ATT&CK FOR TELCO NETWORKS

Sid Rao, Nokia-Bell Labs, Finland

EU ATT&CK Community Workshop, 18-19 May 2020

About me: Sid Rao

Security Researcher, Bell-labs Nokia, Finland

- Threat modeling, network security

Doctoral candidate, Aalto University, Finland

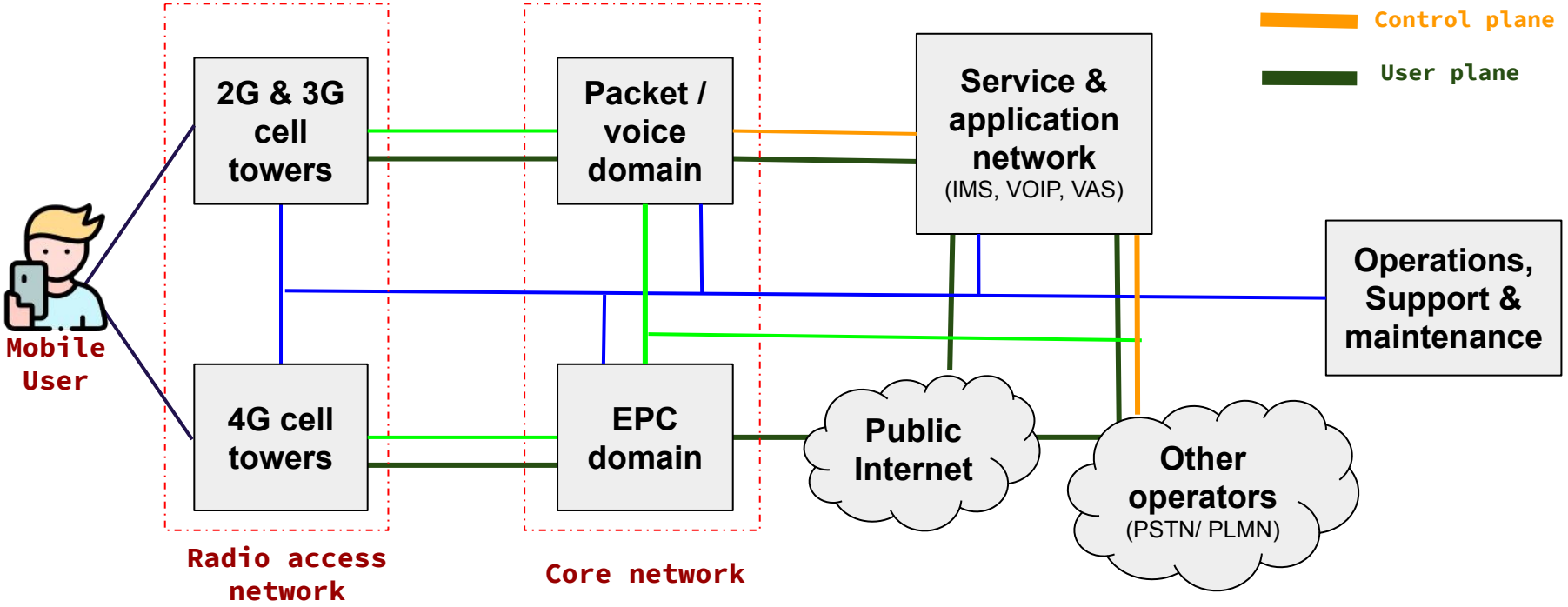
- “Broken authentication problems”
  - Telco networks
  - Password managers
  - Virtual Private Networks
  - Cryptocurrency wallets
  - Browser extensions
  - Google Suite Add-ons

Public Interest Technologist, various NGOs

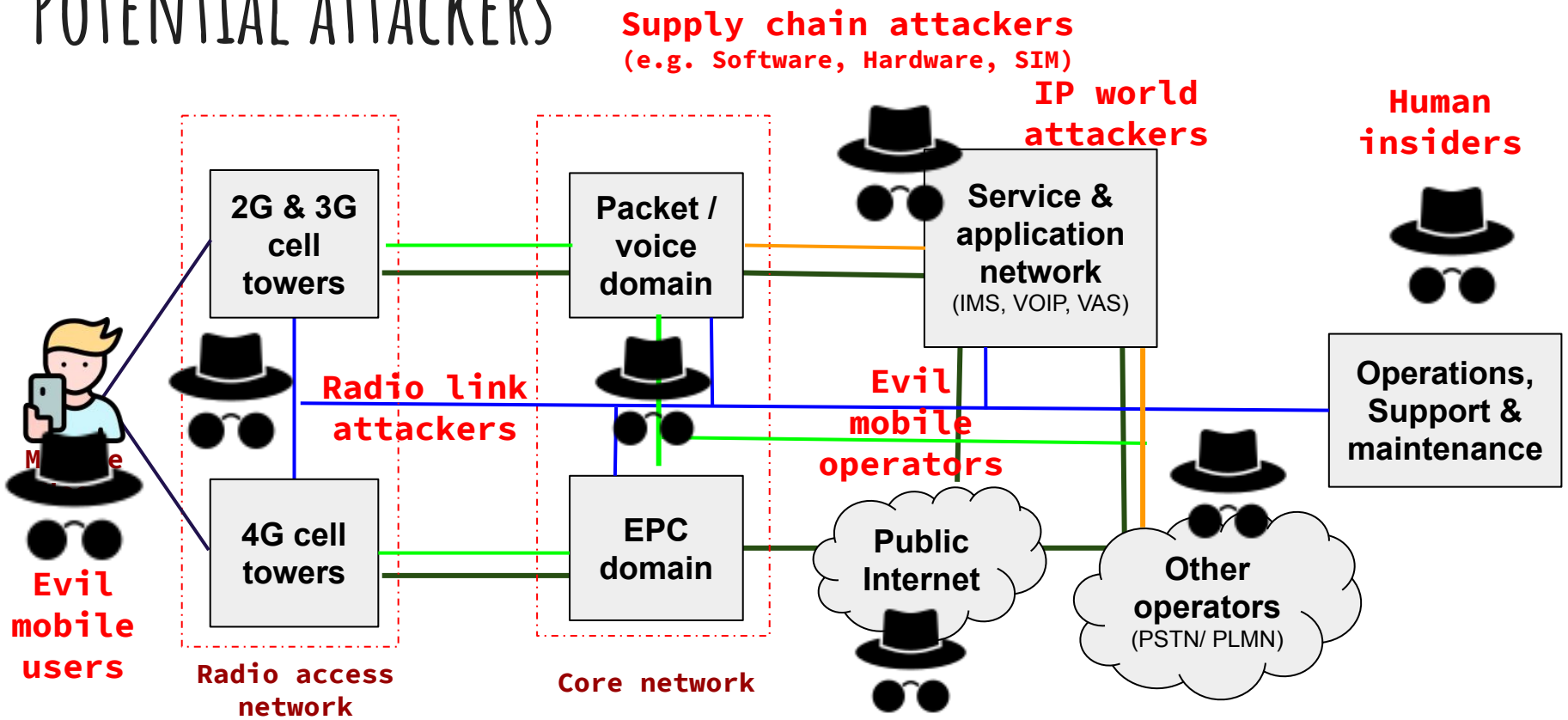
Previously: BlackHat, DefCon, hack.lu, Troopers, Disobey

sidnext2none

Telco network topology



Potential attackers



The story so far (1)

What we wanted:

- Build a telco-specific framework:
  - to quickly model a new attack with familiar taxonomy
  - to compare multiple known attacks similarity in root causes

What we gathered:

- Publications and presentations (from infosec venues)
- Threat landscape studies and best practice guidelines (from standardization and governance bodies)

The story so far (2)

What we did:

→ **Understand** attack flow

→ Deduce **commonalities**

→ **Cross-reference** with defensive solutions

→ **Tactics X techniques** matrix

What we currently have:

- 47 techniques span across 8 tactics
- Concrete examples of using the framework

The matrix

Initial Access	Persistence	Discovery	Lateral Movement	Protocol Misuse	Defense Evasion	Collection	Impact
Attacks from UE	Infect UE hardware or software	Port scanning or sweeping	Exploit roaming agreements	SS7-based attacks	Security audit camouflage	Admin credentials	Location tracking
SIM-based attacks	Infecting SIM cards	Perimeter mapping	Abuse interworking functions	Diameter based attacks	Blacklist evasion	User specific identifiers	Call eavesdropping
Attacks from Radio Access network	Spoofed radio network	Threat intelligence	Exploit platform & service specific vulnerability	GTP-based attacks	Middlebox misconfig exploits	User specific data	SMS interception
Attacks from other mobile networks	Infect network nodes	CN-specific scanning		DNS-based attacks	Bypass firewalls	Network specific identifiers	Data interception
Attacks with access to transport network	Covert channels	Internal resource search		Pre-AKA attacks	Bypass homerouting	Network specific data	Billing frauds
Attacks from IP-based networks		UE knocking			Downgrading		DoS - network
Insider attacks and human errors					Redirection		DoS- user
					UE protection evasion		Identity-based attacks

#1 : Attack Mounting

Initial Access
Attacks from UE
SIM-based attacks
Attacks from Radio Access network
Attacks from other mobile networks
Attacks with access to transport network
Attacks from IP-based networks
Insider attacks and human errors

Persistence
Infect UE hardware or software
Infecting SIM cards
Spoofed radio network
Infect network nodes
Covert channels

Discovery
Port scanning or sweeping
Perimeter mapping
Threat intelligence
CN-specific scanning
Internal resource search
UE knocking

Initial access

- SIM-based attacks
  - SIM swapping, cloning, jacking
- Attacks from radio network
  - IMSI catchers

Persistence

- Infecting network nodes, with malware

Discovery

- The usual ones → port scanning, network mapping, threat intel.
- CN-specific scanning

#2 : Attack Execution

Lateral Movement
Exploit roaming agreements
Abuse interworking functions
Exploit platform & service specific vulnerability

Protocol Misuse
SS7-based attacks
Diameter based attacks
GTP-based attacks
DNS-based attacks
Pre-AKA attacks

Defense Evasion
Security audit camouflage
Blacklist evasion
Middlebox misconfig exploits
Bypass firewalls
Bypass homerouting
Downgrading
Redirection
UE protection evasion

Lateral Movement

- Abuse interworking functionalities
  - 2G ← → 3G ← → 4G communication
- Exploit “Linux” platform-specific vulnerabilities.

Protocol misuse

- Unauthenticated signaling protocols
- Pre-authentication over radio channels

Defense evasion

- Bypass blacklist, firewall or audits
- Downgrade to legacy systems

#3 : Result Gathering

Collection
Admin credentials
User specific identifiers
User specific data
Network specific identifiers
Network specific data

Impact
Location tracking
Call eavesdropping
SMS interception
Data interception
Billing frauds
DoS - network
DoS- user
Identity-based attacks

Collection

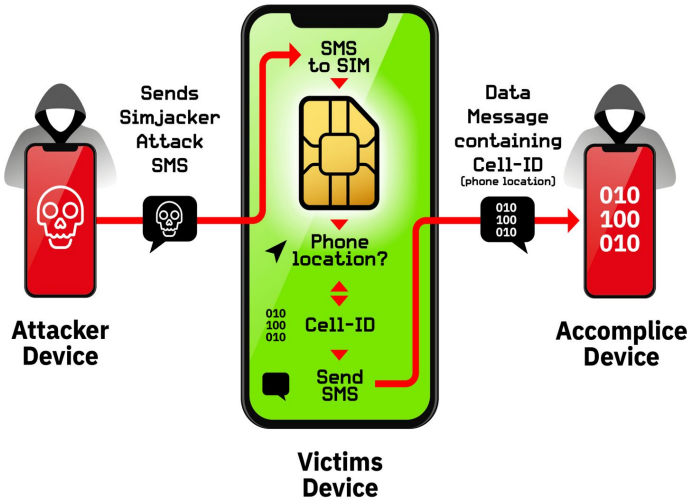
- User-specific
  - Identifiers: e.g. IMSI, IMEI
  - Data: e.g. contents of communication
- Network-specific
  - Identifiers: e.g. IP, Global Titles
  - Data: e.g. Topology, routing data

Impact

- Location tracking
- Call, SMS, Data interception
- Billing frauds
- Signaling DoS and Radio jamming

SIMJACKER

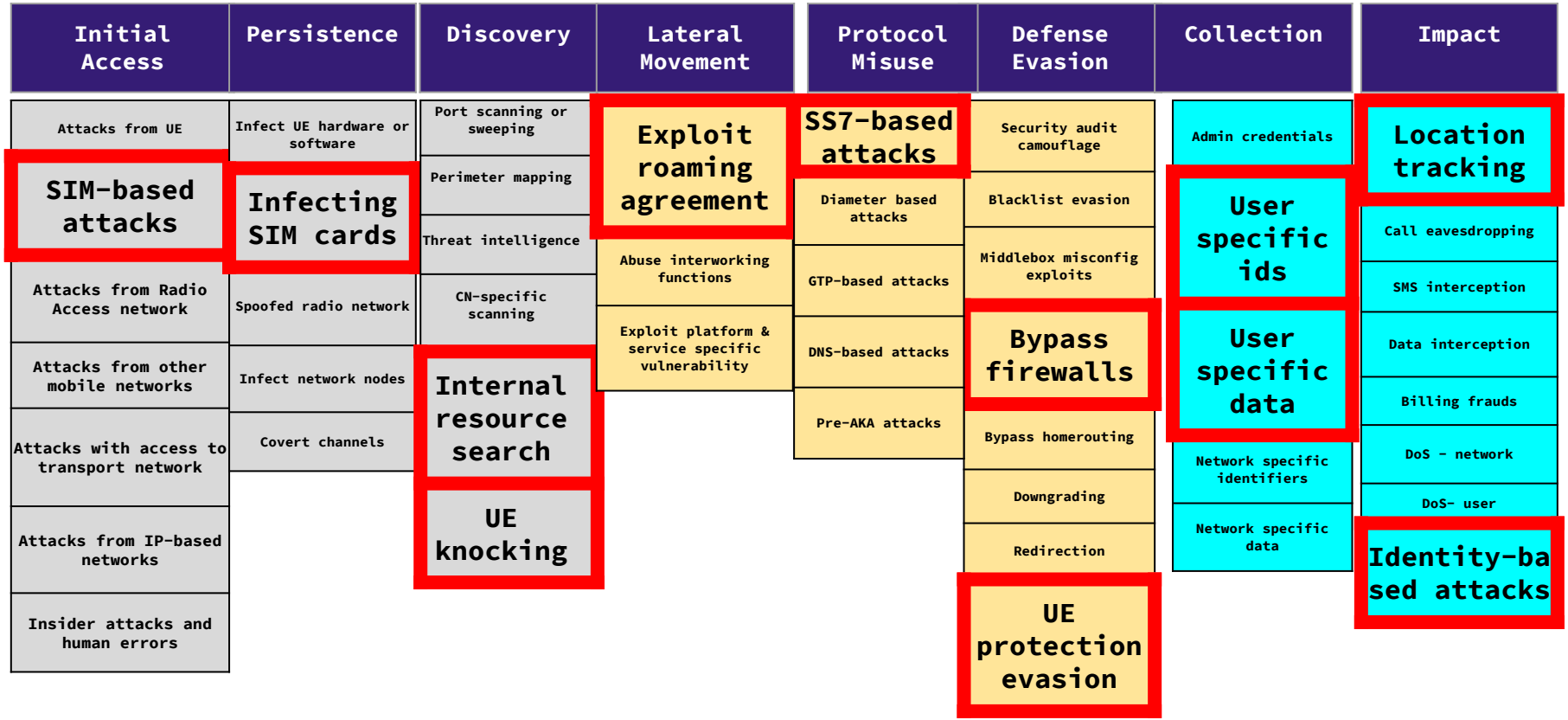
- Large scale espionage campaign on mobile users in multiple countries
- Exploits vulnerable **S@T browser** in UICC cards
- **binary SMS payload** through mobile devices, VAS provider, or SS7
- Mainly used for location tracking + IMEI disclosure



Source: Adaptive Mobile

https://simjacker.com/

Modeling SIMJacker



What NEXT?

- **To build an “Open” community for more collaboration**
  - As of now, Nokia Bell-Labs, Ericsson, and a few more
  - To make the current proposal more concrete
  - To build knowledge base and tools
- **Call for participation and contribution:**
  - ANYONE WHO IS INTERESTED
    - E.g. mobile network operators, equipment vendors, researchers from industry, academia or governance bodies
  - Comments, critics, feedbacks are most welcome.

Sounds interesting?

1. **Read the full paper**

https://arxiv.org/pdf/2005.05110.pdf

2. **Take part in the survey**

https://www.netigate.se/a/s.aspx?s=884150X225761371X45363

Thanks

Contact

sid.rao@nokia.com

Sidnext2none