RSA®CONFERENCE CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Inventor of SSH Protocol
CEO of SSH Communications Security

EFFECTIVE KEY MANAGEMENT & AUDITING UNDER EVOLVING REGULATORY CHALLENGES

Tatu Ylönen
SSH Communications Security

RSACONFERENCE
CHINA 2012
RSA信息安全大会2012

What Is the SSH protocol?

- SSH is a protocol for secure encrypted communication over computer networks
- It ships with every Linux and Unix operating system and nearly all Internet routers, xDSL modems, etc
- SSH is used to provide security for more than half of world's web sites
- Also widely used for file transfers (also on Windows), system management, backups, etc

About the Author

ssh® is a registered trademark of SSH Communications Security (Tectia Corp)

- Developed and published the original SSH as free software in 1995
- Founded SSH Communications Security Corp in 1995
- CEO and controlling shareholder for SSH Communications Security
- Long-term entrepreneur
- Deeply involved in development of solutions for large SSH environments for both commercial SSH products and OpenSSH

SSH Communications Security

Quick Facts

Who we are

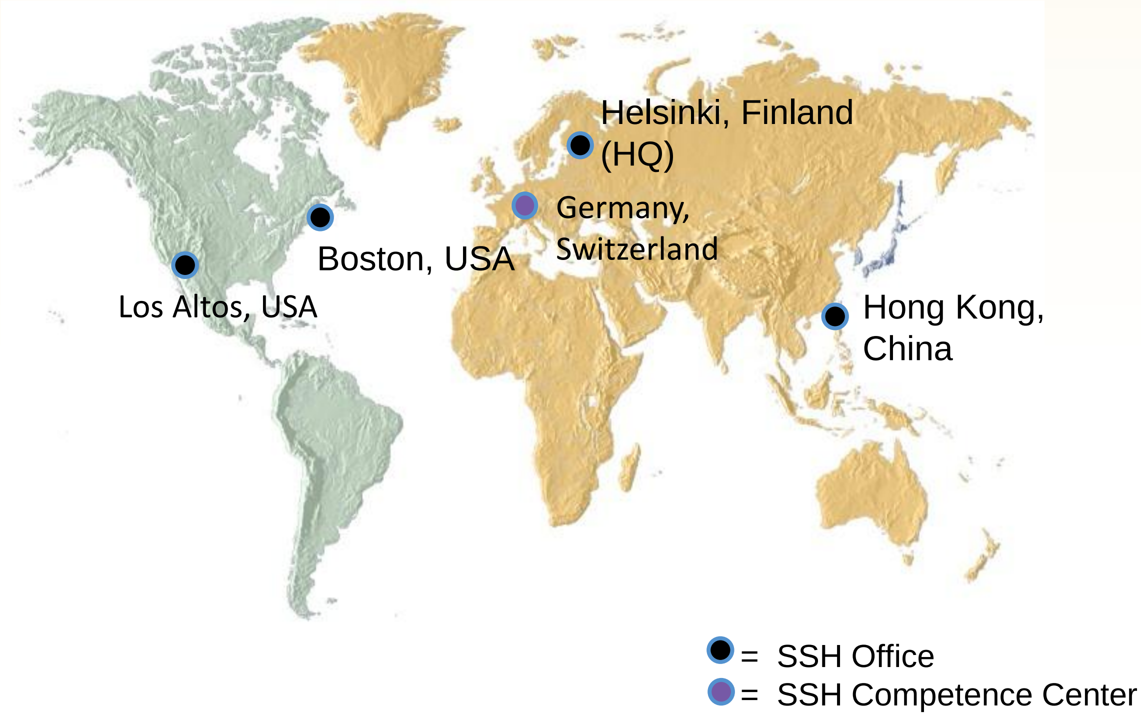
- Inventors of the SSH protocol
- NASDAQ OMX Helsinki (TEC1V)
- Work with large enterprises

What we do

- Cost-saving Linux/Unix security
- Key management for large SSH environments

Customers

- 3000+ customers
- 7 out of top 10 Fortune 500
- 40% of Fortune 500



International Compliance Trends

- **Payment Card Industry Data Security Standard (PCI DSS), 2004**
  - Customer data protection across the entire industry worldwide
- **Sarbanes-Oxley Act (SOX), 2002**
  - Require to establish an adequate internal control structure and include an assessment of its effectiveness in annual report
- **Health Insurance Portability and Accountability Act (HIPAA), 1998**
  - Mandate health plan providers & healthcare clearing houses to protect health information

Evolving Regulations in China

- **Approving and Forwarding the Opinions of China Securities Regulatory Commission on Improving the Quality of Listed Companies**
  - was issued in 2005 by The China Securities Regulatory Commission (CSRC)
- **Central Enterprises Comprehensive Risk Management Guidelines**
  - by State-owned Assets Supervision and Administration Commission of the State Council (SASAC)
- **Stock Exchange Listed Company Internal Control Guidelines**
  - was issued in 2006 by Shanghai Stock Exchange, and in 2007 by Shenzhen Stock Exchange
- **Payment Card Industry (PCI) Data Security Standard (DSS)**
  - has been pushed within leading payment gateways and top online merchants
- **China Sarbanes-Oxley Act (SOX)**
  - was issued in 2008, with supporting guidelines issued in 2010

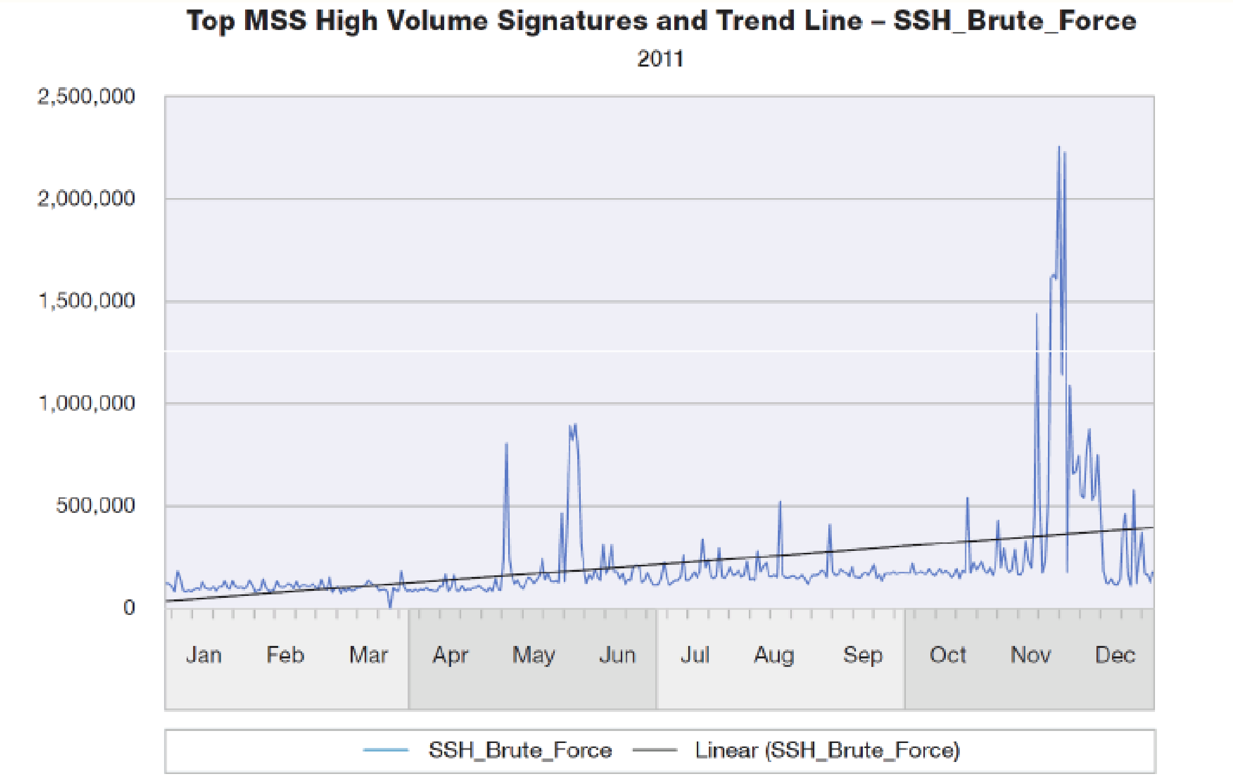
Compliance and SSH

- Most security standards require
  - Knowing who can access what
  - Terminating user's access when employee leaves
  - Changing passwords regularly
  - Securing encryption keys and changing them regularly

SSH Servers Are Increasingly Targets for Attacks

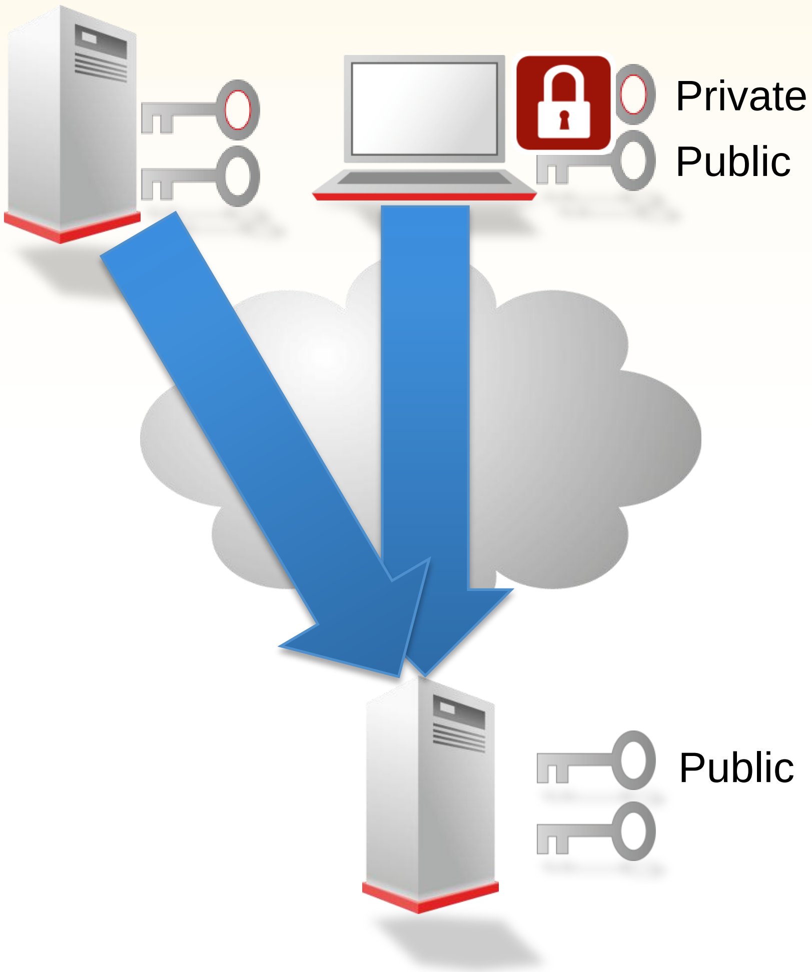
According to the IBM X-Force 2011 Trend and Risk Report, a sharp rise in SSH brute forcing attacks in the latter half of 2011.

E.g. automated password guessing attempts directed at secure shell servers

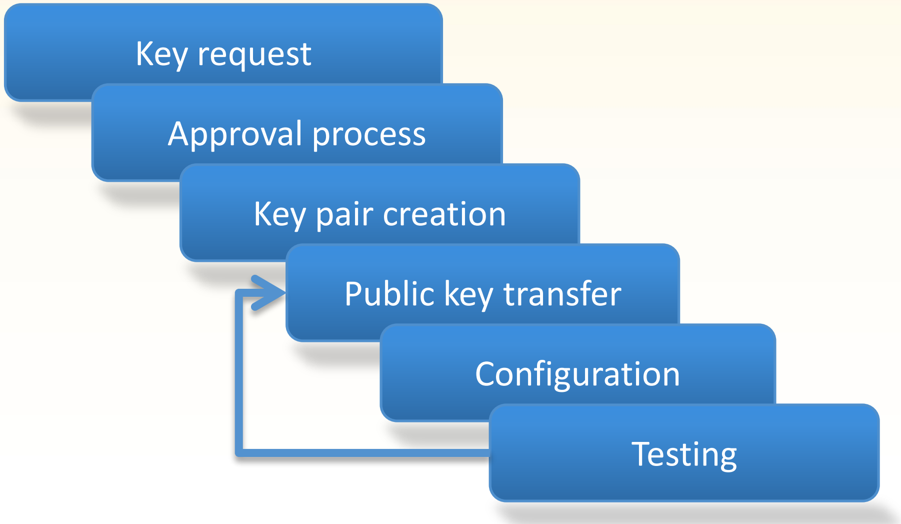


What Are SSH User Keys?

- A key pair, consisting of private and public key, that is used to prove user’s identity during the SSH authentication process
- Client sends digital signature by private key to server; server verifies using public key
- Enables non-interactive authentication
  - Mainly used for scheduled and automated file transfers and other tasks where user interaction is not possible



Typical Key Setup Procedure



Key request

Approval process

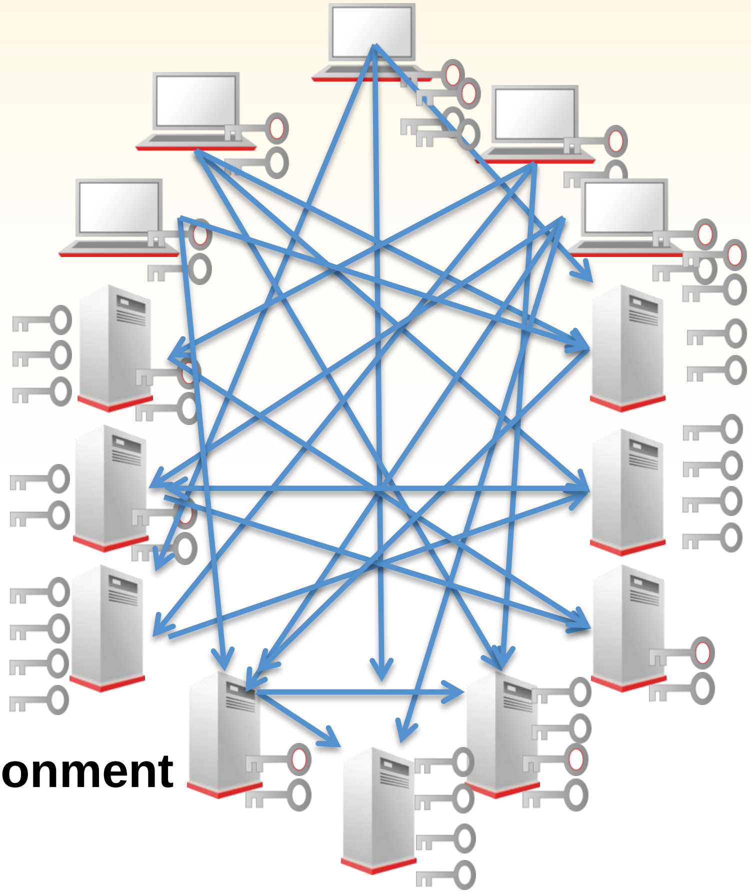
Key pair creation

Public key transfer

Configuration

Testing

Key setup procedure



Complicated environment for user keys

For large IT environments, unmanaged user keys have become a **major security problem**, a **substantial cost** and a **key audit finding**

Cost of Key Management in Large Environments

- A real case of **a major global financial institute** – now have over 100,000 user key pairs between accounts in their systems

Number of computers or virtual machines in environment	20,000
Number of new key setups per year	10,000
Average time per setup	15 min
Average number of systems per setup	10
Number of key removal operations per server per year	2
Time required per operation	30 min
Number of other key operations per server	4
Time required per operation	15 min
Average cost per hour of security admin	US$ 59
Estimated operational costs per year	**US$ 3,835,000**

Audit Requirements on Key Management

- **PCI-DSS**
  - *3.5 “Protect encryption keys used for encryption of cardholder data against disclosure and misuse.”*
  - *3.6 “Fully document and implement all key management processes and procedures.”*

- **COBIT, IT Governance Framework**
  - *DS5.8 - Cryptographic Key Management*
    - *Certification practices, key visibility, creation, storage, distribution and revoke*
  - *Supports SOX and other external audits*
  - *Often referenced on internal security policies*

- **ISO 27001-1**
  - *A.12.3.2 Key Management*

Examples of Risks Related to Unmanaged User Keys

- Administrators who left the organization years ago may still have access (copied private keys)
- Unused user keys still granting access to critical hosts
- Key pairs that have not been changed in years
- Lack of visibility to who has access to what
- Dozens or even hundreds of people with high-level access rights
- Human errors in manual key installation and removal processes

How to Bring SSH User Keys under Management

Based on experience with customers, the following approach for bringing SSH user keys under management provides compliance **and** saves costs:

1. **Discover** existing legacy keys and trust relationships in the environment
2. **Automate** creation and removal of keys and trust relationships (integrate to change control systems)
3. Automatically **rotate** (renew) keys every X months

Auditing Privileged Access and Encrypted Connections

- Another auditing challenge relates to controlling what system administrators do with their privileged access to computers
- A further challenge is monitoring what data is transferred encrypted across corporate firewalls
- Most system administration is nowadays done using encrypted procotols (SSH, Windows Remote Desktop (RDP), HTTP+SSL)
- System administrators like to use existing familiar tools and automated scripts cannot be easily changed

Transparent Monitoring of Encrypted Connections

- Requires access to keys (e.g., SSH host keys)
- Effectively performs friendly man-in-the-middle cryptographic attack on connections
- Enables co-operative inspection of plaintext content of encrypted traffic
- Content can be recorded for audit and sent to a DLP (Data Loss Prevention) system for detecting and preventing data theft
- Solves important audit and forensics problems without requiring workflow changes and works also for non-interactive scripts

Answer the question
from the leaflet and
get a chance to
Win an executive gift!

Get a mini-mooncake
at SSH booth!

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

Contact:

Tatu Ylonen <ylo at ssh.com>
SSH Communications Security
51/F Hopewell Centre
183 Queen’s Road East
Wan Chai, Hong Kong
+852 3602 3072

Thank You