Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Počítačové sítě

Vzdálené přihlášení pomocí SSH
Laboratorní úloha

Mgr. Tomáš Hudec

Počítačové sítě – laboratorní úloha – Tomáš Hudec

Vzdálené přihlášení pomocí SSH (laboratorní cvičení)

▼ Obsah

1 Cíle a předpoklady

Tento text je laboratorním cvičením a předpokládá se, že podle uvedeného postupu bude čtenář/student příklady sám provádět. Cílem je:

- porozumění principu přihlášení na server pomocí protokolu SSH a riziku odsouhlasení veřejného klíče serveru,
- procvičení vzdáleného přihlášení při použití autentizace jménem a heslem,
- porozumění autentizaci pomocí klíče a riziku uložení klíče na disk počítače nešifrovaně,
- zvládnutí vygenerování páru klíčů pro autentizaci a umístění veřejného klíče na server,
- zvládnutí přihlašování při použití autentizace klíčem, používání agenta SSH.

Předpokládá se přístup k serveru (obvykle GNU/Linux) s nakonfigurovaným přístupem pomocí SSH.

1.1 Použité konvence

Jména souborů a příkazů jsou vyznačována takto: `soubor`, `příkaz`

```
příkaz  # komentář
```

Obsahuje-li příkaz nebo uživatelský vstup proměnnou (část, kterou je třeba nahradit skutečnými údaji), je použito následujícího vyznačení:

```
příkaz doslovný-argument proměnná argument-s-proměnnou
```

V ukázkových výpisech z terminálu je použito následujícího vyznačování:

```
výzva-shellu$ uživatelský vstup (příkaz, proměnná) stisknuté klávesy nebo komentář pro vstup
výstup příkazu
```

2 Princip přihlášení

Po navázání spojení a sdělení verzí protokolu SSH si obě strany sdělí použitelné šifrovací algoritmy a započne výměna klíčů. Ta se od verze 2 protokolu SSH provádí metodou Diffie-Hellman:

- Obě strany se shodnou na dvou číslech: generátor g a modulus – (velmi velké) prvočíslo n.
- Klient A i server B si každý zvolí tajné číslo (a, b).
- Každá ze stran pošle druhé straně generátor g umocněný svým tajným číslem modulo n; server zprávu navíc podepíše svým soukromým klíčem k_{private} a připojí svůj veřejný klíč k_{public} (pro ověření podpisu):
  - klient serveru (A → B) pošle $A = g^a \pmod n$,
  - server klientu (B → A) pošle $B = g^b \pmod n$, svůj veřejný klíč k_{public} a podpis $s = E(h(B),\ k_{\text{private}})$.
- Klient ověří pravost serveru (tj. zda se za server nevydává někdo jiný) tak, že porovná obdržený veřejný klíč s dříve uloženým veřejným klíčem serveru, a pokud jej nemá (tj. při prvním připojování k serveru), požádá o ověření pravosti obdrženého klíče serveru uživatele tím, že mu zobrazí otisk klíče (tzv. fingerprint, což je hash klíče serveru). **Uživatel ověří pravost zobrazeného otisku klíče porovnáním s otiskem klíče získaným od správce serveru** (např. zveřejněným na zabezpečené webové stránce) a potvrdí shodu klientu SSH, který si veřejný klíč serveru uloží, takže při příštím připojování dojde k ověření bez nutnosti potvrzení uživatelem.
- Po potvrzení pravosti veřejného klíče serveru klient ověří podpis serveru $h(B) \stackrel{?}{=} D(s,\ k_{\text{public}})$, čímž je ověření autenticity serveru dokončeno (hodnota B pochází ze serveru).
- Obě strany vypočítají společný tajný šifrovací klíč $e = B^a \pmod n = A^b \pmod n = g^{ba} \pmod n = g^{ab} \pmod n$, který případný prostředník (odposlouchávající komunikaci) bez znalosti tajných součástí (a, b) v reálném čase získat nemůže, neboť je tento problém příliš složitý. Tajným klíčem e se šifruje veškerá další komunikace.
- Následuje autentizace uživatele: heslem, klíčem, případně jinou nakonfigurovanou metodou.

Pro podrobnější výklad lze doporučit následující videa (anglicky):

- Diffie-Hellman Key Exchange: How to Share a Secret (9:08),
- Secret Key Exchange (Diffie-Hellman) – Computerphile (8:39),
- Key Exchange Problems – Computerphile (9:17).

3 Klient SSH

Ke vzdálenému přihlášení pomocí SSH je třeba klientská aplikace. Všechny moderní OS SSH již podporují; obvykle se jedná o verzi OpenSSH. Stáhnout a nainstalovat si můžete také PuTTY. V distribuci Debian GNU/Linux a odvozených si můžete snadno nainstalovat případný chybějící software (balíček) příslušným příkazem:

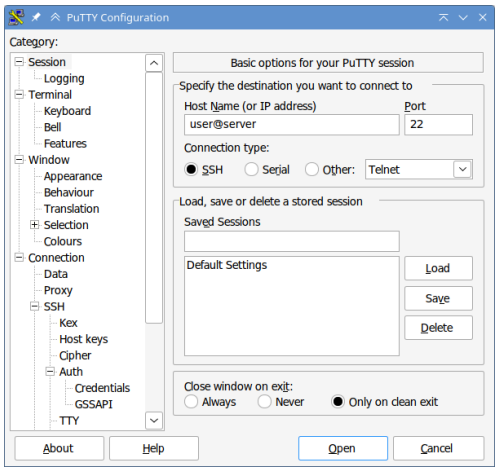
```
sudo apt install openssh-client # klient OpenSSH
sudo apt install openssh-server # server OpenSSH
sudo apt install putty          # klient PuTTY
```

Nepoužívá-li se na systému příkaz `sudo`, je třeba příkaz provést pod uživatelem `root` bez `sudo`. Na uživatele `root` se v tomto případě dá přepnout příkazem `su` a zadáním administrátorova hesla. Pro ostatní distribuce GNU/Linuxu a posixové systémy nepoužívající `apt` konzultujte příslušnou dokumentaci pro instalaci softwaru.

Pro přihlášení uživatele *`user`* na server *`server`* v příkazovém řádku je třeba zadat následující příkaz:

```
ssh user@server
```

Používá-li se PuTTY, je třeba vyplnit políčko Host Name, do kterého je možné připsat i uživatelské jméno, viz obr. 1.



Obr. 1: Konfigurace PuTTY: uživatel a server

Na Fakultě elektrotechniky a informatiky UPCE je pro studenty k dispozici server `fei-os.upceucebny.cz`, na kterém je možné přihlášení zkoušet. Pokud je však počítač, ze kterého se přihlašujete, mimo vnitřní síť UPCE (včetně kolejí a eduroam), je třeba se nejprve přihlásit do VPN (vpn.upce.cz).

Při prvním přihlašování na server se zobrazí výzva pro potvrzení veřejného klíče serveru. V terminále může vypadat takto:

```
The authenticity of host 'fei-os.upceucebny.cz (10.0.86.123)' can't be established.
ED25519 key fingerprint is SHA256:WKbUjrlJj3w5XYvDudlmumo2F/4io72XVsJS4njX4fQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Před odsouhlasením je třeba zkontrolovat, zda zobrazený otisk klíče (fingerprint) patří skutečně serveru. Pro server `fei-os` je otisk klíče zveřejněný společně se stručným návodem na přihlašování v [4]. Potvrzení se provede zadáním celého slova „`yes`“ (prosté „`y`“ nestačí) nebo vložením správného otisku klíče získaného od správce serveru.

Následně je uživatel vyzván k zadání svého hesla, a zadá-li je správně, bude přihlášen.

Celé první přihlášení může v terminále vypadat následovně (zadávané heslo se ani skrytě na terminále vůbec nezobrazuje):

```
user@client:~$ ssh user@fei-os.upceucebny.cz
The authenticity of host 'fei-os.upceucebny.cz (10.0.86.123)' can't be established.
ED25519 key fingerprint is SHA256:WKbUjrlJj3w5XYvDudlmumo2F/4io72XVsJS4njX4fQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'fei-os.upceucebny.cz' (ED25519) to the list of known hosts.
user@fei-os.upceucebny.cz's password: zadání hesla se nezobrazuje
Linux fei-os 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-2 (2023-07-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@fei-os:~$
```

4 Autentizace klíčem

Pro pohodlnější přihlašování bez zadávání hesla je možné využít autentizaci klíčem. Využívá se asymetrické kryptografie: Uživatel si vygeneruje unikátní pár klíčů – soukromý a veřejný. Soukromý klíč nikomu nedá, jeho vlastnictví totiž umožní přihlášení bez znalosti hesla. Veřejný klíč si uživatel umístí na server do příslušného souboru: `.ssh/authorized_keys`

Vygenerovaný klíč musí být skutečně unikátní, aby si případný útočník nemohl vygenerovat stejný pár klíčů. Proto se nepoužívají generátory pseudonáhodných čísel. Skutečně náhodné hodnoty je třeba brát mimo systém (který je deterministický a náhodné hodnoty typicky sám generovat nemůže). Často se pro tyto účely využívá interakce uživatele. Např. PuTTYgen pro Windows vyžaduje od uživatele hýbat myší a ze směrů a časových prodlev generuje náhodné bity. Systém Linux má v jádře vestavěný mechanismus pro získávání náhodných hodnot z prostředí mimo systém. Skutečně náhodné hodnoty lze pak číst ze zařízení `/dev/random`. Je-li v systému dostupný hardwarový generátor náhodných hodnot, Linux jej zpřístupňuje pomocí zařízení `/dev/hwrng`. V Linuxu proto není třeba interakce uživatele při generování klíčů.

Při přihlašování klíčem server použije veřejný klíč uživatele k zašifrování výzvy a očekává, že ji klient úspěšně dešifruje příslušným soukromým klíčem, a dokáže na ni odpovědět. To bez znalosti soukromého klíče není v reálném čase možné (nalezení soukromého klíče může trvat i delší dobu, než je předpokládané stáří vesmíru), takže správnou odpovědí uživatel serveru prokáže svou identitu a server jej přihlásí.

Soukromý klíč je třeba chránit před zneužitím. Pokud si uživatel uloží soukromý klíč v otevřené podobě na počítači nebo flash-disku, který někdo zcizí, může se někdo jiný vydávat se za daného uživatele: přihlásí se na server pomocí zcizeného klíče pod jeho identitou. Proto se soukromý klíč obvykle ukládá na disk šifrovaně. Po vygenerování soukromého klíče zadá uživatel heslovou frázi (passphrase), pomocí které je klíč zašifrován a pak teprve uložen.

Aby uživatel nemusel opakovaně zadávat heslovou frázi při každém přihlašování pomocí klíče, může si na systému spustit tzv. agent SSH. V desktopových systémech GNU/Linux bývá agent obvykle automaticky spuštěn při přihlášení. Ve Windows lze využít program Pageant, který je součástí softwarového balíku PuTTY. Agentu se zadá klíč a příslušná heslová fráze, a ten pak slouží jako prostředník mezi klientem a serverem při autentizaci: klient předá zašifrovaná data agentu, ten je pomocí soukromého klíče uživatele dešifruje a předá zpět klientu. Klient se pak může autentizovat bez interakce s uživatelem (tj. bez zadávání hesla i bez zadávání heslové fráze).

SSH podporuje několik různých asymetrických šifer, které je možné použít pro autentizaci: RSA, DSA, ECDSA a EdDSA. Podle [3] je v současnosti nejvhodnější algoritmus stavějící na problému eliptických křivek EdDSA (Edwards Curve Discrete Logarithm Problem) založený na křivce s označením Ed25519. Z důvodů kompatibility je pak alternativně doporučováno použití algoritmu RSA, který je v protokolu SSH podporován již od počátku.

Pro podrobnější informace o problému eliptických křivek lze doporučit následující videa (anglicky):

- Elliptic Curves – Computerphile (8:41),
- Elliptic Curve Diffie Hellman – Robert Pierce (17:48).

4.2 Generování klíčů pro autentizaci

4.2.1 Generování klíčů pomocí příkazového řádku (OpenSSH)

Po vybrání vhodné asymetrické šifry je možné vygenerovat pár klíčů následujícím příkazem (OpenSSH, Ed25519):

```
ssh-keygen -t ed25519 -C "id-klíče"
```

Případně RSA:

```
ssh-keygen -t rsa -b 4096 -C "id-klíče"
```

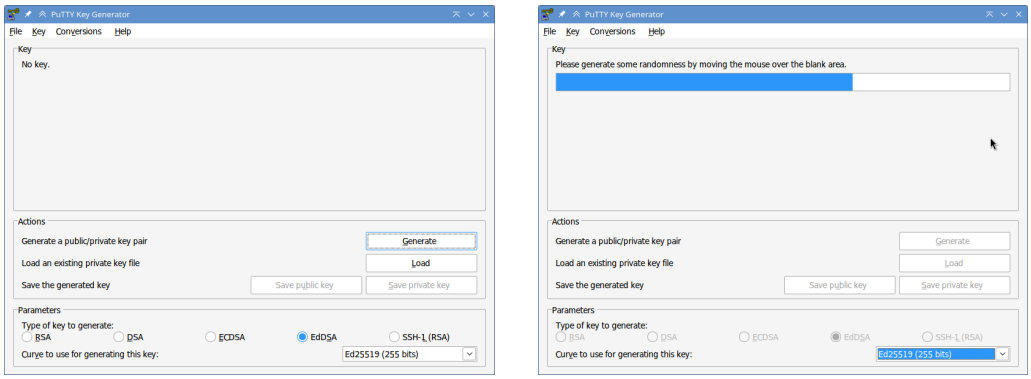
Vynechá-li se přepínač `-C` s identifikátorem, bude klíč uložen s identifikátorem podle přihlášeného uživatele a síťového jména počítače (*user@hostname*). Před uložením je třeba zadat heslovou frázi (passphrase), pomocí které se klíč před uložením zašifruje. Heslová fráze může být prázdná (pak se klíč nešifruje).

Celý výstup může vypadat např. takto (zadávání heslové fráze není na terminále nijak reprezentováno):

```
user@client:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/user/.ssh/id_ed25519): prázdný vstup
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase): zadání heslové fráze se nezobrazuje
Enter same passphrase again: zadání heslové fráze se nezobrazuje
Your identification has been saved in /home/user/.ssh/id_ed25519
Your public key has been saved in /home/user/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:/+nrg6l4euw4URLPo5YpKL+G5SxYU1syJz1T/37Ld+4 user@client
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|      . .        |
|     . = .       |
|    = B = .      |
|   o B OS. .     |
|. = o *  .  .    |
|.O . o o  .+     |
|+ =   .o+ o.oo. o|
| o..  +*o. o*+o=E|
+----[SHA256]-----+
user@client:~$ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDIDT5BQSTXXs6UuLUuRYwHIm/olWkFaSdkvYVk3p3Du user@client
```

4.2.2 Generování klíčů v GUI (PuTTY)

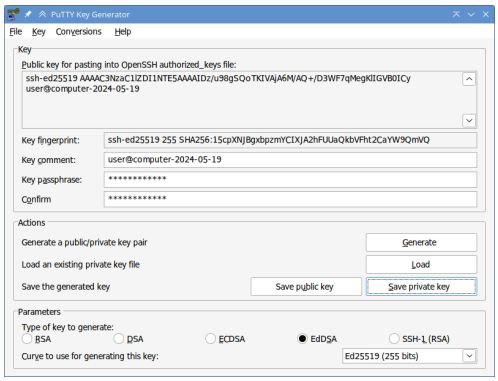
Ve Windows lze použít program PuTTY Key Generator (puttygen.exe). Po zvolení šifry, bitové délky klíče je třeba stisknout tlačítko pro generování (Generate). Během generování je třeba hýbat kurzorem myši, neboť z těchto pohybů získává generátor dostatek náhodných hodnot pro vygenerování unikátního páru klíčů. Viz obr. 2.



Obr. 2: PuTTYgen: Volba algoritmu a generování páru klíčů pro autentizaci

Po vygenerování klíče je vhodné si jej označit komentářem, podle kterého bude klíč snadno identifikovatelný. Vhodné je vložení jména uživatele a počítače, na kterém byl klíč generován, případně také datum.

Soukromý klíč je třeba chránit před zneužitím, takže je důrazně doporučeno vyplnění heslové fráze (passphrase), pomocí které se klíč před uložením na disk zašifruje, čímž se uživatel chrání před zneužitím klíče v případě ztráty/zcizení počítače/disku. Poté je možné klíč uložit stisknutím tlačítka Save private key. Klíč se ukládá do souboru s příponou `ppk` (Putty Private Key). Viz obr. 3.



Obr. 3: PuTTYgen: Uložení soukromého klíče chráněného pomocí heslové fráze

4.3 Nahrání veřejného klíče na server a autentizace klíčem

4.3.3 Nahrání klíče na server pomocí příkazového řádku (OpenSSH)

Veřejný klíč je třeba uložit na server do příslušného souboru. V příkazovém řádku GNU/Linuxu lze využít skript `ssh-copy-id`:

```
ssh-copy-id user@server
```

Skript automaticky vybere uložené veřejné klíče, přihlásí uživatele na server (autentizace heslem) a uloží klíče na server do příslušného souboru (`.ssh/authorized_keys`); pak uživatele odhlásí a vyzve jej k dalšímu přihlášení s autentizací pomocí klíče. Následně je možné se přihlásit bez zadávání hesla pomocí klíče (s případným zadáním heslové fráze pro dešifrování soukromého klíče).

Příklad výstupu:

```
user@client:~$ ssh-copy-id user@fei-os.upceucebny.cz
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install
the new keys
user@fei-os.upceucebny.cz's password: zadání hesla se nezobrazuje
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh 'user@fei-os.upceucebny.cz'"
and check to make sure that only the key(s) you wanted were added.
user@client:~$ ssh user@fei-os.upceucebny.cz
Enter passphrase for key '/home/user/.ssh/id_ed25519': zadání heslové fráze se nezobrazuje
Linux fei-os 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-2 (2023-07-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 20 18:53:15 2024 from 10.0.86.123
user@fei-os:~$
```

Není-li k dispozici skript `ssh-copy-id`, lze nahrát klíč z klienta na server podle následujícího vzoru:

```
cat ~/.ssh/id_ed25519.pub | ssh user@server "mkdir -p .ssh; chmod 700 .ssh; cat >> .ssh/authorized_keys
```

4.3.4 Nahrání klíče na server pomocí GUI (PuTTY)

Veřejný klíč je po vygenerování zobrazen v horní části okna aplikace PuTTYgen (viz obr. 3). Stačí jej označit, zkopírovat do schránky a po přihlášení na server vložit do příslušného souboru. To lze provést následujícím postupem:

- Pomocí myši označíme zobrazený veřejný klíč v okně aplikace PuTTYgen a vložíme jej do schránky (viz obr. 3).
- Pomocí PuTTY se přihlásíme na server (viz obr. 1). Otevře se terminálové okno, ve kterém se autentizujeme heslem.
- po úspěšném přihlášení vytvoříme na serveru adresář `.ssh`, nastavíme mu oprávnění pouze pro vlastníka a vložíme veřejný klíč do souboru `authorized_keys` – v příkazovém řádku na serveru zadáme následující příkazy:

  ```
  mkdir -p ~/.ssh; chmod 700 ~/.ssh; cat >> ~/.ssh/authorized_keys
  ```

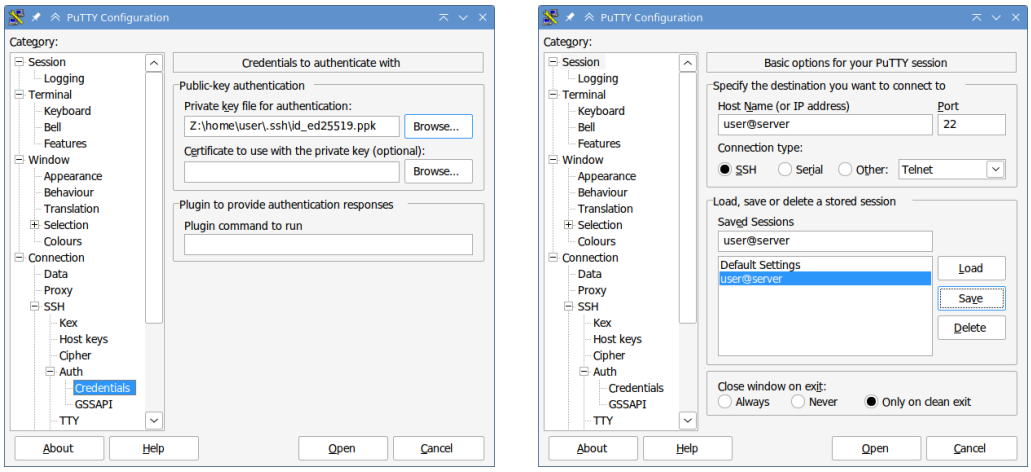
  Nyní je očekáván na vstupu veřejný klíč, vložíme jej tedy ze schránky, přidáme konec řádku (stisknutím klávesy `Enter`) a vstup ukončíme stisknutím `CTRL` + `D`.
- Že je klíč v souboru v pořádku uložen, můžeme zkontrolovat příkazem:

  ```
  cat ~/.ssh/authorized_keys
  ```

  Není-li obsah souboru v pořádku (na každém jeho řádku je jeden klíč), můžeme soubor odstranit (příkazem `rm`) a přidání klíče zopakovat nebo lze soubor upravit editorem (např. `nano`). Obsah terminálu může vypadat následovně:

  ```
  user@fei-os:~$ mkdir -p ~/.ssh; chmod 700 ~/.ssh; cat >> ~/.ssh/authorized_keys
  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDIDT5BQSTXXs6UuLUuRYwHIm/olWkFaSdkvYVk3p3Du user@client Enter,
  CTRL+D
  user@fei-os:~$ cat ~/.ssh/authorized_keys
  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDIDT5BQSTXXs6UuLUuRYwHIm/olWkFaSdkvYVk3p3Du user@client
  user@fei-os:~$ exit
  ```

- Upravíme konfiguraci PuTTY tak, aby se používala autentizace klíčem: Nejprve vyplníme přihlašovací údaje na server (viz obr. 1). Pak v levé části okna vybereme položku Connection → SSH → Auth → Credentials a v pravé části okna vyplníme cestu k souboru s privátním klíčem (Private key file for authentication), viz obr. 4. K tomu lze využít tlačítko Browse a soubor s klíčem vybrat pomocí dialogového okna.
- Abychom nemuseli soukromý klíč pokaždé vyplňovat, uložíme si konfiguraci PuTTY: Vlevo vybereme položku Session a vpravo vyplníme název uložené relace do pole Saved Sessions. Stisknutím tlačítka Save potvrdíme uložení relace, která se nyní bude zobrazovat v seznamu relací (viz obr. 4).



Obr. 4: Konfigurace PuTTY: privátní klíč pro autentizaci a uložení relace (session)

4.4 Využití agenta SSH

Pokud si chce uživatel zjednodušit opakované přihlašování na server tak, aby nemusel pokaždé zadávat heslo nebo heslovou frázi, může využít pro autentizaci zašifrovaným klíčem agenta SSH. Agentem se načte soukromý klíč, zadá se heslová fráze a klientský program SSH bude provádět autentizaci klíčem přes agenta, bez interakce s uživatelem.

4.4.5 Využití agenta SSH v GNU/Linuxu

V desktopovém prostředí GNU/Linuxu agent obvykle již automaticky běží. Pokud ne, konzultujte dokumentaci příslušného GUI anebo distribuce. V terminálu lze agent spustit příkazem `eval $(ssh-agent)`. Kontaktovatelný klientem SSH pak bude pouze z daného terminálu (pokud se v jiném terminálu nenastaví příslušné proměnné prostředí).

Agentu lze přidat klíč příkazem `ssh-add`:

```
user@client:~$ ssh-add
Enter passphrase for /home/user/.ssh/id_ed25519: zadání heslové fráze se nezobrazuje
Identity added: /home/user/.ssh/id_ed25519 (user@client)
```

Klient SSH automaticky agenta při autentizaci zašifrovaným soukromým klíčem kontaktuje a agent autentizaci zprostředkuje.

4.4.6 Využití agenta SSH ve Windows

Ve Windows lze při použití klienta PuTTY využít agent PuTTY nazývaný pageant. Po jeho spuštění se v systémové části hlavního panelu zobrazí ikonka agenta. Kliknutím na ni lze přes menu nebo otevřené okno agenta přidat soukromý klíč (Add key). Po zadání heslové fráze může agent zprostředkovávat autentizaci.

5 Shrnutí

5.5 OpenSSH

Postup konfigurace přihlášení pomocí autentizace klíčem pro OpenSSH (příkazový řádek):

1. `ssh-keygen -t ed25519   # vygeneruje pár klíčů EdDSA, zadá se heslová fráze`
2. `ssh-copy-id user@server # uloží veřejný klíč na server`
3. `ssh-add                 # předá klíč agentu SSH (zadává se heslová fráze)`
4. `ssh user@server         # přihlášení bez zadávání hesla i bez zadávání heslové fráze`

5.6 PuTTY

Postup konfigurace přihlášení pomocí autentizace klíčem pro PuTTY (Windows GUI):

1. Vygenerovat pár klíčů:
   a) spustit PuTTYgen,
   b) vybrat šifru (EdDSA nebo RSA + 4 096 bitů),
   c) kliknout na Generate (viz obr. 2 první),
   d) hýbat myší (viz obr. 2 druhý),
   e) zvolit identifikátor klíče a zapsat jej do komentáře,
   f) vložit heslovou frázi,
   g) uložit soukromý klíč do souboru typu PPK (viz obr. 3).
2. Uložit veřejný klíč na server:
   a) označit veřejný klíč v okně aplikace PuTTYgen a vložit jej do schránky,
   b) spustit PuTTY, zadat jméno serveru a přihlásit se na server,
   c) vytvořit na serveru adresář `.ssh`, nastavit mu oprávnění a vložit veřejný klíč do souboru `authorized_keys`:

      ```
      mkdir -p ~/.ssh; chmod 700 ~/.ssh; cat >> ~/.ssh/authorized_keys
      ```

      vložit ze schránky veřejný klíč, stisknout `Enter` a `Ctrl` + `D`,
   d) odhlásit se ze serveru,
   e) nastavit PuTTY pro používání autentizace klíčem: vyplnit cestu ke klíči v Connection → SSH → Auth → Credentials a uložit konfiguraci (viz obr. 4 první).
3. Spustit agenta Pageant a předat mu klíč:
   a) kliknout na ikonku agenta v systémové části hlavního panelu,
   b) vybrat přidání klíče (Add key),
   c) vybrat klíč PPK na souborovém systému,
   d) zadat heslovou frázi pro klíč.
4. Přihlásit se na server při použití autentizace klíčem: spustit PuTTY, dvojklikem vybrat uloženou relaci nebo jedním kliknutím vybrat a kliknout na Open (viz obr. 4 druhý). V terminálovém okně PuTTY uvidíme hlášku o autentizaci klíčem pomocí agenta a úspěšné přihlášení.

Použité zdroje a další literatura

[1] *OpenSSH Manual Pages* [online]. 2024 [cit. 2024-05-20]. URL: https://www.openssh.com/manual.html

[2] Tatham, Simon: *PuTTY User Manual* [online]. 2024-04-15 [cit. 2024-05-20]. URL: https://www.openssh.com/manual.html

[3] Kontsevoy, Ev: *Comparing SSH Keys – RSA, DSA, ECDSA, or EdDSA?* [online]. Gravitational, 2022-04-07 [cit. 2024-05-20]. URL: https://goteleport.com/blog/comparing-ssh-keys/

[4] Hudec, Tomáš: *SSH – postup pro vzdálené přihlášení pomocí klíče* [online]. Univerzita Pardubice, FEI, 2023-10-05 [cit. 2024-05-20]. URL: https://moodle.upce.cz/moodle/tohu0051/courses/OS/ssh-keys.txt

[5] Veronica: *OpenSSH for Absolute Beginners* [online]. YouTube, Veronica Explains, 2022-02-07 [cit. 2024-05-20]. 22:59. URL: https://www.youtube.com/watch?v=3FKsdbjzBcc

[6] Yu, Brian: *Diffie-Hellman Key Exchange: How to Share a Secret* [online]. YouTube, Spanning Tree, 2024-05-27 [cit. 2024-05-27]. 9:08. URL: https://www.youtube.com/watch?v=85oMrKd8afY

[7] Computerphile: *Secret Key Exchange (Diffie-Hellman) – Computerphile* [online]. YouTube, Computerphile, 2017-12-15 [cit. 2024-05-27]. 8:39. URL: https://www.youtube.com/watch?v=NmM9HA2MQGI

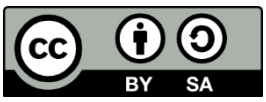
[8] Computerphile: *Key Exchange Problems – Computerphile* [online]. YouTube, Computerphile, 2017-12-29 [cit. 2024-05-27]. 9:17. URL: https://www.youtube.com/watch?v=vsXMMT2CqqE

[9] Computerphile: *Elliptic Curves – Computerphile* [online]. YouTube, Computerphile, 2018-01-16 [cit. 2024-05-27]. 8:41. URL: https://www.youtube.com/watch?v=NF1pwjL9-DE

[10] Pierce, Robert: *Elliptic Curves – Computerphile* [online]. YouTube, Robert Pierce, 2014-12-10 [cit. 2024-05-27]. 17:48. URL: https://www.youtube.com/watch?v=F3zzNa42-tQ

UNIVERZITA PARDUBICE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Vytvořeno v rámci projektu **Digitalizace studijních Agend, Nové TechnologiE, systémy a přístupy k výuce na UPCE**, reg. č. NPO_UPCE_MSMT-16591/2022.



Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY