



Security Risks in IP Telephony

Miroslav Vozňák - Filip Řezáč

<mailto:miroslav.voznak@vsb.cz>
<http://home1.vsb.cz/~voz29>

Outline

- ❑ **Risks and attacks in IP telephony – Introduction**
- ❑ **Design of call automat based on SIPp (SPITFILE)**
- ❑ **How to defend against SPIT ? (theoretical methods)**
- ❑ **Concept of AntiSPIT and its implementation into Asterisk**
- ❑ **Conclusion**

Security Risks in IP telephony

VoIP inherits all associated IP vulnerabilities

Most frequent risks and attacks associated with VoIP

Scanning and Enumerating

- trying to locate VoIP components

Denial of Service

- DoS and Distributed DoS attacks
- can exploit a flaw
- a flood attack

Theft of an account

- especially if the authentication mechanism is based on the MD5 algorithm
- 4,5 mil. USD losses incurred by Edwin Pena from New Jersey

CID Spoofing

- manipulation of Caller ID (CID)

Eavesdropping

- unauthorized interception of voice packets or RTP media streams,
- RTP vs. SRTP or ZRTP
- decoding of signalling messages

Call Hijacking & Redirection

- call intended for one user is redirected to another

```
ACK sip:7204@158.196.146.12;transport=udp SIP/2.0
Via: SIP/2.0/UDP 158.196.192.32:47998;branch=z9hG4bK-d8754z-429c98f2694bf547-1---d8754z-;rport
Max-Forwards: 70
To: <sip:7204@158.196.146.12>;tag=as06fb1164
From: "7002"<sip:7002@158.196.146.12>;tag=9197c599
Call-ID: NzkhNmM2YzZhZDk3NjhmMDUwYTJjZWY5ZWVkmzY4MWM.
CSeq: 3 ACK
Content-Length: 0
```

VoIP Spam

- Spam over Internet Telephony (SPIT)

SPAM over Internet telephony

Hype or reality ?

- Spam, one of the most extended attacks in the Internet environment
- Spam takes 80 - 90% of total attacks on the Internet.

SPIT will be a major threat in future

- the level of annoying factor is even greater than classical Spam,
- on an average we receive 5 Spam emails per day
- instead of unwanted emails we can imagine a machine generating many calls and replaying a message.

SPITFILE – SPIT tool

- we want to point out that SPIT is a real and a very dangerous risk
- based on *Sipp* generator
- Python was chosen for development of our SPIT application

two methods are used for dynamic cooperation with SIPp:

- the variables are sent to SIPp application to initialize voice call
- for the values, which have to be dynamically inserted into XML file, a new function was created (library `xml.dom.minidom`)
- *result* = **SPITFILE**

Our application can generate two types of attacks: Direct and Proxy

Direct mode

The screenshot shows the SPITFILE application window. The title bar reads "SPITFILE". Below the title bar is a menu bar with "File" and "Help". There are two tabs: "Direct" (selected) and "Proxy". The main area contains several input fields and controls:

- Remote IP Address:** A text input field.
- Protocol:** Two radio buttons, "UDP" (selected) and "TCP".
- Your ID:** A text input field.
- Local IP Address:** A text input field.
- Local Port:** A text input field.
- Insert Advert. Message (.pcap, g711μ):** A text input field with a "Browse..." button to its right.
- Advert. Message Duration (sec):** A text input field.
- Number of Calls:** A text input field.
- Interval Between Calls (sec):** A text input field.

At the bottom of the main area are two buttons: "SEND" and "ABORT".

At the very bottom of the window, a footer reads: "Filip Řezáč, Miroslav Vozňák 2009".

It generates SPIT via VoIP PBX (SIP Proxy) and the attack thereupon can run against anything that is available behind the Proxy (also ordinary phones ...)

Proxy mode

The screenshot shows the SPITFILE application window with the 'Proxy' tab selected. The interface includes a menu bar with 'File' and 'Help', and a tabbed interface with 'Direct' and 'Proxy' tabs. The main area contains several input fields and controls:

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

At the bottom of the window, there are two buttons: and . The footer text reads: Filip Řezáč, Miroslav Vozňák 2009.

How can one defend against such a type of attacks?

** methods stated below are not ideas of authors*

Buddylist/ Whitelist

Every subscriber has a list of subscribers. Those who are not on the list cannot initiate a call.

Blacklist

This is a reversed whitelist.

Statistical blacklist

Telephone providers carry out different analyses to create a spammer list.

Voice menu interaction

Before the caller is actually put through to the called subscriber, the caller is directed to the voice menu where he is asked to enter a numeric code (e.g. 123*) to be able to get through to the caller (Voice CAPTCHA?)

Greylist

This is a modified blacklist (whitelist) under which the phone returns the engaged line tone to the caller who is making the call for the first time. It increases a likelihood that the caller is a human person and not a SPIT bot.

Law aspects

It is mandatory not only to construct technical filtering mechanisms, but also to consider implications from telecommunication or privacy protection laws and regulation.

AntiSPIT tool

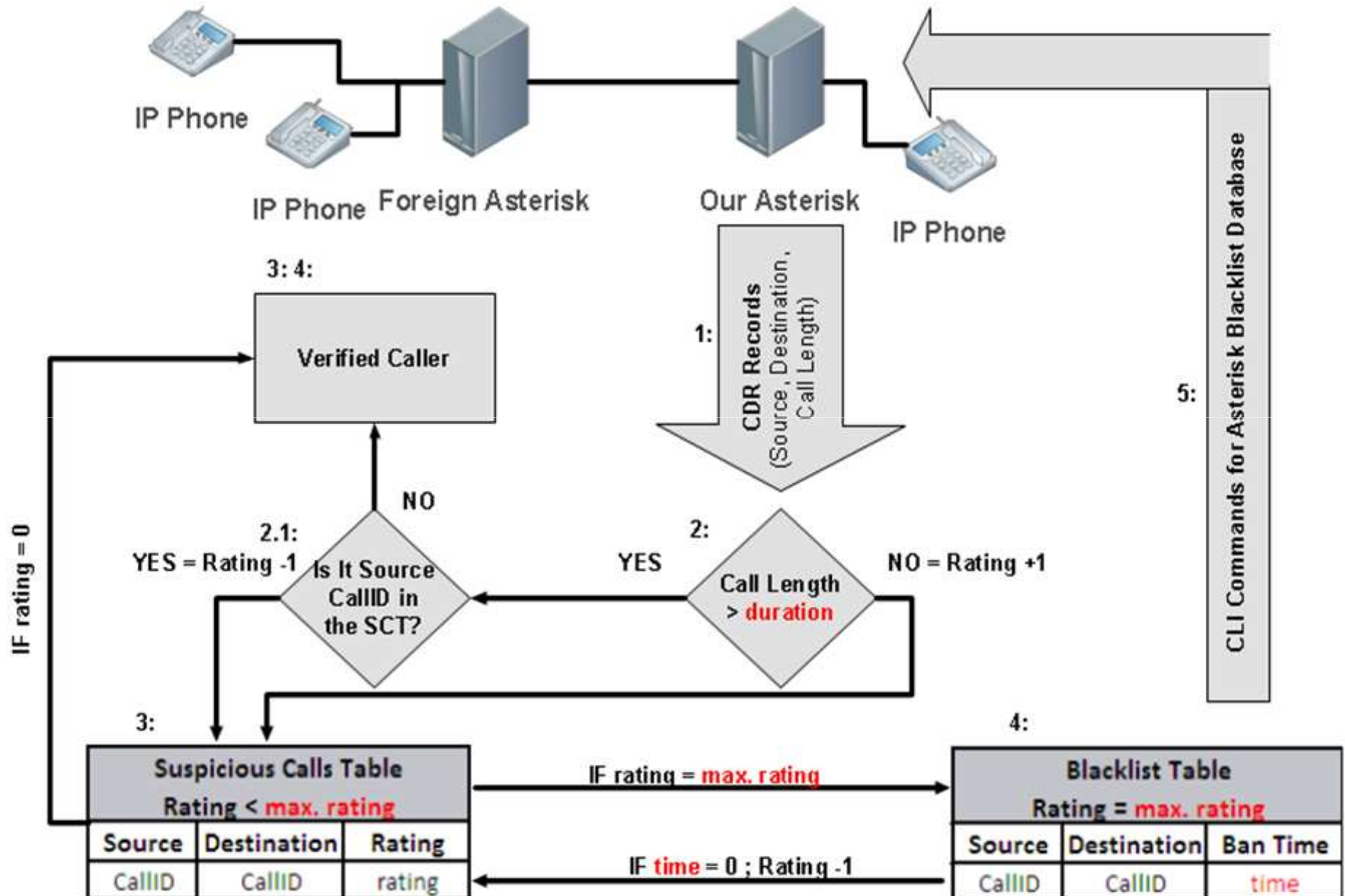
Motivation

- to minimize SPIT

Main ideas

- *Statistical Blacklist* method without participation of called party
- based on human behaviour
- CDR, we can analyze CDR's and sign suspicious calls
- Rating factor in suspicious calls table
- life span of records in Blacklist

AntiSPIT and its implementation into Asterisk



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

AntiSPIT

Logout

Menu

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

Settings

SYSTEM

System version: **v1.0b**

SETTINGS

Call Duration

(If the call duration is less than this level, the caller obtains the status of suspicious caller)

s

1. level BAN time

(How many hours will be the caller blocked)

h

2. level BAN time

(How many hours will be the caller blocked)

h

3. level BAN time

(How many hours will be the caller blocked)

h

Max. rating

(Limit value for Blacklist)



Save

CDR FILE PATH

CDR file full path

Save

Suspicious Calls Table

AntiSPIT System

AntiSPIT

Logout

Menu

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

Suspicious Calls Table

SOURCE	DESTINATION	CALL TIME	RATING	NEW RATING
7001	7002	20.8. 2009 12:05	2	<input type="text" value="2"/> Remove
7003	7008	21.8. 2009 15:27	1	<input type="text" value="1"/> Remove
7006	7009	22.8. 2009 09:25	3	<input type="text" value="3"/> Remove

SYSTEM

System version: **v1.0b**

Blacklist

The screenshot displays the AntiSPIT System web interface. At the top, there is a header with the text "AntiSPIT System" and two buttons: "AntiSPIT" and "Logout". On the left side, there is a "Menu" section with a green header and a list of navigation options: "Home", "Settings", "Suspicious Calls Table", "Blacklist Table", and "Change Password". The main content area is titled "Blacklist Table" and contains a table with the following data:

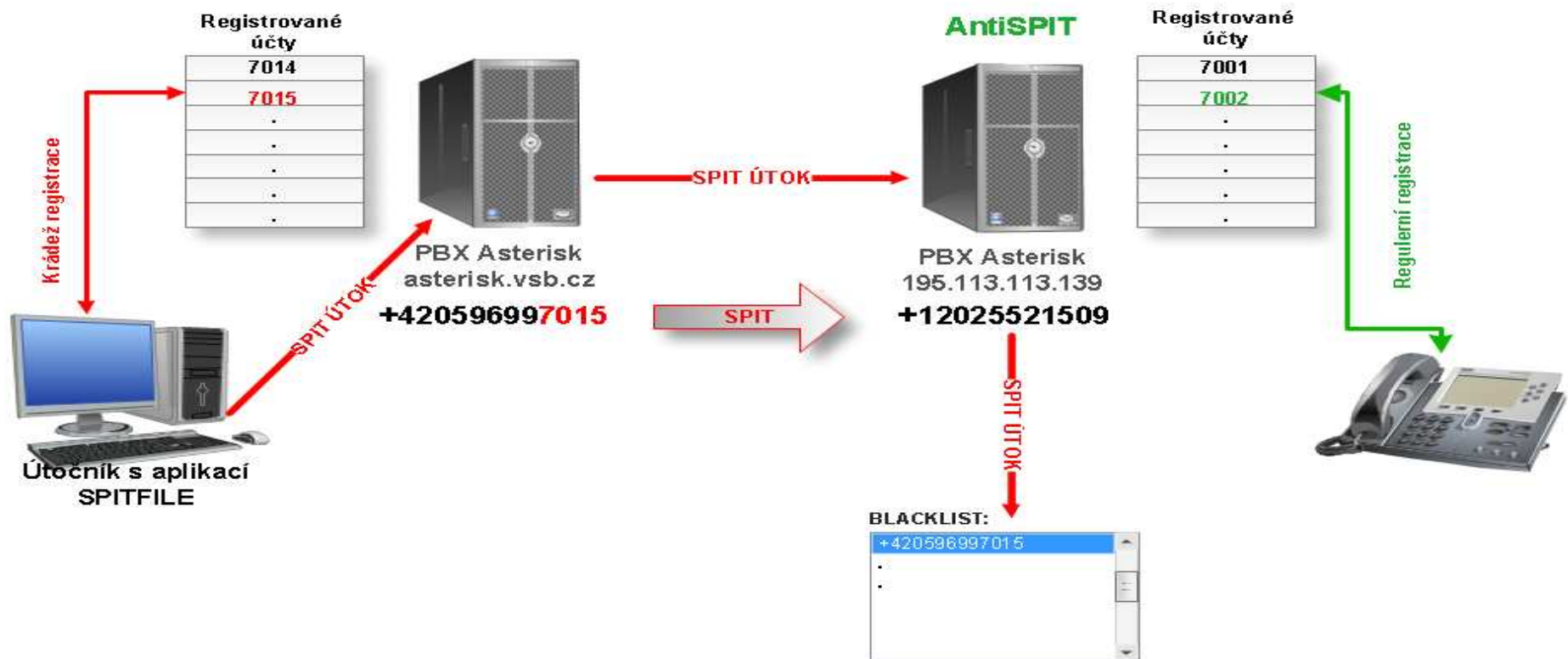
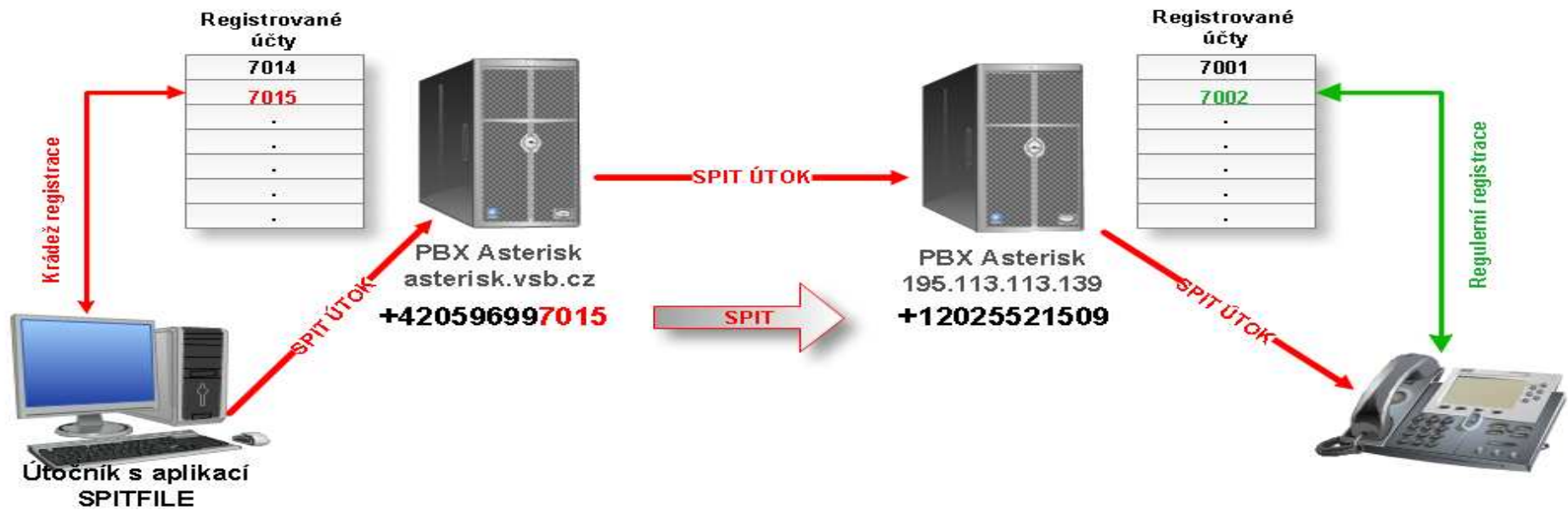
SOURCE	DESTINATION	CALL TIME	BAN	RATING	UNBAN
7006	7009	22.8. 2009 09:25	20.9. 2009 12:05	5	<input type="button" value="UnBAN NOW"/>

On the right side of the interface, there is a "SYSTEM" section with the text "System version: v1.0b".

Kde stáhnout AntiSPIT?

<https://sip.cesnet.cz/>

- v sekci Asterisk



Conclusion

Fortunately, most of telephone calls are charged which functions as a brake but we cannot not rely on it.

SPIT is a threat hanging like the sword of Damocles over the telephony world. Our presentation proves that it is not a mere speculation but a reality !

VOZŇÁK,M.,ŘEZÁČ,F.,RŮŽIČKA,J. *Spam over Internet Telephony with SPITFILE*. Poster at TERENA Networking Conference 2009. Malaga, 9-11.6.2009

VOZŇÁK,M. *Security and Quality of IP Telephony*. Lecture at University of Milan.UNIMI, Italy, 29.6.2009

VOZŇÁK,M.,ŘEZÁČ,F. *Implementation of SPAM over Internet telephony and a defence against this attack*. Publisher: Assisztencia Szervező Kft. Budapest, 32nd International Conference TSP , August 26th-27th 2009, Dunakiliti, Hungary, ISBN 978-963-06-7716-5

VOZŇÁK,M.,ŘEZÁČ,F. *SPAM over Internet Telephony*. Czech Technical University in Prague: 11th International Conference RTT 2009, September 2-4, 2009, Prague, ISBN 978-80-01-04410-0

VOZŇÁK,M.,ŘEZÁČ,F. *ANTISPIT a jeho implementace do Asterisku*. v přípravě na Konferenci Open-source řešení v sítích , 29.10.2009, SU OPF Karviná

**Děkuji Vám za
pozornost**

Dotazy?