

# **Bezpečnost a mezidoménová důvěra**

Jan Růžička  
email,sip:janru@cesnet.cz  
Seminář IP Telefonie  
3. 11. 2006

# Skype

## Uživatel

- jednoduchost instalace a konfigurace,
- jednoduchost užívání,
- schopnost fungovat odkudkoliv,
- dobrou hlasovou kvalitou.

## Správce

- Skype obchází Firewall i Proxy,
- nechěná zátěž pro stroje (SN)
- provoz generovaný Skypem se těžko detekuje a je to potenciální „backdoor“

Uzavřený protokol-systém v otevřeném světě,  
otázka důvěryhodnosti

# Zabezpečení přenosu

- transportu – jako celku
  - “Walled gardens”
  - Isec, VPN
- medií
  - SRTP MiKEY, PKI nebo předem sdílené tajemství
  - ZRTP DH výměna klíčů během sestavování hovoru přes RTP – Short Authentication Strings (omezení možnosti MiTM)

# SIP Autentizace, integrita, utajení

- WWW Digest
- TLS (SIPS) - E2E zabezpečení signalizace je problematické, transitivity důvěra, klientský certifikát zřídka k vidění
- S/MIME
- vkládání ověřené identity
  - Zabezpečený "První hop" - TLS
  - Tokeny, SAML
  - Podepsané některé hlavičky
- Využít Eduroam auth nelze – Digest vs EAP

# SIP Autentizace

SIP/2.0 401 Unauthorized.

Via: SIP/2.0/UDP 195.178.64.172:49252;branch=z9hG4bK.6afb7404;rport=49253.

From: sip:user@cesnet.cz;tag=6c2c90b8.

To: sip:user@cesnet.cz;tag=c10ed4fff3e6fb17efd0bfbdcce87ce2.c76e.

Call-ID: 1814859960@195.178.64.172.

CSeq: 1 REGISTER.

**WWW-Authenticate: Digest realm="cesnet.cz",  
nonce="43eeaeb76e6eec559d737d4f4018dc659c5d282a".**

Server: Sip EXpress router (0.9.5-pre1 (i386/linux)).

Content-Length: 0.

REGISTER sip:cesnet.cz SIP/2.0.

**Authorization: Digest username="user", uri="sip:cesnet.cz", algorithm=MD5,  
realm="cesnet.cz", nonce="43eeaeb76e6eec559d737d4f4018dc659c5d282a",  
response="9e83c39e8a7262901**

Via: SIP/2.0/UDP 195.178.64.172:49252;branch=z9hG4bK.32f02bf2;rport.

From: sip:user@cesnet.cz;tag=6c2c90b8.

To: sip:user@cesnet.cz.

Call-ID: 1814859960@195.178.64.172.

CSeq: 2 REGISTER.

Content-Length: 0.

Max-Forwards: 70.

Expires: 15.

Contact: sip:user@a.b.c.d:1234.

# SIP Autentizace II

INVITE sip:mamut@iptel.org SIP/2.0.

Max-Forwards: 10.

Record-Route: <sip:195.113.222.3;ftag=5DAA94E7;lr=on>.

Via: SIP/2.0/UDP 195.113.222.3;branch=z9hG4bK0a5d.90580ee2.0.

Via: SIP/2.0/UDP 195.113.134.233:5062;branch=z9hG4bK2E1FD348.

CSeq: 262 INVITE.

To: <sip:mamut@iptel.org>.

**Proxy-Authorization: Digest username="bbb", realm="ces.net",  
nonce="43788e90381194d66364fced4dc7097828391e81",  
uri="sip:mamut@iptel.org", cnonce="abcdefghi", nc=00000001,  
response="ed4adec8"**

Content-Type: application/sdp.

From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.

Call-ID: 379332994@195.113.134.233.

Subject: sip:bbb@ces.net.

Content-Length: 234.

User-Agent: kphone/4.2.

Contact: "Franta Vomacka" <sip:bbb@195.113.134.233:5062;transport=udp>.

Remote-Party-ID: "Franta Vomacka" <sip:950070101@ces.net>;party=calling;id-type=subscriber;privacy=off; screen=yes.

.

v=0.

o=username 0 0 IN IP4 195.113.134.233.

s=The Funky Flow.

c=IN IP4 195.113.134.233.

t=0 0.

m=audio 33728 RTP/AVP 0 97.

a=rtpmap:0 PCMU/8000.

a=rtpmap:97 iLBC/8000.

# S/MIME

```
INVITE sip:bob@biloxi.com SIP/2.0
  Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
  To: Bob <sip:bob@biloxi.com>
  From: Alice <sip:alice@atlanta.com>;tag=1928301774
  Call-ID: a84b4c76e66710
  CSeq: 314159 INVITE
  Max-Forwards: 70
  Contact: <sip:alice@pc33.atlanta.com>
  Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
    name=smime.p7m
  Content-Disposition: attachment; filename=smime.p7m
    handling=required
```

```
Content-Type: application/sdp
```

```
v=0
o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com
s=-
t=0 0
c=IN IP4 pc33.atlanta.com ←
m=audio 3456 RTP/AVP 0 1 3 99
a=rtpmap:0 PCMU/8000
```

Zde může být  
i privátní IP  
adresa

# S/MIME II

```
INVITE sip:bob@biloxi.com SIP/2.0
  Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
  To: Bob <sip:bob@biloxi.com>
  From: Alice <sip:alice@atlanta.com>;tag=1928301774
  Call-ID: a84b4c76e66710
  CSeq: 314159 INVITE
  Max-Forwards: 70
  Date: Thu, 21 Feb 2002 13:02:03 GMT
  Contact: <sip:alice@pc33.atlanta.com>
  Content-Type: multipart/signed;
    protocol="application/pkcs7-signature";
    micalg=sha1; boundary=boundary42
  Content-Length: 568
```

--boundary42

# S/MIME II -pokr.

Content-Type: message/sip

INVITE sip:bob@biloxi.com SIP/2.0

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK nashds8

To: Bob <bob@biloxi.com>

From: Alice <alice@atlanta.com>;tag=1928301774

Call-ID: a84b4c76e66710

CSeq: 314159 INVITE

Max-Forwards: 70

Date: Thu, 21 Feb 2002 13:02:03 GMT

Contact: <sip:alice@pc33.atlanta.com>

Content-Type: application/sdp

Content-Length: 147

v=0

o=UserA 2890844526 2890844526 IN IP4 here.com

s=Session SDP

c=IN IP4 pc33.atlanta.com

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s;  
handling=required

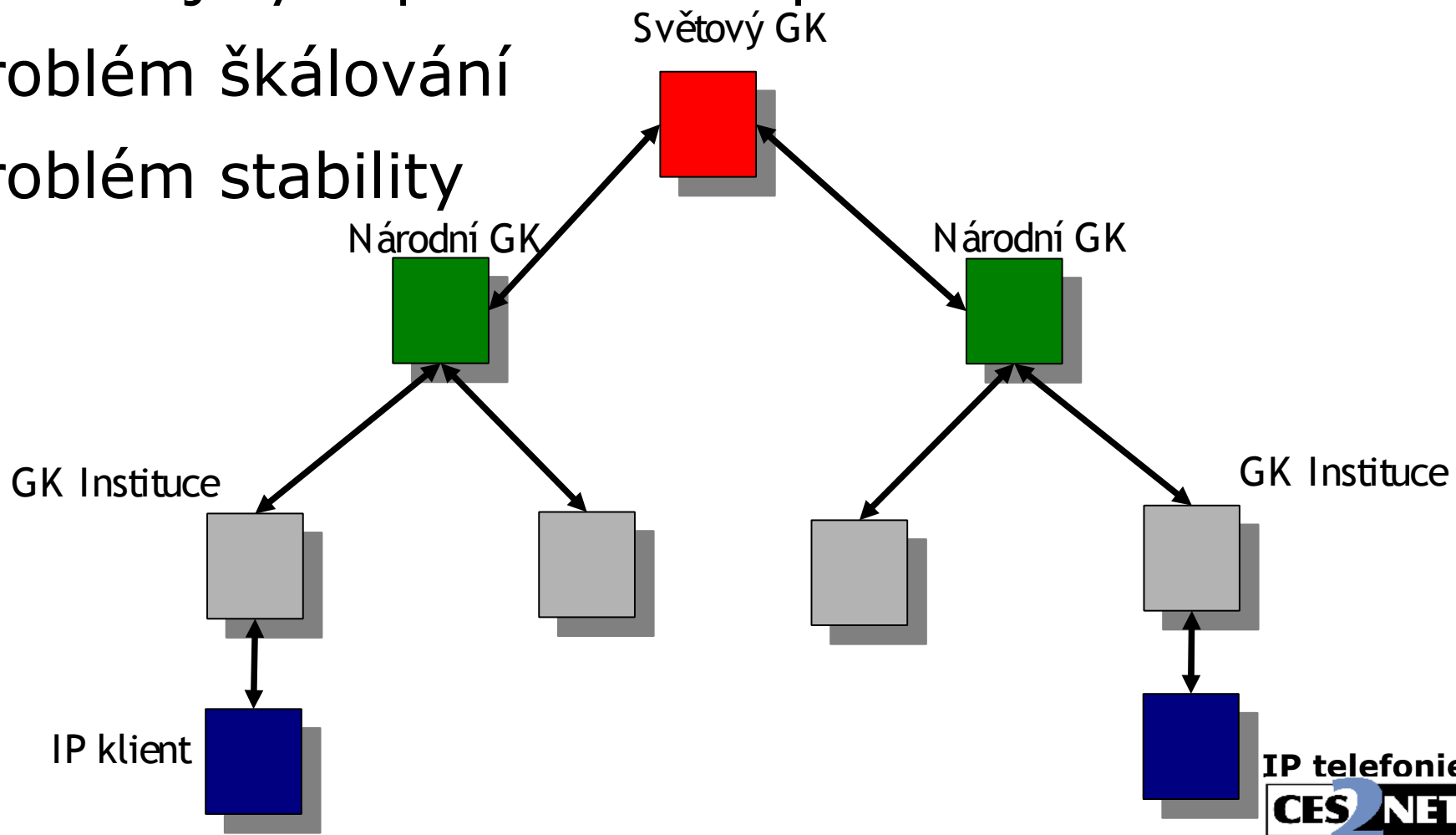
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6  
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj  
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4  
7GhIGfHfYT64VQbnj756

--boundary42-

# Mezidoménová důvěra

- Hierarchie

- Signalizačních prvků (s TLS nebo Ipsec)
- Pomocí jiných protokolů např. OSP
- Problém škálování
- Problém stability



# Mezidoménová důvěra II - SIP

- Vkládání ověřené identity
  - Zabezpečený "První hop" - TLS ,...
  - Odebrání klasických autentizačních hlaviček domácí domény
  - Vložení doménou ověřené identity (SAML, tokeny, podepsání některých hlaviček)
  - Cílová doména ověří integritu a autorizuje na základě politik (federace,...)

# Vkládání ověřené identity

```
INVITE sip:bob@biloxi.example.org SIP/2.0
  Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
  To: Bob <sip:bob@biloxi.example.org>
  From: Alice <sip:alice@atlanta.example.com>;tag=1928301774
  Call-ID: a84b4c76e66710
  CSeq: 314159 INVITE
  Max-Forwards: 70
  Date: Thu, 21 Feb 2002 13:02:03 GMT
  Contact: <sip:alice@pc33.atlanta.example.com>
  Content-Type: application/sdp
  Content-Length: 147
```

```
v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
c=IN IP4 pc33.atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

# Vkládání ověřené identity

- Zajímavé hlavičky

```
sip:alice@atlanta.example.com|sip:bob@biloxi.example.org|  
a84b4c76e66710|314159 INVITE|Thu, 21 Feb 2002 13:02:03 GMT|  
alice@pc33.atlanta.example.com|v=0  
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com  
s=Session SDP  
c=IN IP4 pc33.atlanta.example.com  
t=0 0  
m=audio 49172 RTP/AVP 0  
a=rtpmap:0 PCMU/8000
```

- Vložená identita

```
Identity:"kjOP4YVZXmF0X3/4RUfAG6ffwbVQepNGRBz58b3dJq3prEV4h5Gn  
S4F6udDRCI4/rSK9cl+TFv45nu0Qu2d/0WPP0vvc3JWwuUmHrCwG  
wC+tW7fOWnC07QKgQn40uwg57WaXixQev5N0JfoLXnO3UDoum  
89JRhXPAIp2vffJbD4="
```

```
Identity-Info: <https://atlanta.example.com/atlanta.cer> ;alg=rsa-sha1
```

# Útoky

- Odposlech a modifikace zpráv
  - Odposlech medií
  - Převzetí či ukončení registrace
  - Pozměnění či ukončení hovoru
- Převzetí serveru
  - Redirekce
  - Zahazování
- Realtime komunikace
  - Odložení do fronty neexistuje
  - Obrana vs. omezení dostupnosti

# Útoky II

- DoS, DDoS
  - Útoky na podpůrné systémy – DNS, OS, ...
  - Jednoduchost provedení
  - Rychlé vyčerpání některých prostředků a/nebo velmi rušivé
  - Složitá obrana – autentizace, limity
- SPIT
  - Vyšší náročnost na prostředky spammera
  - Složitá obrana – autentizace

Děkuji za pozornost