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

以有效的审计及密钥管理
迎接不断演变的监管挑战

Tatu Ylönen

SSH Communications Security首席执行官

SSH 协议研发者

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

什么是 SSH 协议?

- 在计算机网络上进行安全加密的通信协议
- 置于每个 Linux 和 Unix 操作系统，以及几乎所有的互联网路由器和 xDSL 调制解调器等
- 保护全球一半以上的网站
- 也广泛用于文件传输（在 Windows 上），系统管理，备份等

关于讲者

ssh® 为SSH Communications Security (Tectia Corp) 的注册商标

- 于1995年开发了第一代的SSH协议，并将它设定为免费软件
- 于1995年创办了SSH Communications Security
- 现为首席执行官及控股股东
- 不仅是一位企业家，更精于技术发展，并为大型商用 SSH 及 OpenSSH 积极研发解决方案

SSH Communications Security

RSA CONFERENCE CHINA 2012

快览

关于我们

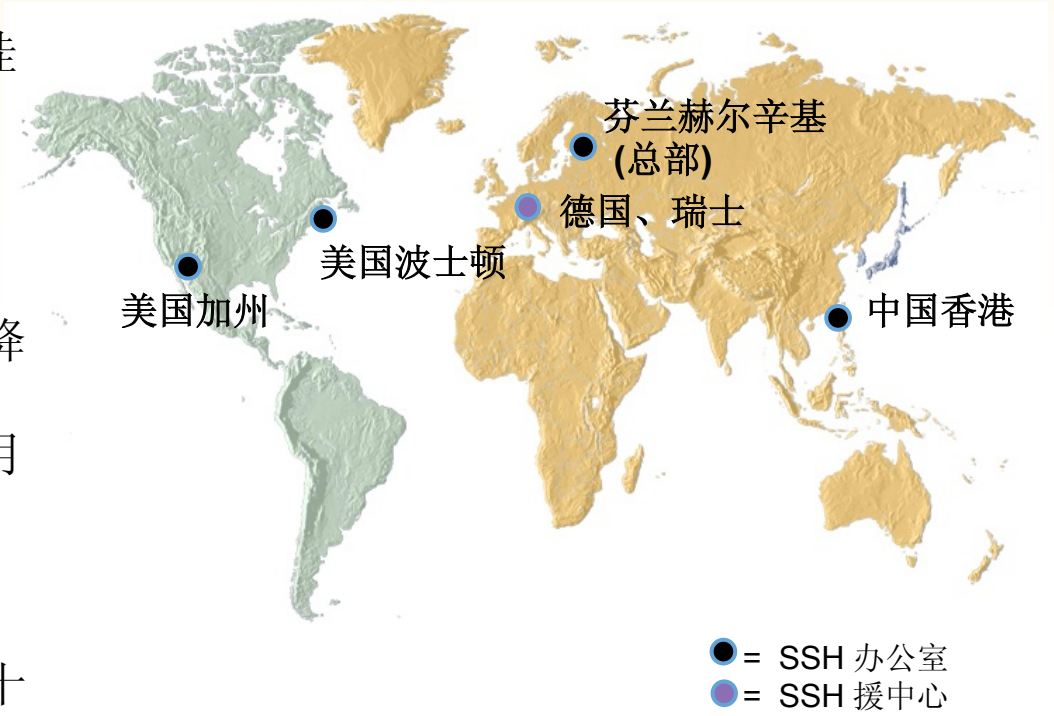
- SSH 协议研发者
- 在赫尔辛基纳斯达克 OMX 挂牌上市 (TEC1V)
- 与大型企业合作

我们的工作

- 为 Linux / Unix 系统安全性降低成本
- 为大型的 SSH 环境管理密钥

我们的客户

- 全球逾 3,000 家企业
- 包括《财富》杂志评选世界十强企业的其中七间
- 四成《财富》杂志评选世界500强企业



国际法规趋势

- **支付卡行业数据安全标准 (PCI DSS), 2004年**
  - 保护全球各行各业的客户数据
- **沙宾法案 (SOX), 2002年**
  - 要求企业制定充足的内部监控措施，包括评估年度报告的可信度及效用
- **健康保险隐私及责任法案 (HIPAA), 1998年**
  - 监管医疗保险供应商及医疗信息交换中心，以保障客户个人资料

中国不断演变的法规

- **国务院批转证监会关于提高上市公司质量意见的通知**
  - 中国证券监督管理委员会 (CSRC) 于2005年颁布
- **中央企业全面风险管理指引**
  - 国务院国有资产监督管理委员会 (SASAC) 颁布
- **证券交易所上市公司内部控制指引**
  - 上海证券交易所及深圳证券交易所分别于2006年及2007年颁布此法案
- **支付卡行业数据安全标准（PCI DSS）**
  - 于国内领先的支付平台及网上商户推广发展
- **中国沙宾法案（SOX)**
  - 于2008年发布，并于2010年颁布配套指引

合规性与 SSH

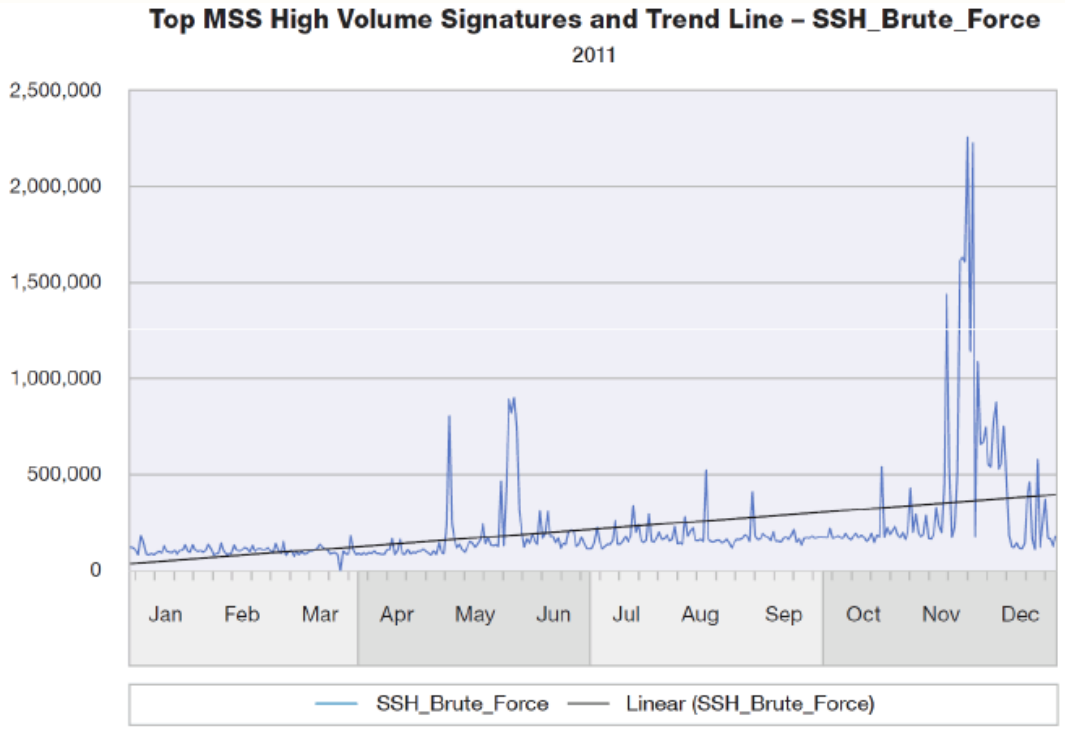
- 大多数安全标准都要求
  - 知道谁可以访问什么内容
  - 员工离开时，终止用户的访问
  - 定期更改密码
  - 保护加密密钥并定期更改

針對 SSH 服务器的攻击越来越多

RSA CONFERENCE CHINA 2012

IBM X-Force 2011趋势及危机报告指出，于2011年下半年度，SSH 暴力解破攻击激增

例如针对SSH服务器的自动化密码猜测攻击

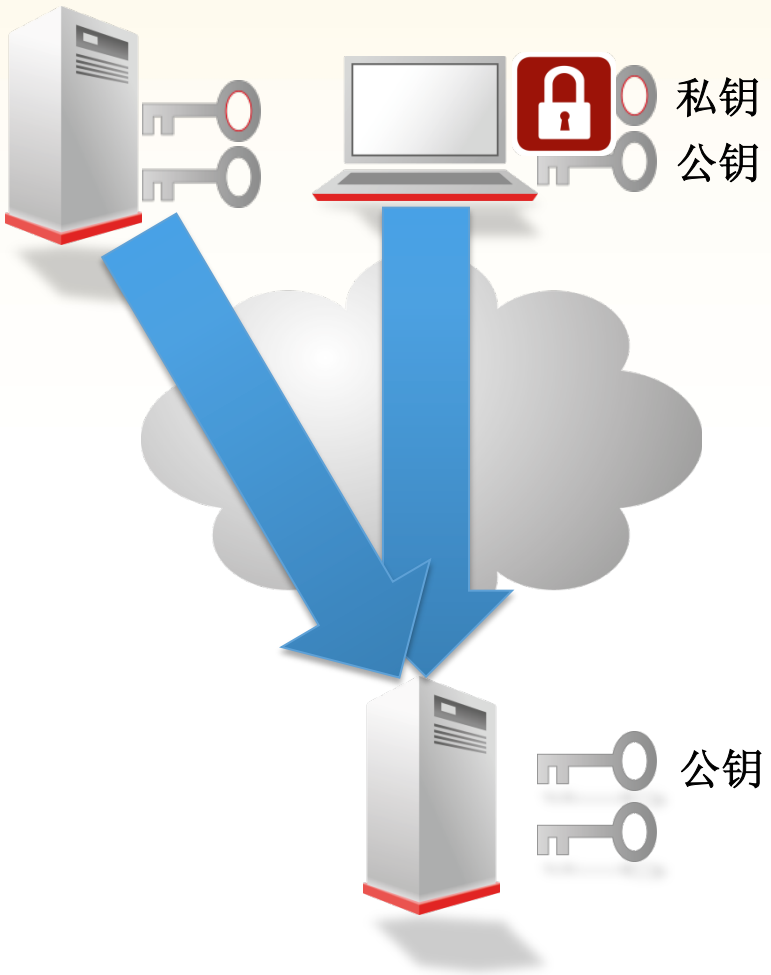


什么是 SSH 用户密钥?

- 在SSH身份验证过程中，一对密钥包括私钥和公钥，以证明用户的身份

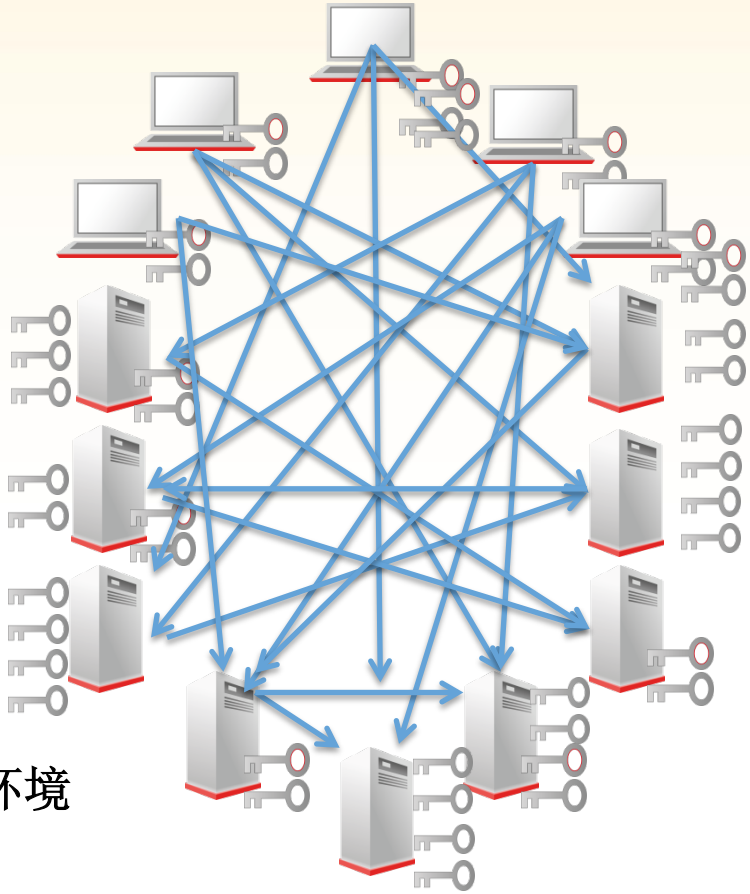
- 客户端通过私钥发送数码签名到服务器，服务器使用公钥进行验证

- 启动非交互式认证
  - 主要用于定期及自动文件传输，以及不能执行用户交互的任务



传统的密钥设置程序

密钥设定程序



用户密钥的复杂环境

对于大型 IT 的环境，未有妥善管理的用户密钥会构成
安全、持续高成本及审计问题

在大型环境的密钥管理成本

RSA CONFERENCE CHINA 2012

- 一所全球领先的金融机构 – 其系统现时拥有超过100,000对用户密钥

计算机或虚拟机的数量	20,000
每年全新设定密钥之数量	10,000
每对密钥设定之平均时间	15分钟
每次设定之系统平均数量	10
每台服务器移除密钥之数量	2
每次操作需时	30分钟
每台服务器的其他密钥操作之数量	4
每次操作需时	15分钟
每小时安全管理之平均成本	59 美元
估计每年平均成本	**3,835,000美元**

密钥管理的审计要求

- **支付卡行业数据安全标准（PCI DSS ）**
  - *3.5*「保护持卡人数据的加密密钥，防止泄露和滥用」
  - *3.6* 「对于所有用以加密持卡人数据的密钥，应制定并实施全面的密钥管理流程和程序」
- **信息及相关技术的管理控制与稽核 (COBIT)**
  - *DS5.8* – 加密密钥管理
    - 认证、密钥透明化、设置、储存、分发及移除
  - 支持沙宾法案 *(SOX)*及其他外部审计要求
  - 经常成为内部安全政策之指
- **ISO 27001-1**
  - *A.12.3.2*密钥管理

未有管理密钥的风险例子

- 管理员在离职数年后仍拥信息访问权限 (复制了私钥)
- 未曾使用的用户密钥仍获授权进入主机
- 多年没有更改私钥及公钥
- 缺乏透明度检视访问权限
- 动辄数十至几百人可访问重要讯息
- 以人手安装及移除密钥，产生人为错误

如何妥善管理 SSH 用户密钥

- 基于客户的经验，机构可采取以下方法妥善管理SSH用户密钥，以提供合规性及节省金钱
  - **找出**现存的私人和公共密钥，以及其信任关系
  - **自动**设定及移除密钥，建立信任关系
  - 每 x 个月自动**更换** (更新) 密钥

特权访问审计和加密连接

- 另一审计挑战涉及到控制系统管理员对计算机进行特权访问
- 另一项挑战是如何跨越企业防火墙， 监控传输中的加密数据
- 现在大多数系统管理都使用加密的网络协议 (SSH, Windows 远程桌面， HTTP+SSL)
- 系统管理员喜欢使用现有熟悉的工具和自动化的脚本

透明的加密连接

- 要求访问密钥 (如 SSH 主机密钥)
- 有效地防范加密连接的中间人攻击
- 对加密流量进行纯文本内容的检测
- 内容被记录作审计用途，并传送到 DLP（防数据丢失）系统，以检测和防止数据被窃取
- 解决重要的审计和取证问题，而不影响工作流程，也能启动非交互式脚本

回答传单上的问题,
有机会获得精美礼品!

在 SSH 展位一尝
迷你月饼!

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

联络:

Tatu Ylonen <ylo@ssh.com>

SSH Communications Security

香港湾仔皇后大道东 **183** 号合和中心 **51** 楼

+852 3602 3072

谢谢！

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012