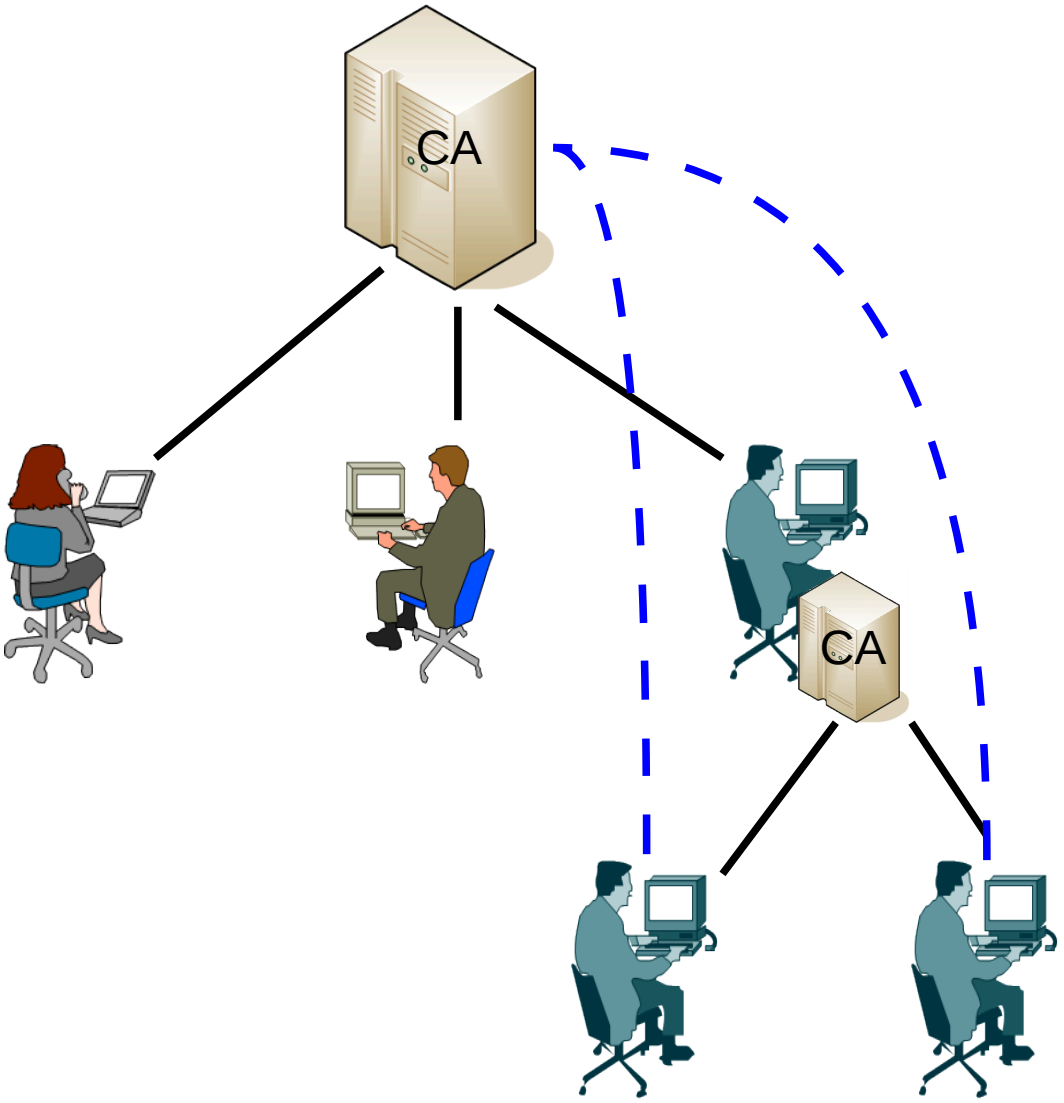
Certifikáty
Použití

Osnova

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

falešná CA



autentizace

Kubr

student

soukromý klíč

přihlášení

náhodné číslo
0110010111010

výzva

digitální podpis (výzva)

podepsaná výzva

autentizováno

podpis

student

soukromý klíč

přihlášení

náhodné číslo
0110010111010

výzva

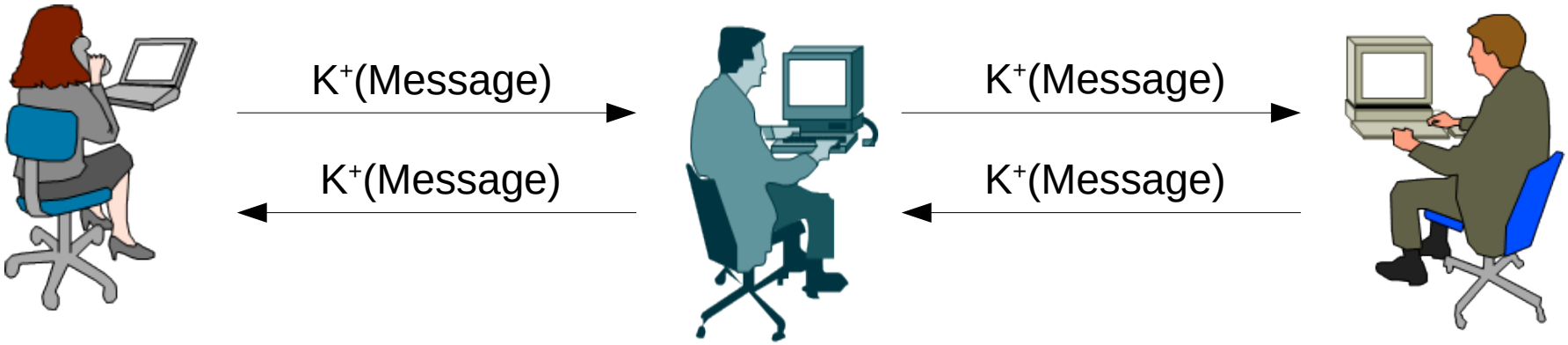
digitální podpis (výzva)

F je jenom moje vina.

podepsaná výzva

Blbost osobně potvrzena

man-in-the-middle



pošta

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

podpis

hlavička (RFC822)

```
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"
```

text zprávy

```
This is a cryptographically signed message in MIME format.

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

Smime text.
```

elektronický podpis a certifikáty

```
--------------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

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIRIzCC
...
c7x7erzBtg0EYDAL/E82K+NC0q1i31K6s3rmgEWoPMgkmVzajJrlQEzupu7ioQBQCH7P6O42
KgAAAAAAAA==
--------------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
```

šifrovaná zpráva

```
MIAGCSqGSIb3DQEHA6CAMIACAQAxggHgMIIB3AIBADCBwzCBrjELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAlVUMRcwFQYDVQQHEw5TYWx0IExha2UgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJU
UlVTVCBOZXR3b3JrMSEwHwYDVQQLExhodHRwOi8vd3d3LnVzZXJ0cnVzdC5jb20xNjA0BgNV
BAMTLVVUTi1VU0VSRmlyc3QtQ2xpZW50IEF1dGhlbnRpY2F0aW9uIGFuZCBFbWFpbAIQJWo0
a+UPg6uzy1VQMdPrvzANBgkqhkiG9w0BAQEFAASCAQA+eTdIf64faFA6KMUWbG/ba2YkTbNc
PLQrtCa8ctktFgWo2XYpbnv2zhyCgknyXBz5GldCtkpvCUqJh7mq294O1viHLlQKQtWTM+eO
BA5MRxHUj9mrsWfq3WfhHnnJR9FJA26QJ0KUonAPpuyTwaFDpdiNijsZXmBcau/htkewZopP
pLRpbX3aG8YpEP2FtqMFK0WnipYp7pBEEBX3t/m5Ue3NvQTcVTpJpO1VOEYPFGa0AndKaaOE
HTDtH45zB+sxYqdVpUkQ4Q9O/Qj/nNrfuA3UtGl7HxPeT77ajw+4MOBOXyxb289qscLXsexw
dplsVHif+0MTTax23qpHhVeMMIAGCSqGSIb3DQEHATAUBggqhkiG9w0DBwQIpYcck7RFCfSg
gARwJ6XyQdyAfQPURwq9Gfdb0HC3YNCbYZo6TmCwhDh1zA7P31G44lgeZXmRwf4paNtHzWq5
ELdkCnp+PrEL8ixlkrzOKVSehrujWu/mB/IVwMnJ9ZY6LGzSfRx6RErnt2udYXE1HVrEWRey
xyvIKcxSmgQIUbCbc95vN1YAAAAAAAAAAAAA
```

problémy

- nedoručení podepsaného emailu a nahrazení nepodepsaným emailem
- Michal Medvecky <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
- Hanshake 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)

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

- *Change Cipher Spec.*
- Finished(HP)

- Data

- 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