Die Secure Shell

Marcel Holtmann
Universität Bielefeld - Technische Fakultät
AG Rechnernetze und verteilte Systeme
marcel@rvs.uni-bielefeld.de

16. Juni 1999

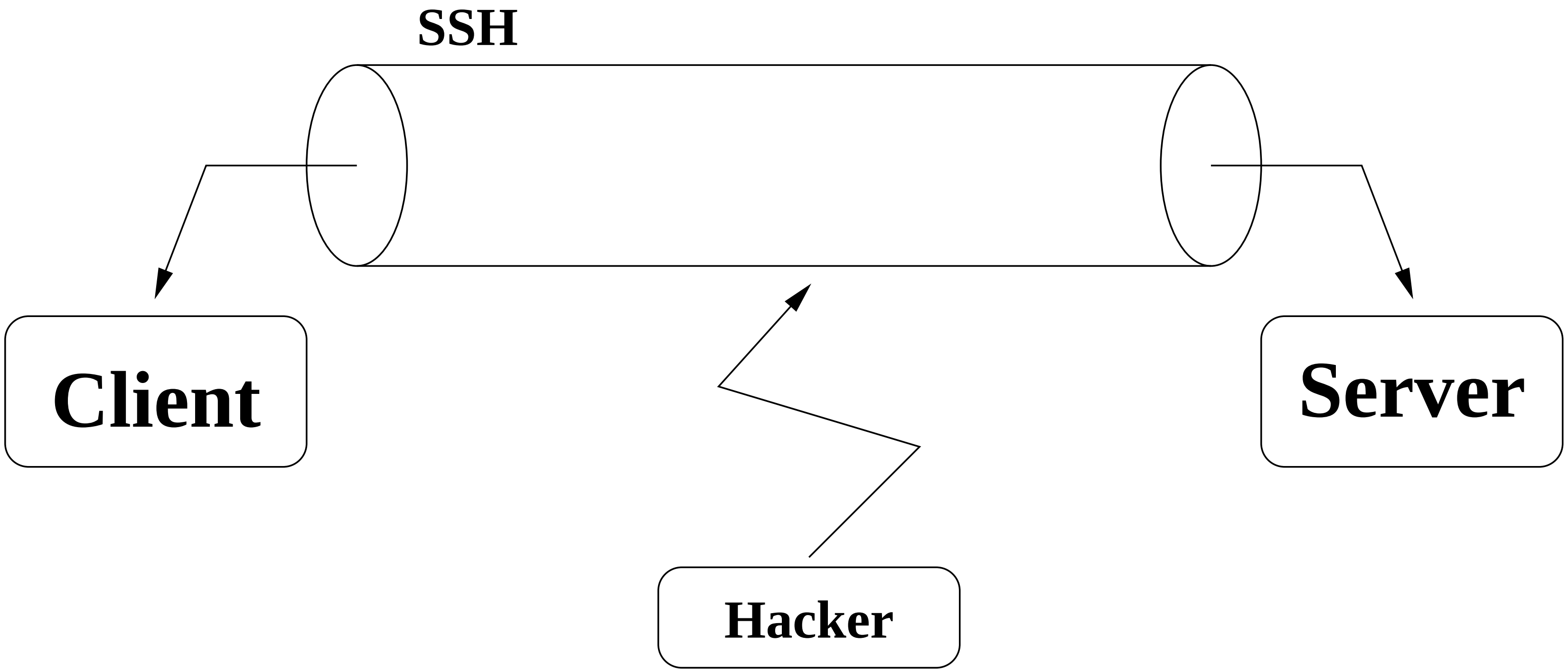
Was ist die SSH?

- SSH ist eine Remote Shell
- Der Datenverkehr ist vollständig verschlüsselt
- Die Implementierung entspricht dem Client-Server-Modell
- Die SSH ist ein Ersatz für die `r`-Tools und `telnet`
- Aber die Shell ist noch viel mehr ...!

Wie funktioniert die SSH?

- Auf dem Server läuft der `sshd`
- Der Server horcht an dem *Well-Known*-Port 22
- Beim Start des Server-Dämon wird ein öffentlicher Schlüssel generiert
- Wenn ein `ssh`-Client eine Verbindung zum Server aufbauen will, fordert er erst den öffentlichen Schlüssel an
- Mit diesem Schlüssel verschlüsselt er dann seinen eigenen Host-Schlüssel und überträgt diesen
- Nach diesem Handshaking erfolgt die verschlüsselte Datenübertragung

Wie funktioniert die SSH?



Vorteile der SSH

- Die Verbindung ist nach dem Handshake vollständig verschlüsselt
- Die Paßwortabfrage erfolgt erst nach dem Handshake - somit gelangt das Paßwort nur verschlüsselt über das Netz
- Ein su-Kommando auf dem Server ist sicher, da der ganze Datenverkehr verschlüsselt wird
- Die Einstellungen für das X11-Protokoll werden auf den Client umgebogen
- Mit einem öffentlichen Client-Schlüssel kann man auch auf die Paßworteingabe verzichten - die Authenfizierung erfolgt dann Anhand des Schlüssels

Was kann man noch?

- Die Secure Shell ist kein reiner Terminalersatz
- Man kann einzelne Ports vom lokales Host auf Ports des Remote Rechners forwarden
- Man kann z.B. den lokalen Port 110 auf einen Remote-Port 110 forwarden
- Dann kann man eine POP3 Verbindung zum lokalen Host machen
- Alle Anfragen werden dann verschlüsselt an den Mailserver gesendet
- Mit diesem Trick lassen sich dann alle unsicheren Dienste sicher machen

Was haben wir gemacht?

- SMTP und das Programm `sendmail`
- POP3 und IMAP
- NIS und NFS
- Der Automounter mit dem `autofs` und dem `amd`
- HTTP und der `Apache`
- Die Secure Shell (SSH Version 1 und 2)

Was gibt es sonst noch?

- SSL
- DHCP
- NTP
- SNMP
- LDAP
- PPP
- X11 und FS

Weitere Services und Programme

- Der *finger*-Service
- Das *make*-Tool
- RCS und CVS
- Backup mit *dump*
- Netzüberwachung mit *Saint/Satan* und *Gabriel*
- und vieles mehr ...