Kapitel 13: Secure Shell (SSH)

Wdh

Schutzziele der Informationssicherheit

- **Vertraulichkeit (engl. confidentiality)**
  - Die Daten sind nur den befugten Parteien zugänglich. Wird in der Regel durch Verschlüsselung erreicht.
- **Integrität (engl. integrity)**
  - Die Daten sind korrekt und wurden während der Übertragung nicht verändert. Änderungen können durch kryptographische Prüfsummen erkannt werden.
- **Authentizität (engl. authenticity)**
  - Die Daten stammen von der erzeugenden Partei. Die Identität der erzeugenden Partei kann durch digitale Signaturen überprüft werden.
- **Verfügbarkeit (engl. availability)**
  - Die Daten bzw. die Systeme können von befugten Personen gelesen oder bearbeitet oder benutzt werden. Wird meist mittels redundanter Systeme adressiert.
- **Verbindlichkeit/Nichtabstreitbarkeit** (engl. non-repudiation)
  - Unzulässiges Abstreiten durchgeführter Handlungen ist nicht möglich.

Authentisierung, Authentifizierung und Autorisierung Begrifflichkeiten

- **Authentisierung** bezeichnet den Nachweis der Identität einer Partei
  - Nachweis kann in verschiedenen Formen erfolgen
    - Eigenschaft: etwas, was die authentisierende Partei ist (bspw. biometrisches Merkmal)
    - Besitz: etwas, was die authentisierende Partei hat (bspw. Personalausweis)
    - Wissen: etwas, was die authentisierende Partei weiß (bspw. Geheimnis/Passwort)
- **Authentifizierung** bezeichnet das Vorgehen zur Überprüfung der Behauptung der Identität, also die Prüfung der behaupteten Authentisierung
- **Autorisierung** bezeichnet die Gewährleistung oder das Einräumen von bestimmten Rechten auf bereitgestellte Dienste oder Ressourcen

„Ich authentisiere mich (aktiv) am SSH-Server mit meinem (privaten) SSH-Schlüssel.
Ich werde vom SSH-Server authentifiziert (passiv) anhand des von mir bereitgestellten Schlüsselmaterials (privater Schlüssel).
Ich bin anschließend auf Grund meiner erfolgreichen Authentisierung autorisiert, auf den SSH-Server der Abteilung Informatik zuzugreifen.“

Wie adressiert SSH die Schutzziele der Informationssicherheit?

- **Vertraulichkeit** (engl. confidentiality)
  - Mittels Verschlüsselungsalgorithmen wie AES, ChaCha20 und RSA
- **Integrität** (engl. integrity)
  - Mittels kryptografischer Primitive, wie MACs, ECDSA, Ed25519, etc.
- **Authentizität** (engl. authenticity)
  - Mittels asymmetrischer Schlüssel
    - Privater und öffentlicher Schlüssel d* Benutzer*in
    - Öffentlicher Schlüssel bzw. Fingerabdruck (engl. fingerprint) des SSH-Servers

Secure Shell

Einführung und Geschichte

- Kryptografisches Netzwerkprotokoll
- Ermöglicht sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke

Technische Daten

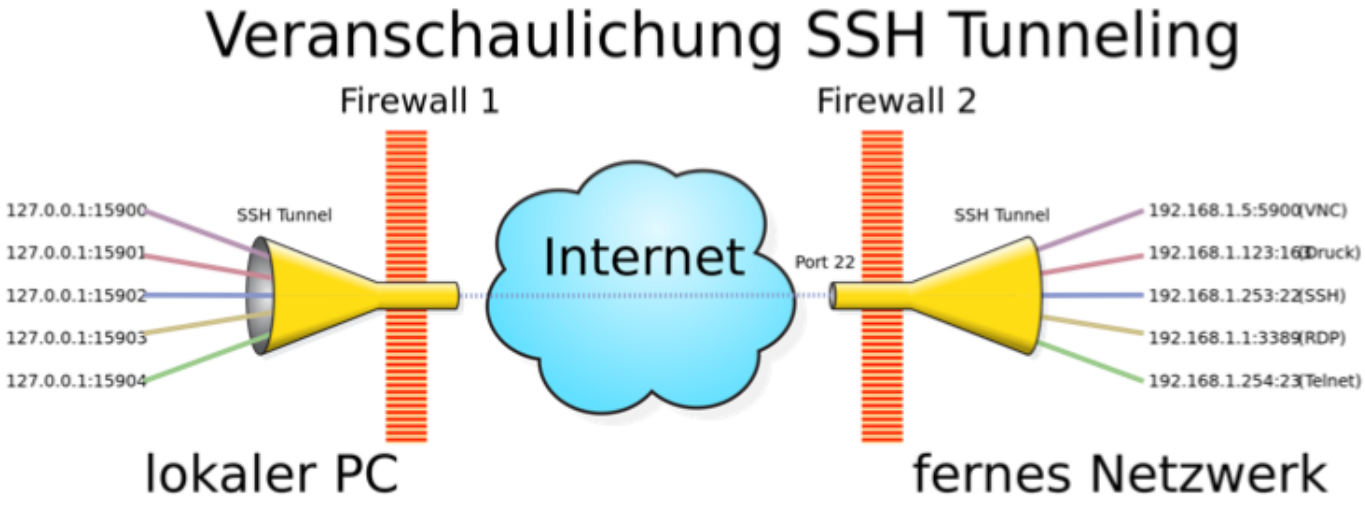
- Im ISO/OSI-Schichtenmodell auf Schicht 7 (Anwendungsschicht).
- Die Internet Assigned Numbers Authority (IANA) hat SSH Port 22 zugeordnet.
- Erlaubt die Verwendung von TCP, UDP und SCTP.
- Verwendet eine Client-Server-Architektur
    - 1-n SSH-Clients verbinden sich mit 1 SSH-Server

Secure Shell Anwendungsfälle

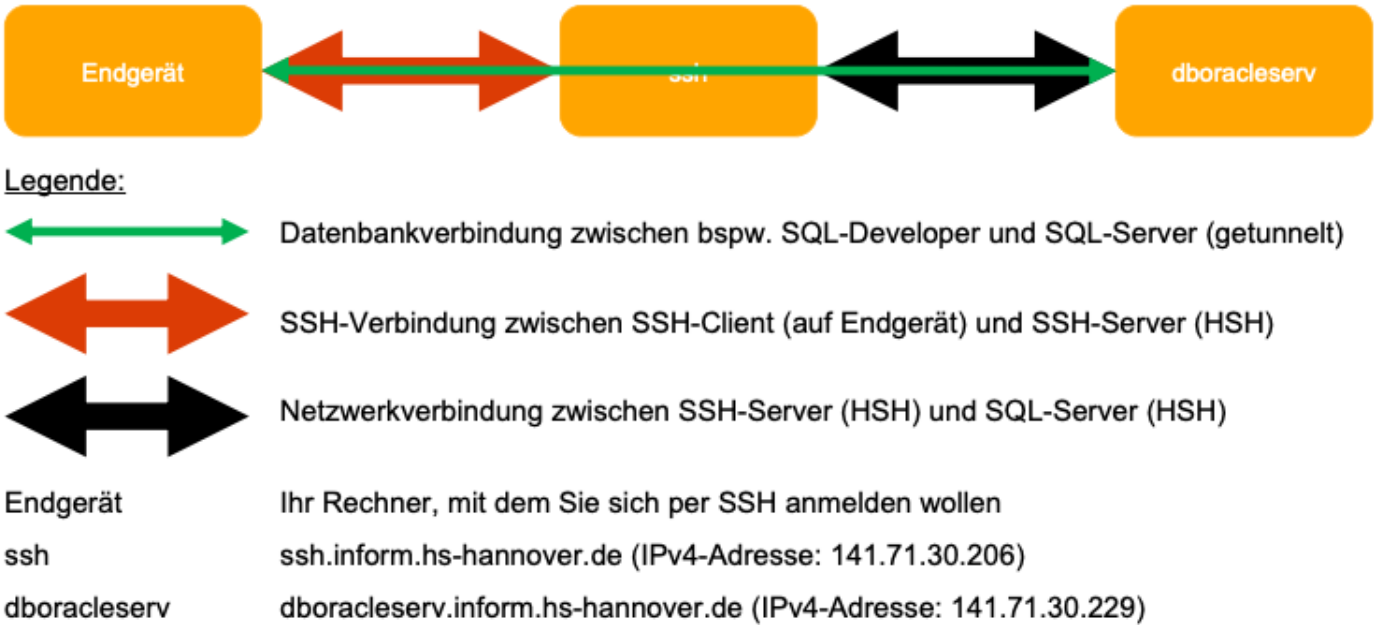
- **Anmeldung an einem entfernten Rechner (ersetzt Telnet und rlogin)**
- **Ausführen eines Kommandos auf einem entfernten Rechner (ersetzt rsh)**
- **Übertragen von Daten von oder zu einem entfernten Rechner** (Kopieren, Backups, Spiegeln, etc.)
    - meist über SCP oder SFTP

- **Port-Forwarding, d.h. das Weiterleiten eines TCP/UDP-Ports** um bspw.
    - den Datenbankserver der Abteilung Informatik von zu Hause aus zu erreichen
    - den Dateiserver der Abteilung Informatik von zu Hause aus zu erreichen
    - einen Serverdienst (bspw. im Rahmen eines studentischen Projekts) in der Abteilung Informatik zu erreichen, der nicht aus dem Internet erreichbar ist
    - aus der Hochschule den eigenen Dateiserver (oder das NAS) zu Hause zu erreichen
    - aus einem WLAN in einem Café die FritzBox zu Hause zu administrieren
    - Dienste auf dem eigenen System anderen in der Ferne zur Verfügung zu stellen (quasi: Port-Forwarding in die umgekehrte Richtung)
    - zwei entfernte Dienste miteinander zu verbinden
- **Tunneling ermöglicht das Einbetten von nahezu beliebigen anderen Netzwerkprotokollen in einen SSH- Tunnel**
    - ermöglicht bspw. den Einsatz von ungesichertem SMB auf Windows-Systemen über das Internet

Tunnel veranschaulicht



Tunnel zum Datenbankserver



Schlüssel verwenden

- Erstellte Schlüssel können mittels `ssh user@hostname` verwendet werden, um eine Verbindung zu einem SSH-Server aufzubauen

Mögliche Aufrufparamter:
`-i` erlaubt die Angabe eines Dateinamens, der den privaten Schlüssel enthält
(bspw. id_rsa im Verzeichnis .ssh)
Um eine Verbindung als User studi zum SSH-Server der Abteilung Informatik aufzubauen:
`ssh -i ~/.ssh/id_rsa studi@ssh.inform.hs-hannover.de`
Voraussetzung hierfür ist, dass die Datei authorized_keys im Benutzer*innen-Ordner .ssh auf dem Server der Abteilung Informatik den zugehören öffentlichen Schlüssel enthält

Port-Forwarding verwenden

Local Forwarding

- Lokaler Port wird weitergeleitet an einen Rechner und Port, der für den SSH-Server erreichbar ist
- SSH-Aufruf um Aufrufparameter `-L` erweitern:

`ssh -L <lokalerPort>:<Hostname>:<Zielport> <userid>@ssh.inform.hs- hannover.de`
Um den Datenbankserver der Abteilung Informatik zu erreichen, werden folgende Werte für die Parameter eingesetzt:
`lokalerPort` Der lokale Port darf frei gewählt werden und darf noch nicht durch einen andere Anwendung belegt sein. Sofern der Port <1024 ist, müssen Administratorrechte vorliegen. Daher sollte ein Port >=1024 verwendet werden. Es macht Sinn, möglichst den gleichen Wert auszuwählen, der durch den `Zielport` vorgegeben ist, d.h. `1521`
`Hostname` Der Host, zu dem getunnelt werden soll; d.h. in diesem Beispiel `dboracleserv.inform.hs-hannover.de` (oder die IP-Adrsse)
`Zielport` Port, der auf dem Zielhost angesprochen werden soll; vorgegeben durch den Oracle-Datenbakserver als `1521`.