Internet Security 1 (IntSi1)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

11 Secure Shell
ssh, scp, sftp

Prof. Dr. Andreas Steffen
M. Liebi

Institute for Internet Technologies and Applications (ITA)

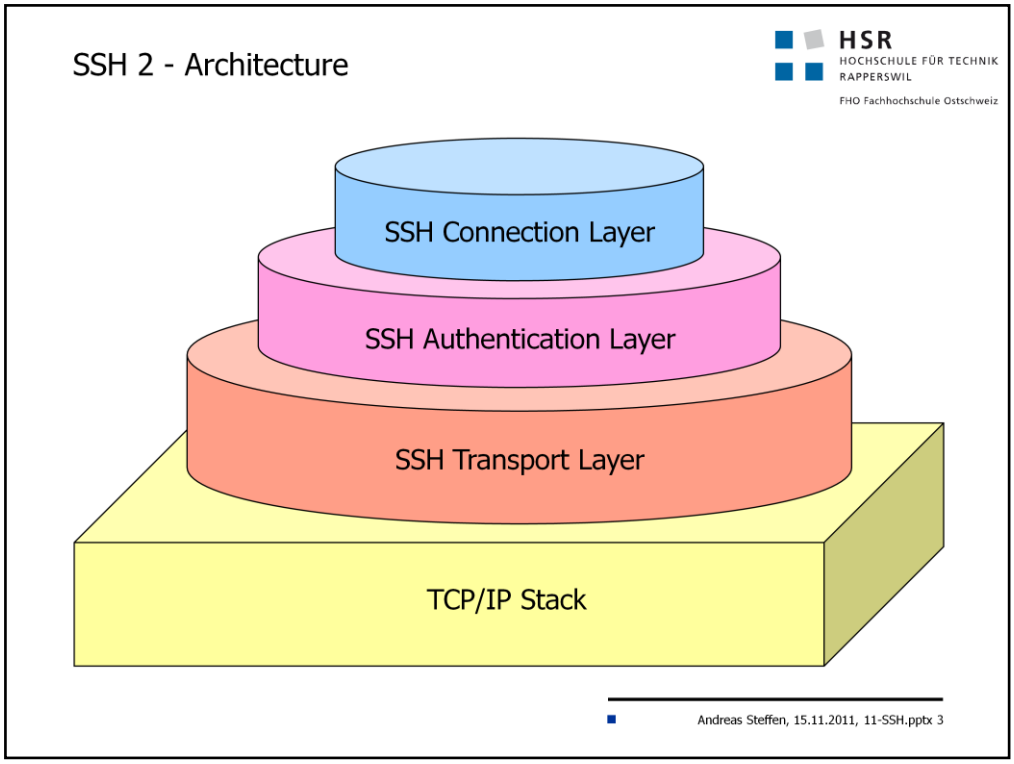
11 Secure Shell

- SSH history
- SSH 2 architecture
- SSH 2 transport layer
- Initial server key discovery
- SSH 2 authentication layer
- SSH 2 connection layer
- SSH 2 TCP/IP Port Forwarding
- SSH 2 Implementations

SSH - History

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- SSH version 1 was created in 1995 by Tatu Ylönen and first released under an open-source license.
- SSH quickly became a popular replacement for the insecure telnet protocol which doesn't offer server authentication and transmits the user credentials in the open.
- Tatu Ylönen founds SSH Communications Security which sells commercial SSH implementations.
- Under the auspices of the IETF, version 2 of the SSH protocol is developed. In a rewrite the protocol is split into a transport, connection, and authentication layers.
- The complete suite of SSH RFCs was released in January 2006
- SSH version 1 is vulnerable to various kinds of attacks and should not be used any more.
- No security flaws are known for the current SSH version 2.



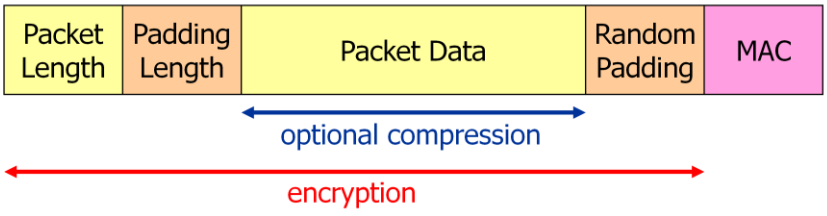
In January 2006 the SSH 2 Protocol architecture became an official Internet Standard:

- RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers
- RFC 4251 The Secure Shell (SSH) Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4253 The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254 The Secure Shell (SSH) Connection Protocol
- RFC 4255 Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
- RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol

SSH 2 – Transport Layer

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The transport layer provides algorithm negotiation, key exchange and server authentication and sets up a cryptographically secured connection that provides integrity, confidentiality and optional compression.
- The key exchange uses the Diffie-Hellman protocol with a 1024 bit modulus and thus ensures perfect forward secrecy.
- The server authentication is based on RSA or DSS signatures and uses either raw public keys or X.509, PGP or SPKI certificates.



Andreas Steffen, 15.11.2011, 11-SSH.pptx 4

SSH 2 Transport Layer Protocol: RFC 4253

Initial Server Key Discovery

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The first time a client connects to a ssh server, it is asked to verify the server's key.

```
[djm@roku djm]$ ssh root@hachi.mindrot.org
The authenticity of host 'hachi.mindrot.org (203.36.198.102)'
    can't be established.
RSA key fingerprint is cd:41:70:30:48:07:16:81:e5:30:34:66:f1:56:ef:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
root@hachi.mindrot.org's password: xxxxxxxx
Last login: Tue Aug 27 10:56:25 2002
[root@hachi root]#
```

- This is done to prevent an attacker impersonating a server, which would give them the opportunity to capture the password or the contents of the session.
- Once the server's key has been verified, it is recorded by the client in `~/.ssh/known_hosts` so it can be automatically checked upon each connection.

SSH 2 – Authentication Layer

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The authentication layer provides several mechanisms for user authentication. These include traditional password authentication as well as public-key or host-based authentication mechanisms.
- Password-based authentication: username and password are transmitted securely over the encrypted ssh transport layer. On the server a normal password-based login takes place.
- Public-key-based authentication: The user signs a challenge sent by the server with her private key. The public portion `id_rsa.pub` of the user's key must either be installed by the server in the file `~/.ssh/authorized_keys` first or sent interactively embedded in a trusted certificate.

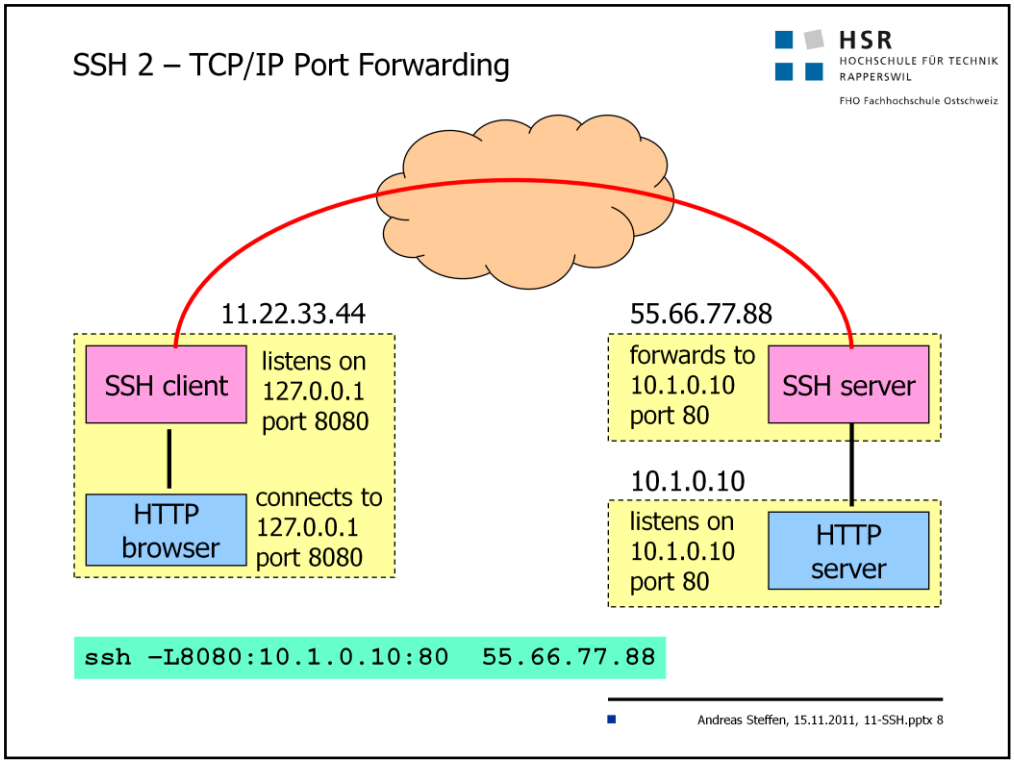
SSH 2 Authentication Protocol: RFC 4252

SSH 2 – Connection Layer

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- The connection layer provides
  - interactive login sessions: `ssh -l antje srv.kool.net`
  - remote execution of commands: `ssh antje@srv.kool.net "rm *"`
  - Secure remote copy of files and directories via scp or sftp commands
  - forwarded TCP/IP connections
  - and forwarded X11 connections
- All of these channels are multiplexed into a single encrypted tunnel.

SSH 2 Connection Protocol: RFC 4254


SSH 2 – TCP/IP Port Forwarding
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz
11.22.33.44
SSH client
listens on
127.0.0.1
port 8080
HTTP
browser
connects to
127.0.0.1
port 8080
55.66.77.88
forwards to
10.1.0.10
port 80
SSH server
10.1.0.10
listens on
10.1.0.10
port 80
HTTP
server
ssh -L8080:10.1.0.10:80 55.66.77.88
Andreas Steffen, 15.11.2011, 11-SSH.pptx 8

SSH 2 – Implementations

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- OpenSSH for OpenBSD
  - http://www.openssh.org
- Portable OpenSSH for Linux, Unix, Mac OS X
  - http://www.openssh.org
- PuTTY for Windows
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/
- WinSCP graphical Windows scp and sftp client
  - http://winscp.net/