



VoIP

Teorie a praxe IP telefonie

4. dvoudenní odborný seminář

23. a 24. listopadu 2010 v Kongresovém centru Hotelu Olšanka

Security and Frauds in IP telephony

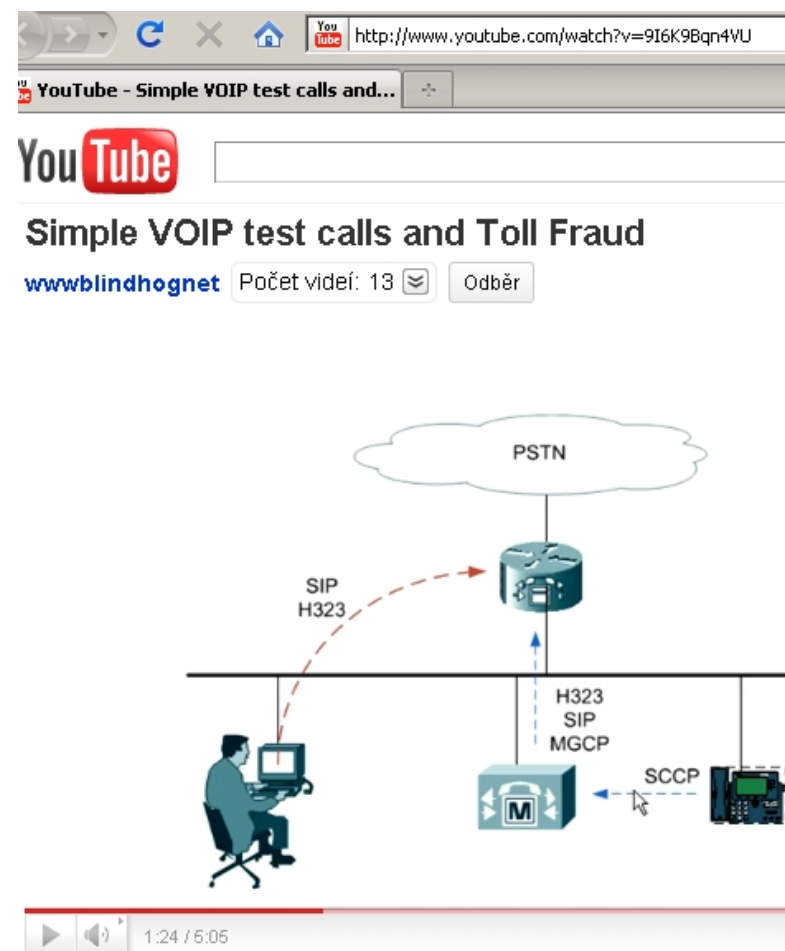
Miroslav Vozňák

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

<mailto:miroslav.voznak@vsb.cz>
<http://homel.vsb.cz/~voz29>

Důvody podvodů v telefonii

- ☐ **úspora nákladů**
- ☐ **dosažení zisku**
(např. podvody s čísly se spec. tarify)
- ☐ **skrytí vlastní identity**
(např. vydírání, ...)
- ☐ **jiné důvody**
(např. uživatel našel na YouTube podrobnou instruktáž)



Identifikace míst zneužití

VoIP Protocol and
Application Security

OS Security

Supporting Service Security
(web server, database, DHCP)

Network Security (IP, UDP, TCP, etc)

Physical Security

Policies and Procedures

☐ SPIT, call hijacking, odposlech,,
modifikace ..

☐ buffer overflows, worms, DoS na OS

☐ SQL injection, útok na DHCP a
další podpůrné komponenty

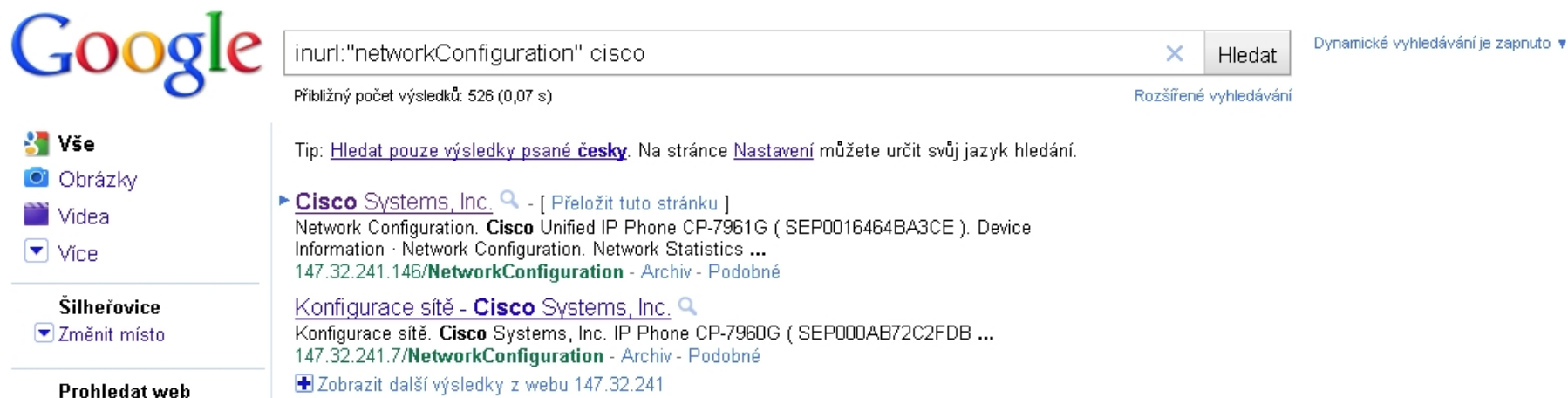
☐ SYN flood, ICMP, trivial flooding,

☐ Reboot, napájení

☐ slabé hesla, nevyhovující bezp.
politika

VoIP Footprinting

- ❑ příliš mnoho stop na Internetu
- ❑ ENUM – zlatá studnice pro spamera
- ❑ GOOGLE – kamarád, který např. najde odkazy na management zařízení



Google

inurl:"networkConfiguration" cisco × Hledat Dynamické vyhledávání je zapnuto ▼

Přibližný počet výsledků: 526 (0,07 s) Rozšířené vyhledávání

Tip: [Hledat pouze výsledky psané česky](#). Na stránce [Nastavení](#) můžete určit svůj jazyk hledání.

► [Cisco Systems, Inc.](#) - [Přeložit tuto stránku]
Network Configuration. **Cisco** Unified IP Phone CP-7961G (SEP0016464BA3CE). Device Information · Network Configuration. Network Statistics ...
[147.32.241.146/NetworkConfiguration](#) - Archiv - Podobné

[Konfigurace sítě - Cisco Systems, Inc.](#)
Konfigurace sítě. **Cisco** Systems, Inc. IP Phone CP-7960G (SEP000AB72C2FDB ...
[147.32.241.7/NetworkConfiguration](#) - Archiv - Podobné

[+](#) Zobrazit další výsledky z webu 147.32.241

Vše
Obrázky
Videa
Více

Šilheřovice
[Změnit místo](#)

Prohledat web

VoIP Footprinting

Cisco Systems, Inc. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://147.32.241.7/DeviceInformation

Cisco Systems, Inc.



Informace o zařízení

Cisco Systems, Inc. IP Phone CP-7960G (SEP000AB72C2FDB)

Adresa MAC	000AB72C2FDB
Název hostitele	SEP000AB72C2FDB
Číslo tel. v adr.	9921
ID zavedené apl.	P00308010100
ID zavedeného systému	PC0303010000
Verze	8.1(1.0)
DSP	4.0(5.0)[A0]
Rozšiřující modul 1	
Rozšiřující modul 2	
Revize hardwaru	2.4
Sériové číslo	INM0632A30U
Model telefonu	CP-7960G
Codec	ADLCodec
Amps	5V Amp
Revize C3PO	2
Indikace hlas. zpráv	NE

Informace o zařízení

[Konfigurace sítě](#)

Statistiky sítě

[Ethernet](#)

[Port 1 \(Sb\)](#)

[Port 2 \(Přístup\)](#)

[Port 3 \(Telefon\)](#)

Logy zařízení

[Zobrazení ladění](#)

[Statistiky zásobníku](#)

[Stavová hlášení](#)

Statistiky datového toku

[Tok 1](#)

[Tok 2](#)

Scanning, Enumeration and Attack

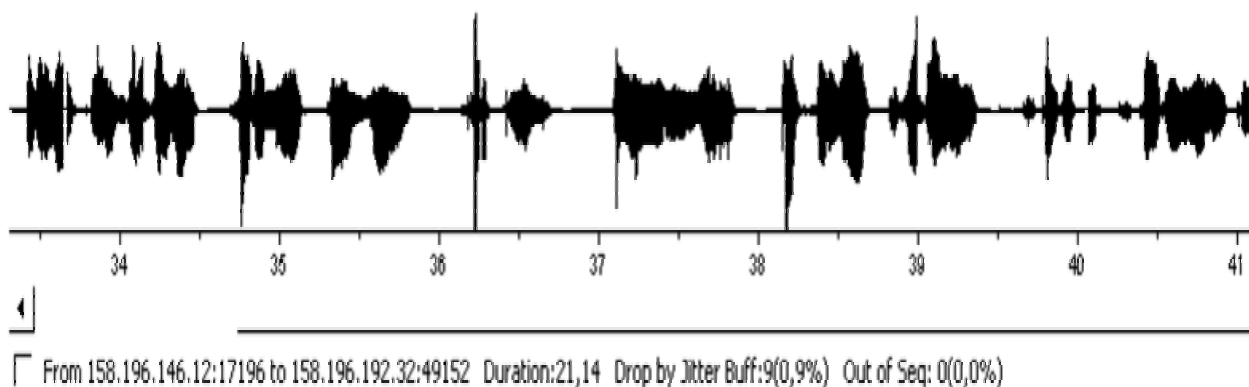
- ☐ prvním krokem bude pravděpodobně **Nmap**,
 - porty UDP/TCP, 5060/5061

- ☐ potom sofistikovanější nástroj typu
 - **Netcat, SIPSCAN, SiVuS, SIPVicious**

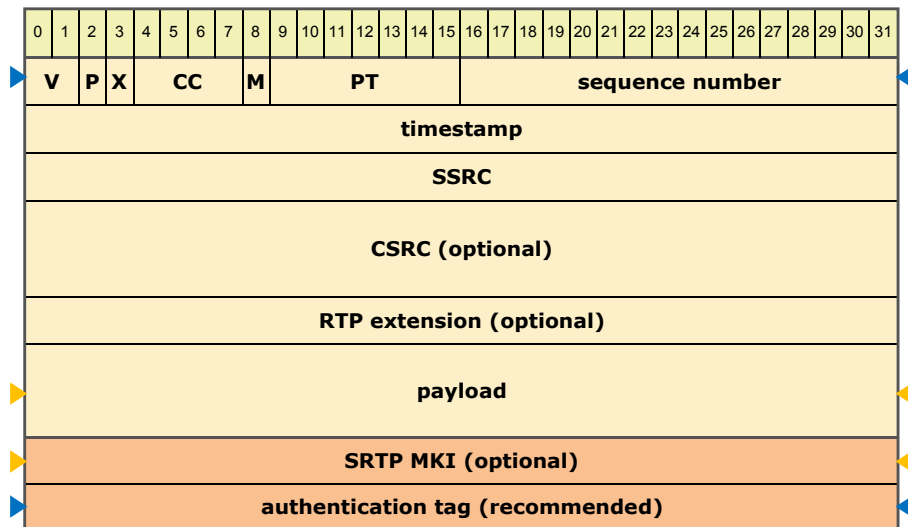
- ☐ pro vyřazení služby stačí mnohdy DoS útok vedený pomocí **Inviteflood**

Zabezpečení médií v IP telefonii

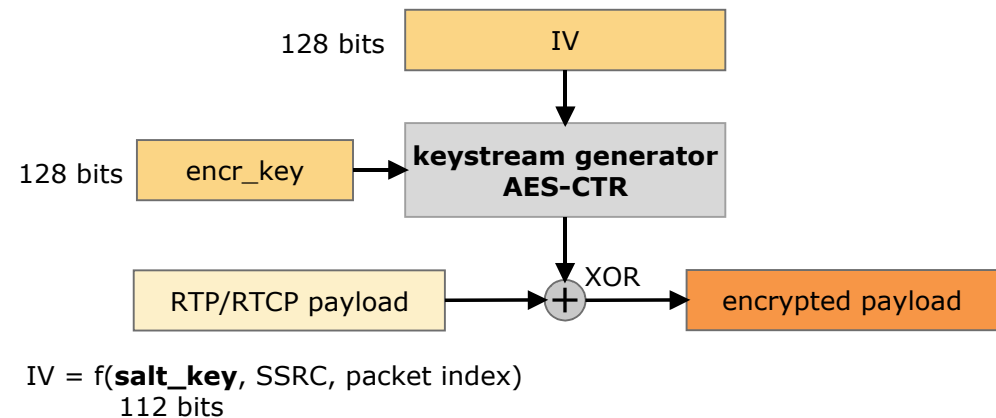
- ❑ nešifrovaný Real Time Protocol (RFC1889 z roku 1995)
- ❑ RTP pakety mohou být zachyceny a obsah přehrán



- ❑ šifrovaný SRTP (RFC 3711 z roku 2004)
- ❑ zajišťuje utajení a integritu přenášených dat
- ❑ AES-CTR - generátor pseudonáhodných klíčů



▶▶ authenticated
▶▶ encrypted



❑ **vylepšení** SRTP: Zimmermann Real-time Transport Protocol (ZRTP)

❑ ZRTP je ve stavu RFC návrhu

❑ **Výhody ZRTP:**

- zpětná kompatibilita se SRTP (detekce módu)
- vylepšení výměny Master klíče (DH algoritmus)

Techniky zabezpečení SIP signalizace

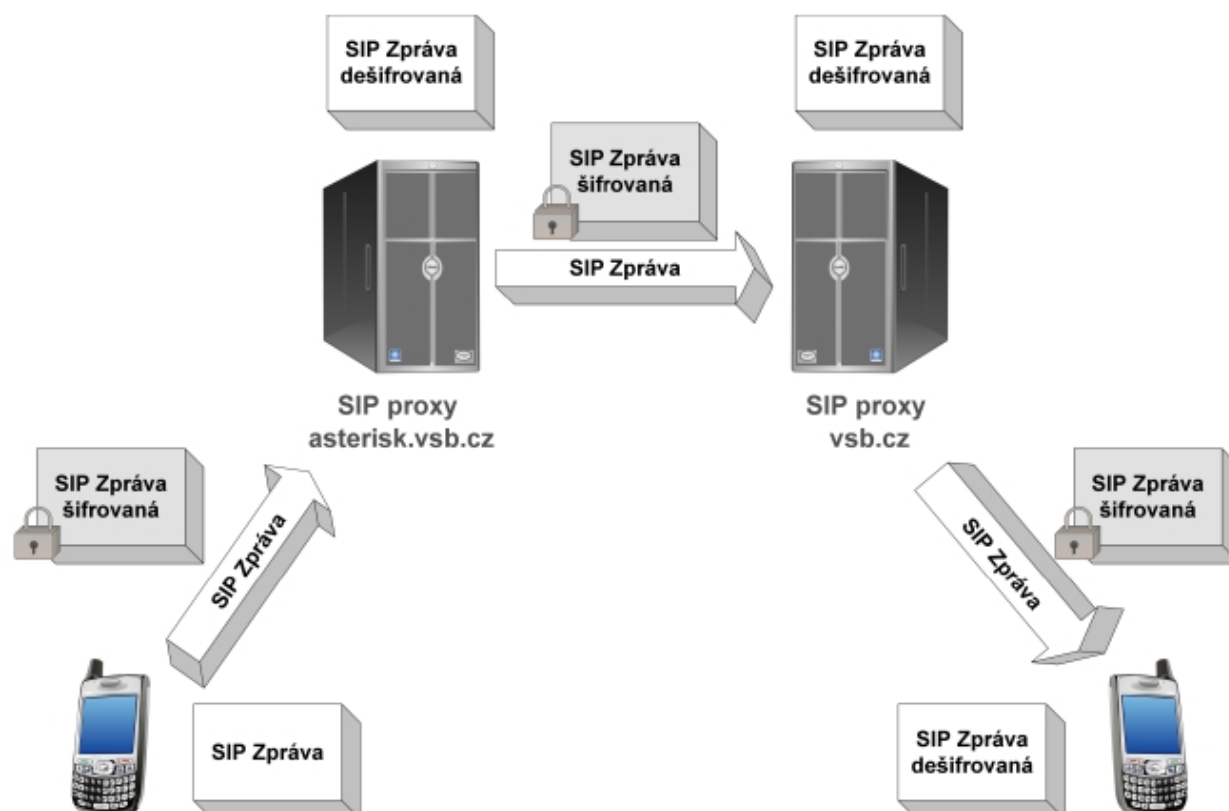
- ❑ HTTP Basic Authentication, zastaralé
- ❑ HTTP Digest Authentication, nejpoužívanější
- ❑ Secure MIME (**S/MIME**), využití pokročilejších metod veřejných klíčů PKI, využívá se minimálně
- ❑ **SIPS**, použití šifrovaného protokolu TLS, nejbezpečnější řešení.

Aplikace Digest Authentication v SIP

- ❑ UA posílá žádost, která je odmítnuta odpovědí
401 Unauthorized Response
407 Proxy Authentication Required
- ❑ odpověď nese informace, jak požadavek autentizovat
Authentication scheme: Digest
Realm
Nonce
do výpočtu vstupuje ještě RURI a password (tajné heslo)
- ❑ **MD5** , výsledkem je hash, řetězec je ověřen na serveru

TLS scénář

□ hop by hop

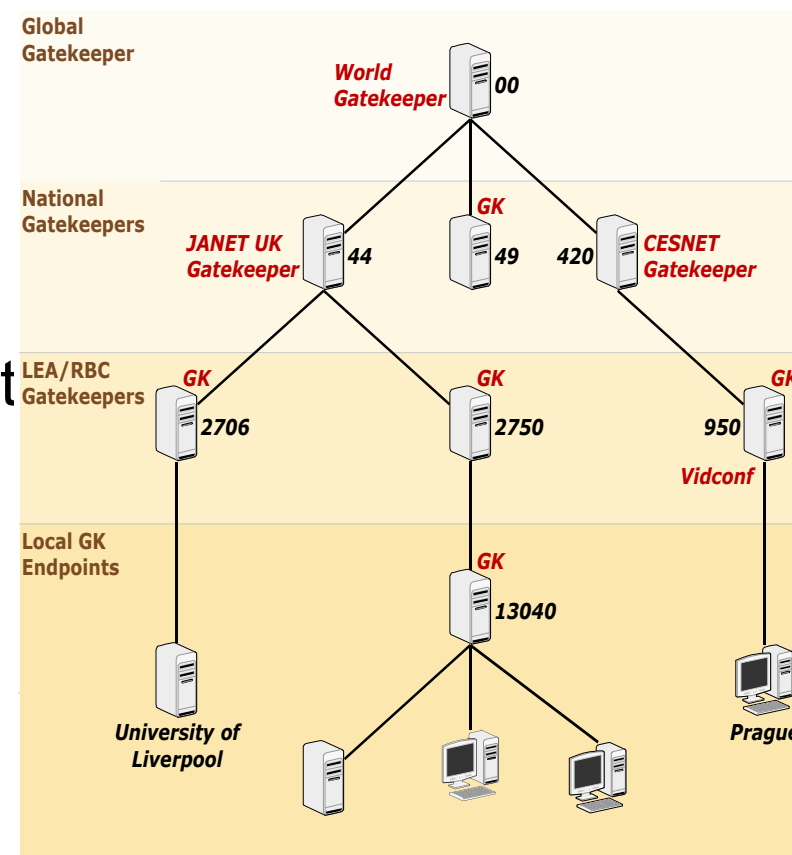


System mezikoménové důvěry

- ❑ v počátku **bilaterální** dohody
- ❑ architektura **GDS (H.323)**, hierarchický systém směrování, vyvinuto v rámci TF-VVC (TERENA)

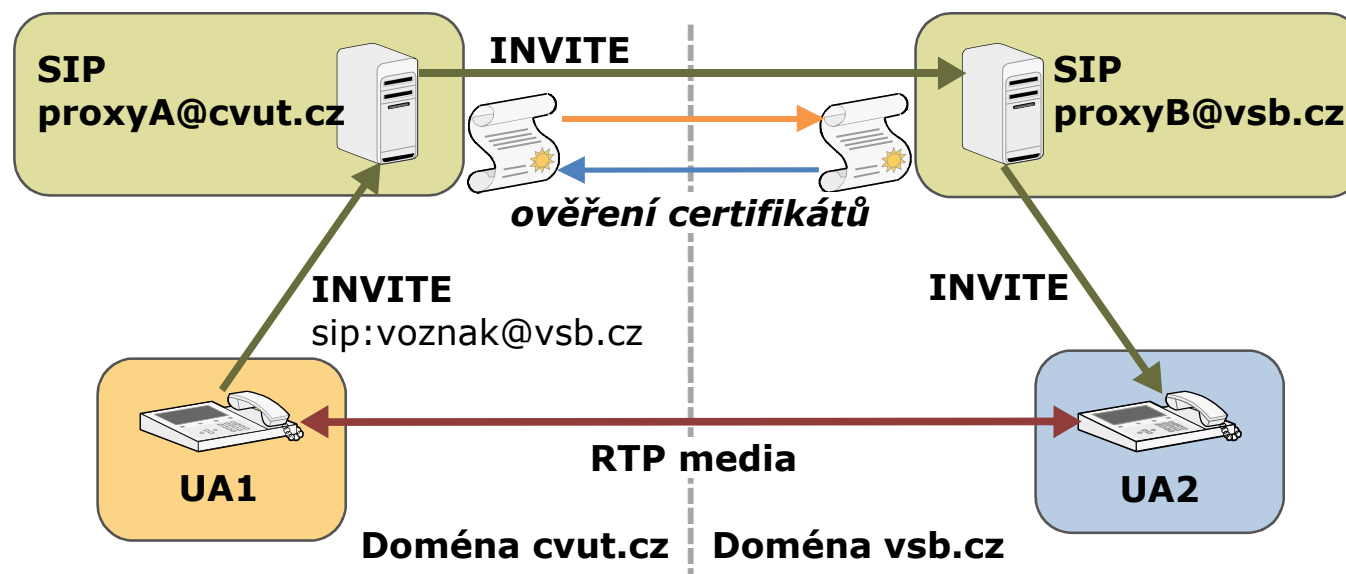
- ❑ **SIP** pracuje s doménami (součást URI adresy - host), architektura **SIP identity** (kontroverzní téma – vývoj vážne), SAML (Security Assertion Markup Language) – výměna založena na XML (SAML profil)

- ❑ preferuje se **SIPS (TLS)**



- ❑ **použití TLS**, implementace do openSER, Asterisk, atd.
- ❑ TLS identifikuje SIP zdroj ve formě domény, certifikát obsahuje název hostitele proxyB@vsb.cz a potvrdí tak identitu SIP Proxy (doména je součást URI)

TLS (Transport Layer Security)



Klasifikace rizik dle VoIPSA

- ❑ **Social threats** (obtěžování, narušení soukromí, spam, uvedení v omyl vystupováním pod nepravou identitou)
- ❑ **Eavesdropping** (odposlouchávání)
- ❑ **Interception and modification** (útočník získává informace o spojení, které mu umožňují provést – přesměrování volání, změnu identity, obecně jakoukoliv změnu obsahu přenášených dat)
- ❑ **Service abuse** (zneužití služby – obcházení autentizace, podvody s registrací, krádež účtu a následné zneužití)
- ❑ **Intentional Interruption of service** (DoS útok)
- ❑ **Other Interruptions of Service** (napájení, vyčerpání zdrojů, záměrné docílení latence)

Nejčastěji se setkáváme

- ❑ s monitorováním a **skenováním** VoIP sítě, získání citlivých údajů a jejich zneužití (E.Pena – 4,5 mil. USD a řada útoků i v ČR), MD5 hash (slabé heslo a chyby v implementaci)
- ❑ **DoS a DDoS**, triviální nástroje UDP či TCP flood, ale možný i INVITE flood anebo zahltit Registrar server registracema
- ❑ **Odposlech**
- ❑ **CID Spoofing** (manipulace s CID)

méně se již setkáváme s

❑ **Modifikací a manipulací** se signalizací v Real-Time
- s nástrojem Scapy proveditelné

např. Built-up Call Aborting, odchytím ACK - změním na BYE, upravím branch, tag a CSeq, odešlu a způsobím ukončení hovoru (náhodné rozpojování)

```
ACK sip:filip@158.196.40.19:5070;transport=udp SIP/2.0
CSeq: 1 ACK
Via: SIP/2.0/UDP 158.196.40.18:5063;
    branch=z9hG4bK64475aaa-bda6-da11-8dc2-0013d4e2956d;rporl
From: ' ' filip 1 ' ' <sip:filip@158.196.40.18>;
    tag=dc7250a7-bda6-da11-8dc2-0013d4e2956d
Call-ID: f26b50a7-bda6-da11-8dc2-0013d4e2956d@pcbuslab11
To: <sip:filrez@ekiga.org>; tag=22acb79d-bda6-da11-8d2e-0013d4e
Contact: <sip: filip@158.196.40.18:5063; transport=udp>
....
```

RTP Data Redirecting, modifikací obsahu SDP terminuji RTP stream na jiný cíl

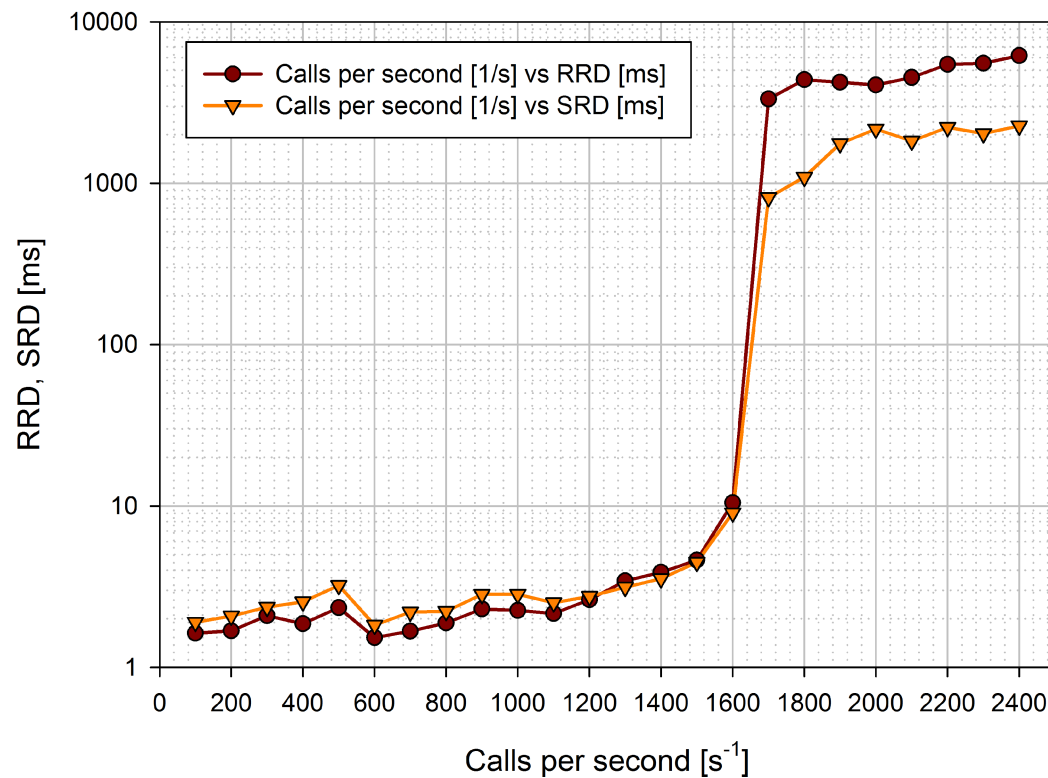
```
v=0  
o=- 1140424487 1140424487 IN IP4 158.196.40.19  
s=Opal SIP  
c=IN IP4 158.195.40.19  
t=0 0  
m=audio 5012 RTP/AVP 101 114 115 3 107 110 0 8  
a=rtpmap:101 telephone-event/8000  
a=ftpm:101 0-15  
a=rtpmap:114 SPEEX/16000
```



```
v=0  
o=- 1140424487 1140424487 IN IP4 10.0.0.1  
s=Opal SIP  
c=IN IP4 10.0.0.1  
t=0 0  
m=audio 5003 RTP/AVP 101 114 115 3 107 110 0 8  
a=rtpmap:101 telephone-event/8000  
a=ftpm:101 0-15  
a=rtpmap:114 SPEEX/16000
```

vyčerpání zdrojů – SIP generátor volání, dosažení limitních hodnot

RRD and SRD



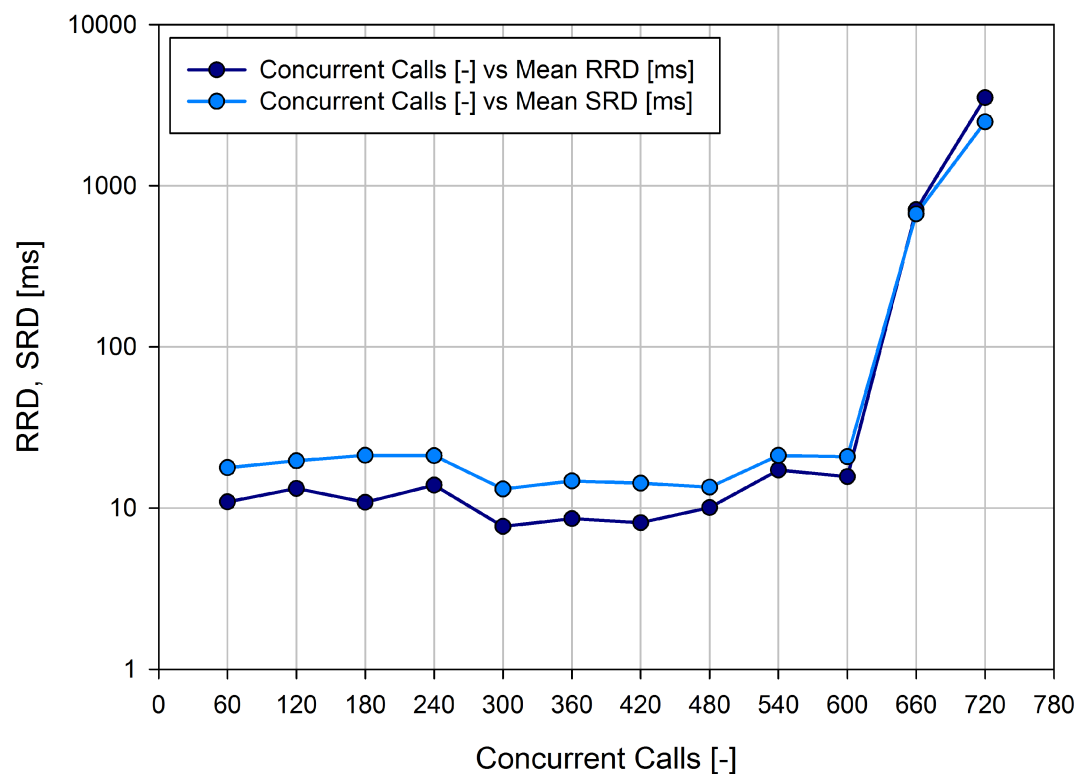
openSIPS 1.6

SIP Proxy

Registration Request Delay
Session Request Delay

vyčerpání zdrojů – SIP generátor volání, dosažení limitních hodnot

RRD and SRD (G711u to G711u)

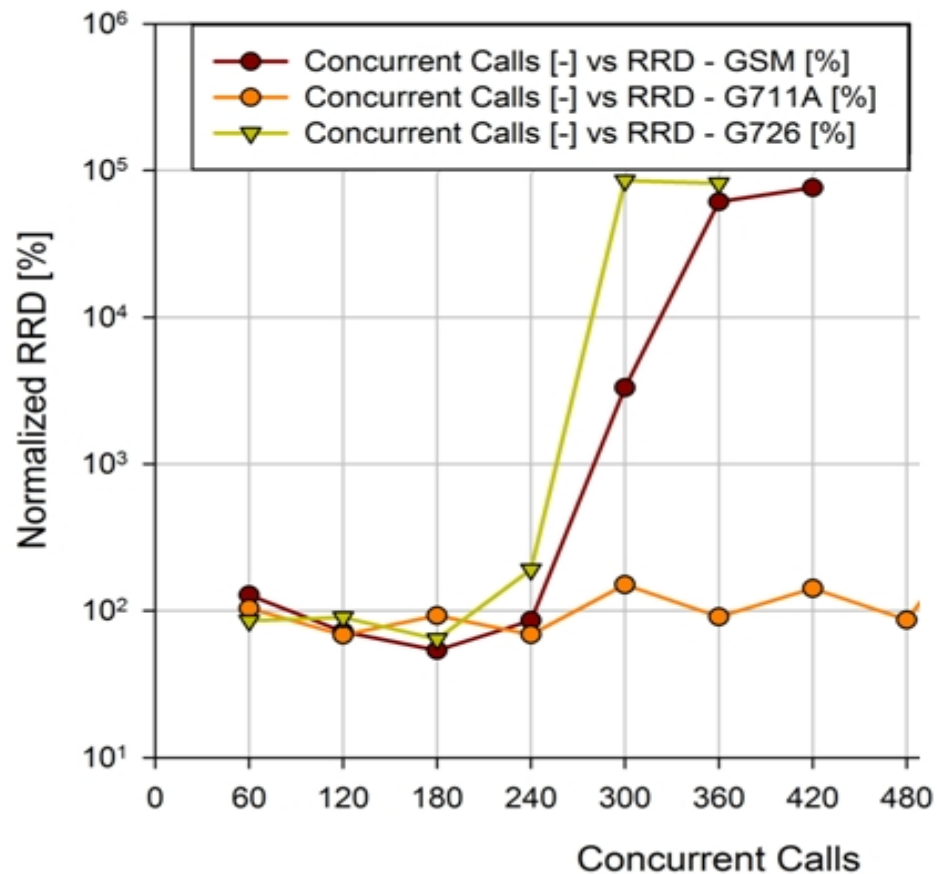


Asterisk 1.6

B2BUA

vyčerpání zdrojů – transcoding, normalizované výsledky

Normalized RRD (100% relates to non-codec translation)



Asterisk 1.6

B2BUA

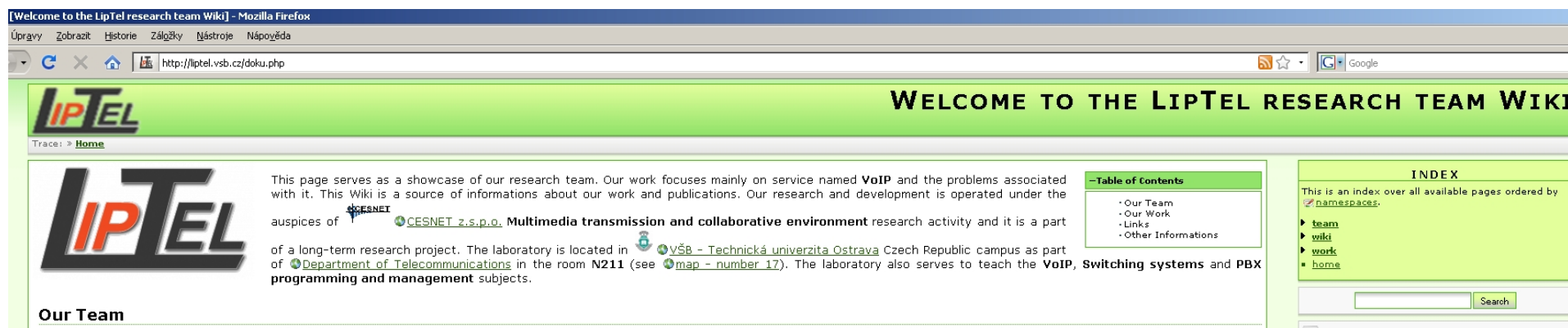
$$P_{RF} = \frac{P_{CT}}{P} \cdot 100$$



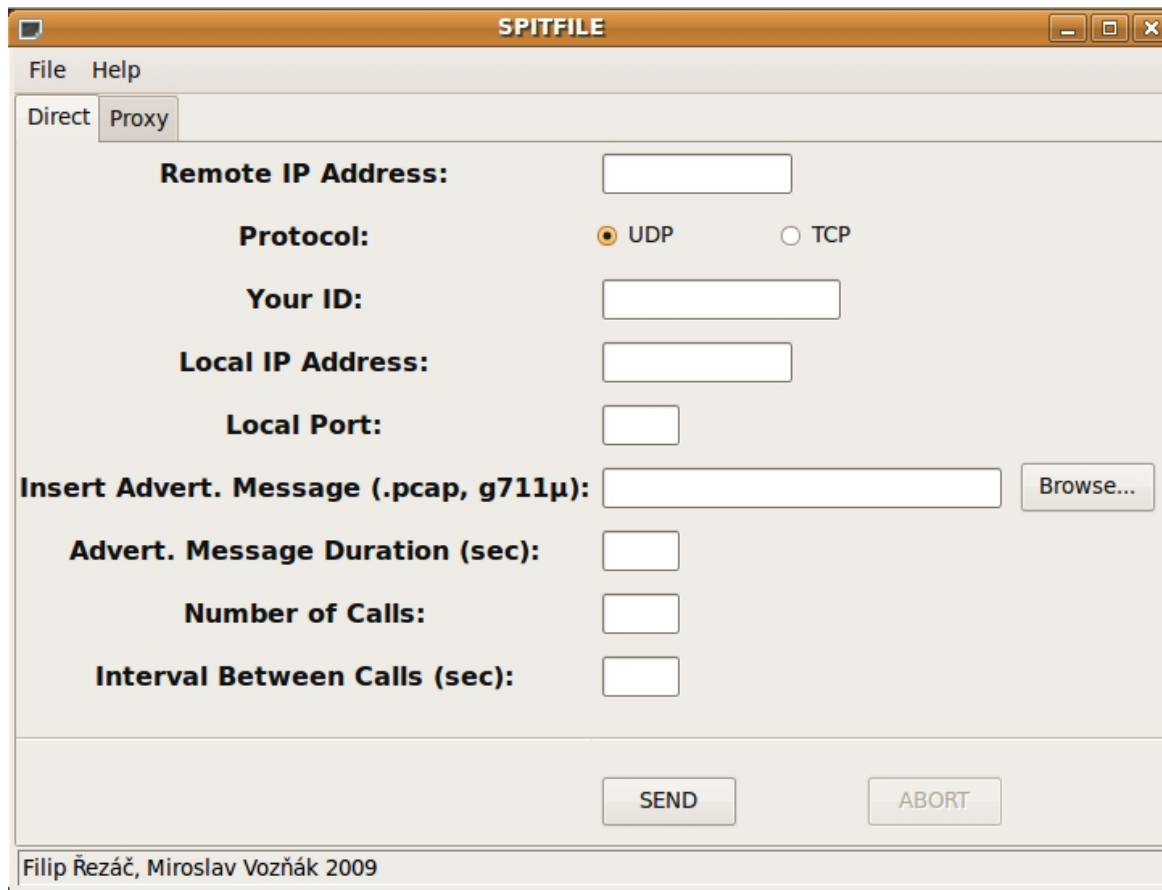
Spam over Internet

Telephony

- ❑ vývoj nástroje generující volání s přehráním záznamu postaveném na protokolu SIP
- ❑ Lab of IP telephony na VŠB-TUO (LIPTTEL)
- ❑ **motivace**, SPIT = reálná hrozba v telefonii



- ❑ při vývoji použít Phyton, xml.dom.minidom a SIPp
- ❑ dva typy režimů: Direct a SIP Proxy

The image shows a screenshot of a software application window titled 'SPITFILE'. It has a menu bar with 'File' and 'Help'. Below the menu bar are two tabs: 'Direct' (selected) and 'Proxy'. The 'Direct' tab contains several input fields and controls: 'Remote IP Address:' with a text box; 'Protocol:' with radio buttons for 'UDP' (selected) and 'TCP'; 'Your ID:' with a text box; 'Local IP Address:' with a text box; 'Local Port:' with a text box; 'Insert Advert. Message (.pcap, g711μ):' with a text box and a 'Browse...' button; 'Advert. Message Duration (sec):' with a text box; 'Number of Calls:' with a text box; and 'Interval Between Calls (sec):' with a text box. At the bottom of the window are two buttons: 'SEND' and 'ABORT'. The footer of the window reads 'Filip Řezáč, Miroslav Vozňák 2009'.

SPITFILE

File Help

Direct Proxy

Remote IP Address:

Protocol: ☒ UDP ☐ TCP

Your ID:

Local IP Address:

Local Port:

Insert Advert. Message (.pcap, g711μ): Browse...

Advert. Message Duration (sec):

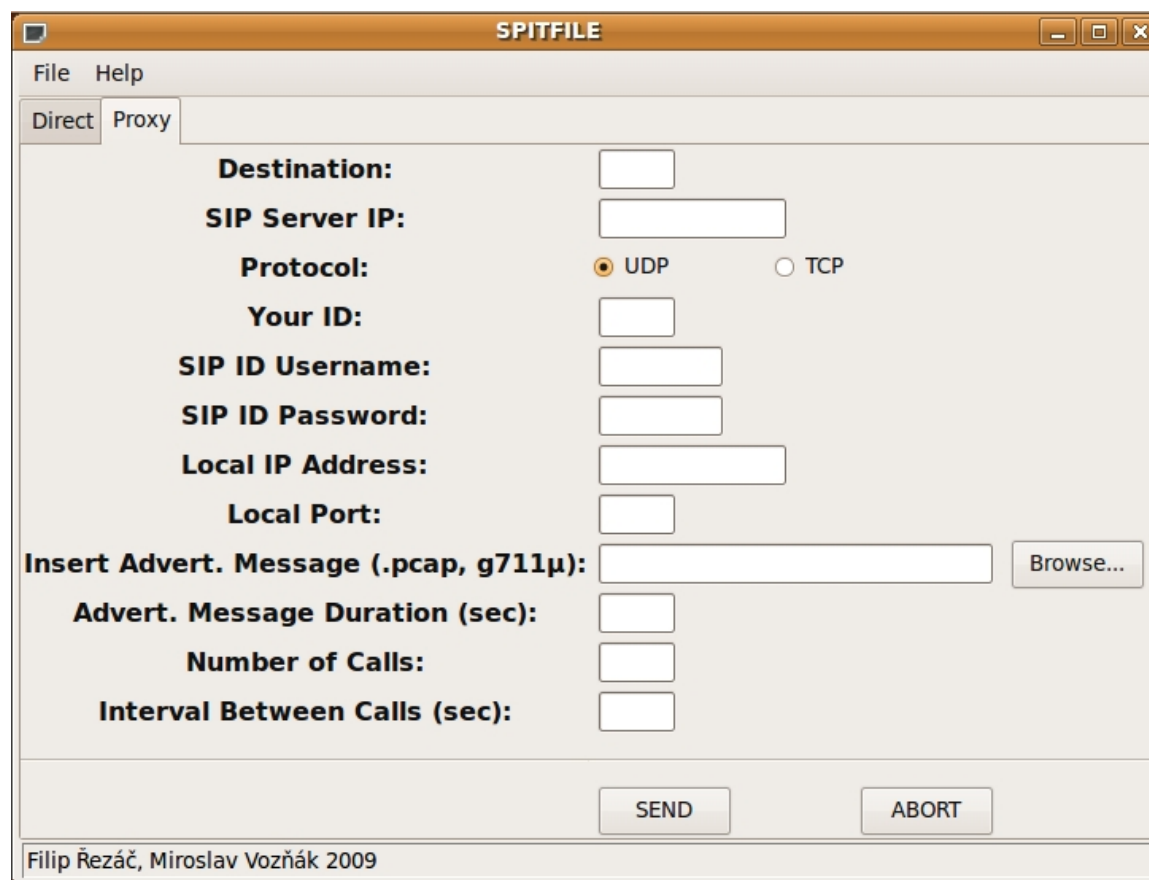
Number of Calls:

Interval Between Calls (sec):

SEND ABORT

Filip Řezáč, Miroslav Vozňák 2009

- ❑ řada IP telefonů nepřijímá volání na IP (pouze SIP Proxy)
- ❑ přes SIP Proxy lze generovat volání kamkoliv (i na mob. tel.)



The image shows a screenshot of the SPITFILE application window. The window has a title bar with the text "SPITFILE" and standard window controls. Below the title bar is a menu bar with "File" and "Help". There are two tabs: "Direct" and "Proxy", with "Proxy" currently selected. The main area contains several input fields and labels:

- Destination:** [text input]
- SIP Server IP:** [text input]
- Protocol:** ☒ UDP ☐ TCP
- Your ID:** [text input]
- SIP ID Username:** [text input]
- SIP ID Password:** [text input]
- Local IP Address:** [text input]
- Local Port:** [text input]
- Insert Advert. Message (.pcap, g711μ):** [text input] **Browse...** [button]
- Advert. Message Duration (sec):** [text input]
- Number of Calls:** [text input]
- Interval Between Calls (sec):** [text input]

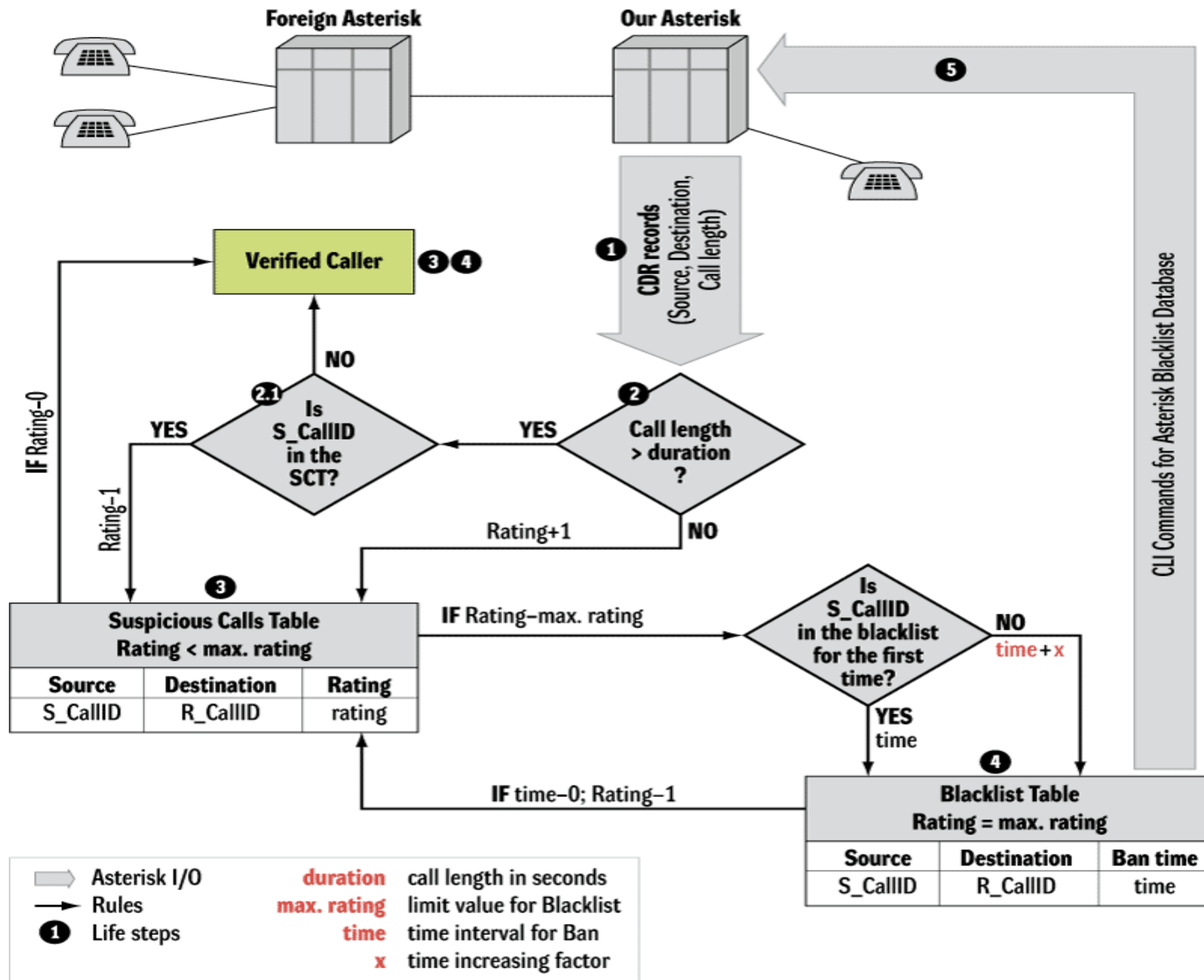
At the bottom of the window are two buttons: **SEND** and **ABORT**. The footer of the window contains the text: "Filip Řezáč, Miroslav Vozňák 2009".

Obrana proti SPITFILE

- ☐ udržování seznamů: Buddylist, Whitelist, Blacklist, Greylist
- ☐ hlasový strom (výzva k vložení kódů)
- ☐ voice CAPTCHA (a jiné prakticky nepoužitelné nesmysly ...)
- ☐ právní aspekty

vývoj ANTISPIT (vývoj hradil CESNET v roce 2009)

- ☐ založen na Blacklistu (bez participace volaného)
- ☐ tabulka SCT (podezřelá volání), recidiva = přesun na Blacklist
- ☐ implementace do Asterisku



Installation

- Welcome!
- **System requirements**
- Database
- Cron Settings
- System Settings
- Done!

System requirements

PHP version > 4.3	✓
Mysql extension	✓
Writable Config Files	✓

Legend

- ✓ : OK
- ✗ : Error, the component is necessary!

[Next Step](#)

Settings

AntiSPIT System

AntiSPITLogout

Menu

[→ Home](#)

[→ Settings](#)

[→ Suspicious Calls Table](#)

[→ Blacklist Table](#)

[→ Change Password](#)

Settings

SETTINGS

Call Duration (If the call duration is less than this level, the caller obtains the status of suspicious caller)	5 s
1. level BAN time (How many hours will be the caller blocked)	5 h
2. level BAN time (How many hours will be the caller blocked)	24 h
3. level BAN time (How many hours will be the caller blocked)	240 h
Max. rating (Limit value for Blacklist)	5 ▼
Save	

CDR FILE PATH

CDR file full path	/path/to/cdr/file.log
Save	

SYSTEM
System version: **v1.0b**

Blacklist

AntiSPIT System

AntiSPIT Logout

Menu

- Home
- Settings
- Suspicious Calls Table
- Blacklist Table
- Change Password

Blacklist Table

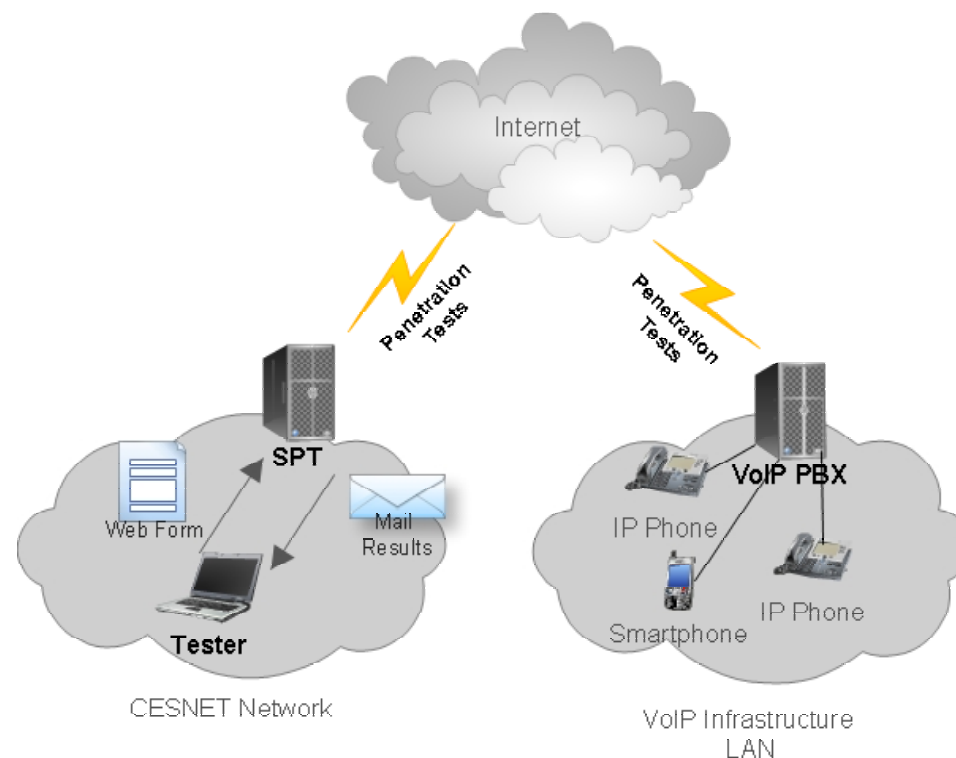
SOURCE	DESTINATION	CALL TIME	BAN	RATING	UNBAN
7006	7009	22.8. 2009 09:25	20.9. 2009 12:05	5	UnBAN NOW

SYSTEM
System version: **v1.0b**

Download ANTISPIT from <https://sip.cesnet.cz>

SIP Penetrační testování

- vývoj na Cesnetu
- penetrační test se snaží proniknout do testovaného zařízení
- cílem je upozornit na slabiny,
- podmínky užití dovolují test pouze zařízení ve vlastní správě
- modularita SPT (dnes čtyři moduly – SM, DoS, RM a SPIT)
- běží jako webová služba



Scanning and Monitoring Module

- The potential attacker needs to find out the most information about a particular component.
- Used to test the security level against attacks aimed at obtaining information (open ports, SIP accounts and password) by means of common and available tools – **Nmap, SIPVicious**.

• **Time Requirements:** $T_{sm} = T_e + T_p + T_n$ E_{nr}, P_{nr} - Range of tested numbers/ passwords.

Test for open ports T_n E_{dr}, P_{dr} - File containing strings of alpha-num characters / passwords.

Test for SIP accounts $T_e = (E_{nr} + E_{dr}) \cdot c$ $c = 0.02603$ - Time constant.
 $E_{valid} = (E_{nr} + E_{dr}) - E_{invalid}$

Test for SIP passwords $T_p = [E_{valid} \cdot (P_{nr} + P_{dr})] \cdot c$

Denial of Service Module

- Testing module sends a large volume of adjusted or otherwise deformed packets to the target component so that it is unable to provide its core services.
- To generate Flood DoS, the system uses two applications - Udpflood and Inviteflood.

• **Time Requirements:** $T_{dos} = T_{udp} + T_{invite}$

CPU load:

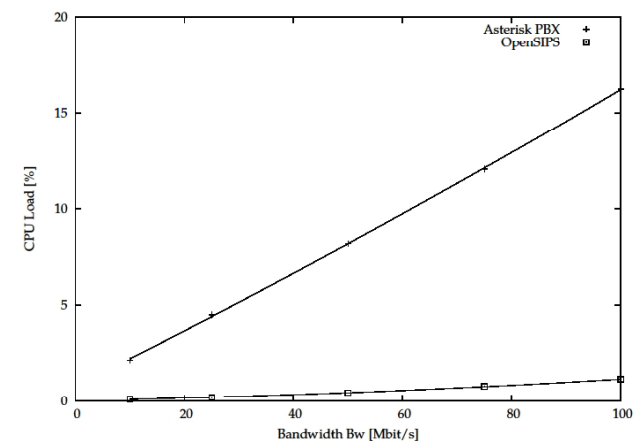
Test with Udpflood $T_{udp} = (FS_{udp} \cdot P_n) / B_w$

Test with Inviteflood $T_{invite} = (FS_{invite} \cdot P_n) / B_w$

FS_{dos}, FS_{invite} - Ethernet framework (1414 B, 1140 B).

P_n - Number of packets generated.

B_w - Bandwidth.



Registration Manipulation Module

- The system can also test SIP servers' security, i.e. measures against manipulating the registration.
- To carry out this test, the system uses **Reghijacker** application which substitutes the legitimate account registration with a fake, non-existing one -> can easily be expanded to a very popular Man-in-the-Middle attack.
- Time required to carry out the test is insignificant compared to operational times of other modules.
- **Time Requirements** T_{rm}

SPIT Module

- SIP call is initiated from the caller's account, and the end device with the registered account of the called party starts ringing. Once the call is answered, a pre-recorded message is played and the call terminated.
- Time required is determined by the length of the pre-recorded message.

• **Time Requirements** T_{spit}

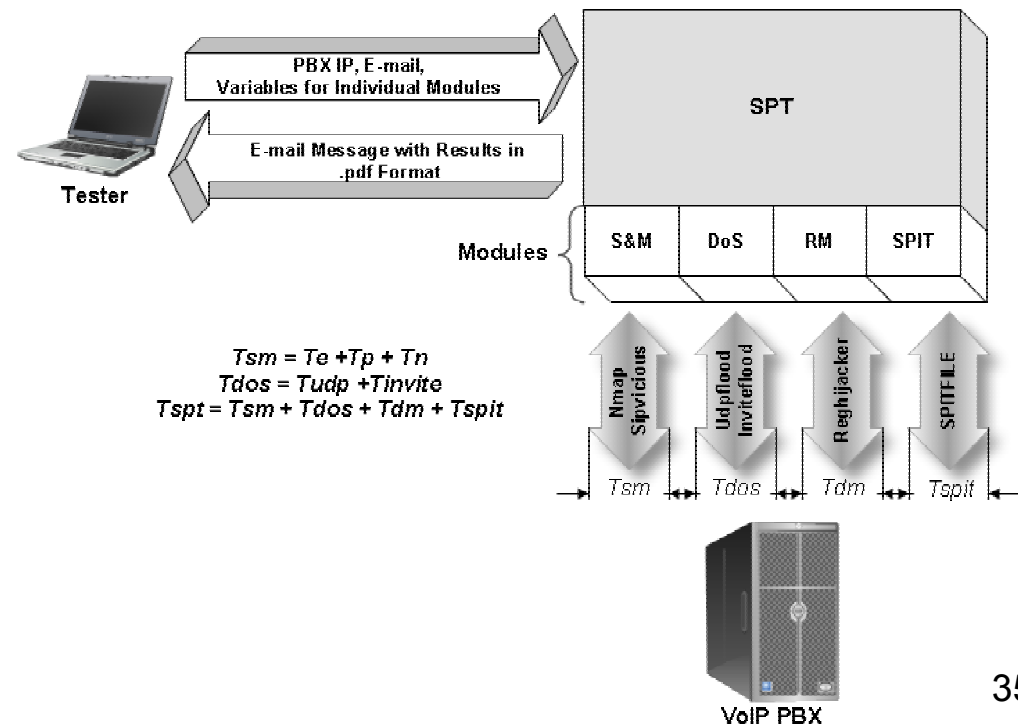
Testing and Countermeasures

- The final report on penetration tests which the tester receives via e-mail, will contain an analysis and methods which should limit or completely mitigate potential security gaps.
- Time requirements of the whole system depends on many factors and can radically change in accordance with the type of tests requested by the tester. Its value is for reference only.

•Time Requirements:

$$T_{spt} = T_{sm} + T_{dos} + T_{rm} + T_{spit}$$

$$\begin{aligned} T_{sm} &= T_e + T_p + T_n \\ T_{dos} &= T_{udp} + T_{invite} \\ T_{spt} &= T_{sm} + T_{dos} + T_{dm} + T_{spit} \end{aligned}$$



SPT application

Pen Test

[Home](#)[Logout](#)

New Test 

[→ Main \(Ok\)](#)[→ S & M](#)[→ DoS](#)[→ RM](#)[→ Spit](#)

Menu

[→ Results](#)[→ Logout](#)

[Main](#)[S & M](#)[DoS](#)[RM](#)[SPIT](#)

Main

MAIN SETTINGS

SIP server IP address	158.196.132.13
Tester`s email address	voznak@yahoo.com

[NEXT](#)

SM module

New Test 

- Main **(Ok)**
- S & M
- DoS
- RM
- Spit

Menu

- Results
- Logout

Main **S & M** DoS RM SPIT

Scanning & Monitoring

PORT SCANNING

Enabled	☐ No ☒ Yes
Port range	☒ Default ports (20,21,22,23,53,80,443,5004,5060)

EXTENSIONS SCANNING

Enabled	☐ No ☒ Yes
Extensions range	☐ Default extensions (100 - 999)
List of passwords	☐ Default passwords (100 - 999) Procházet...

DoS Module

New Test

→ Main (ok)

→ S & M (ok)

→ DoS

→ RM

→ Spit

Menu

→ Results

→ Logout

MainS & MDoSRMSPLIT

Denial of Service

DENIAL OF SERVICE

Enabled☐ No ☒ Yes

UDP FLOOD

Enabled☒ No ☐ Yes

INVITE FLOOD

Enabled☐ No ☒ Yes

Number of packets5000000

Valid extension☒ Random valid extension

PREV

NEXT

Registration and Manipulation Module

[Home](#) [Logout](#)

New Test

- Main (Ok)
- S & M (Ok)
- DoS (Ok)
- RM
- Spit

Menu

- Results
- Logout

[Main](#) [S & M](#) [DoS](#) **[RM](#)** [SPIT](#)

Registration Manipulation

REGISTRATION MANIPULATION

Enabled	☐ No ☒ Yes	
SIP ID username		☒ Random valid account
SIP ID password		

[PREV](#) [NEXT](#)

SPIT Module

Home Logout

New Test 

- Main (ok)
- S & M (ok)
- DoS (ok)
- RM (ok)
- Spit

Menu

- Results
- Logout

Main S & M DoS RM **SPIT**

SPIT

SPIT ATTACK

Enabled	☐ No ☒ Yes	
Random valid extension	☐ Random valid extension 	
Caller SIP ID username	7204	☐ Random valid account
Caller SIP ID password	*****	

PREV SEND

Results

New Test 

→ Main (Ok)

→ S & M (Ok)

→ DoS (Ok)

→ RM (Ok)

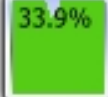
→ Spit (Ok)

Menu

→ Results

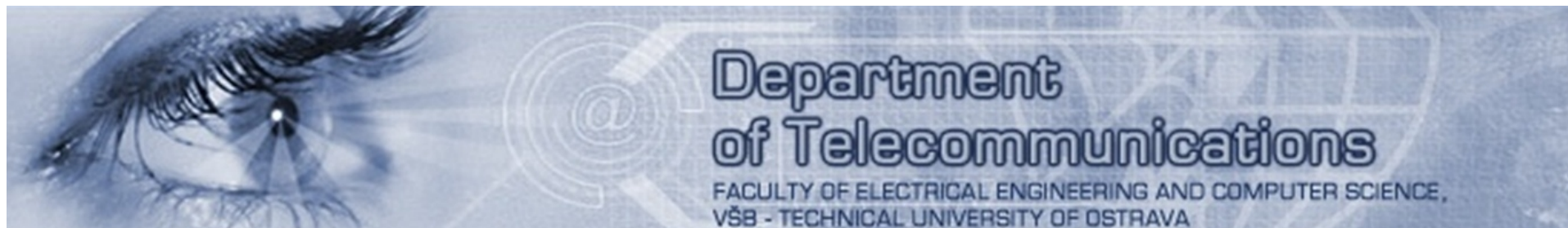
→ Logout

33.9%



Results

DATE	MAIN	S & M	DOS	RM	SPIT	OPERATION
(26) 2010-11-01 19:02:08	complete	complete	disabled	disabled	disabled	Result
(27) 2010-11-01 19:10:41	complete	complete	complete	complete	complete	Result
(28) 2010-11-01 19:27:59	complete	complete	disabled	disabled	disabled	Result
(31) 2010-11-03 12:37:50	aborted	aborted	aborted	aborted	aborted	<i>Aborted</i>
(32) 2010-11-03 12:42:36	complete	complete	complete	complete	complete	Result
(33) 2010-11-03 17:31:47	complete	disabled	disabled	disabled	disabled	Result
(34) 2010-11-03 17:33:39	complete	disabled	complete	complete	complete	Result
(35) 2010-11-03 17:34:40	complete	working	waiting	waiting	disabled	Abort



Děkuji Vám za pozornost

Q & A