VoIP podvody

poznatky o podvodných hovorech
do zahraničí a ochraně proti nim
s využitím SIP firewallu a SIP antifraudu

Konference CSNOG
28. a 29. května 2019, Brno

Ivo Fišer
30 let vývoje telefonního SW
(3 roky práce na antifraudu)

Co je telefonní podvod ?

- **Druhy:** zneužití služebních telefonů, odposlechy hovorů, obtěžující zlomyslná volání (stalking), falešné telefonní karty, účelová inzerce s kontakty na prémiová čísla, prodej uměle generované terminace, falšování tel. čísla volajícího, přetížení tel. systémů (TDoS), manipulace s výnosy mezi operátory (ekonomické i daňové podvody), napojení na cizí tel. vedení, podvodné napojení do fixní tel. sítě nebo provoz velké GSM brány, podvodné prozvánění, podvodné hovory do zahraničí nebo na domácí prémiová čísla, ... , ... , atd.

- **Motivace:** kriminální skrytí identity, psychologické pohnutky (dokázat to), bezplatné vlastní hovory, úspora výdajů za nákup hovorů, finanční profit z telefonních podvodů

- **Pachatelé:** obchodně a technicky zdatní telefonní operátoři za případné pomoci „externistů“ (pracovníci oběti, ruští či asijští pracovníci, studenti IT, ...)

Podvodné hovory do zahraničí

příklady možné škody při 5 současných hovorech

cílová tel. síť	sazba	škoda za 1 hod	škoda za 1 den
Monaco KFOR	9 Kč/min	2.700,- Kč	64.800,- Kč
Lithuania special	12 Kč/min	3.600,- Kč	86.400,- Kč
Western Samoa	16 Kč/min	4.800,- Kč	115.200,- Kč
Kuba	19 Kč/min	5.700,- Kč	136.800,- Kč
St. Helena	32 Kč/min	9.600,- Kč	230.400,- Kč
Falkland Islands	33 Kč/min	9.900,- Kč	237.600,- Kč
Togo	35 Kč/min	10.500,- Kč	252.000,- Kč
Iridium satellite	125 Kč/min	37.500,- Kč	900.000,- Kč

Škody: v roce 2010 v ČR min. 21 mil. Kč (dle ČTÚ),
celosvětově údajně miliardy USD za rok (dle CFCA)

Postup napadení SIP ústředny

- vyhledání SIP zařízení (tel. ústředny)
- vyhledání SIP účtu (tel. čísla volajícího)
- zjištění hesla SIP účtu (typicky MD5)
- zjištění prefixu pro mezinárodní hovory
- zjištění cílové země (tel. čísla volaného)
- vlastní realizace podvodných hovorů
- inkaso výnosů od předchozího operátora,
  který na podvodu také profituje (svou marží),
  ... , ... , atd. (až po oběť, která to vše zaplatí)

(obtížně postižitelná mezinárodní kriminalita)

Vyhledávání SIP zařízení

- téměř výhradně pomocí SIP žádosti OPTIONS (výjimečně REGISTER či INVITE), očekávána je jakákoli SIP odpověď
- na portu 5060 přišel 1. pokus do 13 min (podobně na jiných IP)
- za období 120 dnů bylo na portu 5060 přijato > 10.000 pokusů
- registrovány byly taky pokusy na portech 5010, 5020, 5030, 5040, 5045, 5050, 5055, 5065, 5070, 5075, 5080, 5090, 5100, 5200, 5300, 5400, 5500, 5600, 5800, 5900
- na portech jiných než 5060 přišel 1. pokus do 1 hod až 85 dnů
- zdrojem pokusů bylo 930 různých IP adres s 204 různými netnames (Palestina, USA, Netherlands, France, Russia, ...)
- položka User-Agent obsahovala převážně „friendly-scanner“ a v display-name převažoval „sipvicious“, obojí ukazuje na časté používání SIP scanneru **svmap** (ze skupiny SIPVicious)

(detekováno provozem pasivního SIP honeypotu)

Vyhledávání SIP účtu

- využívány SIP žádosti REGISTER a INVITE, očekávána je SIP odpověď 401 Unautorized nebo „ideálně“ 200 OK
- testována jsou tel. čísla přípojek 0..9, 00..99, 000..999, ..., ..., ale i různá jména SIP účtů: test, Test, admin, Admin1, abc, abc1001, user, user1, Bavaria, Bloger, biology, cracking, demo, demo1, higway, joker, Malta, St.Lucia, secret, ...
- následuje zjištění hesla SIP účtu „standardními“ metodami (slovník hesel, zadní vrátka, hrubá síla, otevřený účet, ...)

Vyhledání prefixu volby

- využívá výhradně SIP žádosti INVITE, je nutné pro přechod do mezinárodní sítě (v ČR 00), případně do veřejné sítě (typicky 0), případně PIN před tel. volbou, např.: 00, 000, 900, 800, 700, 8, 88 až 888888888 (dtto 7, 9), nebo různé obskurní řetězce obsahující číslice i znaky +, #, $, ~, /, *, ...

Vyhledání cíle VoIP podvodu

- využívá SIP žádosti INVITE (+ znalost čísla a hesla SIP účtu i znalost prefixu pro zahraniční volání) a očekává odpověď 180 Ringing, 183 Session Progress, 200 OK, ... apod.
- **po zablokování podvodu pachatel dále zkoušel hovory do těchto zemí:** Albánie, Ázerbájdžán, Bělorusko, Barma, Bulharsko, Burkina Faso, Burundi, Dominikánsko, Džibutsko, Ellipso (satelitní síť), Eritrea, Estonsko, Falklandy, Grenada, Gruzie, Guinea, Honduras, Chile, Irák, Jamajka, Keňa, Kiribati, Kongo, Komory, Kuba, Liberie, Lichtenštejnsko, Litva, Lotyšsko, Madagaskar, Moldávie, Niger, Norfolkské ostrovy, Polsko, Rakousko, Rumunsko, Rusko, San Marino, Severní Korea, Sierra Leone, Slovinsko, Somálsko, Středoafrická republika, Šalamounovy ostrovy: Španělsko, Tákžikistán, Togo, Tunisko, Ukrajina, Vanuatu, Zimbabwe

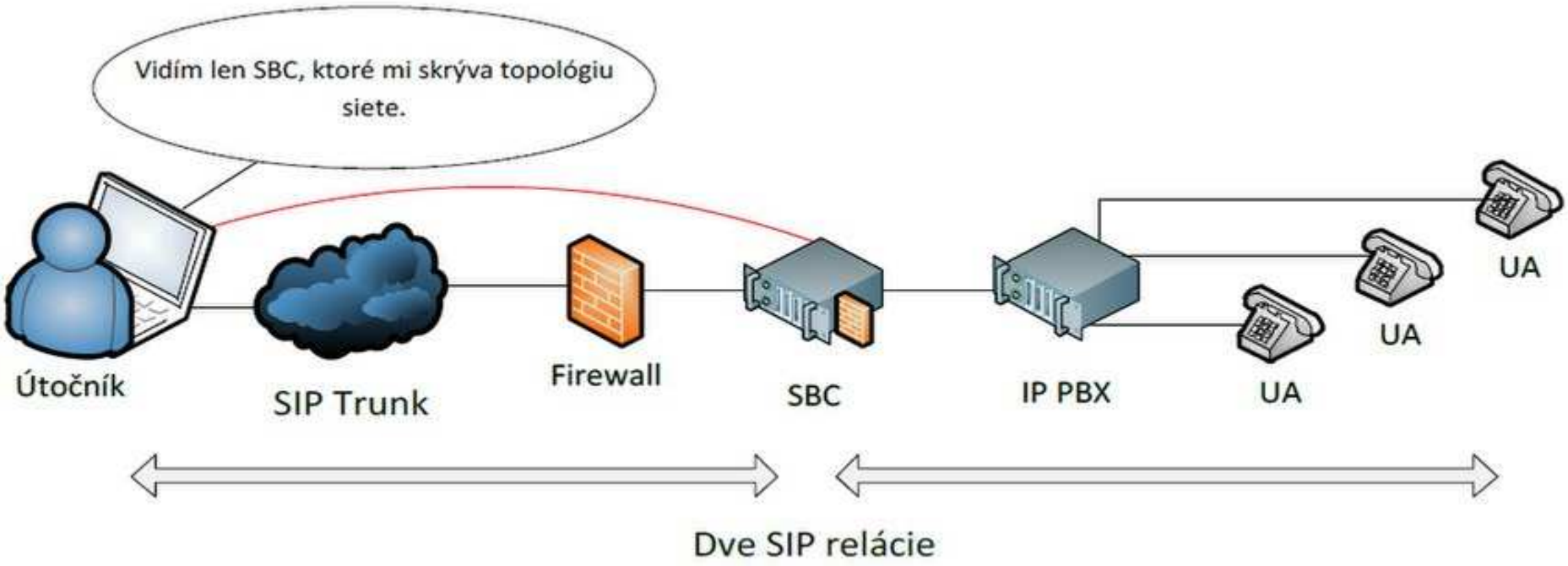
Konkrétní možnosti ochrany

- mechanická ochrana VoIP ústředen
- zabezpečená administrace VoIP ústředen
- umístění VoIP zařízení na neveřejných IP adresách
- umístění VoIP zařízení na nestandardních UDP portech
- ochrana VoIP svazků pomocí IP adresy protější strany
- ochrana stabilních IP telefonů pomocí jejich IP adresy
- silná hesla pro registraci IP telefonů a bran
- vložení umělé prodlevy do vyhodnocování hesla SIP účtu
- kontrola opakování špatných hesel s blokováním SIP účtu
- NEkonkrétní reakce na chybné SIP autentizace
- ochrana VoIP ústředny síťovým firewallem
- ochrana VoIP ústředny SIP firewallem a SIP antifraudem
- užívání zabezpečených verzí SIP a RTP protokolu

- užívání kreditního způsobu úhrady hovorného
- ochranný PIN před zahraničními hovory (nebo před všemi)
- blokování služby pro SIP telefony na zahraniční IP adrese
- blokování zahr. hovorů pro telefony, kde o ně není zájem
- utajení IP adres a názvů zařízení v SIP signálech
- blokování SIP žádostí přijatých z podvodných IP adres (*)
- blokování SIP žádostí obsahujících podvodné IP adresy (*)
- blokování SIP žádostí obsahujících zakázané názvy (*)
- povolení hovorů pouze do skutečně potřebných zemí (*)
- limit počtu souběžných hovorů do zahraničí (*)
- limit opakujících se podobných hovorů do zahraničí (*)
- blokování SIP žádostí majících znaky VoIP podvodů
- trvalý monitoring objemu a cílů zahraničních hovorů
- získávání zkušeností provozováním SIP honeypotů
- automatická nebo manuální kontrola CDR záznamů
- uzavření vhodné pojistné smlouvy

SIP firewall

(= SBC systém, Session Border Controller, hlasový firewall, ...)



doporučené pro ochranu všech vnějších SIP svazků
funguje jako B2BUA (= back to back user agent)

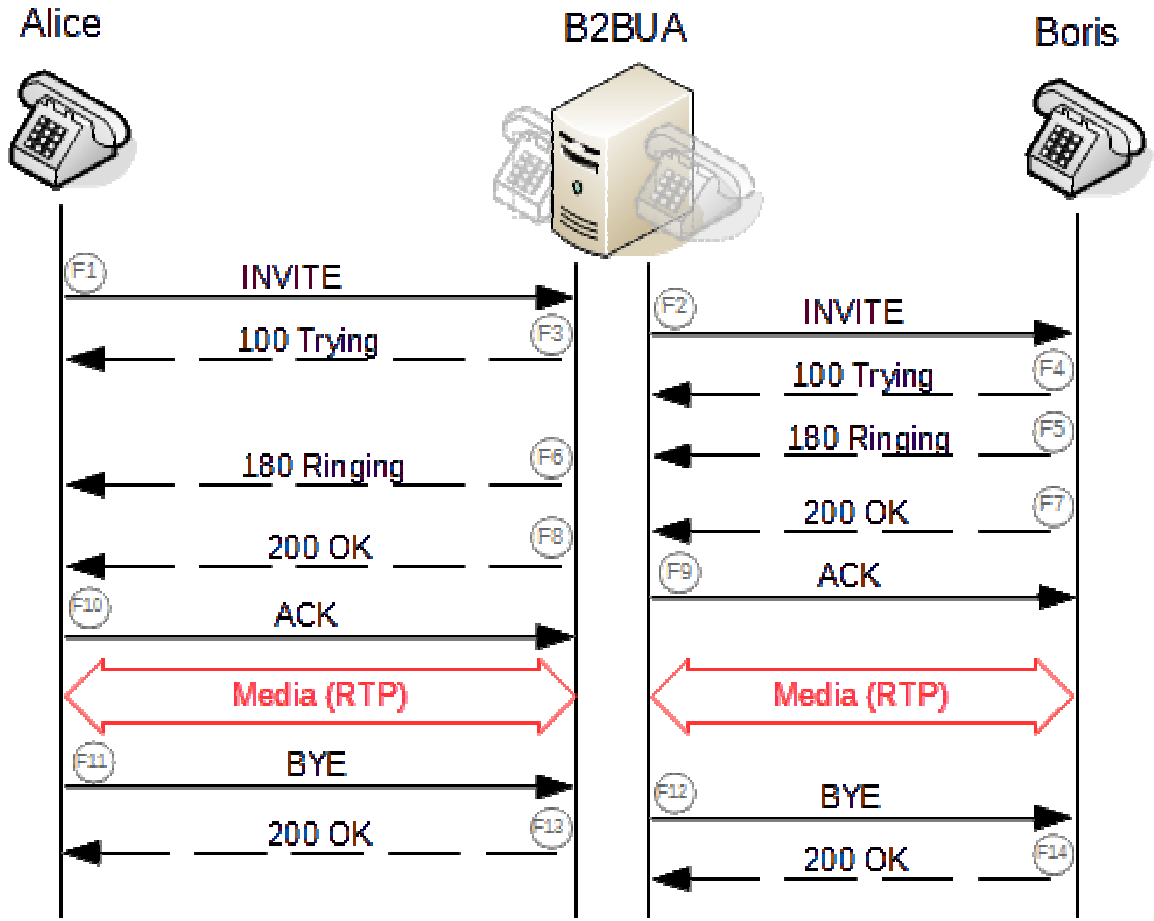
Citlivé údaje v SIP signálech

```
INVITE 602639883@217.101.29.108 SIP/2.0
Via: SIP/2.0/UDP 180.66.160.15:5060;branch=z9hG4-bK80fsx5sy805
Via: SIP/2.0/UDP 180.66.160.22:5060;branch=z9hG4-bK5eae145d
From: "505686611" <sip:505686611@180.66.160.5>;tag=as71c9dffdF3ws
To: „602639883" <sip:602639883@217.101.29.108>
Call-ID: dvScftN8-RK4eMsuT-S5nYiZBO-8GQMJK11-94Hv8n3w-t2cV
CSeq: 102 INVITE
User-Agent: Asterisk PBX 1.8.13.1 deb7u3
Max-Forwards: 30
Contact: <sip:505686611@180.66.160.15:5060>
Content-Type: application/sdp
Content-Length: 232

v=0
o=root 1147220652 1147220652 IN IP4 180.66.160.5
s=Asterisk PBX
c=IN IP4 180.66.160.21
t=0 0
m=audio 10610 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendrecv
```

Princip SIP firewallu

vzájemně skrývá IP adresy VoIP ústředen a
jména v položkách User-Agent, Server i SDP



zároveň může kontrolovat SIP žádosti INVITE a blokovat
nepovolené hovory do zahraničí (SIP antifraud), viz (*)

Zkušenosti s VoIP ochranou

u tranzitního telefonního operátora propojujícího
malé a střední VoIP operátory na ostatní telefonní sítě

- **I. fáze** – jen se zpětnou kontrolou volání (2010 až 2022)
  cca 8 až 12 podvodů ročně se škodou N x 100 tis. Kč/rok

- **II. fáze** – s omezením zahraničních hovorů závislým na
  denní době a na dnech volna či svátcích (2013 až 2017)
  cca 2 až 3 podvody ročně se škodou pod 100 tis. Kč/rok

- **III. fáze** – s využitím SIP firewallu + SIP antifraudu na
  vstupní i výstupní SIP svazky tranzitních VoIP ústředen
  (2018 až ...) prozatím žádný VoIP podvod a bez škod !!!

Shrnutí zkušeností

- telefonní podvody existovaly, existují a existovat budou, měnit se bude pouze jejich podoba
- neexistuje žádná zázračná metoda ochrany, proto je vždy potřebné kombinovat více způsobů vhodných pro danou operátorskou či pobočkovou SIP ústřednu
- všichni velcí operátoři používají SIP firewally a měli by je určitě mít taky VoIP operátoři všech velikostí i majitelé pobočkových ústředen
- stejně jako mají být počítače a servery chráněny antivirovým SW, měla by i každá VoIP ústředna být chráněna svým SIP antifraudem

Další zdroje informací

- 34 odkazů pod články **VoIP podvod**, **SIP firewall**, **SIP antifraud** a **SIP honeypot** publikovanými na *cs.wikipedie.org/wiki/VoIP_podvod (atd.)*

- 5 přednášek z konferencí **Teorie a praxe telefonie** dostupných na *ip-telefon.cz/archiv-prednasek.html* (viz roky 2014, 2012 a 2010)

- 4 přednášky ze semináře **Česká a moravská VoIP telefonie** dostupné na *ip-telefon.cz/archiv-prednasek.html*

- 2 přednášky ze semináře **Slovenská VoIP telefonie** dostupné na *ip-telefon.cz/archiv-prednasek.html*

Děkuji za pozornost

Dotazy, zkušenosti, připomínky, ... ?

Ivo Fišer
ivo.fiser@xphonet.cz

pracovník poskytovatele služby VoIP antifraud pro ochranu
proti drahým podvodným telefonním hovorům do zahraničí