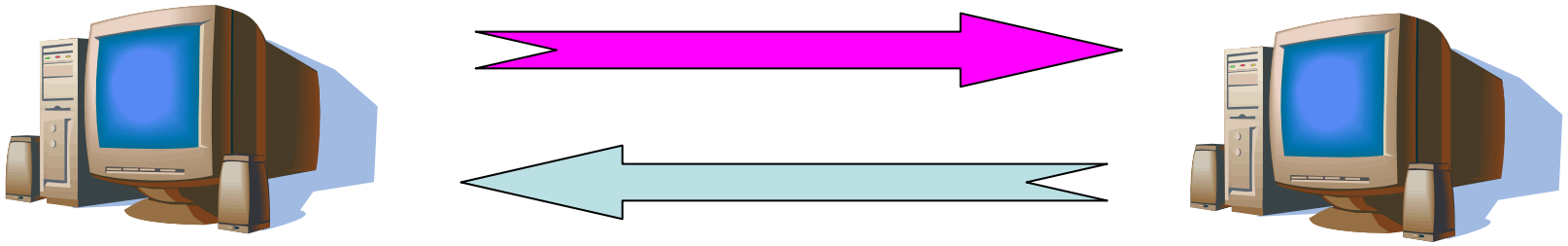
PV157 – Autentizace a řízení přístupu

Autentizace počítačů



Autentizace počítačů

- Na základě adresy počítače
  - MAC
  - IP
- Na základě tajné informace
  - Symetrická kryptografie
  - Asymetrická kryptografie

Autentizace podle adresy

- Autentizace na základě (síťové) adresy
  - MAC adresa ethernetové síťové karty
    - Přepínače (switch)
    - Svázání portu přepínače pouze s určitou MAC adresou
    - Svázání IP adresy pouze s určitou MAC adresou
  - IP adresa počítače
    - Řízení přístupu k síťovým službám (přístup k webovým stránkám na základě IP adresy)
    - Paketové filtry (součást firewallů) pracují na základě IP adresy a čísla portu odesilatele a příjemce (zdroj a cíl)

Autentizace podle adresy

- Úroveň bezpečnosti autentizace podle adresy
  - MAC adresy nejsou tajné (viz např. protokol/příkaz ARP)
  - MAC adresu ethernetové karty lze jednoduše změnit
  - IP adresu lze změnit
  - Je možné nesprávně uvést zdrojovou adresu (odesilatele) – IP spoofing
  - ! ! ! Automatické reakce na útoky (datagramy) s nesprávnou zdrojovou adresou (např. firewall odřeže přístup z určité domény)

Soubor .rhosts

- Soubor .rhosts
  - Nastavuje unixový uživatel se svém domovském adresáři (např. /home/zriha/.rhosts)
  - Globální důvěra: soubor /etc/hosts.equiv
  - Povoluje kdo může jeho účet používat (protokoly rlogin, rsh, rexec, …)
  - Nahrazuje autentizaci heslem (např. protokolem telnet)
  - Formát řádků: stroj [login]
    např. queen.math.muni.cz
    aisa.fi.muni.cz
    krusty.math.muni.cz riha
  - Uvedeným strojům důvěřujeme (že správně uvedou uživatelské jméno)
  - Možné útoky: počítač neuvede správně login uživatele, DNS, routing nebo IP spoofing

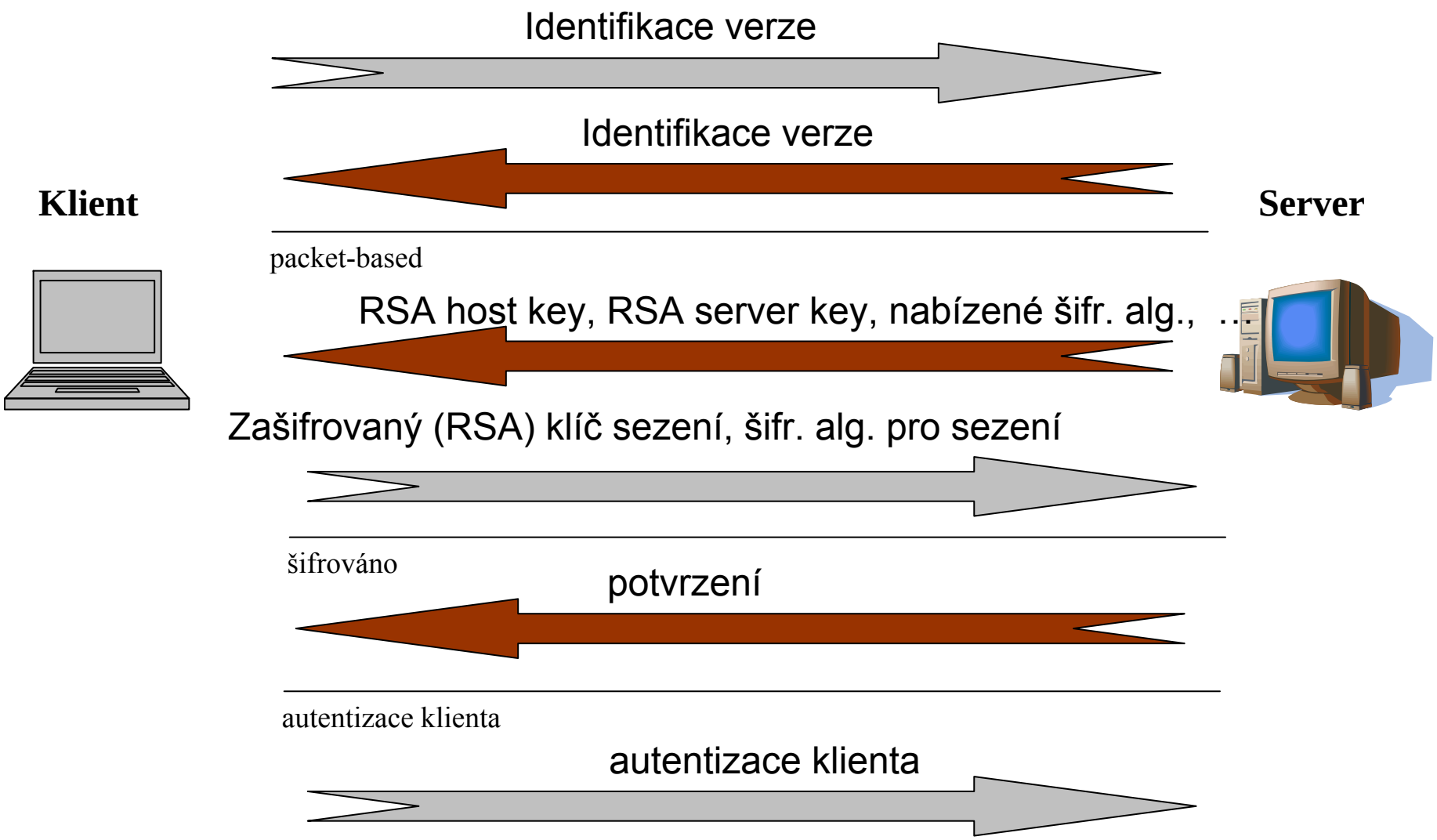
Autentizace na základě tajné informace

- Tajné informace
  - Hesla
  - Tajné symetrické klíče
  - Soukromé asymetrické klíče
- Jak tyto tajné informace ukládat?
  - Nešifrovaně v čisté podobě – počítač k nim má jednoduchý přístup, ale jsou přístupné i všem uživatelům s dostatečnými právy (hackeři)
  - Šifrovaně/chráněné heslem – při startu počítače (programu) je nutné manuálně zadat heslo/šifrovací klíč, slabé heslo znamená slabou ochranu, po celou dobu použití jsou tajné informace v paměti

Protokol ssh

- Protokol „secure shell“ (ssh)
- Slouží k přihlášení klienta (uživatele) k serveru
- Autentizace serveru i klienta
- Server
  - RSA host key (dlouhodobý)
  - RSA server key (generovaný každou hodinu)
- Metody autentizace klienta
  - .rhosts nebo /etc/hosts.equiv
  - .rhosts nebo /etc/hosts.equiv s RSA autentizací klienta (počítače)
  - RSA autentizace klienta (uživatele)
  - Heslo uživatele

Protokol ssh



Protokol ssh

- Šifrovací algoritmy pro šifrování sezení (klient vybírá z možností nabízených serverem)
  - 3DES (povinná podpora), ve verzi 1 i DES
  - AES - doporučené
  - Twofish - doporučené
  - Blowfish - doporučené
  - IDEA
  - Serpent
  - Arcfour
  - CAST128
- Šifrovací/podepisovací algoritmy pro autentizaci klienta/serveru
  - Od verze 2 je kromě RSA podporován i algoritmus DSA
- Obrana vůči útokům
  - Odposlech hesla a pozdější přehrání
  - DNS spoofing
  - IP spoofing
  - Routing spoofing

Protokol ssh: debug režim (ssh -v)

```
debug1: Connecting to aisa.fi.muni.cz [147.251.48.1] port 22.
debug1: Connection established.
debug1: identity file /home3/zriha/.ssh/identity type -1
debug1: Remote protocol version 1.99, remote software version OpenSSH_3.4p1
debug1: Local version string SSH-1.5-OpenSSH_3.1p1
debug1: Waiting for server public key.
debug1: Received server public key (768 bits) and host key (1024 bits).
debug1: Host 'aisa.fi.muni.cz' is known and matches the RSA1 host key.
debug1: Found key in /home3/zriha/.ssh/known_hosts:5
debug1: Encryption type: 3des
debug1: Sent encrypted session key.
debug1: Received encrypted confirmation.
debug1: Doing password authentication.
zriha@aisa.fi.muni.cz's password:
debug1: Requesting pty.
debug1: fd 3 setting TCP_NODELAY
debug1: Requesting shell.
debug1: Entering interactive session.
```

Asymetrické klíče pro autentizaci uživatele

- Soukromé klíče uživatele
  - ~/.ssh/identity
  - ~/.ssh/id_dsa
- Veřejné klíče uživatele
  - ~/.ssh/identity.pub
  - ~/.ssh/id_dsa.pub
- Vytvoření klíče: příkaz ssh-keygen

```
bash-2.05$ ssh-keygen -f /tmp/test -t rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /tmp/test.
Your public key has been saved in /tmp/test.pub.
The key fingerprint is:
82:dd:71:7a:c4:ac:1c:de:b0:d3:d6:5b:63:7d:7c:76 zriha@queen.math.muni.cz
```

Protokol ssh

- Ověření integrity veřejného klíče serveru
- Soubory
  - /etc/ssh/known_hosts
  - /etc/ssh/known_hosts2
  - ~/.ssh/known_hosts
  - ~/.ssh/known_hosts2
  - Formát: počítač délka_klíče klíč
  - Např.: aisa 1024 37
    92648095391895266660461031814637345286469741285
    19463898291113200170437591638902829526627999663
    57470373079794594589737234564882145189758891946
    37391967788396230335631144998324780320375923657
    36181174418615708849459044374454744143100510826
    95360610857954348154578413482365924024485042273
    51129807154870221237653119

Protokol ssh

- První připojení k serveru

```
The authenticity of host 'ws24 (147.251.82.224)' can't be established.
RSA key fingerprint is 8e:08:9a:70:67:d6:7a:83:37:19:81:f9:a4:de:46:29.
Are you sure you want to continue connecting (yes/no)?
```

- Klíč serveru změněn

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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
8e:08:9a:70:67:d6:7a:83:37:19:81:f9:a4:de:46:29.
Please contact your system administrator.
Add correct host key in /home_zam/zriha/.ssh/known_hosts to get rid of this
message.
Offending key in /home_zam/zriha/.ssh/known_hosts:165
RSA host key for ws24 has changed and you have requested strict checking.
Host key verification failed.
```

Protokol ssh

- Autentizace pomocí RSA/DSA klíče
  - Soubor
    - ~/.ssh/authorized_keys
    - ~/.ssh/authorized_keys2
  - Soubor obsahuje veřejné klíče uživatele(ů)
  - Obdoba .rhosts, ale pro silnou autentizaci
- Autentizační agent
  - ssh-agent
  - Zadám passphrase jen jednou
  - Agent uloží klíč do paměti
  - Následné autentizační požadavky řeší agent

Autentizace…

- Autentizace zpráv, protokoly
  - Postaveny na kryptografii
  - Redukce problémů na ochranu kryptografických klíčů
- Autentizace uživatelů
  - Hesla a PINy jsou obdobné (velmi slabé „klíče“)
  - Další možnosti
    - tokeny – často analogické využití pro autentizaci strojů i uživatelů
    - biometriky – jen pro autentizaci uživatelů
  - viz následující blok přednášek

Otázky?

Příští přednáška: 30. 3. 2010 v 10:00

matyas@fi.muni.cz & zriha@fi.muni.cz

Polosemestrální písemka (I)

- 20. 4. 2010
  - Dvě skupiny od 10:00 a 11:00 – rozpis v ISu
  - Body jsou kladné i záporné
  - Záporné bodování je vyšší a nižší
    - Podle toho jak špatně je dané odpověď
  - Volné otázky u polosemestrální písemky nebudou
  - Celkem asi 30 bodů, což je 30 % celkového počtu bodů pro hodnocení zkoušky
  - Kdo bude nemocný nebo jinak omluven v ISu bude mít přepočítané body z finální písemky
    - Tj. náhradní termín polosemestrálky není

Polosemestrální písemka (II)

- Organizační pokyny
  - Přijďte včas (čas nás tlačí)
  - S sebou jen ISIC a pero (případně náhradní pero)
  - Čekejte u spodního vchodu do D3, seřaďte se přibližně podle abecedy
  - Odchod bude probíhat horním vchodem

Příklad otázky

Jak zajistíme integritu veřejného klíče

:c1 Pomocí párového privátního klíče

:c2 Pomocí klíčované hašovací funkce

:c3 Pomocí certifikátu veřejného klíče

:c4 Částečným utajením veřejného klíče

:c5 Utajením soukromé části veřejného klíče

:c1 -3

:c2 -2

:c3 ok 4

:c4 -3

:c4 -4