ANTISPIT a jeho implementace do Asterisku

Miroslav Vozňák – Filip Řezáč
VŠB - Technical University of Ostrava
Department of Telecommunications
Faculty of Electrical Engineering and Computer Science
17. listopadu 15, 708 33 Ostrava – Poruba

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

Osnova příspěvku

- Rizika a útoky v IP telefonii
- Návrh a realizace volacího automatu (SPITFILE)
- SPITFILE - Direct a Proxy režim
- Jak bojovat proti SPIT ?
- Koncept AntiSPIT a jeho implementace do Asterisku
- Závěr

Rizika a útoky v IP telefonii

Denial of Service

- DoS a DDoS útoky
- útočník se snaží vyřadit službu z provozu
- využitím implementační chyby
- zahlcením

Krádež účtu

- riziko je vysoké u nešifrované komunikace
- HTTP Digest v SIPu, používá hashovací funkci (implementace MD5 – sipcrack)
- TLS – krádež samotného účtu odposlechem prakticky nemožná (jedině i se zařízením)
- následné zneužití účtu ke generování volání

4,5 mil. USD –Edwin Pena (tzv. VoIP bandita z New Jersey)

CID Spoofing

- manipulace s ID (CID)

Odposlech

- neautorizovaný odposlech dekódováním RTP
- při použití SRTP těžce proveditelné a se ZRTP prakticky neproveditelné

Call Hijacking & Redirection

- teoreticky možné (modifikace obsahu v SDP, re-INVITE)

VoIP Spam

- Spam over Internet Telephony (SPIT)

SPAM over Internet telephony
Hype or reality ?

- Spam, jeden z nerozšířenějších útoků v Internetu
- Spam představuje 80 - 90% celkových útoků

SPIT svým potenciálem představuje významnou hrozbu

- úroveň obtěžování je značně vyšší než u klasického spamu
- průměrně dostáváme 5 spamů denně
- namísto nechtěných emailů – automat generující volání a přehrávající zprávu

SPITFILE – SPIT nástroj

motivace

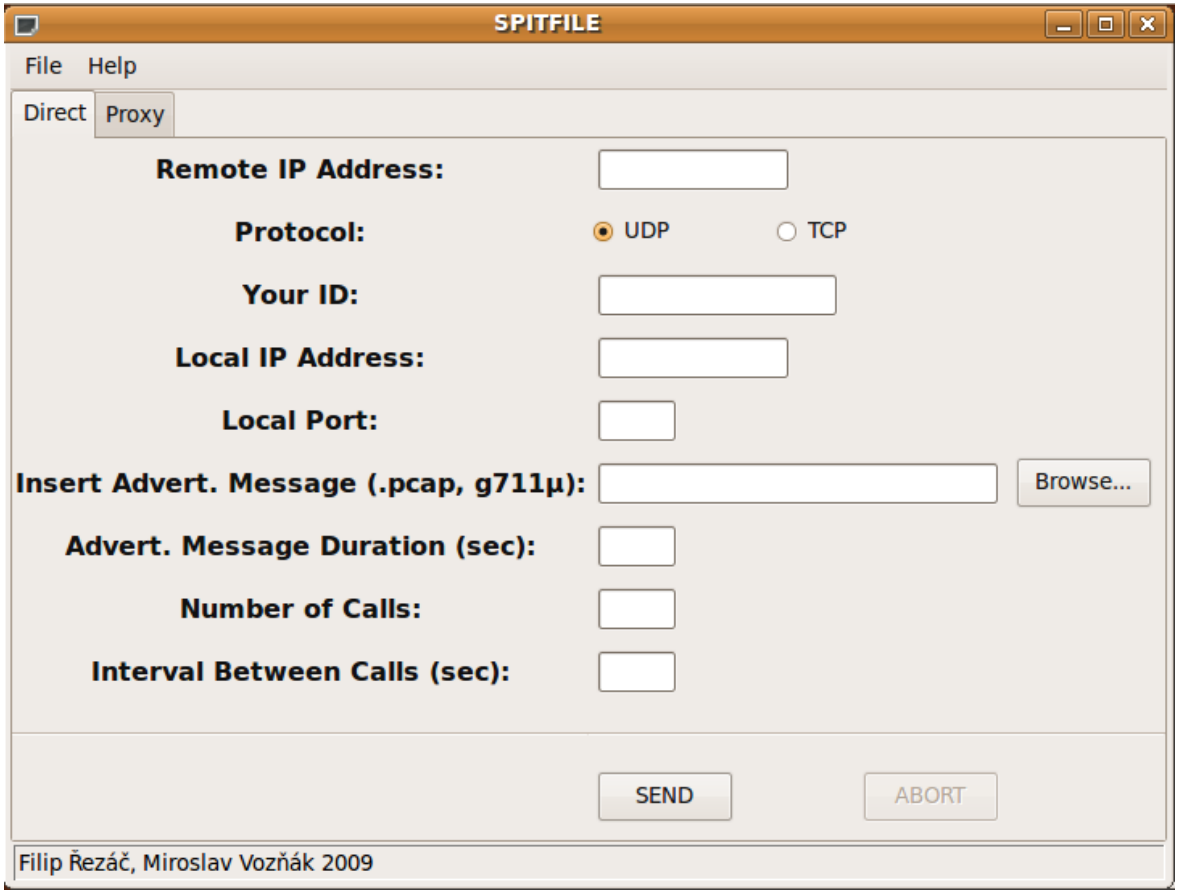
- ukázat, že SPIT představuje značnou a reálnou hrozbu

charakteristika SPITFILE

- jednoduchost použití
- využití generátoru Sipp
- vývojové prostředí aplikace – Python, využití wxPython GUI
- dvě metody použité pro spolupráci se Sipp: přímé použití proměnných jako parametry spuštění Sipp a nepřímé použití hodnot k vygenerování XML souborů s připravenými scénáři (knihovna xml.dom.minidom)
- vyžaduje Python≥v2.6 ,Sipp≥v2.1, Python-wxgtk≥v2.6

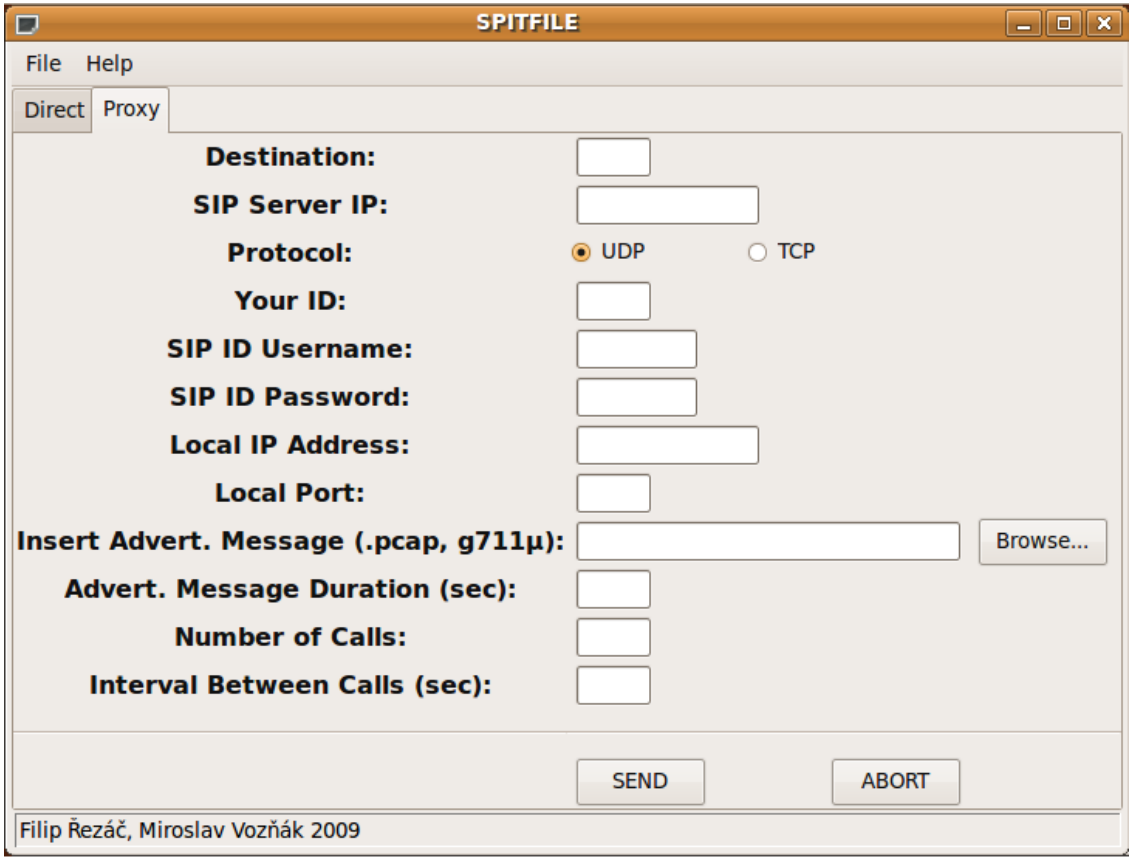
- umožňuje dva typy režimů pro SPIT : Direct a Proxy

Direct mode



Proxy mode

• generuje SPIT přes SIP Proxy, tzn. potencionálním cílem může být cokoliv dosažitelné přes SIP Proxy (včetně pevných linek či mobilních telefonů)



Jak se můžeme bránit ?

** níže uvedené metody nejsou nápadem autorů příspěvku*

Buddylist/ Whitelist
Každý má list účastníků, kteří se mohou dovolat. Kdo není na listu, tak se nedovolá. Listy se mohou sdílet - net of trust.

Blacklist
Reverzní Whitelist, volaný si sám list spravuje anebo participuje na jeho správě.

Statistical blacklist
Poskytovatel sám provádí analýzy za účelem odhalení spammera, není nutná participace volaného, vše funguje automaticky a existuje i možnost korekce na listu.

Voice menu interaction

Volající je vyzván k vložení kódu či prochází hlasovým menu a poté je spojen. Tím se snižuje riziko, že volající je stroj (to je diskutabilní – nepočítá s automatickým rozpoznáváním hlasu).

Greylist

Modifikovaný blacklist/whitelist, poprvé volající dostane obsazovací tón a podruhé se dovolá, tím se opět snižuje riziko, že volající je SPIT bot (opět diskutabilní, neboť metoda je postavena na úpřímné snaze se dovolat).

Law aspects

Vhodný doplněk technických mechanizmů, potencionální útočník by si měl uvědomit právní důsledky svého počínání.

AntiSPIT - tool

hlavní myšlenky

• použití metody *Statistical Blacklist* , nebudeme vyžadovat participaci volaného, systém musí fungovat autonomně, ale s možností do něj zasáhnout

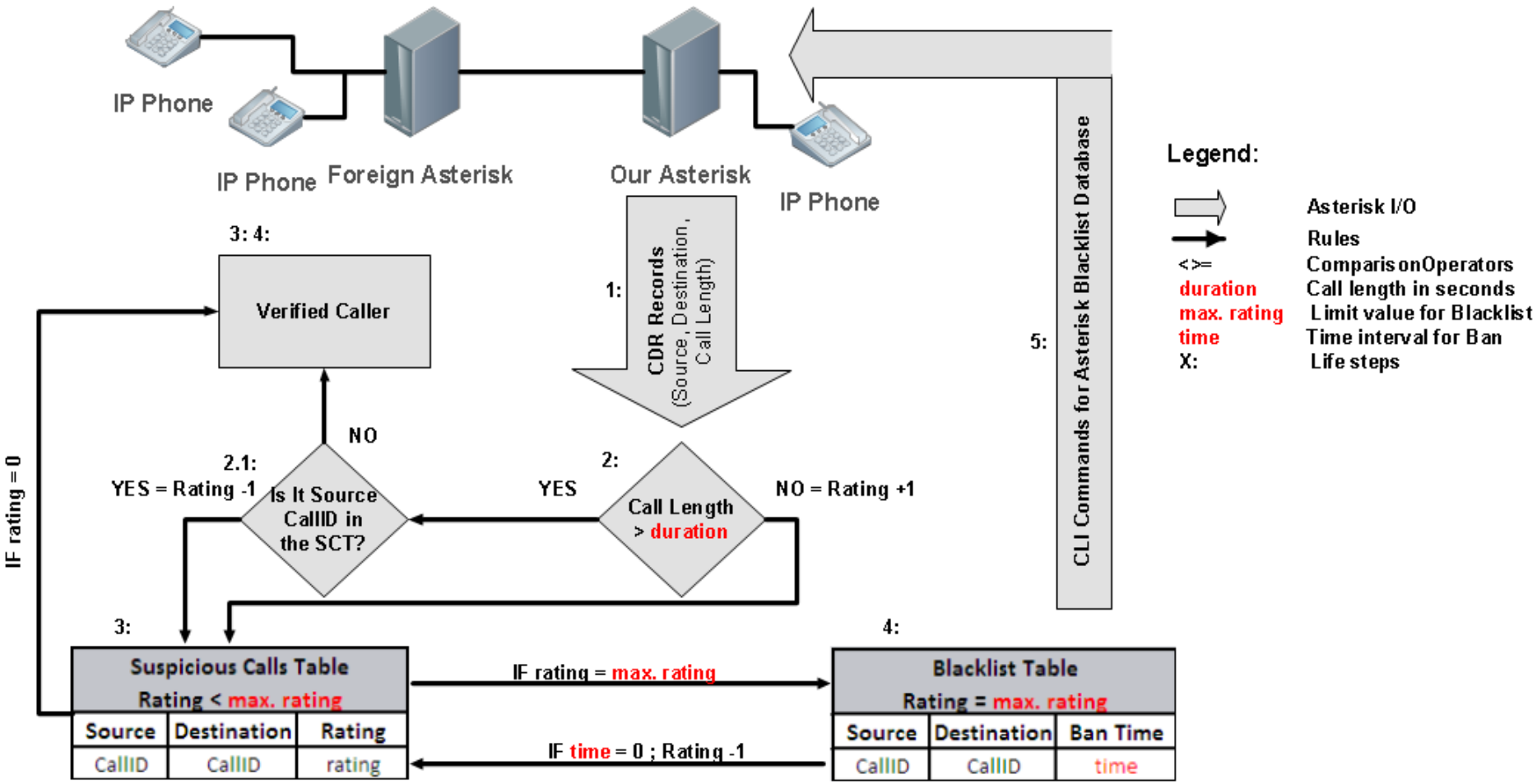
• využití vlastnosti přirozenosti lidského chování (pokud mne někdo obtěžuje = reakce)

• CDR (každá ústředna generuje CDR), můžeme záznamy analyzovat a označovat podezřelá volání

• recidivita chování rychlého ukončení spojení způsobuje navýšení hodnoty faktoru podezření (Rating factor), ale je možné i jeho snížení delším hovorem

• při překročení limitní hodnoty faktoru podezření dojde k záznamu do Blacklistu, ten je časově omezen (BanTime) a zpět se vrátí do tabulky podezřelých volání, recidivita = navýšení BanTime

AntiSPIT – implementace pro Asterisk



AntiSPIT System

AntiSPIT | Logout

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 obtaines 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**

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	2 Remove
7003	7008	21.8. 2009 15:27	1	1 Remove
7006	7009	22.8. 2009 09:25	3	3 Remove

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

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**

ZÁVĚR

SPITFILE a AntiSPIT jsou postaveny na open-source nástrojích

- jsou funkční a odzkoušeny na katedře telekomunikační techniky FEI VŠB-TUO
- pro rozsáhlejší ověřovací experiment je úskalím najít vhodnou množinu testerů
- většina telefonních hovorů je zpoplatněna (naštěstí brzda pro SPIT)
- SPIT je reálnou hrozbou a je potřebné být připraven
- věříme, že námi provedný aplikovaný výzkum najde reálné využití a bude přínosem do oblasti obrany proti SPIT

PODĚKOVÁNÍ

Autoři děkují sdružení CESNET za podporu při vývoji aplikací SPITFILE a AntiSPIT, bez které by výše prezentovaný výstup aplikovaného výzkumu nevznikl.

Děkuji za pozornost

Q&A