Secure Shell (SSH)

Úvod

- SSH je realizace bezpečného vzdáleného virtuálního terminálu
  - Zajišťuje šifrovanou komunikaci mezi nedůvěryhodnými počítači přes nedostatečně chráněnou síť
    - Předpokládá, že je možné odposlechnout všechnu komunikaci mezi hosty
    - Poskytuje různé metody ověřování
    - Šifruje data vyměňovaná mezi hostitelskými systémy
  - Bylo určeno jako náhrada nedostatečně chráněných programů, jako je rlogin, rsh atd.
  - Zahrnuje i schopnost pro bezpečný přenos souborů
    - Secure copy (scp)
  - Zahrnuje schopnost bezpečně fowardovat spojení X11 i TCP porty
- Je velmi populární a často používaný
  - Není nezranitelný

Ověřování v SSH1

- Prostředky pro ověřování podporované v SSH
  - Jednoduché ověřování pomocí rhosts
    - Uživatelské/systémové jméno v ~/.rhosts a ~/.shosts
    - Snadno zranitelný IP/DNS spoofingem
    - Pro tento režim činnosti vyžaduje zvláštní komplilaci
  - Ověřování založené na ověřování hostitelských systémů
    - Použití RSA k ověření klíče hostitelského systému
    - Používá soubor ~/.rhosts pro ověření uživatele
  - Ověřování založené na uživatelích a hostitelských systémech
    - Ověřování RSA klíče hostitelského systému
    - Ověřování RSA klíče uživatele
- Pokud skončí ověřování chybou, je klient vyzván k zadání hesla
  - Všechna komunikace je šifrována

Protokol pro výměnu klíčů v SSH1

- Server má pár veřejný/tajný klíč
  - Klient zná předem veřejný klíč serveru
    - Musí být poslán předem bezpečným kanálem
- Server pošle klientovi veřejný klíč a náhodný klíč serveru
  - Klient ověří veřejný klíč
- Klient pošle náhodný relační klíč zašifrovaný hostitelským a serverovým klíčem
  - Zbytek relace je šifrován relačním klíčem

Protokol pro výměnu klíčů v SSH2

- Je použit Diffie-Hellman algoritmus pro výměnu klíčů
    - Algoritmus založený na principu přenosu veřejných klíčů
    - Dva uživatelé si mohou vyměnit tajný klíč nedůvěryhodnou linkou bez předchozího sdílení jakéhokoliv tajemství
- Digitální podpis ověřuje identitu serveru vzhledem ke klientovi
- Výsledkem výměny klíčů je sdílený tajný klíč
    - Používá se pro šifrování do konce relace
- Datová integrita je kontrolována pomocí MD5
- Podporuje několik šifrovacích mechanizmů
    - IDEA, Blowfish. DES, Triple DES, …

SSH v praxi

- Veřejný a tajný klíč hosta se generuje při instalaci SSH
    - Veřejný klíč musí být v ~/.ssh/known_hosts na vzdálených systémech
- Ke generování uživatelských veřejných a tajných klíčů je použit příkaz ssh-keygen
    - Vyžaduje aby uživatel vložil heslo
    - Veřejný klíč je kopírován do ~/.ssh-authorized_keys na vzdálených systémech
- ssh-agent a ssh-add eliminují potřebu pro opakované psaní hesla
- ověřování heslem je zranitelné použije-li se útok hádáním hesla
- X11 a forwardování portu vytváří šifrovanou rouru skrz Internet
    - Může být použita pro zajištění zabezpečeného přístupu nezabezpečeným aplikacím jako je SMTP.
    - Může být použito k obejití obranných valů
- Dostupné jako Open Source software (OpenSSH)