Erik Brändli

Technologie ITSecX

Erik Brändli

Hüseyin Bozkurt

SSH

Remote Shell

Contents

[Changelog 1](#_Toc422322530)

[SSH 2](#_Toc422322531)

[Produktdaten 2](#_Toc422322532)

[Globale Anwendung 3](#_Toc422322533)

[Entscheidungsgrundlagen 3](#_Toc422322534)

# Changelog

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Datum* | *Name* | *Unterschrift* |
| Erstellt | 16.06.15 | Erik Brändli |  |
| Geprüft | 17.06.15 | Hüseyin Bozkurt |  |
| Freigegeben |  |  |  |

## SSH

### Produktdaten

Erscheinungsjahr 1997  
Aktuelle Version 6.47  
programmiert in C, C++, Python, Lua

Secure Shell oder SSH bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann. Häufig wird diese Methode verwendet, um lokal eine entfernte Kommandozeile verfügbar zu machen, das heißt, auf einer lokalen Konsole werden die Ausgaben der entfernten Konsole ausgegeben und die lokalen Tastatureingaben werden an den entfernten Rechner gesendet. Genutzt werden kann dies beispielsweise zur Fernwartung eines in einem entfernten Rechenzentrum stehenden Servers. Die neuere Protokoll-Version SSH-2 bietet weitere Funktionen wie Datenübertragung per SFTP.

Nachdem einige Schwachstellen in der Integritätsprüfung von SSH-1 bekannt geworden waren, wurde 1996 mit SSH-2 eine überarbeitete Version des Protokolls entwickelt. Sie ist inkompatibel zu SSH-1. Dabei wurde unter anderem das Protokoll in verschiedene Einzelteile aufgegliedert und somit die Verwendung sicherer Verschlüsselungs- und Authentifikations-Algorithmen ermöglicht. Damit wurde die Schwachstelle beseitigt. Derzeit gilt das Protokoll als sicher.

## Globale Anwendung

SSH ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein unsicheres Netzwerk. Dadurch dient es unter anderem als Ersatz für die Vorgänger rlogin, telnet und rsh; diese übertragen jeglichen Netzverkehr, darunter auch die Passwörter, unverschlüsselt.  
SSH ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein unsicheres Netzwerk. Dadurch dient es unter anderem als Ersatz für die Vorgänger rlogin, telnet und rsh; diese übertragen jeglichen Netzverkehr, darunter auch die Passwörter, unverschlüsselt.

Das ursprüngliche Anwendungsgebiet ist das Anmelden an entfernten Rechnern über ein Netzwerk (meistens das Internet), doch insbesondere SSH-2 ist nicht nur auf Terminalfunktionen beschränkt.

* SFTP und SCP bieten kryptographisch sicherere Alternativen zu FTP und RCP.
* X11 kann über SSH transportiert und somit gesichert werden.
* Über SSH können beliebige TCP/IP-Verbindungen getunnelt werden (Portweiterleitung); dabei wird jeweils ein einzelner Port von einem entfernten Server auf den Client weitergeleitet oder umgekehrt. So kann etwa eine ansonsten unverschlüsselte VNC-Verbindung abgesichert werden.
* Ein SSH-Client kann sich wie ein SOCKS-Server verhalten und ermöglicht somit einen automatisierten Zugriff auf entfernte Rechner durch den SSH-Tunnel, etwa zum Umgehen einer Firewall.
* Über SSHFS kann ein entferntes Dateisystem auf dem lokalen Rechner gemountet werden.
* Mit „ssh-keyscan“ kann der öffentliche Schlüssel eines entfernten Rechners ausgelesen werden. Damit kann man unter Zuhilfenahme des zugehörigen öffentlichen Schlüssels zum Beispiel feststellen, ob die IP-Adresse und/oder der DNS-Eintrag eines SSH-Servers manipuliert worden ist

1. Secure System Administration (Sichere Systemverwaltung) zur Absicherung der Fernverwaltung von Servern. Ersetzt telnet, rlogin etc.
2. Secure Application Tunneling (Sicheres Tunneln) zum transparenten Schutz TCP/IP-basierender Anwendungen als „End-to-End-Security“.
3. Secure Remote Command Execution (Sichere Ausführung von Kommandos) zur Ausführung einzelner Kommandos auf einem anderen Rechner. Dabei werden stdin, stdout und stderr transparent weitergeleitet.

## Entscheidungsgrundlagen

SSH verschlüsselt den gesamten Datenverkehr, login als auch die übertragenen Daten

Es ist momentan als Stable und als sicher eingestuft. Außerdem bittet SSH die tunnel-technologie an was ermöglicht, das alle Daten durchs SSH-Protokoll geschleust werden.