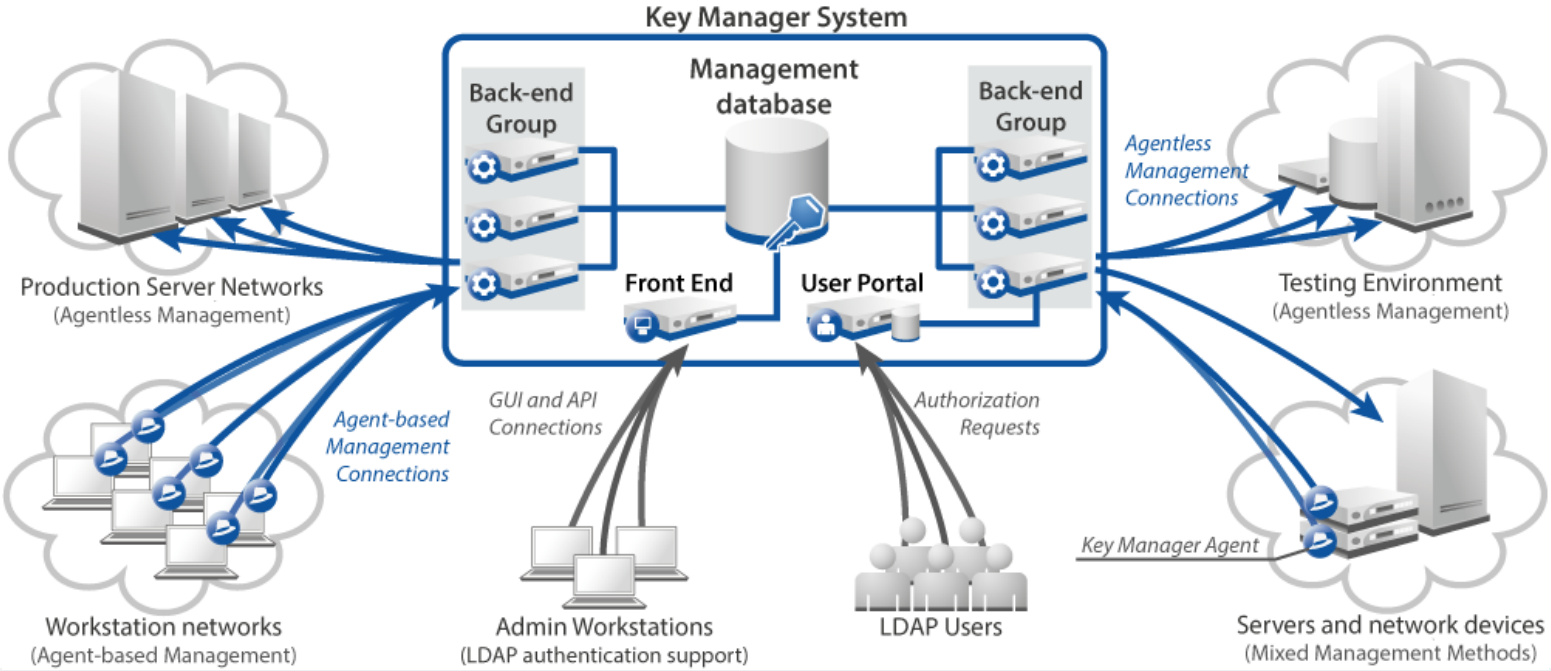
- A Top 5 Global Bank
  - Over 10,000 servers on their network
  - 1.5 million Secure Shell User Keys identified
  - 10% or 150,000 User Keys were unknown AND ALSO HAD ROOT ACCESS
  - No ability to monitor and enforce Secure Shell user access
  - Failed SOX & MAS Audit

Universal SSH Key Manager

Management & Governance

Discover → Monitor → Lockdown → Remediate → Manage

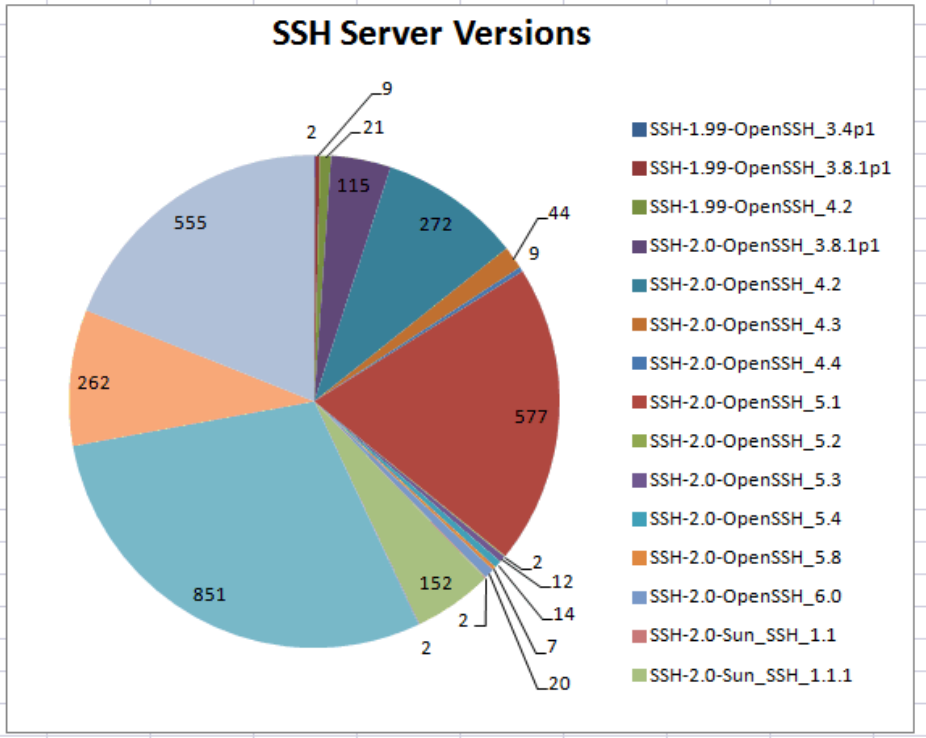
- Hosts, Users, SSH Keys and Trust-Relationships
- Logins and Key Usage
- Unauthorized Operations
- Relocate Keys and Lock Down Servers
- Remove Obsolete and Policy Violating Keys
- Automate and Integrate Life Cycle Management of Your SSH



Example finding and statistics from remediation project

Status after 12 months of Remediation Project

- Total locked servers 3133 (approx. 500 apps)
- 495 million key logins captured
- 60% of logins are directed towards 10 servers
- Only 4% of keys in the environment are in active use

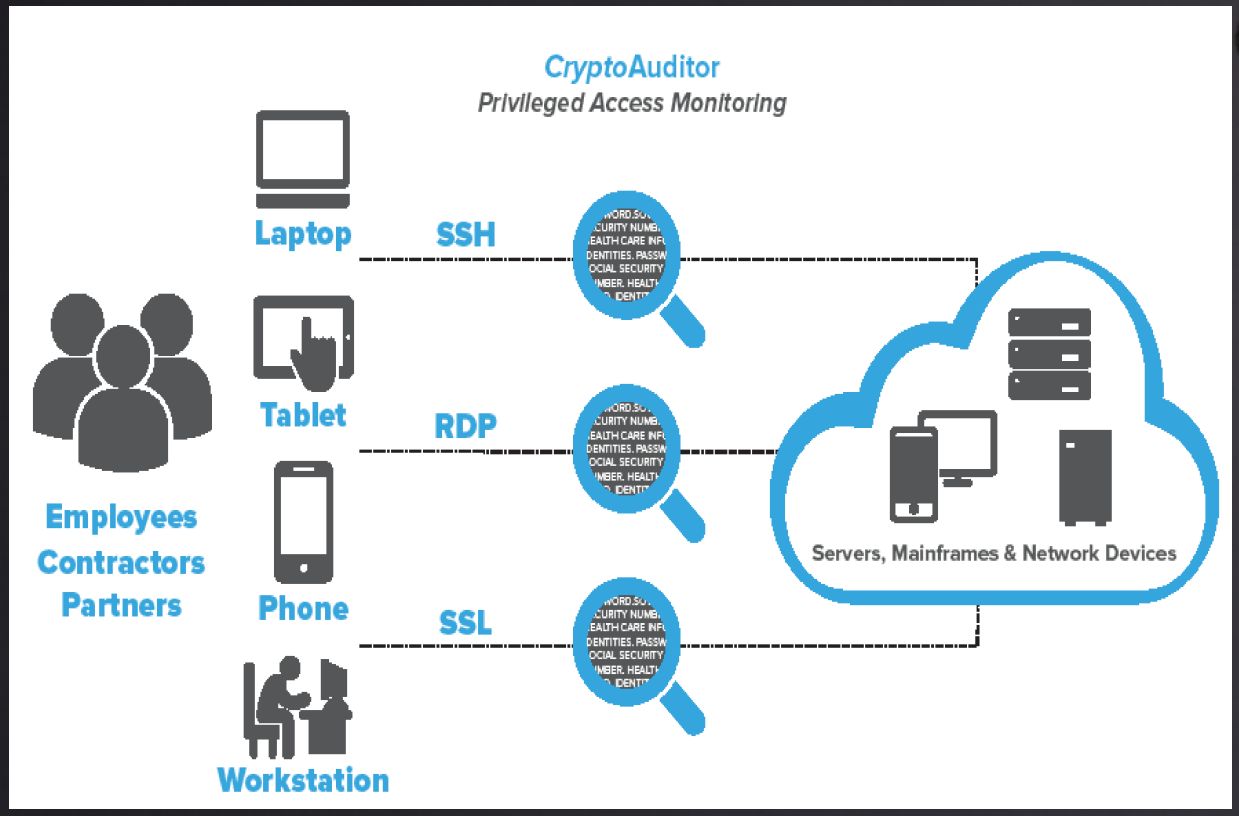


Servers	Private keys	Public keys	Unknown authorizations
3133	88410	929937	545222
Averages	28	297	174

Industry Case 2: International Financial Institution

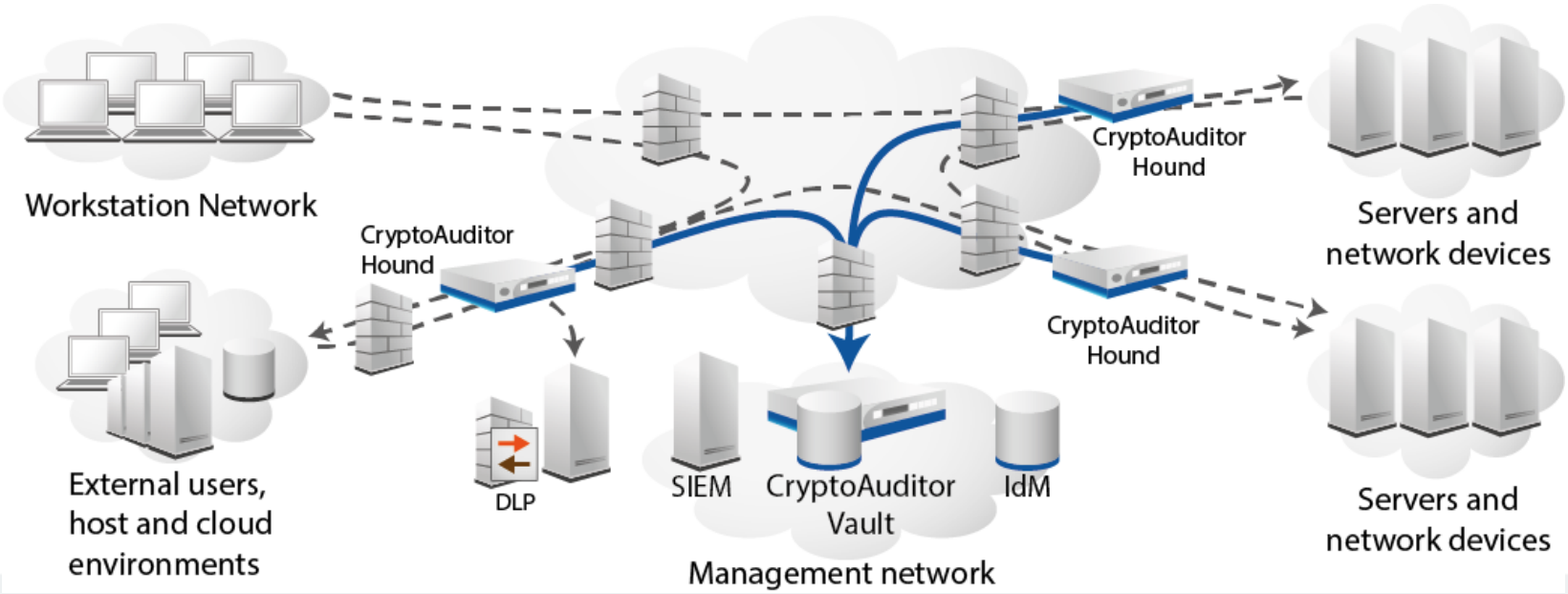
- Specializes in the settlement of securities transactions, as well as acting as Central Securities Depository. Must be compliant with Basel II.
- Various data centers and many external third party administrators.
  - No ability to monitor their remote connections nor encrypted traffic.

The Paradox: Blinded by encryption



CryptoAuditor: Privileged Access Monitoring

Inline and Agentless	Strong Authentication	Audit Encrypted Traffic	Integrate	Manage
•Quick Installation, transparent	•UserId mapping/ LDAP •Combine access control with phone SMS...	• Audit SSH, SSL, RDP, SFTP •Central Forensic Video repository	•Send sessions to DLP, IDS, AV, SIEM	• Real Time Actions, Alerts and Reporting



What can *you* do now?

SSH Key Access Control Questions

- Can you identify trust relationships (SSH key pairs)?
- Are your key creation procedures centralized and controlled?
- Do you remove keys?
- Do you rotate keys?
- Could you provide a compliance report?

Encrypted Privileged Access Control Questions

- What solutions do you have in place for meeting Privileged Access compliance requirements?
- Do you have a Data Loss Prevention solution? Does it inspect encrypted content ? (RDP, SSH, SFTP or TLS)
- If a Windows or UNIX administrator attempted to steal data or damage systems, could you stop them? Could you capture a complete record of what they did?
- Do external administrators know critical server passwords, or internal administrators share credentials?
- Could you provide a compliance report?

Next Steps

- Be proactive! You **Can** take control.
- Create a Project or use the flow of an existing one to solve these security and compliance issues
- Contact Us or our partner Security Brokers for a Proof of Concept


Thank You
Contact: elba.horta@ssh.com
ssh

CryptoAuditor Extra Technical Slides

Principle of CryptoAuditor

- Connections are inspected based on application protocol (SSH, RDP, other TCP…), port, IP address, VLAN ID and/or username of the connections.
  - No deep-packet inspection. Inspection rules are application protocol specific.
- SSH & RDP are inspected at application layer enabling control of these protocols at sub-channel level.
- Currently any other TLS-encrypted TCP-based protocols can be audited too, but the application protocols are not understood.
- Full payload and metadata of the connections can be inspected.

Security of Hounds and Vault

Hound security:

- Hounds do not store end user data or session information. Hound listens only the configured listener ports and management port 4772. Hound also has data connection to vault for sending captured sessions.
- Authentication-related data is fetched from the central Vault only as needed. Intercepted user sessions are unencrypted for generating stored connections only, and re-encrypted before being relayed to their intended destination. Stored connection information is immediately sent to the Vault for storage, rather than stored on the Hound.
- Listener ports are for intercepting SSH, RDP and other configured TCP sessions. All these sessions are terminated at the hound and will not expose any user credentials etc. There is no connection from listener port to Vault
- Management connection is opened from vault to hound. Hound listens port 4772 where it has SSH server running. SSH server has been configured to allow connections only using public key authentication and Vault management user. Vault private key is naturally in vault. This means that the connection is only allowed by the Vault user and from the Vault.
- Data channel from Hound to vault is secured using TLS. both hound and vault use certificates for authentication and trusting only each others certificates and therefore malicious man-in-the-middle between hound and vault is not possible

Vault Security

- Vault should be placed into secure management network that is monitored against any suspicious activities. Vault can be accessed through web-UI, https. SSH Access can be enabled for troubleshooting purposes when needed.
- Encryption is done using AES-128 and the encryption key is connection-specific. The encryption key itself is encrypted with a 2048-bit RSA public key. The RSA key pair is zone-specific: each zone has its own key pair. Passphrase is needed to open the connections
- The SSH keys and passwords that are stored in the Vault's key safe are encrypted using AES-128. The encryption key itself is encrypted with a 2048-bit RSA public key

Performance

- Concurrent connections **per Hound**, audit level full, no indexing:
  - 3000 SSH terminal connections, typical administrative use

  OR
  - 300 RDP connections, typical administrative use

- Concurrent connections **per Vault**, audit level full, no indexing:
  - 6000 SSH terminal connections, typical administrative use

- Connection open rate:
  - 3 new SSH or RDP connections per second

- Throughput of unaudited traffic in Router and Bridge modes:
  - 930 Mbit/s (full duplex)

- Throughput of audited SFTP traffic:
  - Audit level metadata: 400 Mbit/s

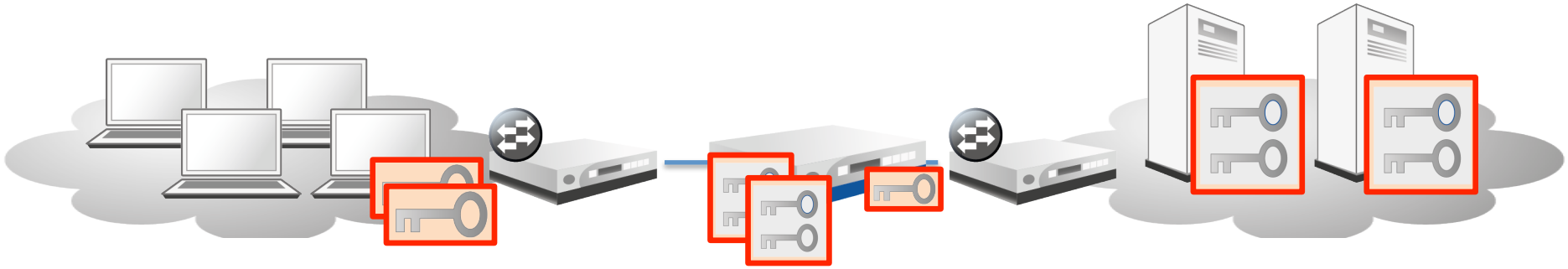
Server authentication with CrA

Option 1: Import server hostkeys to CryptoAuditor

1. Server hostkeys are imported to CryptoAuditor key storage
2. When client connects to server, CryptoAuditor intercepts the connections and presents server's identity
3. As client already trusts server's identity, connection is established transparently
4. CryptoAuditor connects to the end server and validates its identity
5. Connections (Client to CrA, CrA to server) are established and proceed to user authentication phase

Pros: 100% Transparent to the end user and existing processes

Cons: Requires server privatekeys to be copied to CryptoAuditor. Maintainability in large deployments. Private keys are encrypted for security.



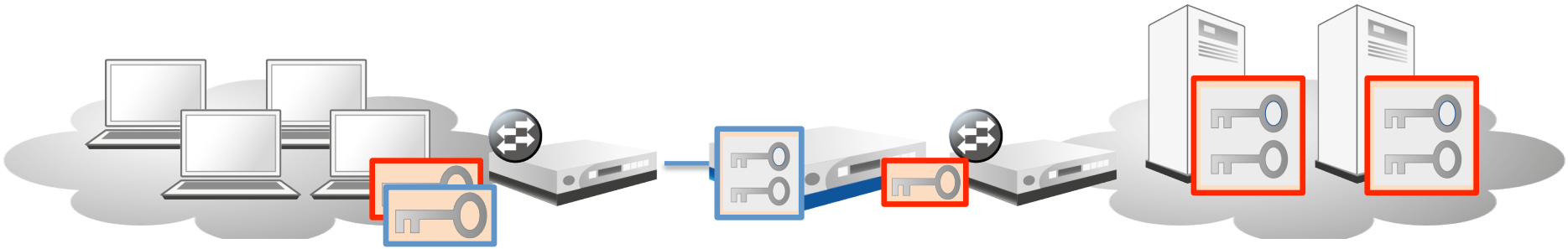
Server authentication with CrA

Option 2: CryptoAuditor presents its own server hostkey to clients

1. When client connects to server, CryptoAuditor intercepts the connections and presents its own identity to the client
2. As the identity is different than the already trusted one, user is prompted a notification that server identity has changed
3. If approved, new key is stored and used for further connections
4. CryptoAuditor connects to the end server and validates its identity
5. Connections (Client to CrA, CrA to server) are established and proceed to user authentication phase

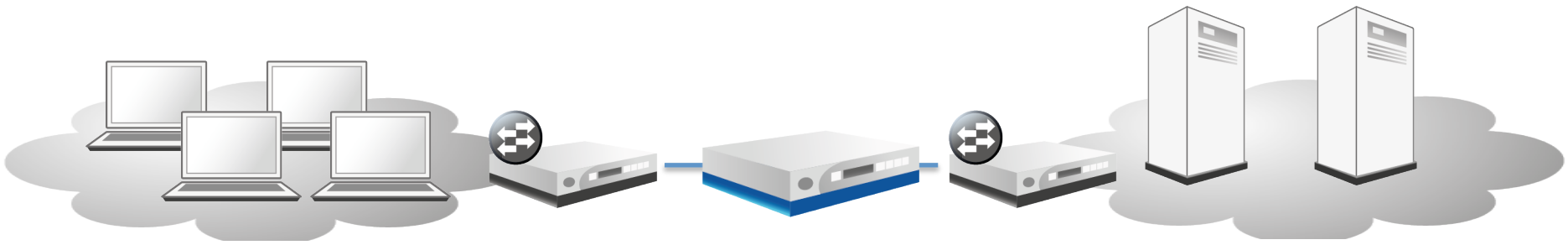
Pros: No need to import any keys. No hostkey maintenance

Cons: Requires users (clients) to approve new key. This is one time operation. New key must also be approved for all the automated processes.



User authentication, Password

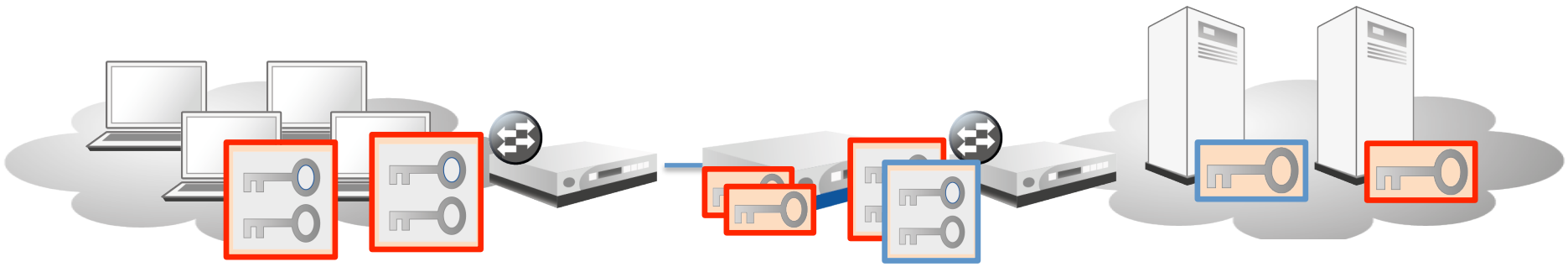
1. Server offers available user authentication methods to CryptoAuditor (Password, keyboard-interactive, kerberos, public key etc)
2. CryptoAuditor offers available user authentication methods to the client (can be the options passed from the server, or based on CrA configuration)
3. Client selects authentication method, for example Password
4. User enters password credentials and credentials are forwarded to the end server for validation
5. If password is correct, connections (Client to CrA, CrA to server) are established
6. Alternatively/additionally password can also be validated on CryptoAuditor before passing the connection to end server to provide additional layer of authentication (can be used for example with UserID and authentication mapping functionalities)



User authentication, Public key with CrA

When CryptoAuditor is deployed

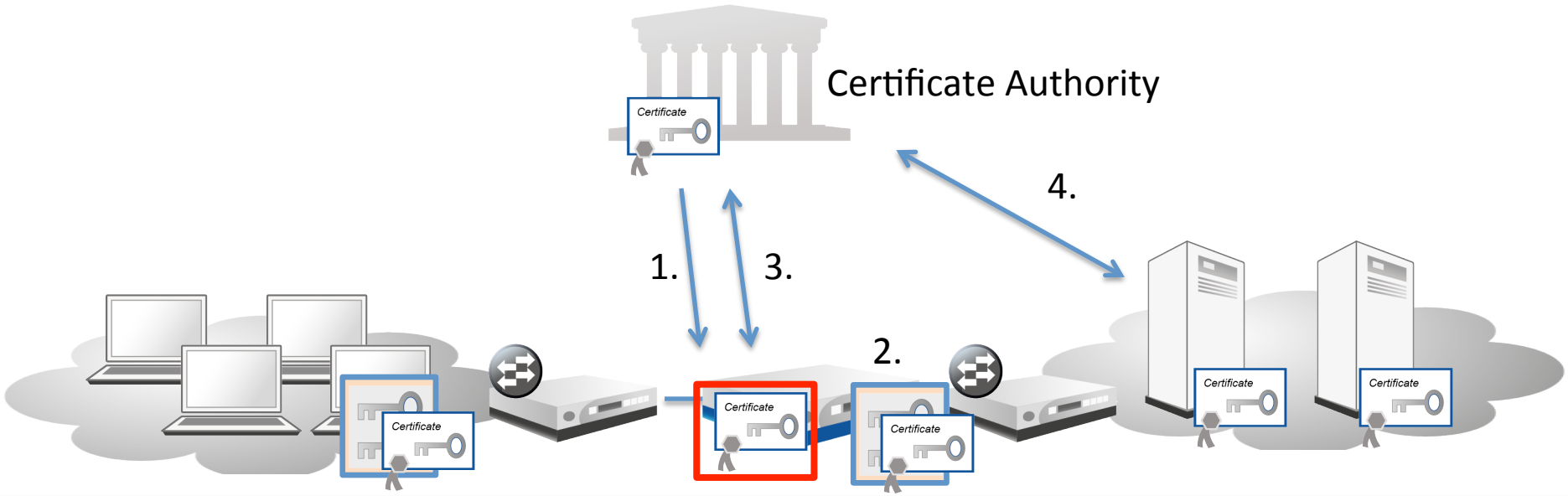
1. Users' authorizations have to be imported to CryptoAuditor to establish connection between the client and CrA
2. Users' privatekeys have to be imported to CrA (red keys) to establish connection between CrA and target server
3. Alternatively new keypairs can be created (blue keys), imported to CrA and pushed out to target servers to be used for authencation



User authentication, Certificates (either SW or stored on smartcard

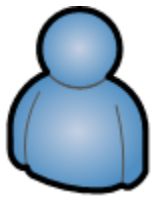
When CryptoAuditor is deployed

1. Trust-Anchor (rootCA) certificate has to be installed on CrA (red)
2. Additional certificate(s) can be enrolled for CrA (userIDs connecting to target servers)
3. When client connects, user's certificate is validated against the trusted CA certificate
4. Connection from CrA to target server is validated against trusted CA certificate. Alternatively this stage can be done using keys or other authentication methods (users are still authenticated using certificates against CrA)



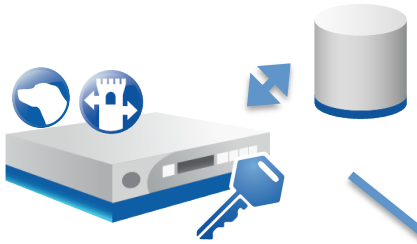
CryptoAuditor in Bastion host mode

1. User logs into Hound using his own user account and specifies end targer server using inline destination syntax user@target_server@hound



Joe

2. User is authenticated against AD, userID/target server is validated and if ok, userID is mapped into defined service account using defined rules, such as oracle

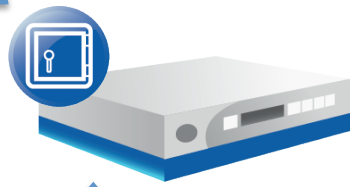


AD

oracle

3. 'oracle' private key is installed to CryptoAuditor and used for target server authentication

4. All the user's commands, server outputs, file transfer commands and content are audited and recorded



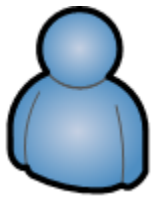
5. Session stats and content can be further sent to external tools such as DLP and SIEM in real time

CryptoAuditor in Transparent Mode (Router/ bridge)

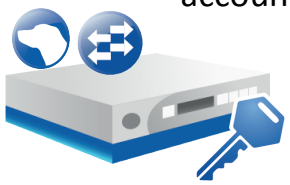
1. User connects directly to the target server own_userID@target_server

2. CryptoAuditor Hound captures the session directly from the network stream (inline)

3. User is authenticated against AD, userID/target server is validated and if ok, userID is mapped into defined service account using defined rules, such as oracle



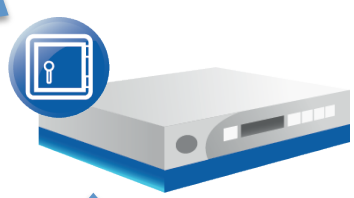
Joe



oracle

4. 'oracle' private key is installed to CryptoAuditor and used for target server authentication

5. All the user's commands, server outputs, file transfer commands and content are audited and recorded



6. Session stats and content can be further sent to external tools such as DLP and SIEM in real time