

MITM on PSTN

novel methods for intercepting phone calls

Mg.sc.comp, Mg.phys. Kirils Solovjovs



- Work
 - Owner&Hacker at Possible Security, LV
 - RA, Institute of Electronics and Computer Science, LV
- Play
 - Destroyer of e-signatures
 - Author of RouterOS jailbreaks
- Talk
 - Hackfest, CCC, Hack in the Box, Nullcon, BalCCCon, Disobey, ...∞
 -  @k@chaos.social

What are we doing here today

- PSTN & MNs
- Social engineering
- Attack!
 - Simultaneous ring attack
 - Diversion attack
 - Interception tactic
 - Alteration tactic



What is PSTN

- Public switched telephone network
 - worldwide!
- Single global address space of phone numbers
- Old-school

How secure is PSTN 🤡

Feature	PSTN
Connectivity and Switching	Dedicated lines are required for circuit switching and transmission
Power Source	Hard wired telephone lines will remain active during a power outage
Emergency Services	911 calls will allow emergency responders to trace the exact location of the caller's source
Bandwidth	Reserved in advance, 64kbps, highly stable, dropped calls rare
Security	Highly secure with dedicated telephone lines
Soft Phones	Soft phones are unavailable
Integration	Does not support third party integrations

Source: versadial.com

CLIP

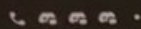
- Caller Line Identification Presentation



CLIP

- Caller Line Identification Presentation
- US also has CNAM
 - Caller Name Delivery
- CLIR = Caller Line Identification Restriction

11:14



H+ 48

Zvans no:

ret project empolyee

NUMBERS - 077 83 100 100

Atbildēt

Velciēt augšup, lai atbildētu



SS7

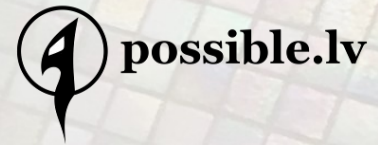
- Signalling System 7
 - set up and tear down of circuits (calls)
 - number translation
 - prepaid billing
 - diversion
 - etc.

Social engineering



Kirils Solovjovs · @k@chaos.social
<https://kirils.org>

MITM on PSTN
Hackfest, Quebec City, Canada



Mobile networks

- A5/1 broken
- No mutual authentication on Um
 - FakeBTS / IMSI catchers
- Part of PSTN

Tactic 1

Interception of phone calls

Attack 1

Simultaneous ring attack

Activities Linphone jūn 2 11:12

user@pstnclient: ~

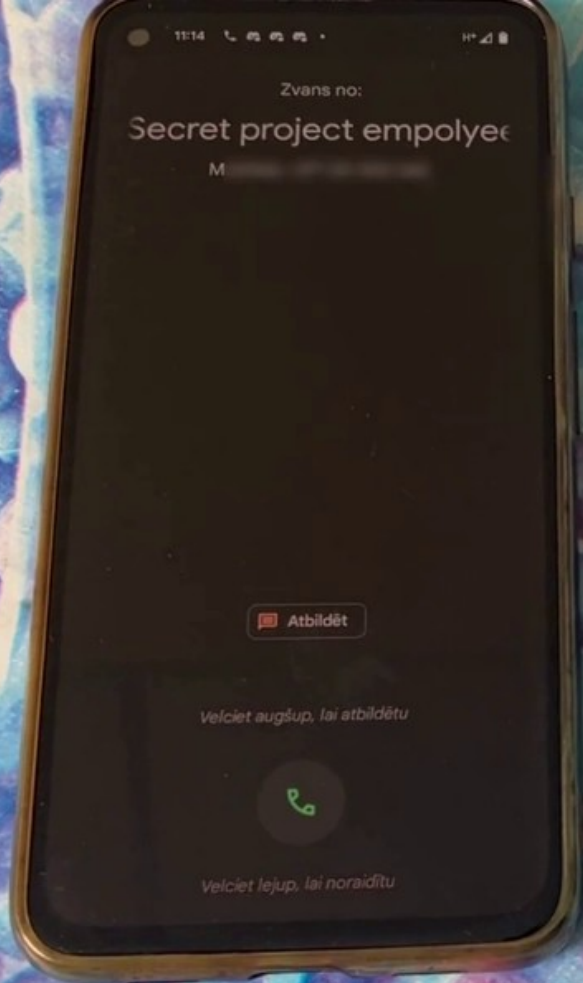
CHAT FEATURE IS UNAVAILABLE
This **functionality** and many more useful features are available with ZoiperS PRO

Audacity

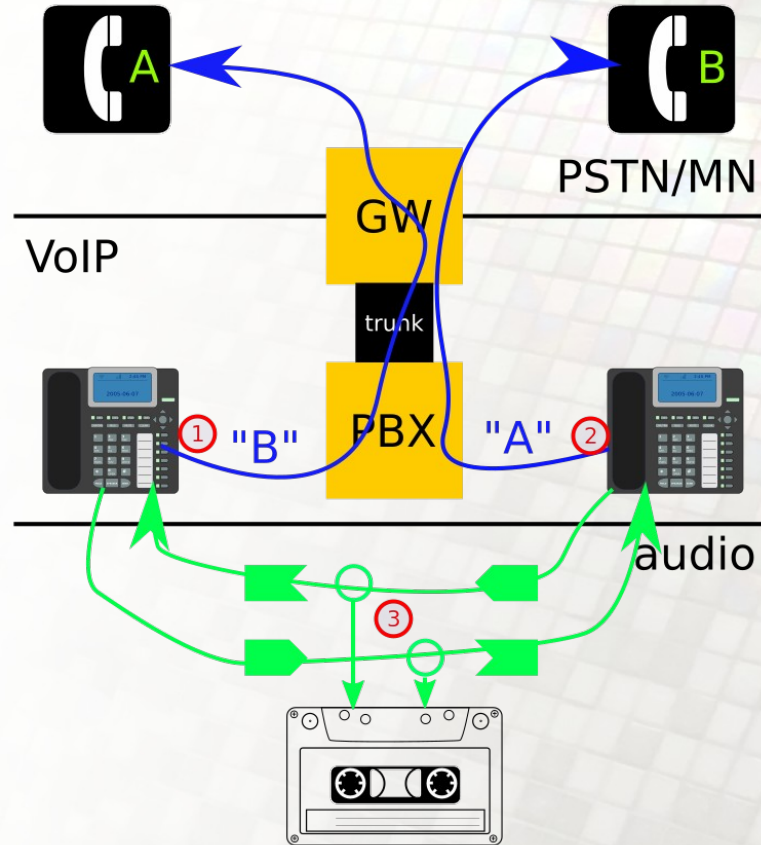
Analyze Help

Project Rate (Hz): 44100 Snap-To: Off Audio Position: 00 h 01 m 00,685 s Start and End of Selection: 00 h 00 m 00,000 s 00 h 00 m 00,000 s

Recording. Disk space remaining for recording: 0 hours and 45 minutes. Actual Rate: 44100

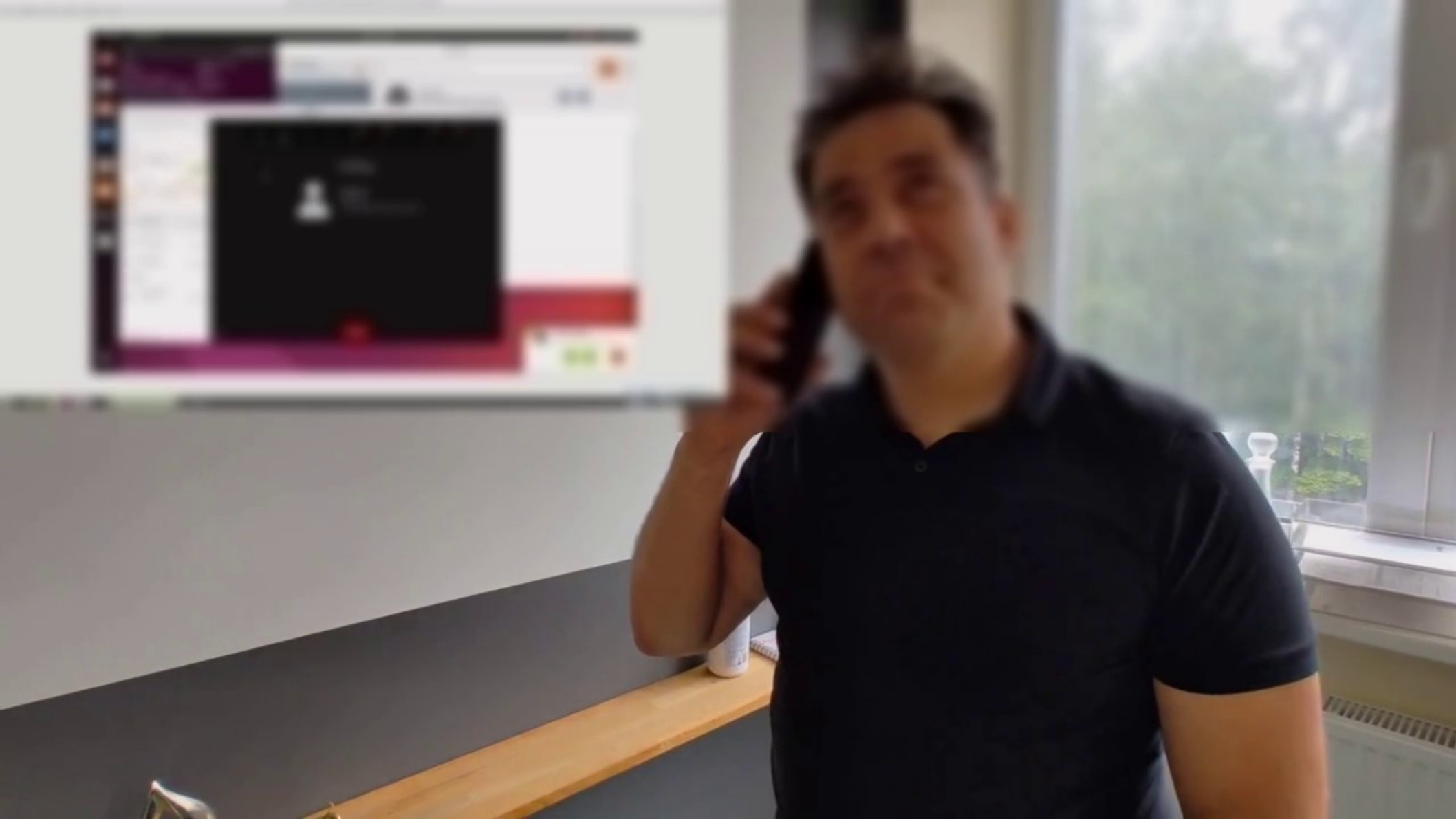


Simultaneous ring attack

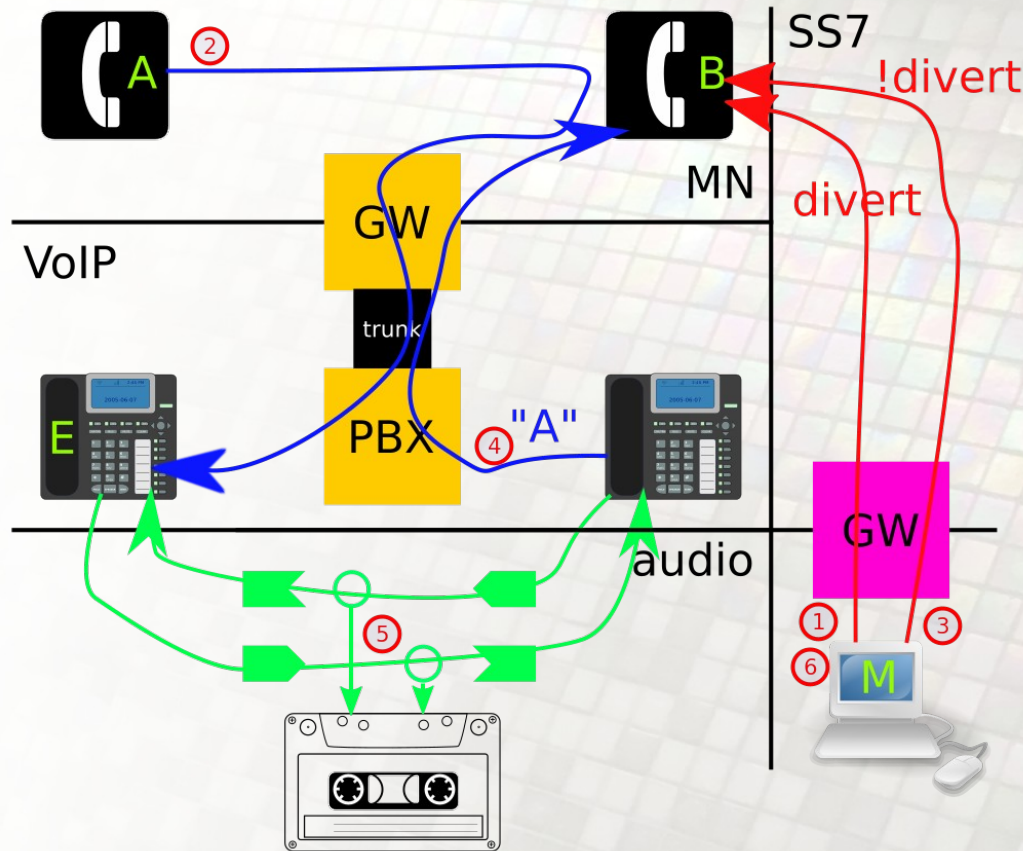


Attack 2

Diversion attack



Diversion attack



* can also be rerouted using e164.arpa and a host of other techniques

The diversion part (ENUM)

- RFC2916 / RFC6116 „E.164 number and DNS”
- (E.164) +351 220408000
- dig NAPTR 0.0.0.8.0.4.0.2.2.1.5.3.e164.arpa.

```
10 10 "u" "E2U+pstn:tel" "!^.*$!tel:15143939876!" .
```

- ~~• dig SRV _sip._udp.voip.up.pt~~
~~5 10 5060 sbcuporto.voip.up.pt.~~
- ~~• dig A sbcuporto.voip.up.pt. +short~~
~~193.137.59.178~~

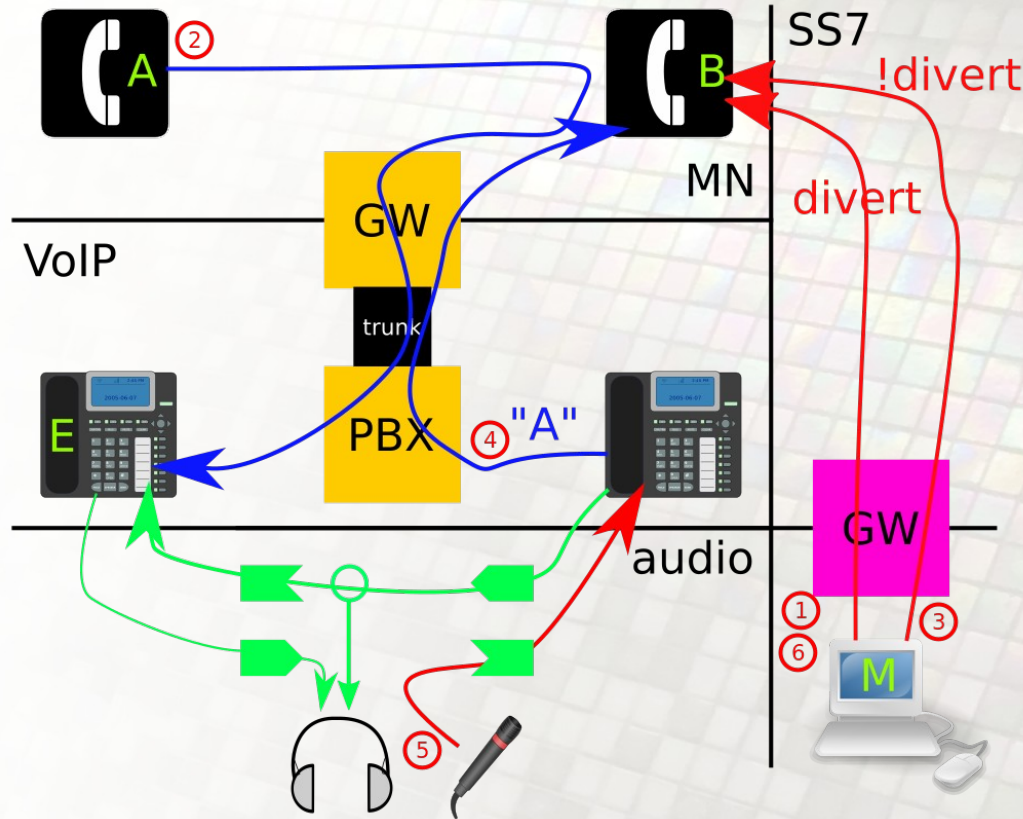
The diversion part (SocEng)

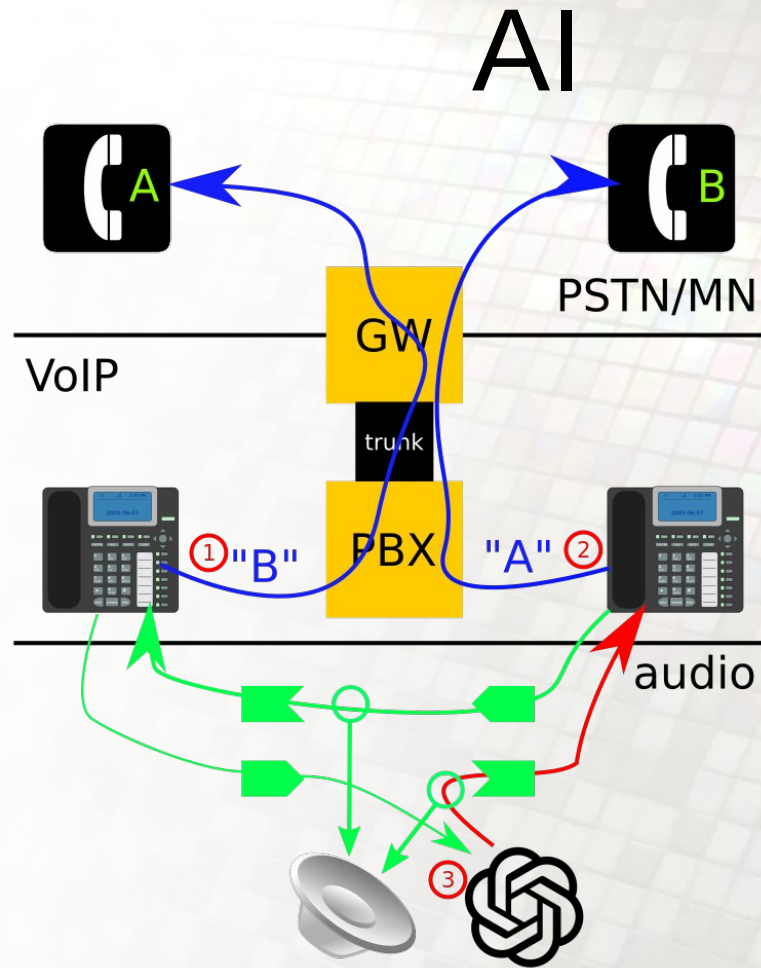
- Physical attacks
 - just take the phone and call *21*0015143939876#
- Vishing
 - Hello, this is Dog, please call *21*0015143939876# to get 1000 CAD
- Phishing
 - <http://eja.lv/3sp>

Tactic 2

Alteration of phone calls

Asynchronous substitution





Proposed solutions



- SS7 firewalls
- Verification of routed CLIP
- DNSSEC
- Encrypted comms



Thank you!

slides --> <https://kirils.org/>



@k@chaos.social

MITM on PSTN
Hackfest, Quebec City, Canada



INSTITUTE OF
ELECTRONICS AND
COMPUTER SCIENCE



possible.lv