Podstawowy warsztat informatyka

PWI

Instytut Informatyki Uniwersytetu Wrocławskiego

Wykład 3

częściowo na podstawie slajdów Jakuba Michaliszyna

Co jeszcze warto wiedzieć

- Używanie $*$ i ? w poleceniach.
- Pliki ukryte (nazwa od kropki).
- Znaki ``.

Co jeszcze warto wiedzieć

- Używanie $*$ i ? w poleceniach.
- Pliki ukryte (nazwa od kropki).
- Znaki ``.

```
ls .*
```

Co jeszcze warto wiedzieć

- Używanie $*$ i ? w poleceniach.
- Pliki ukryte (nazwa od kropki).
- Znaki ``.

```
ls .*
```

```
ls .[^.]*
```

Przed nami:

- Konta użytkowników.
- Łączenie zdalne.
- Tworzenie i zabijanie procesów.

Użytkownicy

- Kim ja jestem? `id`

Użytkownicy

- Kim ja jestem? `id`
- Kim są wszyscy? `cat /etc/passwd`.

Użytkownicy

- Kim ja jestem? `id`
- Kim są wszyscy? `cat /etc/passwd`.
- nazwa użytkownika : hasło : id : id głównej grupy : opis : katalog domowy : program uruchamiany przy logowaniu.

Użytkownicy

- Kim ja jestem? `id`
- Kim są wszyscy? `cat /etc/passwd`.
- nazwa użytkownika : hasło : id : id głównej grupy : opis : katalog domowy : program uruchamiany przy logowaniu.
- hasła są w `/etc/shadow`.

Użytkownicy

- Kim ja jestem? `id`
- Kim są wszyscy? `cat /etc/passwd`.
- nazwa użytkownika : hasło : id : id głównej grupy : opis : katalog domowy : program uruchamiany przy logowaniu.
- hasła są w `/etc/shadow`.
- Zwykli użytkownicy i super użytkownicy.

Użytkownicy

- Kim ja jestem? `id`
- Kim są wszyscy? `cat /etc/passwd`.
- nazwa użytkownika : hasło : id : id głównej grupy : opis : katalog domowy : program uruchamiany przy logowaniu.
- hasła są w `/etc/shadow`.
- Zwykli użytkownicy i super użytkownicy.
- `su, sudo`.

ssh

ssh umożliwia szyfrowane łączenie się z innymi komputerami

ssh

```
$ ssh scheduler.ii.uni.wroc.pl
The authenticity of host 'scheduler.ii.uni.wroc.pl' can't be established.
ECDSA key fingerprint is ce:96:82:44:25:7c:47:21:a8:0a:76:55:49:4b:d3:1a.
Are you sure you want to continue connecting (yes/no)? yes
```

ssh

```
$ ssh scheduler.ii.uni.wroc.pl
The authenticity of host 'scheduler.ii.uni.wroc.pl' can't be established.
ECDSA key fingerprint is ce:96:82:44:25:7c:47:21:a8:0a:76:55:49:4b:d3:1a.
Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'scheduler.ii.uni.wroc.pl' (ECDSA) to
the list of known hosts.
piotrek@scheduler.ii.uni.wroc.pl's password:
```

ssh

```
$ ssh scheduler.ii.uni.wroc.pl
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now
(man-in-the-middle attack)! It is also possible
that the RSA host key has just been changed. The fingerprint
for the RSA key sent by the remote host is ab:cd:ef:gh
Please contact your system administrator. Add correct host
key in /home/user/.ssh/known_hosts to get rid of this message

Offending key in /home/user/.ssh/known_hosts:1
RSA host key for user.server has changed and you have
requested strict checking. Host key verification failed.
```

Hasła

Top 25 most common passwords by year according to SplashData

Rank	2011[6]	2012[7]	2013[8]	2014[9]	2015[10]	2016[5]	2017[11]	2018[12]	2019[13]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou	123123
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess	abc123

Szyfrowanie asymetryczne

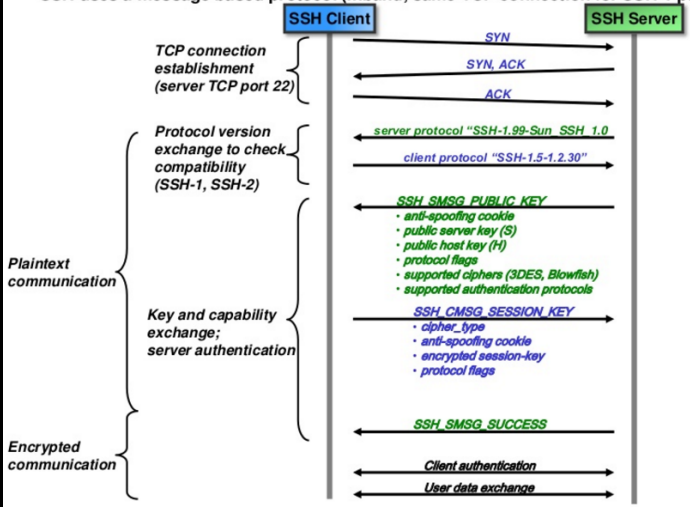
Są bezpieczniejsze sposoby logowania niż poprzez podawanie hasła.
https://security.stackexchange.com/questions/3887/is-using-a-public-key-for-logging-in-to-ssh-any-better-than-saving-a-passwor

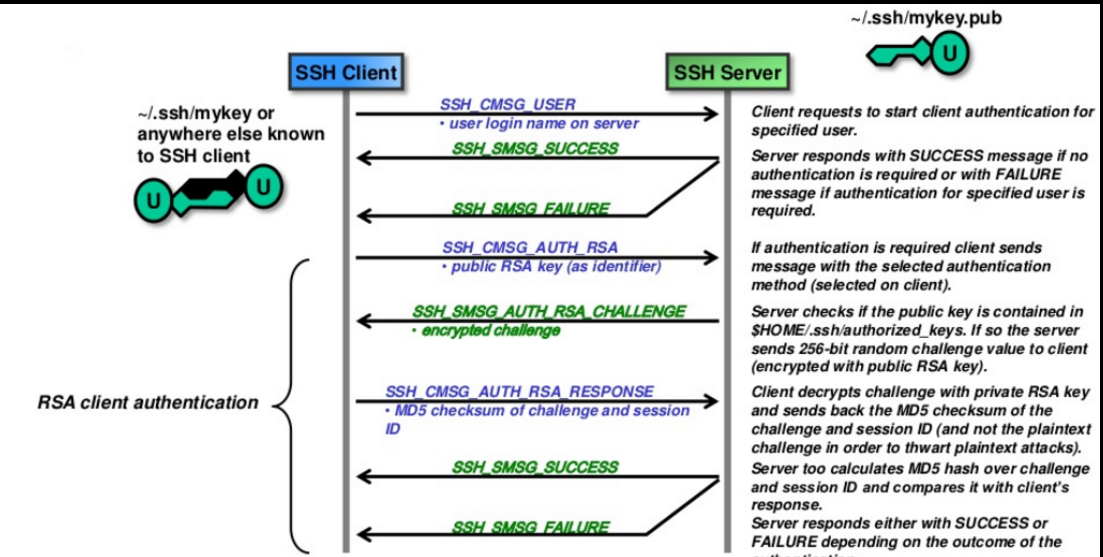
Klucze prywatne i publiczne

Użytkownik generuje dwa klucze - prywatny i publiczny.
Wiadomość zakodowaną kluczem publicznym można odkodować tylko prywatnym.
Nie da się (szybko) wyliczyć klucza prywatnego na podstawie publicznego.

3. SSH-1 protocol

SSH uses a message based protocol (inband, same TCP connection for SSH-1 protocol and for user data).





Klucze prywatne i publiczne

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/me/.ssh/id_rsa):
Created directory '/home/me/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/me/.ssh/id_rsa.
Your public key has been saved in /home/me/.ssh/id_rsa.pub.
The key fingerprint is:
a9:49:2e:2a:5e:33:3e:a9:de:4e:77:11:58:b6:90:26 me@host
The key's randomart image is:
+--[ RSA 2048]----+
|      ..o        |
|     (...)       |
|o=++.            |
+-----------------+
```

Wgrywanie klucza

Klucz prywatny jest naszą tajemnicą!
Klucz publiczny wgrywamy na serwer:

```
ssh-copy-id www.example.com
```

i już!

Inne ważne funkcje

Tunelowanie
Komunikacja z programami graficznymi (-X)
screen przez ssh
Hasła do kluczy i ssh-agent

scp

scp używa ssh do kopiowania plików

```
scp plan.txt jmi@ii.uni.wroc.pl:.
```

Po dwukropku jest ścieżka na zdalnym serwerze.
Można również kopiować w drugą stronę.

```
scp jmi@ii.uni.wroc.pl:fotki/* zdjecia
```

Prawa dostępu

- `ls -al`

```
drwxr-xr-x+ 1 jmi None      0 Oct  2 12:24 .
drwxrwxrwt+ 1 jmi None      0 Jan 23  2014 ..
-rw-------  1 jmi None  11531 Oct  7 17:05 .bash_history
-rwxr-xr-x  1 jmi None   1494 Jan 23  2014 .bash_profile
```

Prawa dostępu

- `ls -al`

```
drwxr-xr-x+ 1 jmi None      0 Oct  2 12:24 .
drwxrwxrwt+ 1 jmi None      0 Jan 23  2014 ..
-rw-------  1 jmi None  11531 Oct  7 17:05 .bash_history
-rwxr-xr-x  1 jmi None   1494 Jan 23  2014 .bash_profile
```

- d | rwx | rwx | rwx
  czy katalog? | prawa właściciela | prawa grupy | prawa pozostałych

Prawa dostępu

- `ls -al`

```
drwxr-xr-x+ 1 jmi None      0 Oct  2 12:24 .
drwxrwxrwt+ 1 jmi None      0 Jan 23  2014 ..
-rw-------  1 jmi None  11531 Oct  7 17:05 .bash_history
-rwxr-xr-x  1 jmi None   1494 Jan 23  2014 .bash_profile
```

- d | rwx | rwx | rwx
  czy katalog? | prawa właściciela | prawa grupy | prawa pozostałych
- chmod; r=4, w=2, x=1.

Prawa dostępu

- `ls -al`

```
drwxr-xr-x+ 1 jmi None      0 Oct  2 12:24 .
drwxrwxrwt+ 1 jmi None      0 Jan 23  2014 ..
-rw-------  1 jmi None  11531 Oct  7 17:05 .bash_history
-rwxr-xr-x  1 jmi None   1494 Jan 23  2014 .bash_profile
```

- d | rwx | rwx | rwx
  czy katalog? | prawa właściciela | prawa grupy | prawa pozostałych
- chmod; r=4, w=2, x=1.
- chmod +x aby uczynić plik wykonywalnym, ./program aby uruchomić program.

Interpreter poleceń

- Przekierowania: `cat /proc/cpuinfo > dane`
  `wc -l < dane`
  `rm > log`
  `wc 2> dane`
  Deskryptor 0 (stdin) - domyślnie klawiatura, 1 (stdout) - ekran, 2 (stderr) - ekran.

Interpreter poleceń

- Przekierowania: `cat /proc/cpuinfo > dane`
  `wc -l < dane`
  `rm > log`
  `wc 2> dane`
  Deskryptor 0 (stdin) - domyślnie klawiatura, 1 (stdout) - ekran, 2 (stderr) - ekran.
- Potoki: `cat /proc/cpuinfo | tee dane | wc -l .`

Interpreter poleceń

- Przekierowania: `cat /proc/cpuinfo > dane`
  `wc -l < dane`
  `rm > log`
  `wc 2> dane`
  Deskryptor 0 (stdin) - domyślnie klawiatura, 1 (stdout) - ekran, 2 (stderr) - ekran.
- Potoki: `cat /proc/cpuinfo | tee dane | wc -l` .
- Równoczesne wykonanie! (cf. `cat | grep b`).

PATH

- Zmienne:
  Y=ls
  Y
  $Y

PATH

- Zmienne:
  Y=ls
  Y
  $Y
- Zmienna PATH.

PATH

- Zmienne:
  Y=ls
  Y
  $Y
- Zmienna PATH.
- export PATH=$PATH: /opt/bin

PATH

- Zmienne:
  Y=ls
  Y
  $Y
- Zmienna PATH.
- export PATH=$PATH: /opt/bin
- printenv

PATH

- Zmienne:
  Y=ls
  Y
  $Y
- Zmienna PATH.
- export PATH=$PATH: /opt/bin
- printenv
- whereis