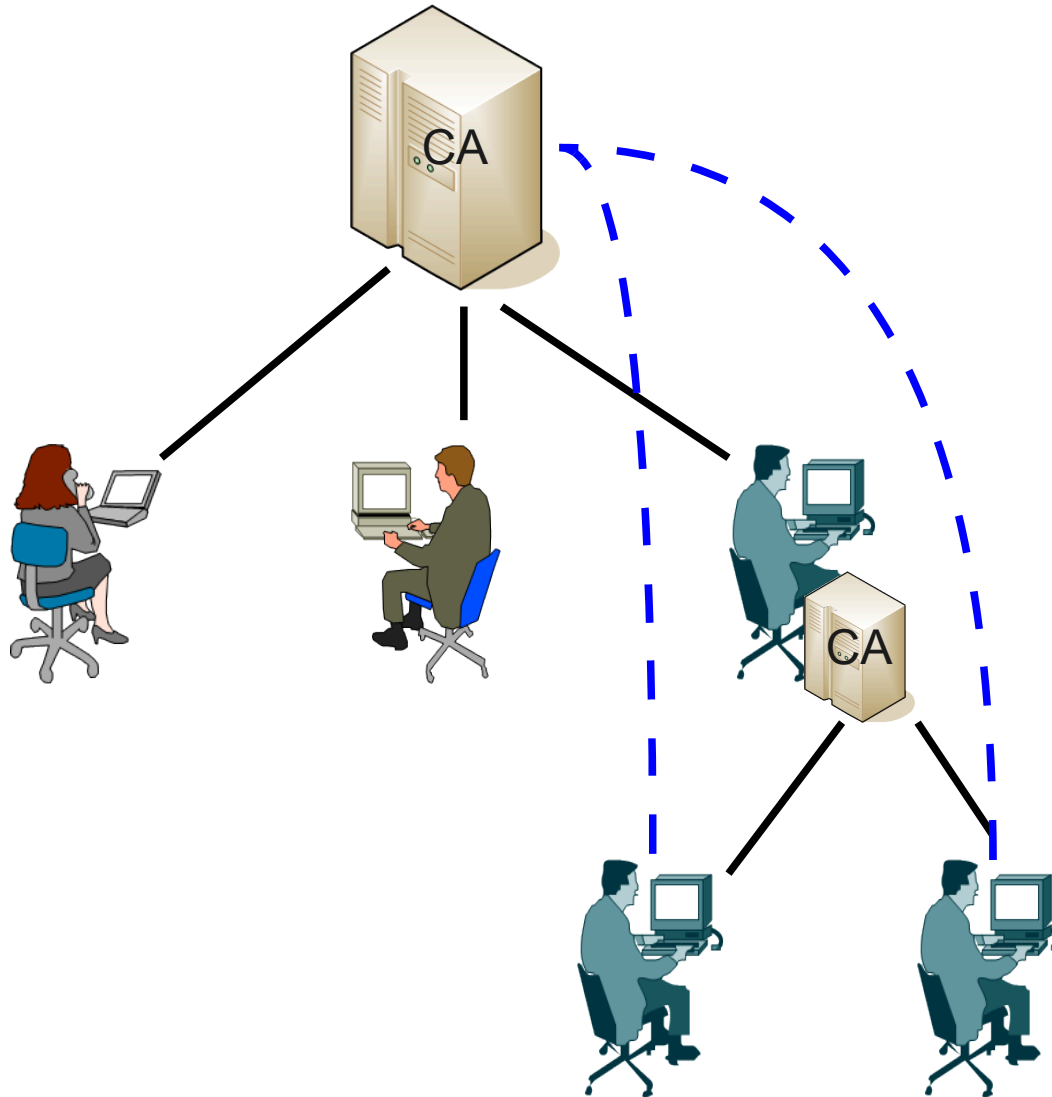


# Certifikáty použití

# Osnova

- problémy s použitím certifikátů
  - falešná CA
  - autentizace x podpis
  - MITM
- certifikáty a email
- ssl
- ssh
- ...

# falešná CA



# autentizace

Kubr



student



soukromý  
klíč

náhodné číslo  
0110010111010

přihlášení

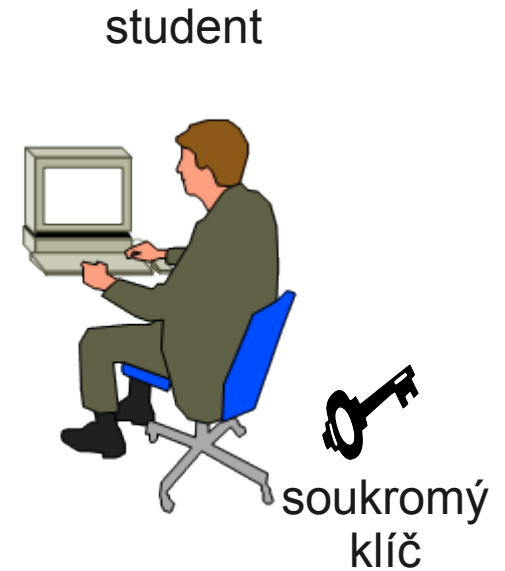
výzva

digitální podpis (výzva)

autentizováno

podepsaná výzva

# podpis



náhodné číslo  
0110010111010

F je jenom moje vina.

Blbost osobně potvrzena

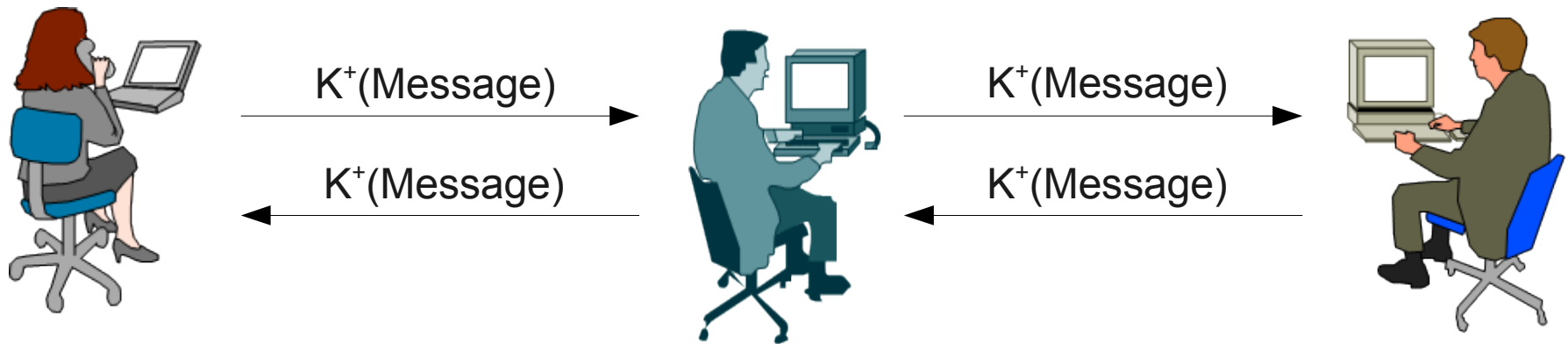
přihlášení

výzva

podepsaná výzva

digitální podpis (výzva)

# man-in-the-middle



# pošta

- technologie
  - pgp
  - s/mime
- podpis
- šifrování
- problémy
- speciality

# podpis

Return-Path: <kubr@fel.cvut.cz>  
Date: Tue, 09 Mar 2010 12:27:08 +0100  
From: Honza Kubr <kubr@fel.cvut.cz>  
User-Agent: Thunderbird 2.0.0.23 (X11/20090817)  
MIME-Version: 1.0  
To: "Ing. Jan Kubr" <kubr@fel.cvut.cz>  
Subject: pokus smime  
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="-----  
ms000107050108090704080201"

hlavička (RFC822)

This is a cryptographically signed message in MIME format.

text zprávy

-----ms000107050108090704080201  
Content-Type: text/plain; charset=ISO-8859-2; format=flowed  
Content-Transfer-Encoding: 7bit

Smime text.

-----ms000107050108090704080201  
Content-Type: application/x-pkcs7-signature; name="smime.p7s"  
Content-Transfer-Encoding: base64  
Content-Disposition: attachment; filename="smime.p7s"  
Content-Description: S/MIME Cryptographic Signature

elektronický podpis  
a certifikáty

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAoIIRIzCC  
...  
c7x7erzBtg0EYDAL/E82K+NC0q1i31K6s3rmgEWoPMgkmVzajJrlQEzupu7ioQBQCH7P6O42  
KgAAAAAAAAA==  
-----ms000107050108090704080201--



# šifrování

- identifikace veřejného certifikátu 1-n
- n x symetrický klíč, zašifrovaný veřejnými klíči
- zpráva zašifrovaná symetrickým klíčem
  
- složka sent
  - přidaný klíč šifrovaný mým veřejným klíčem

# šifrování

hlavička (RFC822)

Return-Path: <kubr@fel.cvut.cz>  
Message-ID: <4B964BCB.7020201@fel.cvut.cz>  
Date: Tue, 09 Mar 2010 14:23:23 +0100  
From: Honza Kubr <kubr@fel.cvut.cz>  
User-Agent: Thunderbird 2.0.0.23 (X11/20090817)  
MIME-Version: 1.0  
To: "Ing. Jan Kubr" <kubr@fel.cvut.cz>  
Subject: sifrovani  
Content-Type: application/x-pkcs7-mime; name="smime.p7m"  
Content-Transfer-Encoding: base64  
Content-Disposition: attachment; filename="smime.p7m"  
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHgMIIB3AIBADCBwzCBrlELMAkGA1UEBhMCMVVMxCzAJBgNVBAgTAIVUMRcwFQYDVQQHEw5TYWx0IExha2UgQ2I0eTEeMBwGA1UEChMVVGhlIFVTRVJUUIVTVCB0ZXR3b3JrMSEwHwYDVQQLEExodHRwOi8vd3d3LnVzZXJ0cnVzdC5jb20xNjA0BgNVBAMTLVVUTi1VU0VSRmlyc3QtQ2xpZW50IEF1dGhIbnRpY2F0aW9uIGFuZCBFbWVpbAIQJWo0a+UPg6uzy1VQMdPrvzANBgkqhkiG9w0BAQEFAASCAQA+eTdlf64faFA6KMUWbG/ba2YkTbNcPLQrtCa8ctktFgWo2XYpbnv2zhyCgknyXBz5GldCtkpvCUqJh7mq294O1viHLIQKQtWTM+eOBA5MRxHUj9mrsWfq3WfhHnnJR9FJA26QJ0KUonAPpuyTwaFDpdiNijsZXmBcau/htkewZopPpLRpbX3aG8YpEP2FtqMFK0WnipYp7pBEEBX3t/m5Ue3NvQTcVTpJpO1VOEYPFGa0AndKaaOEHTDtH45zB+sxYqdVpUkQ4Q9O/Qj/nNrfuA3UtGI7HxPeT77ajw+4MOBOXyxb289qscLXsexw dplsVHif+0MTTax23qpHhVeMMIAGCSqGSIb3DQEHATAUBggqhkiG9w0DBwQlpYcck7RFCfSg gARwJ6XyQdyAfQPURwq9Gfdb0HC3YNcbYZo6TmCwhDh1za7P31G44lgeZXmRwf4paNtHzWq5 ELdkCnp+PrEL8ixlkrzOKVSehrujWu/mB/IVwMnJ9ZY6LGzSfRx6RErnt2udYXE1HVrEWRRey xyvIKcxSmgQIUbc95vN1YAAAAAAAAAAAAAAAAA

šifrovaná zpráva

# problémy

- nedoručení podepsaného emailu a nahrazení nepodepsaným emailem
- Michal Medvecký <[kubr@fel.cvut.cz](mailto:kubr@fel.cvut.cz)>
- nedůvěryhodná CA
  - přijmutí odlišného certifikátu
  - akceptování kořenového certifikátu (z řetězu)

# Enhanced Security Services for S/MIME

- podepsaná doručenka
  - pozor - lze zatajit převzetí
- bezpečnostní návěští
  - označení stupně utajení
- bezpečné konference
  - podpis
    - není problém
  - šifrování
    - zašifrováno pro všechny odběratele

# SSL a TLS

- mezi aplikací a TCP
- autentizace serveru na základě cert. serveru
- autentizace klienta na základě cert. klienta (opt.)
- kontrolní součet fragmentů
- nevidí do aplikačních dat
- nepodepisuje zprávy a transakce

# Protokoly SSL a TLS

- Record Layer Protocol (RLP)
  - šifruje a podepisuje fragmenty
- Handshake Protocol (HP)
  - příprava protokolové suity
    - protokol šifrování a kontrolního součtu, komprimační alg.
    - data pro výpočet hlavního tajemství
- Change Cipher Specification Protocol (CCSP)
  - pravená suita → aktuální suita
- Alert Protocol (AP)
  - signalizace závad

# nová relace

ClientHello(HP)

ServerHello(HP)

Certificate(HP)

CertificateRequest(HP)

ServerHelloDone(HP)

Certificate(HP)

ClientKeyExchange(HP)

CertificateVerify(HP)

*Change Cipher Spec.*

Finished(HP)

*Change Cipher Spec.*

Finished(HP)

Data

Data

# obnovení relace

- ClientHello(HP)
  - *Change Cipher Spec.*
  - Finished(HP)
  - Data
- ServerHello(HP)
  - *Change Cipher Spec.*
  - Finished(HP)
  - Data



# sdílené klíče

- client\_random (ClientHello)
- server\_random (ServerHello)
- PreMasterSecret (ClientKeyExchangeMessage)
  - pro RSA náhodné číslo zašifrované  $K^+$  serveru
- vznikne blok sdílených tajemství
  - výpočet kontrolního součtu klient → server
  - výpočet kontrolního součtu server → klient
  - symetrický šifrovací klíč klient → server
  - symetrický šifrovací klíč server → klient
  - inicializační vektory

# HTTPS

- konfigurace
  - anonymní server
  - autentizace klientů
- problém s certifikáty
- virtuální servery
  - s jedním klíčem
  - s více klíči

# apache (httpd.conf)

```
LoadModule ssl_module modules/mod_ssl.so
```

```
Listen 443
```

```
<VirtualHost _default_:443>
```

```
...
```

```
    SSLEngine on
```

```
    SSLCertificateFile /etc/apache2/ssl/server.cer
```

```
    SSLCertificateKeyFile /etc/apache2/ssl/server.key
```

```
...
```

```
</VirtualHost>
```

# apache - autentizace klienta

```
<VirtualHost _default_:443>
```

```
...
```

```
SSLVerifyClient require
```

```
SSLVerifyDepth 10
```

```
SSLCACertificateFile /etc/apache2/ssl/ca.cer
```

```
...
```

```
</VirtualHost>
```

# odkazy

- <http://www.root.cz/clanky/ssl-autentizacia-s-webovym-serverom-apache/>
  - nastavení apache
- <http://wiki.cacert.org/VhostTaskForce>
  - virtuální servery