MITM on PSTN

novel methods for intercepting phone calls

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

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, BalCCon, 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

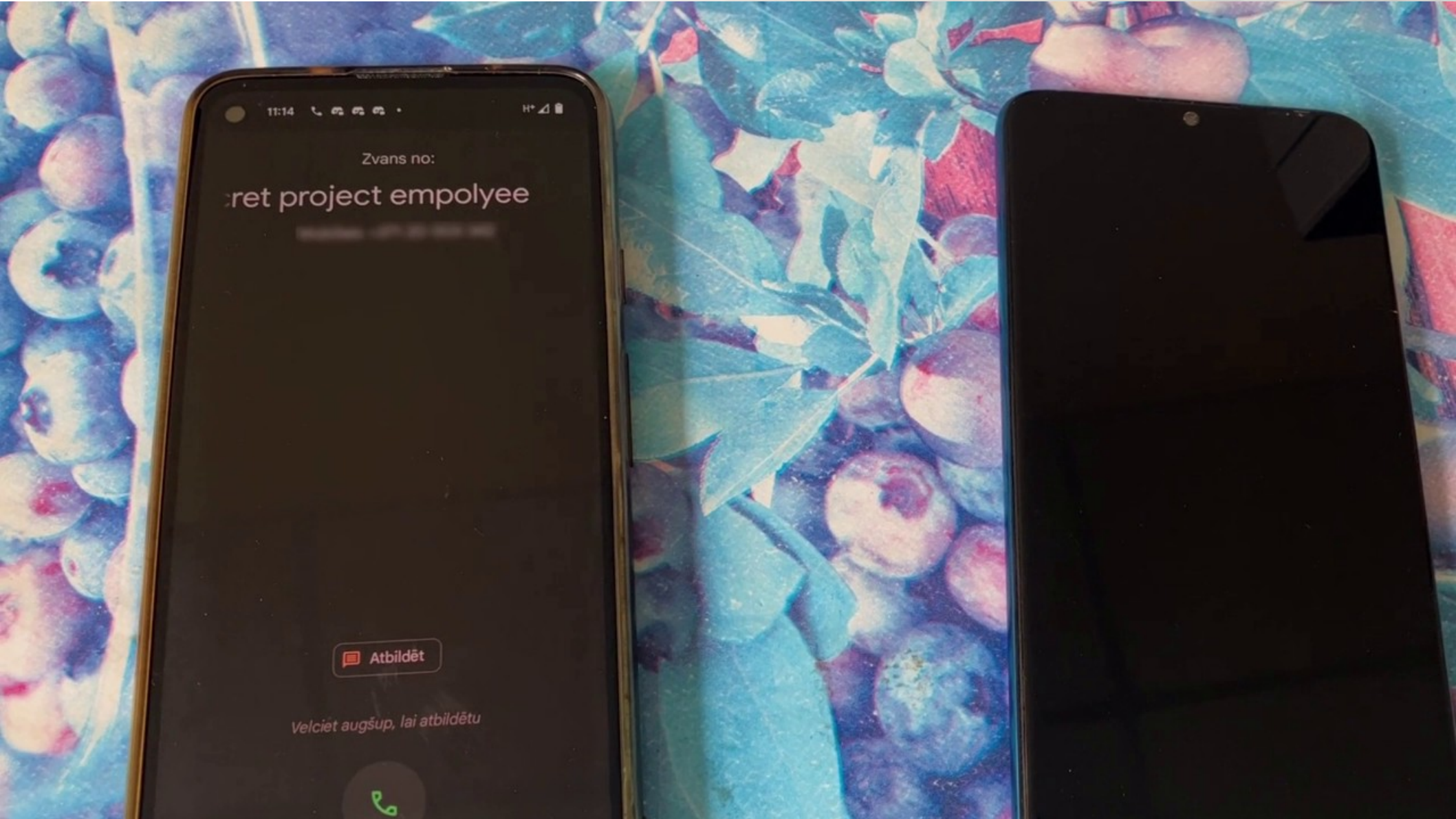
CLIP

- Caller Line Identification Presentation


10:55
S
Notiek zvanīšana...
polyee
Super Se
Cipartat.
Izslēgt
Skaļrunis
Vēl
John Doe
Message
Reminder

CLIP

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


11:14
Zvans no:
ret project empolyee
Atbildēt
Velciet 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
DefCamp, Bucharest, Romania

Mobile networks

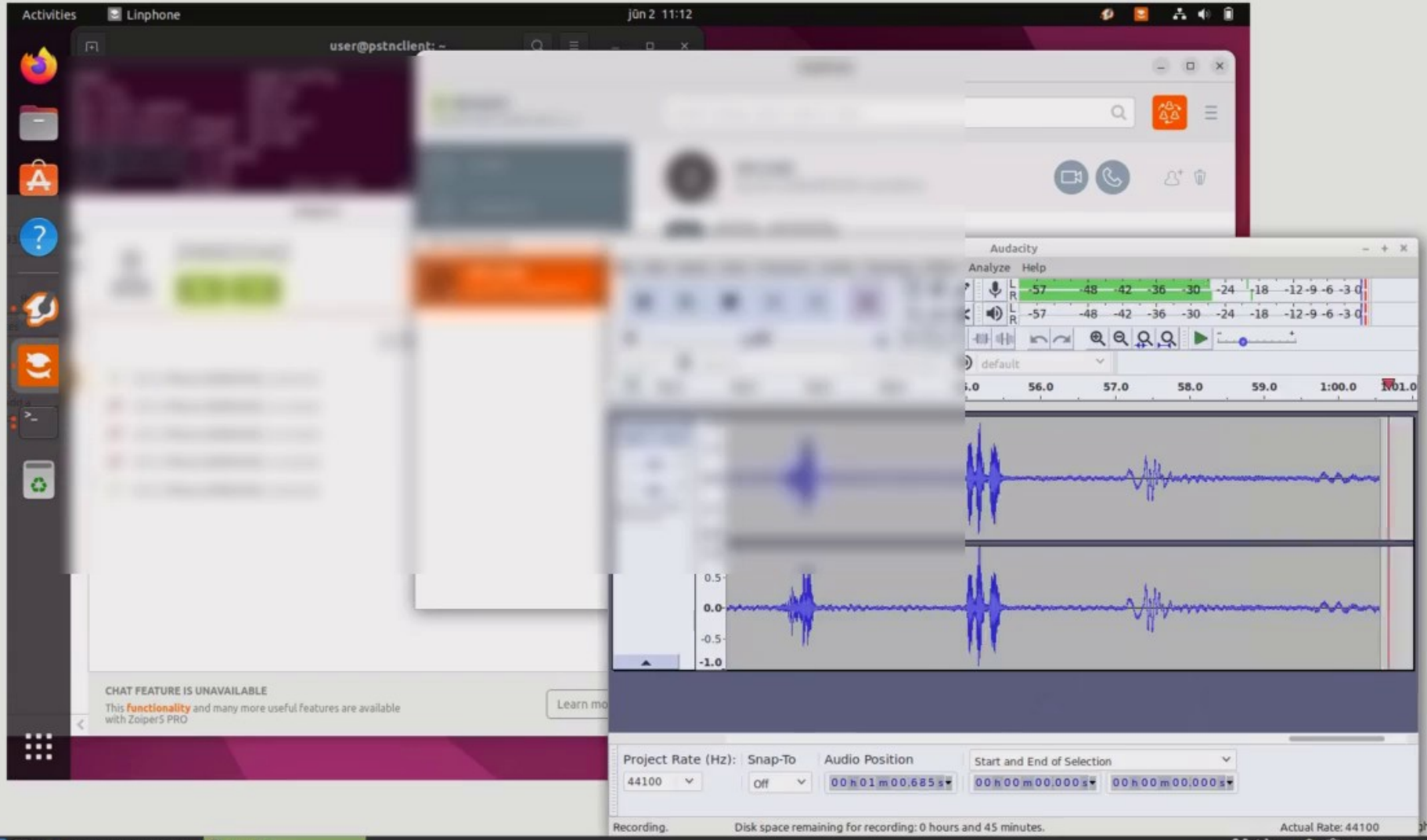
- A5/1 broken
- No mutual authentication on Um
  - FakeBTS / IMSI catchers
- Part of PSTN

Tactic 1

Interception of phone calls

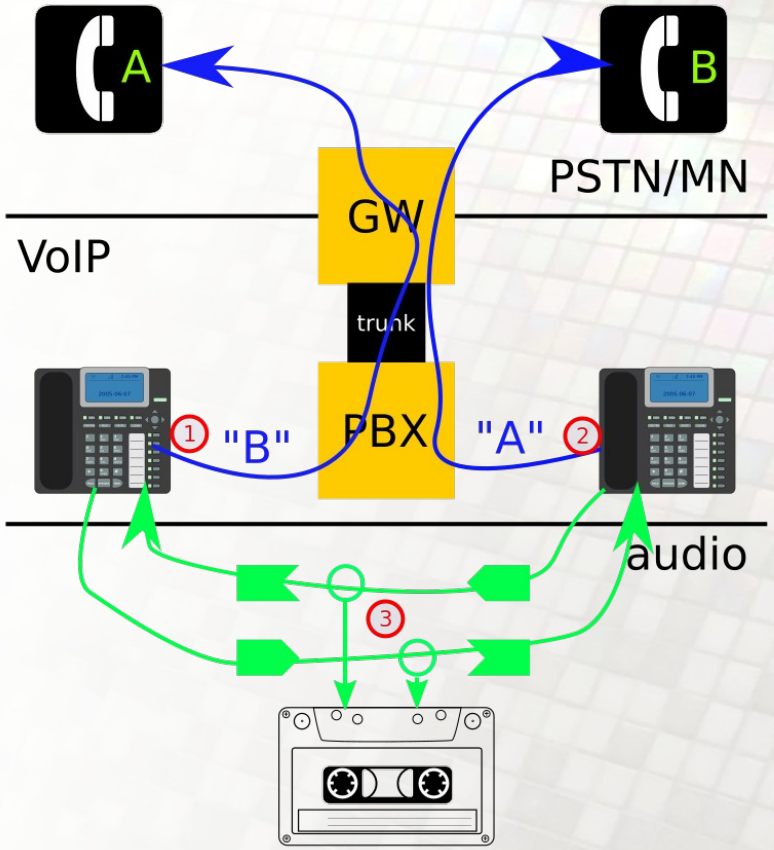
Attack 1

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 Zoiper5 PRO
Audacity
Analyze Help
Project Rate (Hz):
Snap-To
Audio Position
Start and End of Selection
44100
Off
Recording.
Disk space remaining for recording: 0 hours and 45 minutes.
Actual Rate: 44100

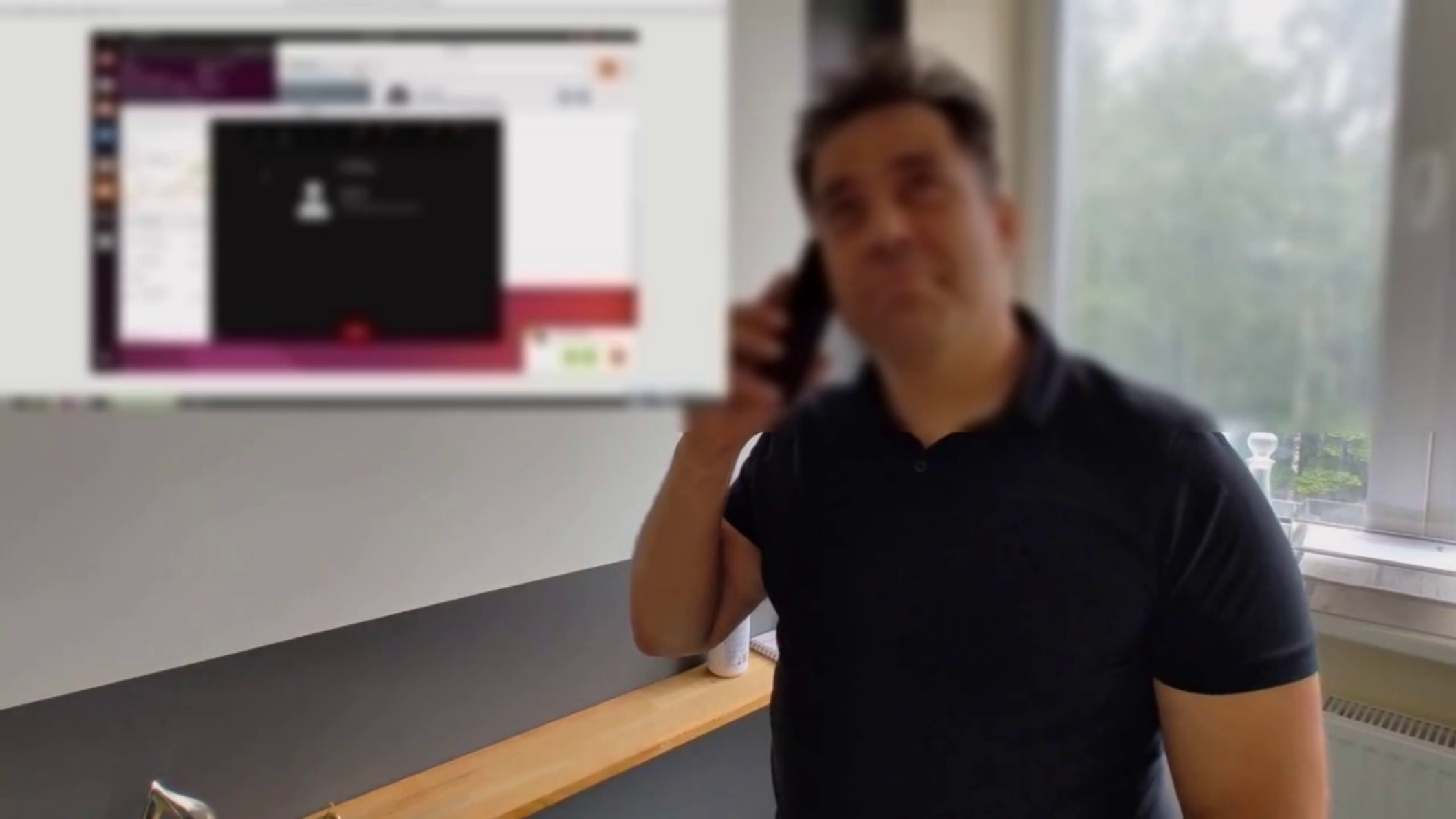

11:14
Zvans no:
Secret project empolyee
M
Atbildēt
Velciet augšup, lai atbildētu
Velciet lejup, lai noraidītu
John Doe
+3
Message
Reminder

Simultaneous ring attack

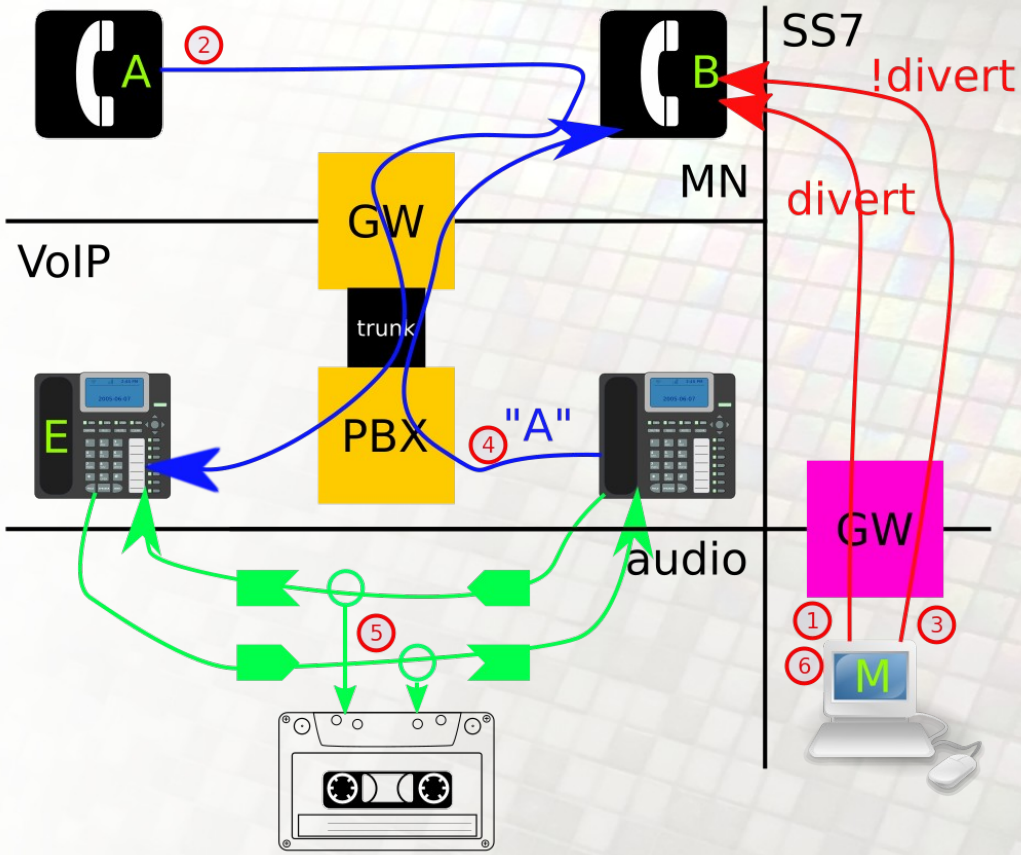


Attack 2

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.

  101 10 "u" "E2U+sip" "!^.*$!sip:220408000@voip.up.pt!" .
- 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 (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:40212024455!" .
- 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

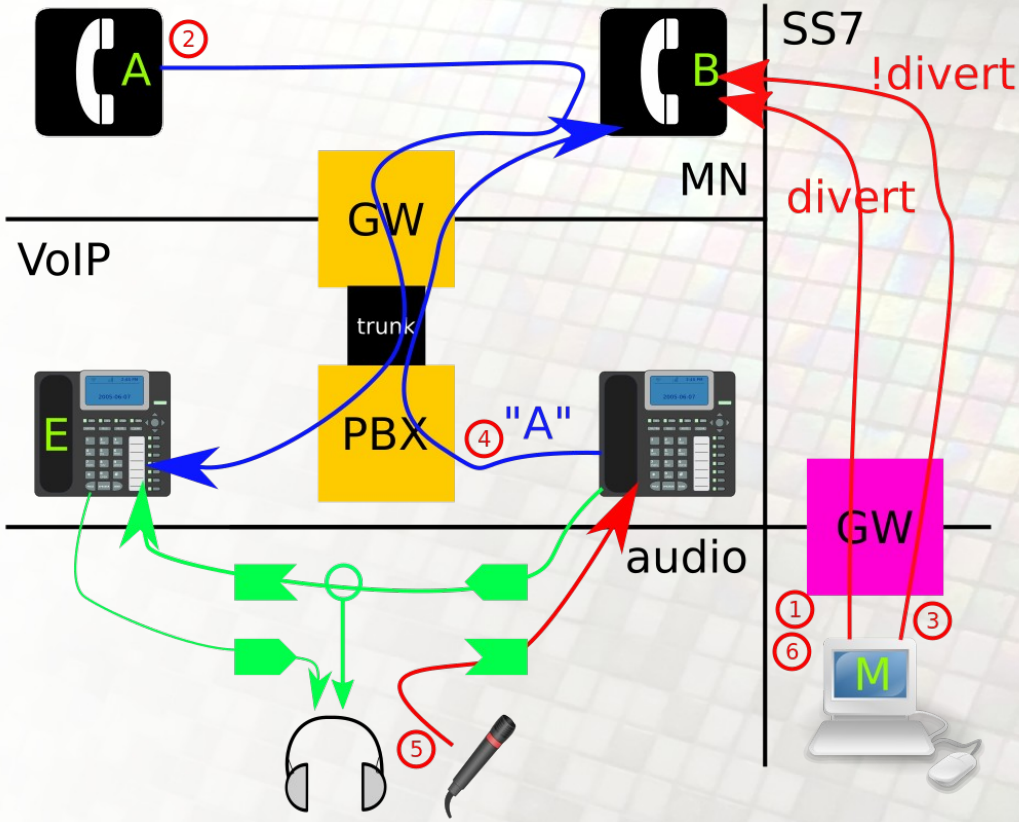
The diversion part (SocEng)

- Physical attacks
  - just take the phone and call *21*004021202445 5#
- Vishing
  - Hello, this is Dog, please call *21*004021202445 5# to get 1000 CAD
- Phishing
  - http://eja.lv/3t4

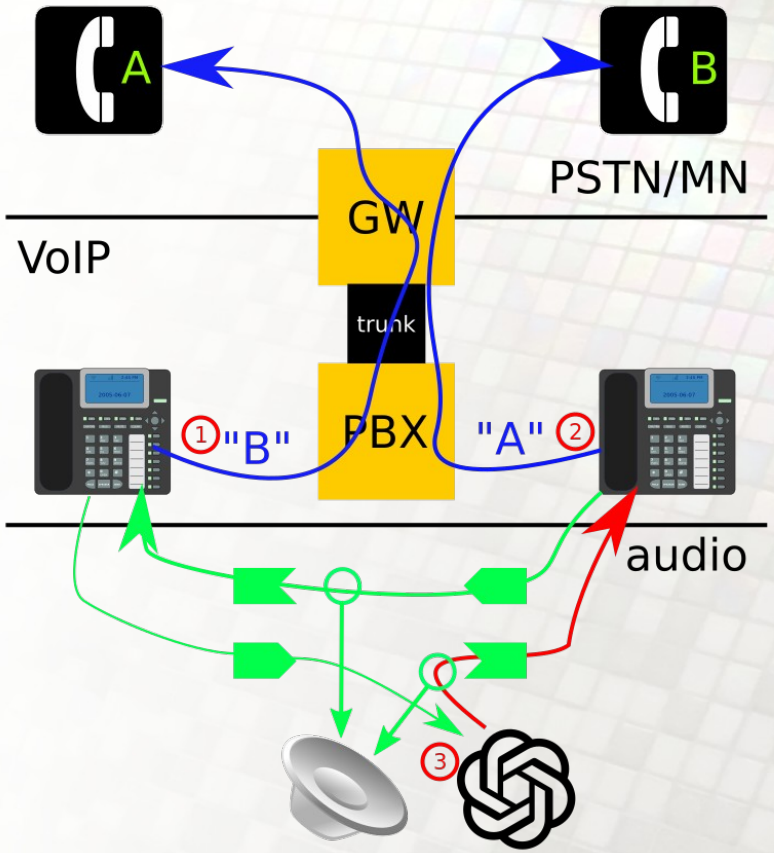
Tactic 2

Alteration of phone calls

Asynchronous substitution



AI



Proposed solutions

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

Thank you!

slides ==> https://kirils.org/

@k@chaos.social

MITM on PSTN
DefCamp, Bucharest, Romania

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

possible.lv