

A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a magnifying glass resting on it. A blue vertical bar is overlaid on the left edge of this image.

DECT Hacking

Walter Sprenger



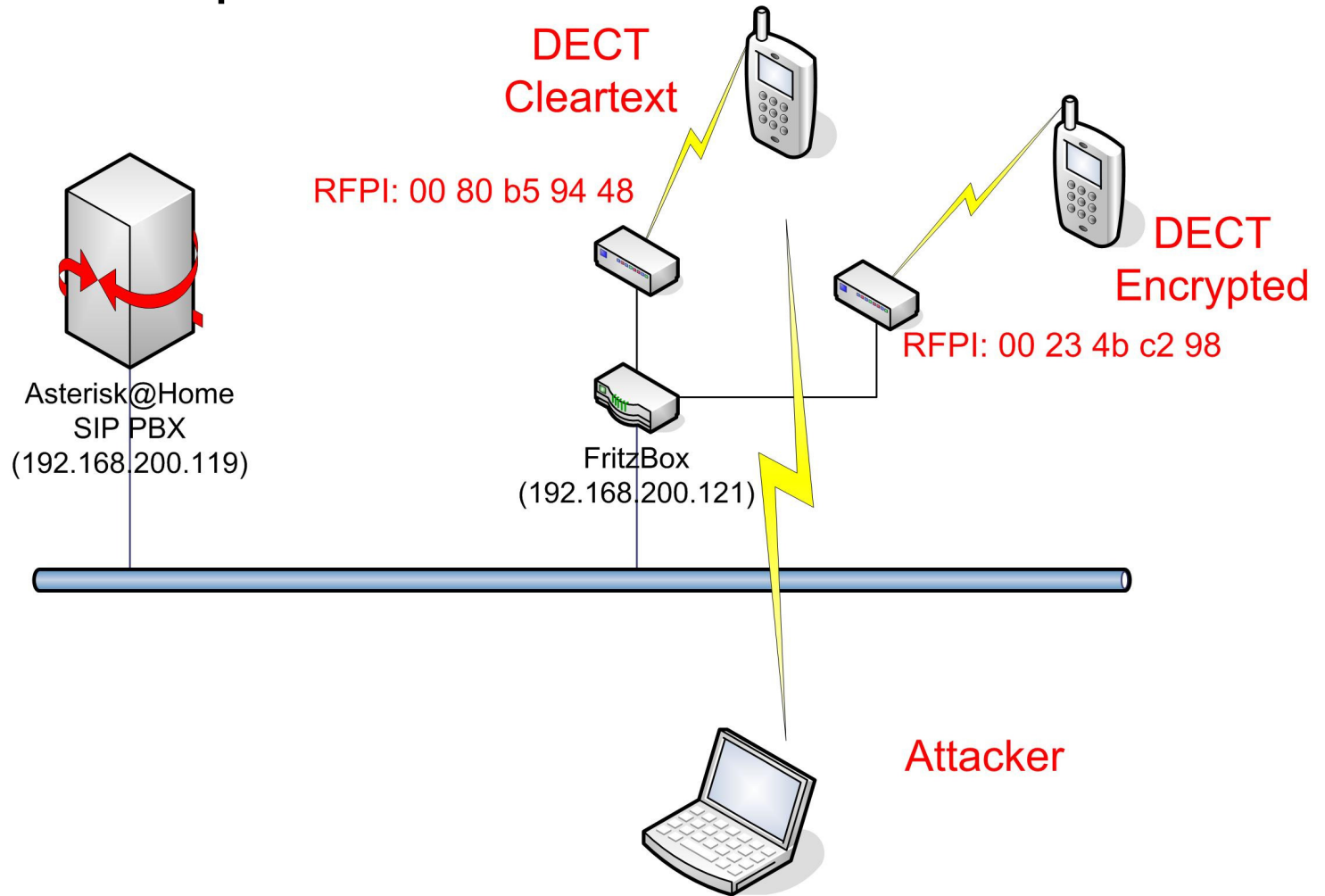
Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Introduction Wargame Case



Two DECT telephones



Hardware Requirements



Hardware

- ★ COM-ON-AIR PCMCIA Card (Typ 2 or 3)
- ★ Laptop with PCMCIA



Software

- ★ Linux
- ★ Tools from www.dedected.org

The logo for trac, featuring a red paw print icon to the left of the word "trac" in a bold, black, sans-serif font. Below the logo, the text "Integrated SCM & Project Management" is written in a smaller, black, sans-serif font.

COM-ON-AIR Linux Driver Project

To use the COM-ON-AIR PCMCIA card on Linux, we decided to v

To get the source checkout our svn repository:

```
svn co https://dedected.org/svn/trunk dedected
```

then see the corresponding README files

DECT Abbreviations



FP - Fix Part (Base Station)



PP - Portable Part (mobile phone)



RFPI: Radio Fixed Part Identity

- ◆ Address of Base Station
- ◆ Example: 00 80 b5 94 48

IPI: International Portable User Identity

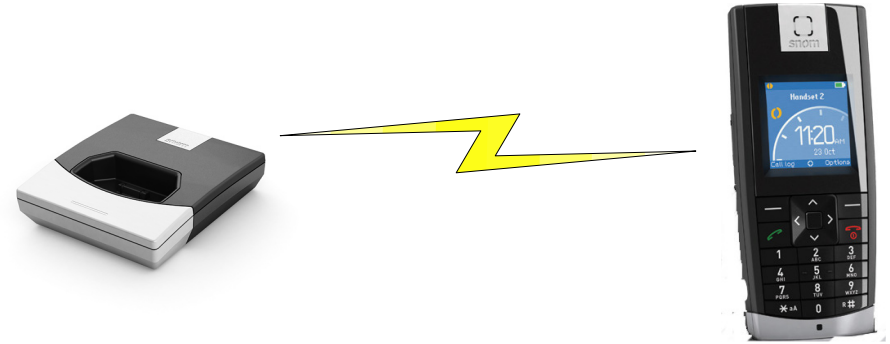
- ◆ Address of mobile phone
- ◆ Example: 11 22 33 44 55

Security Features



Encryption

- ★ Encryption of Voice Data
- ★ Encryption of Control Data



Authentication

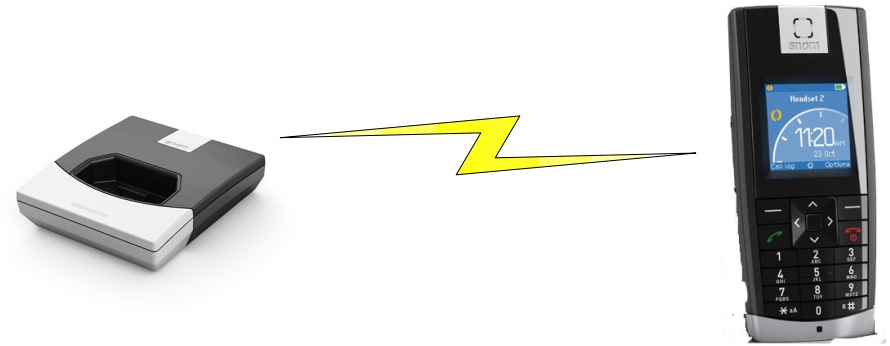
- ★ Base station authenticates mobile phone
 - ★ Prevents man in the middle attacks
 - ★ Prevents unauthorized usage of phone line
- ★ Mobile phone authenticates base station
 - ★ Prevents man in the middle

Problems identified by dedected.org



Encryption

- ✦ Only voice data encrypted
- ✦ No encryption at all



Authentication

- ✦ Base stations authenticates mobile phone
 - ✦ Mostly implemented
- ✦ Mobile phone identifies base station
 - ✦ Sometime implemented

Demo DECT Hacking



Capture DECT traffic

Convert captured files

Play wave files

Conclusion



Verify if your phone is listed as insecure on www.dedected.org

No possibility to update firmware known to Compass

Buy a new phone that supports encryption and mutual authentication or do not use DECT phones for confidential conversations

Questions

