



Bezpečnost v IP telefonii

Seminář IP telefonie a videokonferencí 19.11.2008

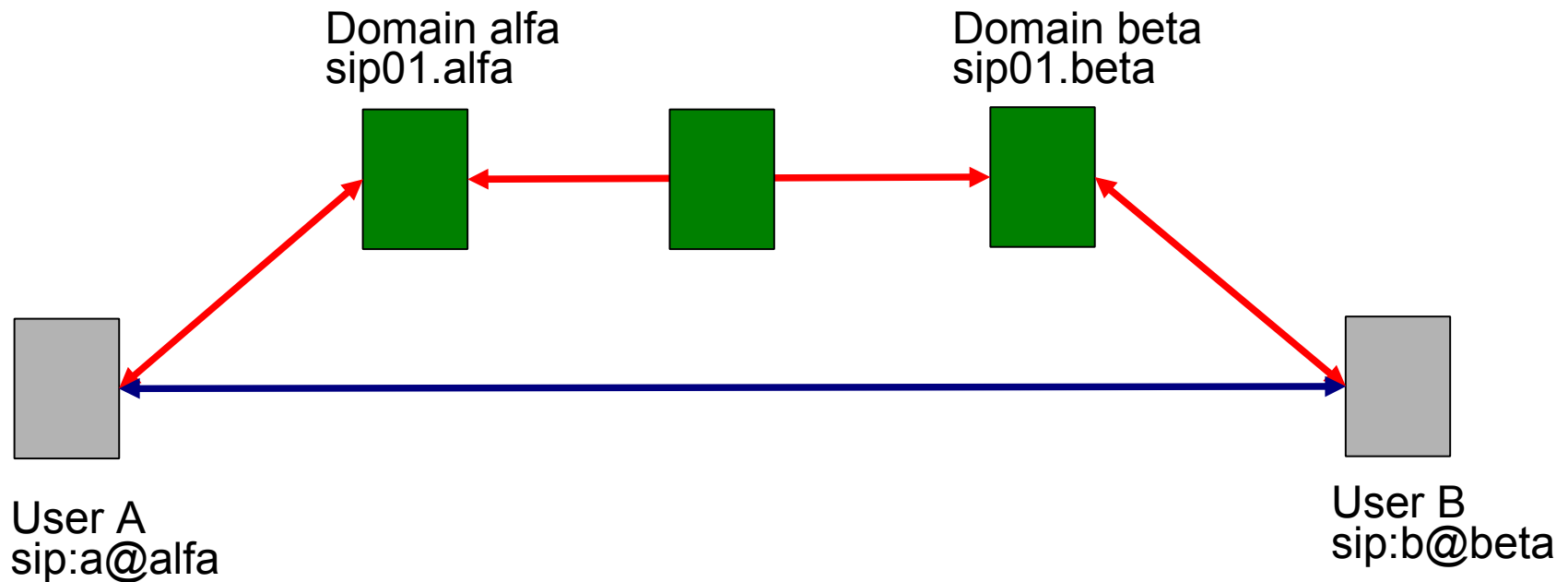
Jan Růžička

jan.ruzicka@cesnet.cz



IP telefonie

- **Simulujeme telefonní síť pomocí mnohem složitějšího souboru zařízení vyvinutého ke komplexnímu přenosu dat.**
 - Přináší nové služby
 - Konvergence prostředků, sítí,.....
 - Jsou nutná čísla?
- **SIP - momentálně nejpoužívanější otevřený protokol**
 - způsobil masivní rozvoj IP telefonie
 - Stav v ČR – Vše budováno s ohledem na minimální náklady i u zákazníka – to může nést technologická omezení
 - Očekává se technologický posun s nárůstem počtu uživatelů
 - Podpora u velkých operátorů (IMS?)
 - Poplatky – paušál?

SIP „trapezoid“



- Enterprise vs. P2P
- Autentizace heslem a jiné metody vs. polohou
- Identita člověka vs. stroje
- Domácí část
- Meziúmenová část, i více než jeden krok

 DATA
 SIP

Útoky na infrastrukturu

- **Útoky na prvky infrastruktury**
 - sip servery, brány
- **Útoky na podpůrné systémy**
 - DNS
- **Jednoduchost provedení**
 - SIP už sice dávno není jednoduchý, ale stále je dost jednoduchý
- **Rychlé vyčerpání některých prostředků**
 - Například ISDN linky do ústředny
- **Ostrovky vs. mezidomenová komunikace**
 - Email také nefunguje jen uvnitř firmy

DNS

- **Velmi používaný a citlivý prvek systému**
- **Přeložit číslo na URI**
 - ENUM
- **Přeložit část URI na bod obsluhy služby (server a port)**
 - “servisní” NAPTR

```
IN NAPTR 80 50 "s" "SIP+D2T" "" _sip._tcp.cesnet.cz.
```
 - SRV záznamy

```
_sip._udp.cesnet.cz IN SRV 0 1 5060 ser.cesnet.cz
```
 - A, AAAA záznamy
- **DŮVĚRYHODNOST - DNSSEC**

DNSSEC

- **Nástup DNSSEC – slepice nebo vejce**
- **Informaci je nutné dostat do aplikace**
- **Nedostatek knihoven v aplikacích**
 - Vložení DNSSEC resolveru do cesty (BIND, unbound) těsně před službu – na tomtéž stroji
- **Další možná využití**
 - Úložiště certifikátů ...
- **Stav v ČR – podepsané .cz i .0.2.4.e164.arpa**

Co je ENUM

- Slouží k *mapování* různých adresových a jmenných prostorů mezi sebou
- Výchozím prostorem je *prostor telefonních čísel*
- Cílovým prostorem může být jakékoliv URI (Uniform Resource Indicator)
- **Využití (v IP telefonii)**
 - Příchozí – ostatní vám mohou volat a vy říkáte „kam“
 - Odchozí - Voláte vy a nemusíte mít každého ve svém lokálním směrovacím seznamu (informaci spravuje držitel čísla)
- **ENUM není telefonování zadarmo**
- **ENUM (zlatý důl spammera !?)**
 - Držitel čísla zveřejňuje jen to co chce aby bylo vidět
 - Dobře prohledatelný strom (pevné kroky, NXDOMAIN)

ENUM různé typy

- veřejný uživatelský ENUM e164.arpa
- veřejný operátorský - infrastrukturní ENUM
- privátní ENUM
 - nrenum.net – EDU strom
 - e164.org, e164.info
 - Podnikové stromy = interní směrování v distribuovaných prostředích

	order	pref	flags	service	regexp	replacement
IN NAPTR	50	50	"u"	"E2U+sip"	"!^(.*)\$!sip:janru@cesnet.cz!"	.
IN NAPTR	100	50	"u"	"E2U+sip"	"!^\++420(.*)\$!sip:\\1@cesnet.cz!"	.
IN NAPTR	200	50	"u"	"E2U+h323"	"!^\++(.*)\$!h323:\\1@cesnet.cz!"	.

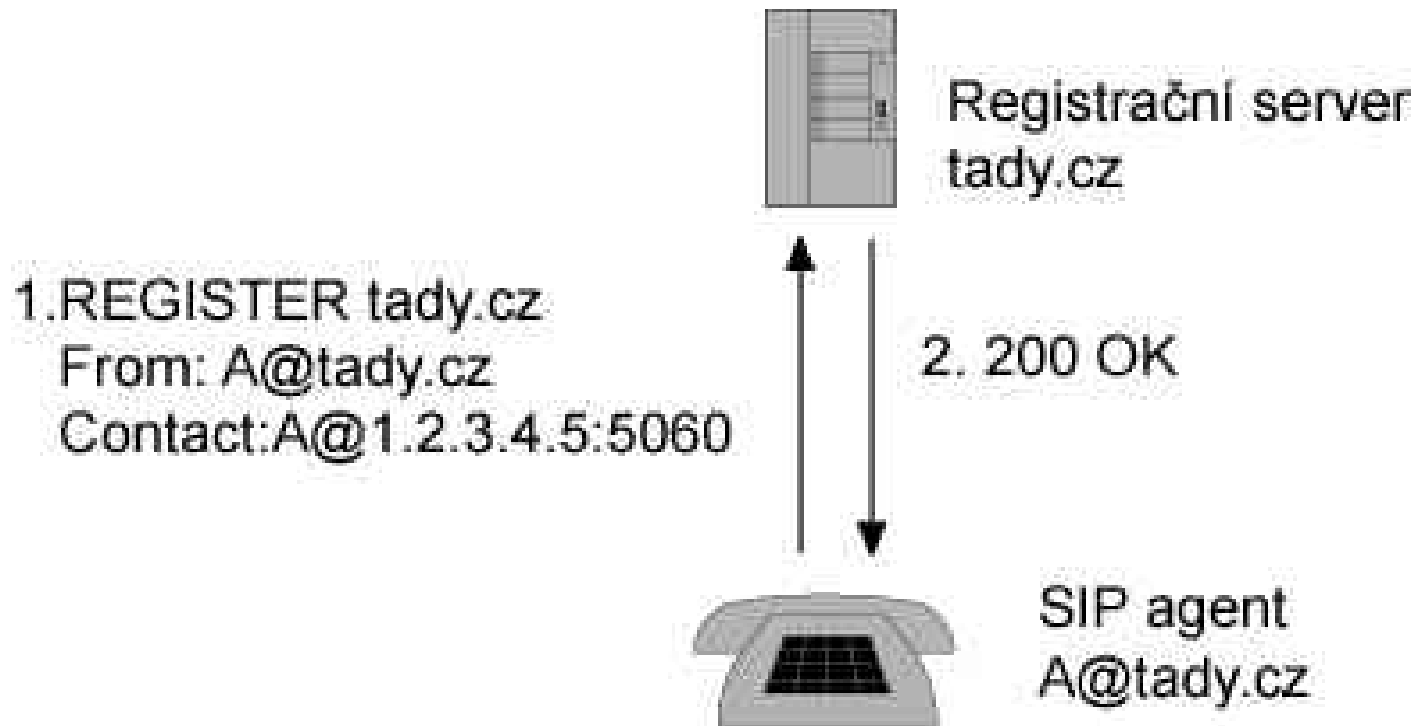
- **Důvěryhodnost odpovědi – DNSSEC**
- **ověřování oprávněnosti záznamů - validace**

Útoky na signalizační úrovni

- **Odposlech a modifikace zpráv**
 - Odposlech medií - E2E šifrování (SRTP, ZRTP, problematika výměna klíčů)
 - Převzetí či ukončení registrace
 - Pozměnění či ukončení hovoru
 - Podvržení identity
- **SPIT**
- **Podstata komunikace v reálném čase**
 - Odložení do fronty je problém
 - Obrana vs. možné omezení dostupnosti služby

Registrace

- Vytvoření vazby mezi konkrétní polohou (IP) klienta a je identifikátorem v SIP doméně



Registrace

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.

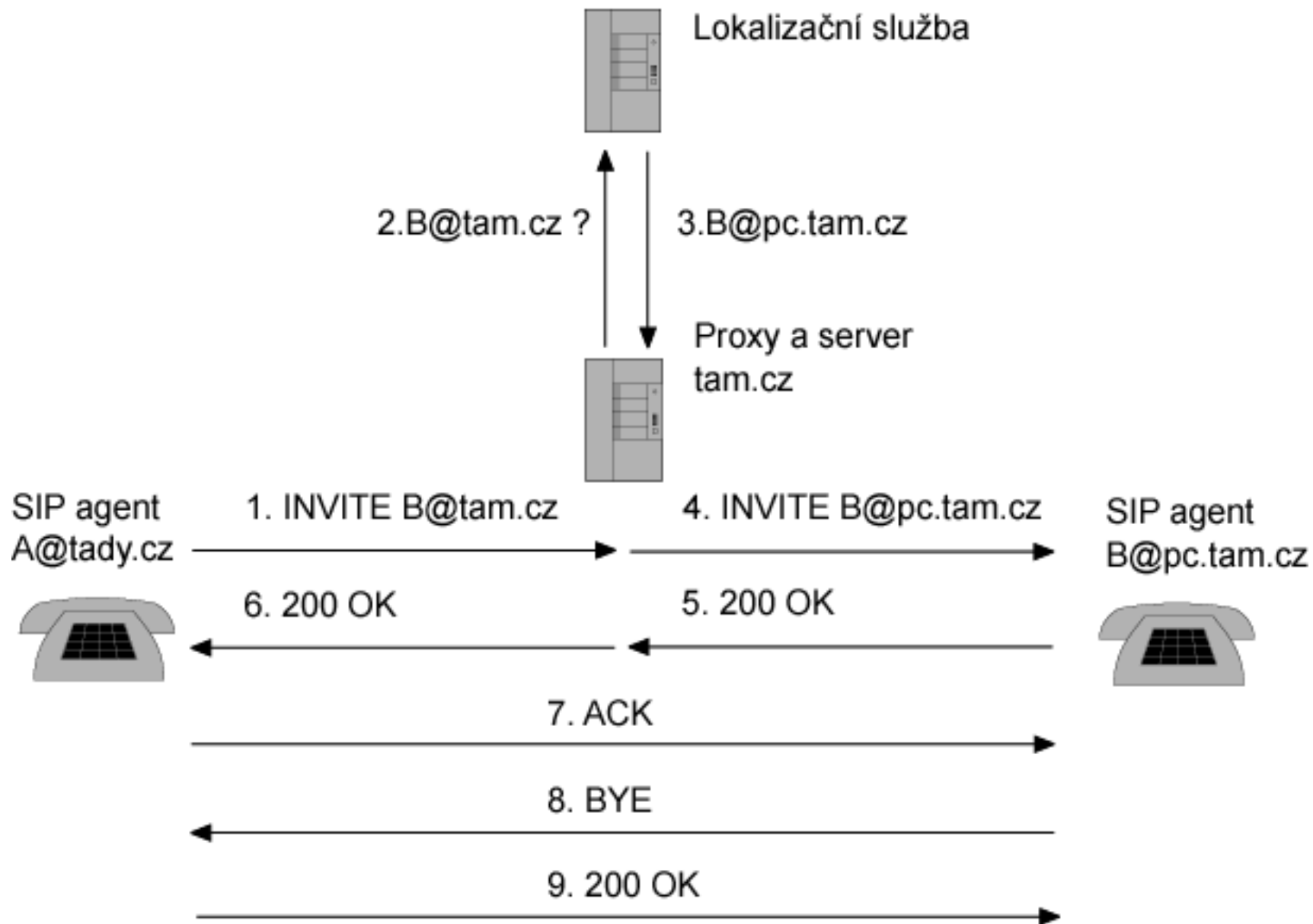
Content-Length: 0.

Max-Forwards: 70.

Expires: 15.

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

Hovor



INVITE

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:97iLBC/8000.

SPIT

- **Hovory, IM, Prezence**
- **Hovor = zvonění telefonu, které okamžitě vyruší**
 - Mail „jen“ spadne do schránky
- **ZATÍM není moc vidět**
 - Ostrůvky
 - Cena je vyšší než u emailu, ale nižší než PSTN, některé typy ochrany lze překonat botnety a levnou pracovní silou.
 - Důležité je nezaspat – nesmíme se dostat do situace, jaká je u mailu, ale uzavřené ostrůvky nejsou řešení.
- **IETF EG – RUCUS**
 - Průzkum navrhovaných metod a standardizace těch efektivních
- **RFC5039 SIP s SPAM**

Metody obrany

- **Silná = důvěryhodná identita**
- **Domácí část - první krok**
 - nahrazení či zabalení HTTP Digest
 - TLS – perzistentní spojení - „obálka“, nutně nemusí být klientské certifikáty, chrání i odpovědi
- **Mezidoménová identita – obdoba DKIM**
 - TLS – Hop By Hop – omezené na 1 skok
 - P-Asserted-Identity je nedostačující
 - SIP Identity (RFC4474) a SIP SAML
 - Princip vložení doménového podpisu
 - Problémy s čísly
 - Domény důvěry

Metody obrany II

- **Whitelisty, Blacklisty ...**
- **Problém počátečního představení iniciátora**
- **Interakce s uživatelem**
 - CAPTCHA (IVR),
 - výpočetní zátěž – problém poměru výkonu zařízení
 - mikroplatby
- **Silná identita jako podmínka fungování předchozích bodů pro následnou komunikaci**
- **Centralizovaná architektura jako u PSTN**

Dotazy?

Děkuji za pozornost.