MITM uzbrukumi publiskajam komutējamajam telefonu tīklam

Kirils Solovjovs · @k@masts.lv
https://kirils.org

MITM uzbrukumi PSTN
„Esi drošs”, Latvija

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

possible.lv

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

- Strādāju
  - Possible Security, vadītājs, hakeris
  - Elektronikas un datorzinātņu institūts, zinātniskais asistents
- Izklaidējos
  - E-parakstu apokaliptiķis
  - Mikrotik RouterOS jailbreak autors
- Stāstu
  - Hackfest, CCC, Hack in the Box, Nullcon, BalCCon, Disobey, …∞
  - @k@masts.lv & @k@chaos.social

Šodien apskatīsim

- PSTN & mobilie tīkli
- Sociālā inženierija
- Uzbrukumā!
  - Vienlaicīgā zvana uzbrukums
  - Pārvirzīšanas uzbrukums
  - Pārtveršanas taktika
  - Modifikācijas taktika

Kas ir PSTN

- Publiskais komutējamais telefonu tīkls
  - Public switched telephone network
  - vispasaules tīkls
- Vienota telefona numuru adrešu telpa
- Arhaiska sistēma

Cik drošs ir 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

Avots: versadial.com

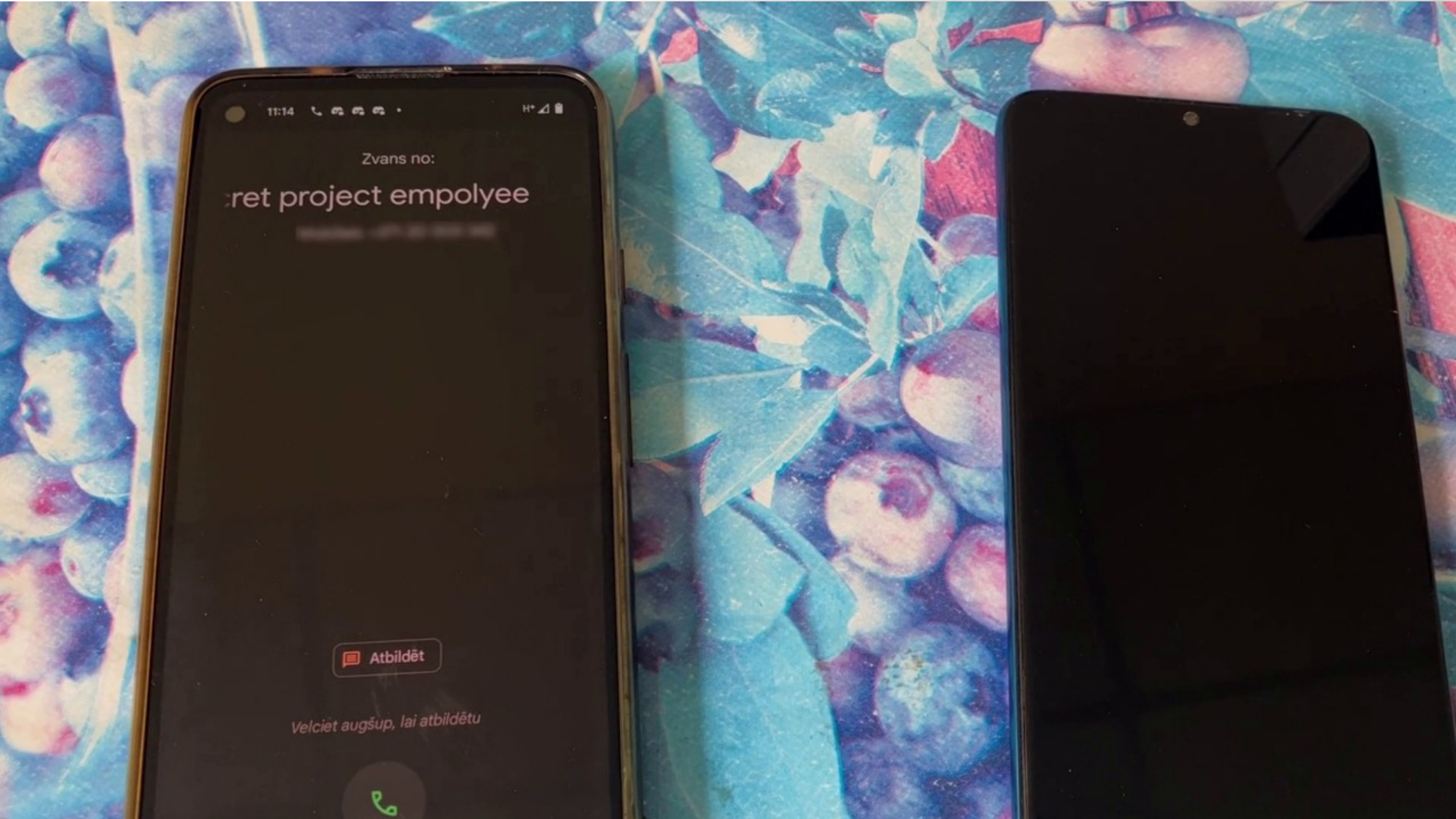
CLIP

- Zvanītāja numura identifikācija
  - Caller Line Identification Presentation


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

CLIP

- Zvanītāja numura identifikācija
  - Caller Line Identification Presentation
- Ziemeļamerikā ir arī CNAM
  - Caller Name Delivery
  - Zvanītāja vārda piegāde
- CLIR
  - Caller Line Identification Restriction
  - Zvanītāja numura identifikācijas ierobežojums


11:14
Zvans no:
ret project empolyee
Atbildēt
Velciet augšup, lai atbildētu

SS7

- Signalizācijas sistēma Nr. 7 / Signalling System 7
  - ķēžu slēgumu (zvanu) izveide un nonešana
  - numuru translācija
  - priekšapmaksa
  - pārvirzīšana
  - utt.

Sociālā inženierija

Kirils Solovjovs · @k@masts.lv
https://kirils.org

MITM uzbrukumi PSTN
„Esi drošs”, Latvija

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

possible.lv

Mobilie tīkli

- A5/1 salauzts
- Abpusējas autentifikācijas neesamība gaisa saskarnē
  - FakeBTS / IMSI ķērāji
- PSTN daļa

Taktika Nr. 1

Telefona zvanu pārtveršana

Kirils Solovjovs · @k@masts.lv
https://kirils.org

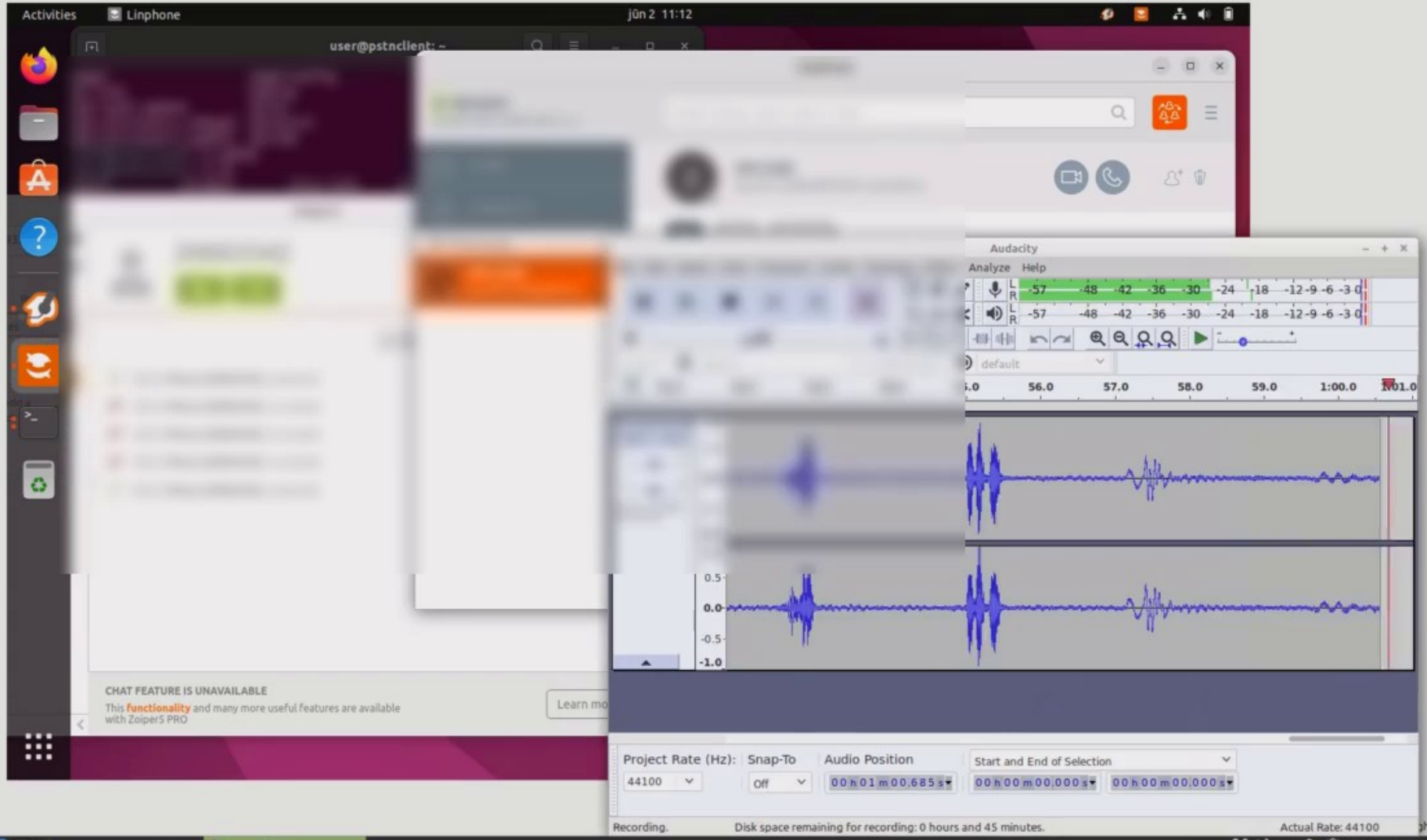
MITM uzbrukumi PSTN
„Esi drošs”, Latvija

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE
possible.lv

Uzbrukums Nr. 1

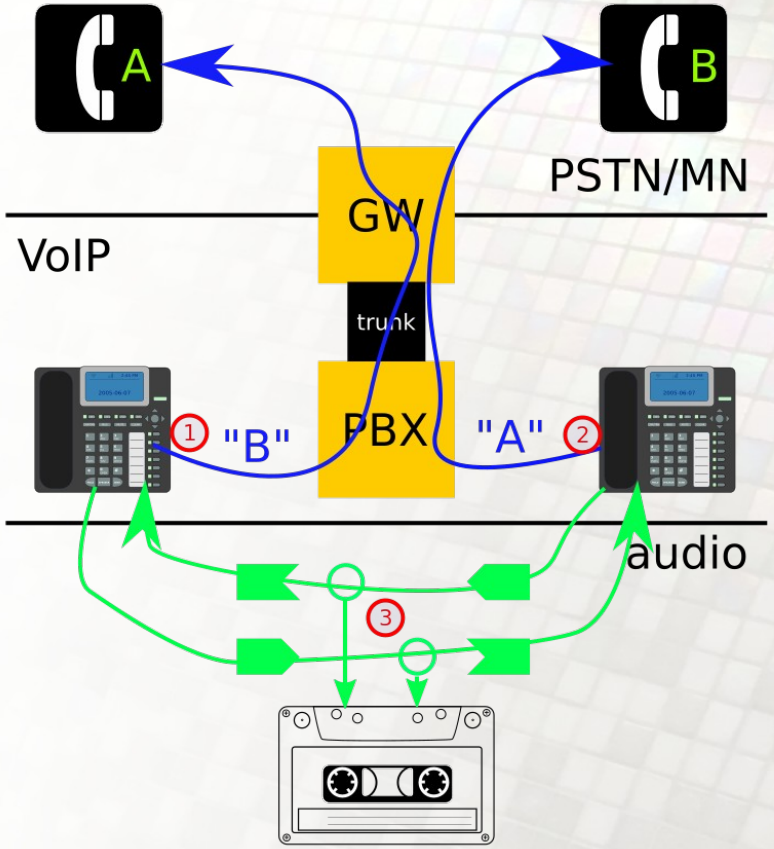
Vienlaicīgā zvana uzbrukums

Kirils Solovjovs · @k@masts.lv
https://kirils.org


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

Vienlaicīgā zvana uzbrukums

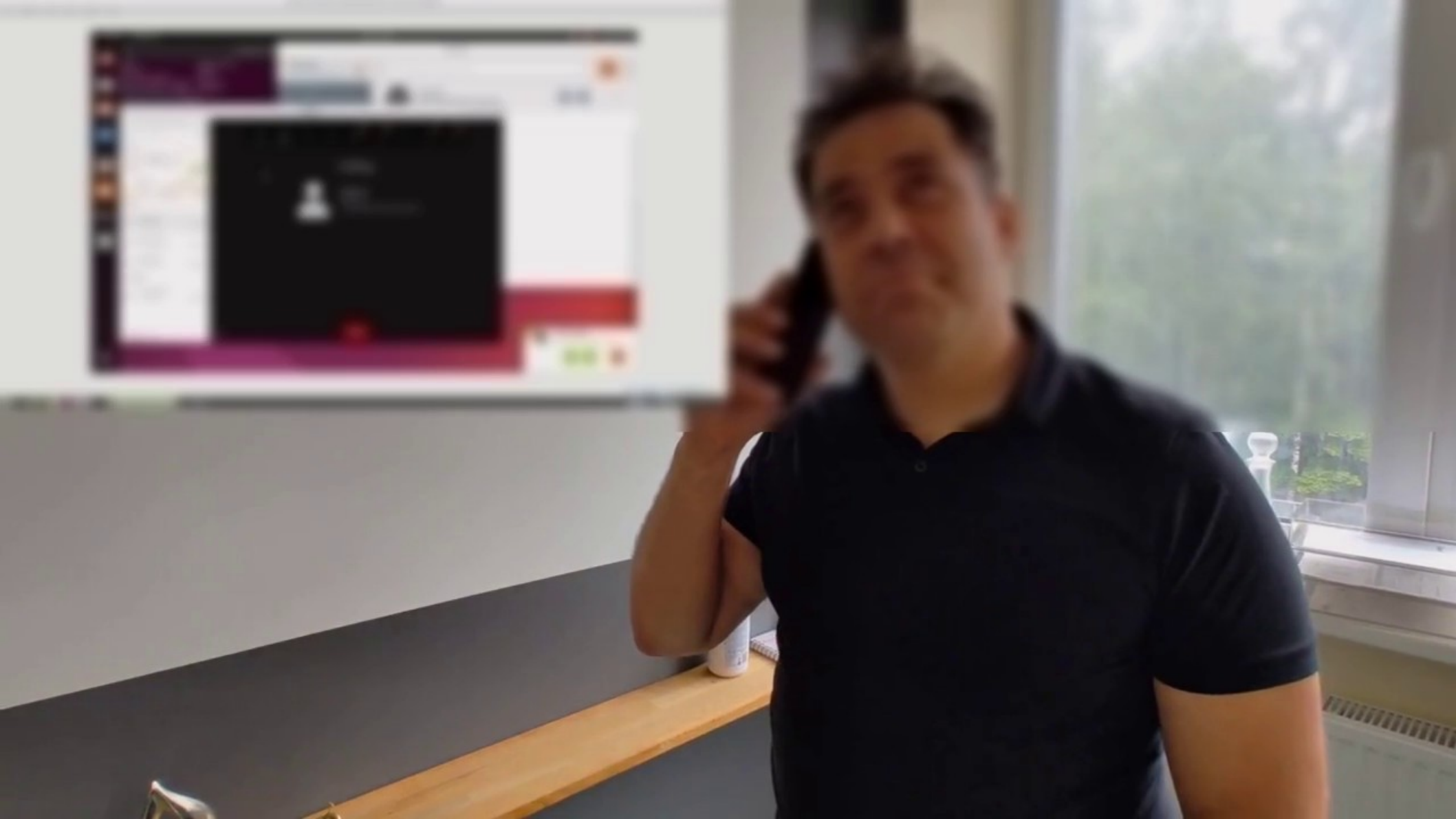


Uzbrukums Nr. 2

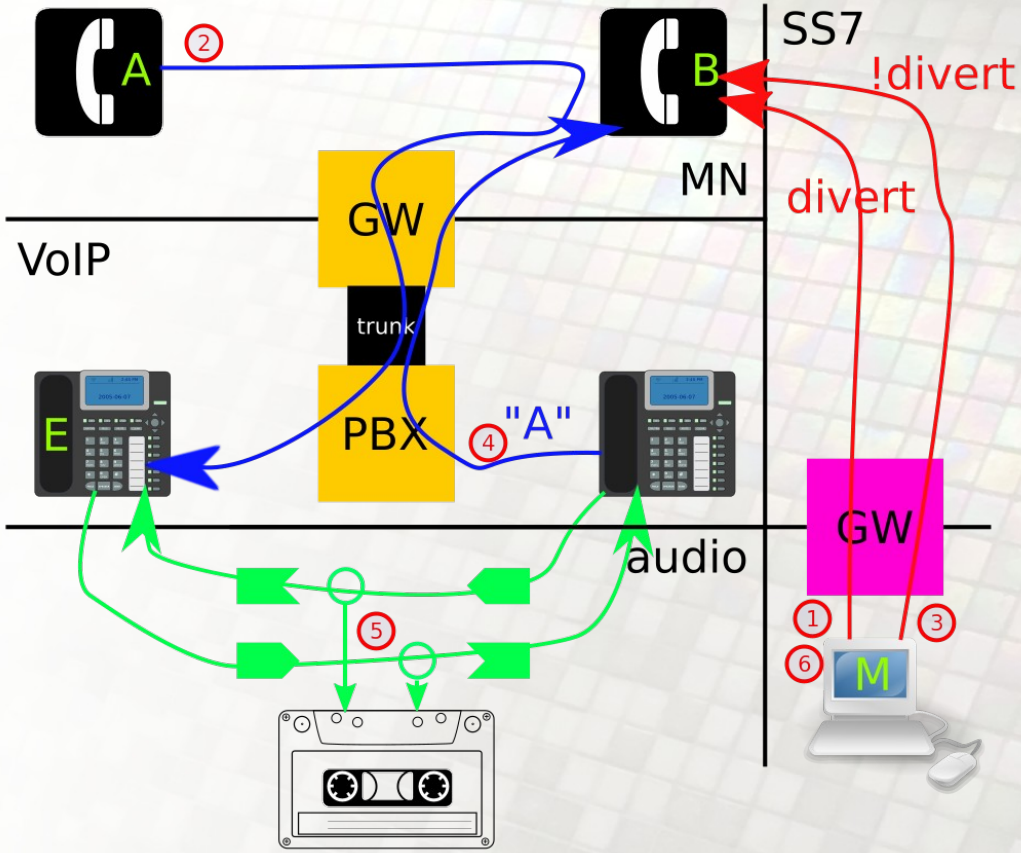
Pārvirzīšana

Kirils Solovjovs · @k@masts.lv
https://kirils.org

MITM uzbrukumi PSTN
„Esi drošs”, Latvija



Pārvirzīšanas uzbrukums



* zvani var tikt pāradresēti, arī izmantojot e164.arpa un daudzas citas metodes

Pārvirzīšanas daļa (ENUM)

- RFC2916 / RFC6116 „E.164 number and DNS”
- (E.164) +371 67660999
- dig NAPTR 9.9.9.0.6.6.7.6.1.7.3.e164.arpa.

  0 0 "U" "E2U+SIP" "!^(.*)$!sip:\\1@159.148.8.103!" .

Pārvirzīšanas daļa (ENUM)

- RFC2916 / RFC6116 „E.164 number and DNS”
- (E.164) +371 67660999
- dig NAPTR 9.9.9.0.6.6.7.6.1.7.3.e164.arpa.

  0 0 "u" "E2U+pstn:tel" "!^.*$!tel:37198765432!" .

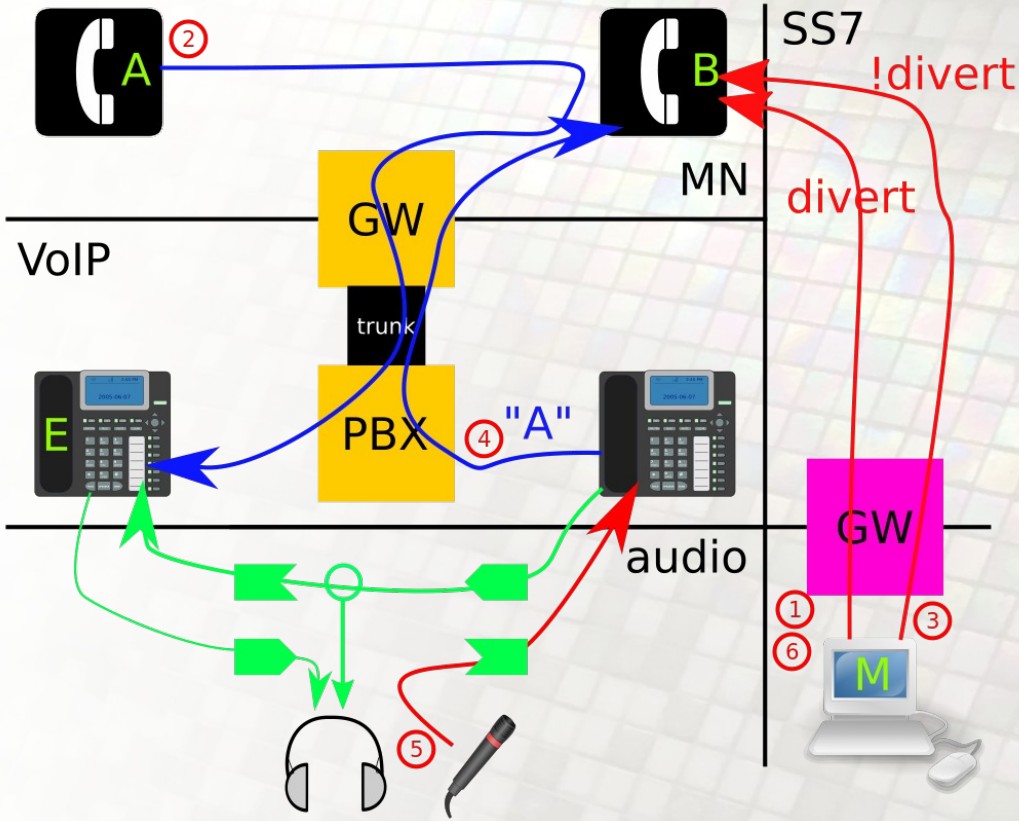
Pārvirzīšanas daļa (SocEng)

- fiziskie uzbrukumi
  - pagrābjam telefonu un zvanām *21*003719876543 2#
- vikšķerēšana
  - Sveiki, te Interneta Šerifs, lūgums steidzami piezvanīt *21*003719876543 2#, lai saņemtu 500 *euro*
- pikšķerēšana
  - http://eja.lv/3t6

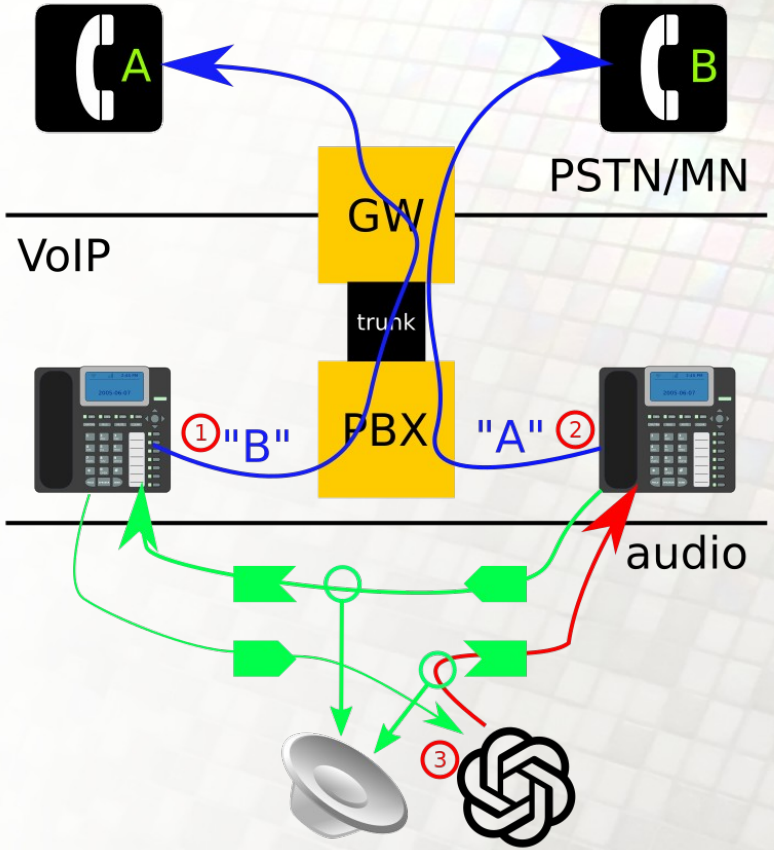
Taktika Nr. 2

Telefona zvanu modifikācija

Asinhrona aizvietošana



Mākslīgais intelekts



Piedāvātie risinājumi

- SS7 ugunsmūri
- CLIP verifikācija
- DNSSEC
- Šifrētie sakari

Pateicos!

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

@k@masts.lv

MITM uzbrukumi PSTN
„Esi drošs”, Latvija

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

possible.lv