ATT&CK for Telecom

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

Jonathan Olsson Ericsson

> whoami

—sweden

—security researcher

—13 years working with telecommunications security

—interests: family, bbq, mtb, bjj

Thanks for your support!
—Leena Mattila
—Loay Abdelrazek

Background

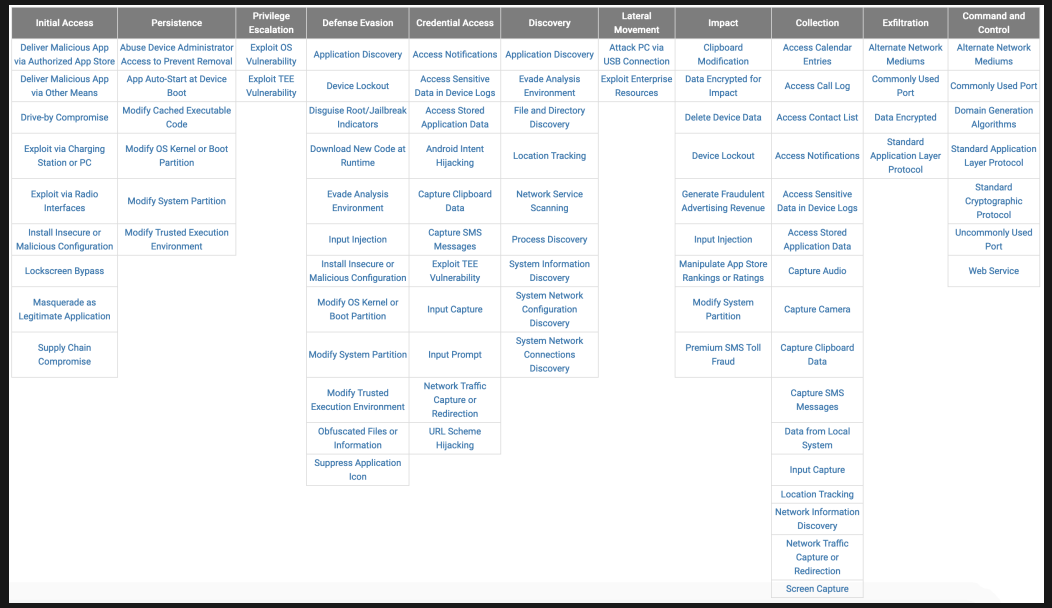
- Mobile networks are Critical National Infrastructure
- National interests to secure mobile networks
- Existing security frameworks address functional requirements, product testing, and deployment guidelines
- Need for a framework that documents post-compromise adversary behavior

What would it be used for?

- Adversary profiling and emulation
- Red teaming
- Assessment of implemented defenses and detection
- Assessment of SOC maturity
- Development of tools
- Cyber threat intelligence

Why not just use ATT&CK as-is?

- ATT&CK is a great tool initially focused on enterprise (Windows, Linux, Mac)
- Now with matrices for mobile devices, cloud and ICS
- But…none are a great fit for modelling attacks against telecom networks
- Telecom networks are complex, comprised of multiple domains each built on diverse principles

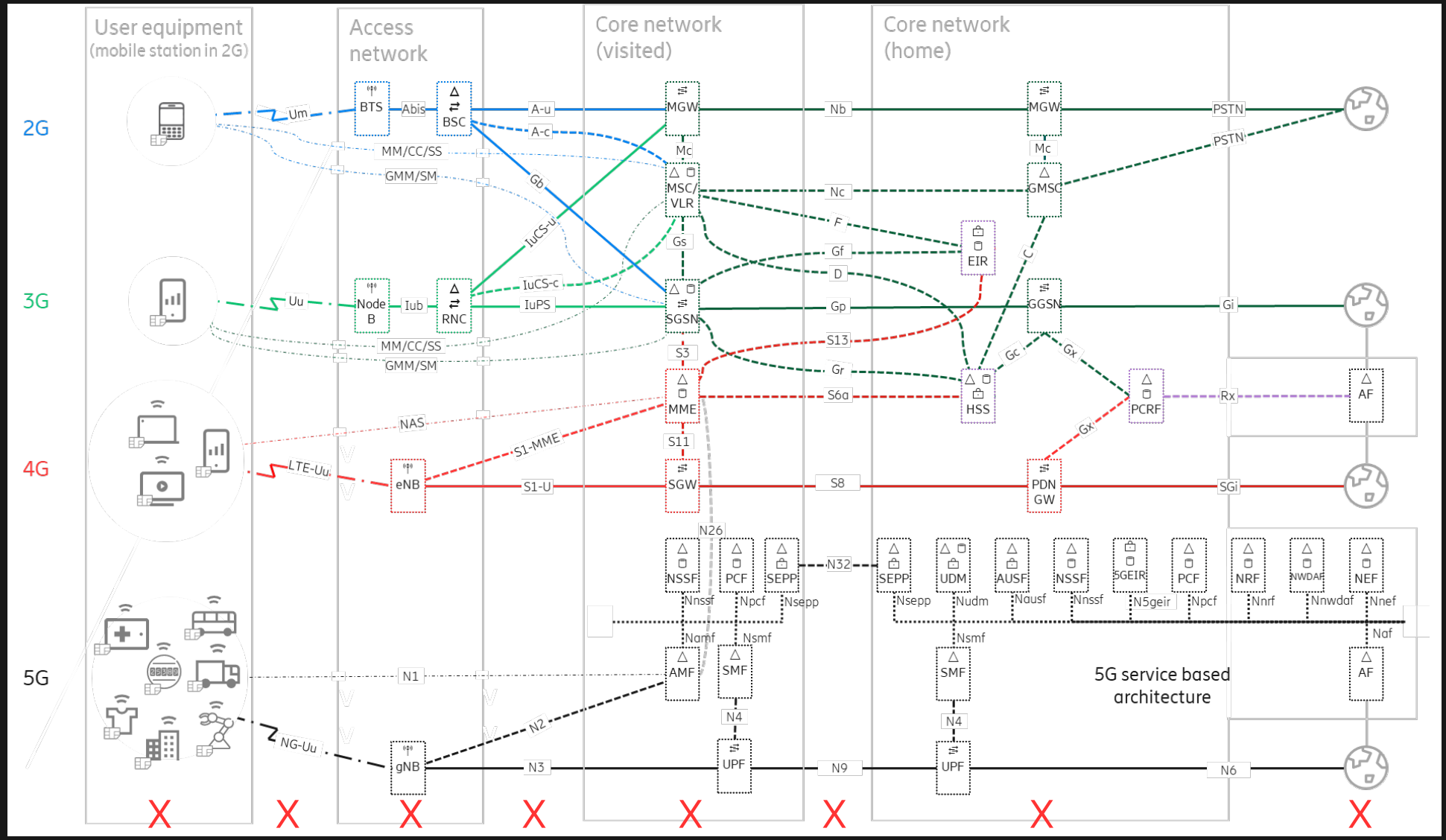


Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera		
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data		
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages		
			Obfuscated Files or Information	URL Scheme Hijacking				Data from Local System		
			Suppress Application Icon					Input Capture		
								Location Tracking		
								Network Information Discovery		
								Network Traffic Capture or Redirection		
								Screen Capture		

Source: https://attack.mitre.org/matrices/mobile/

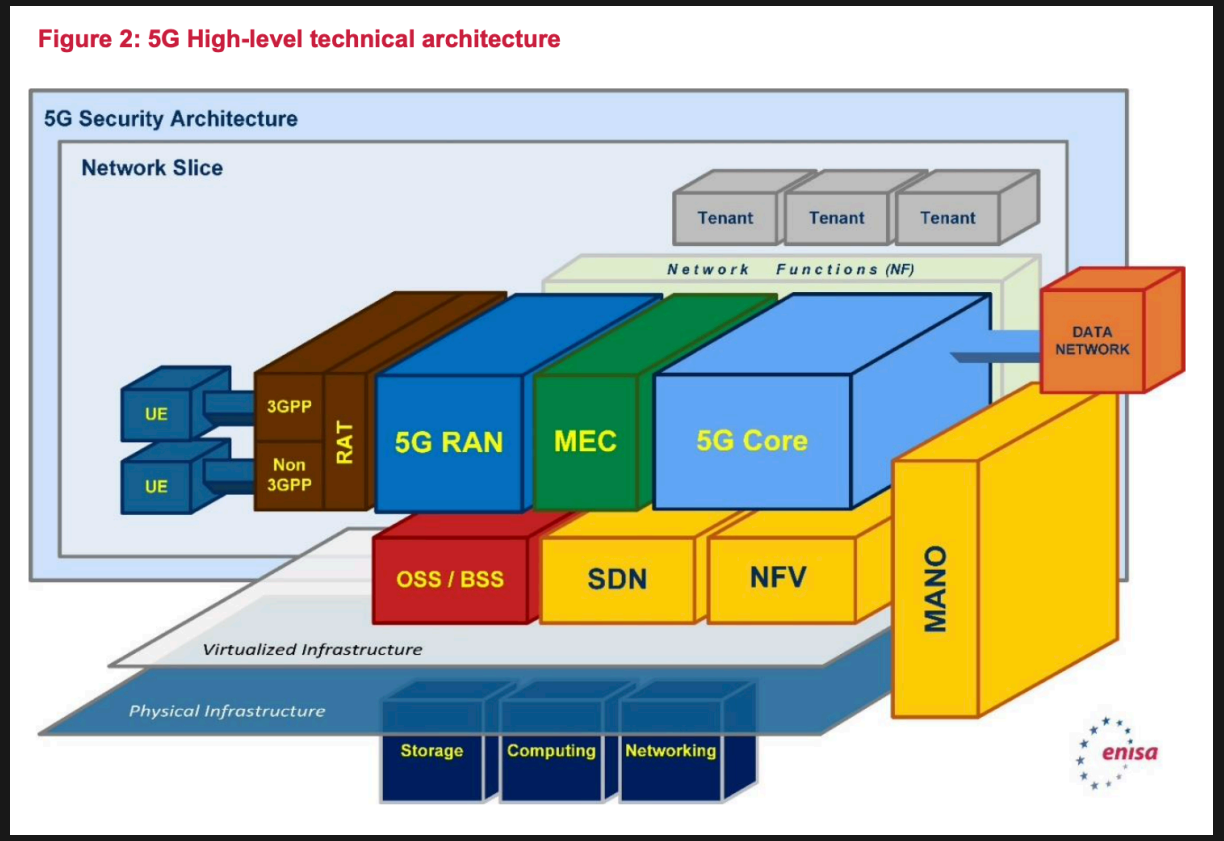
To fully capture the whole telecom environment one would need to use several matrices
- adversaries pivot between environments

3GPP mobile networks – functional architecture



It's more than connecting A to B

- Standardized functional architecture with well-defined interfaces and protocols for multi-vendor interoperability
- But product implementations vary
- Operated through different management systems
- Requires multi-domain orchestration
- Realized in various deployment environments: cloud, enterprise IT, telecom, mobile devices, IoT



Source: ENISA Threat Landscape for 5G Networks

Something familiar, but with a telecom flavor

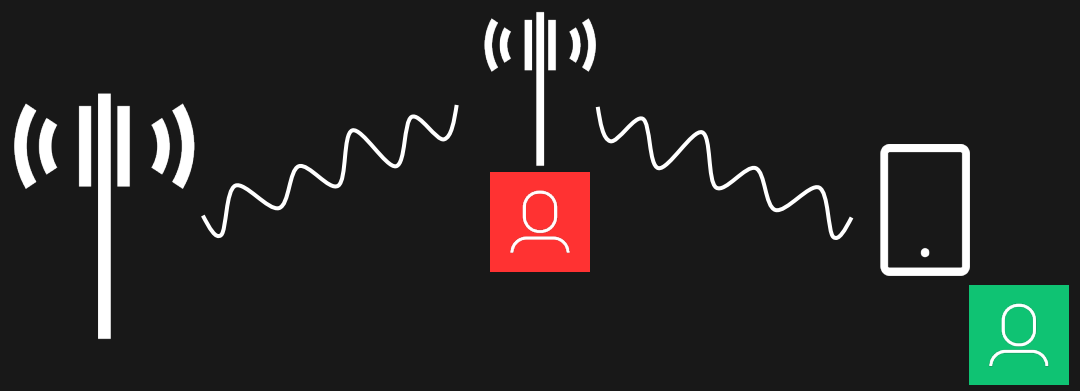
Initial Access	Persistence	Defense Evasion	Discovery	Lateral Movement	Collection	Impact
Attacks from UE	Downgrade attacks	Security audit camouflage	Neighbouring cells discovery	Abusing interworking functionalities	Admin credentials	Service interference
SIM-based attacks	Infecting UE hardware or software	Blacklist evasion	Port scanning or sweeping	Exploit platform and service specific vulnerabilities	Subscriber data	UEs out of sync
Attacks on the radio interface	Infecting SIM cards	Middlebox misconfiguration exploits	Perimeter mapping	Exploit roaming agreements	Network data	Time of day attacks
Attacks with physical access to the network elements	Spoofed radio network	Firewall bypass	Threat intelligence gathering	Valid accounts		Base stations out of sync
Attacks with access to hardware interfaces	Infecting network nodes	Home routing bypass	CN-specific scanning			Location tracking
Attacks from other mobile network	Covert channels	Downgrade of radio generation	Internal resource search			Calls eavesdropping
Attacks with access to transport network	Jamming	Redirection	UE knocking			SMS interception
Attacks from IP-based networks	Protocol misuse	UE protection evasion	Protocol misuse			Data interception
Attacks on exposed management web applications		Protocol obfuscation				Billing fraud
Valid accounts		Protocol misuse				DoS - network
Supply chain compromise		Exploitation for Evasion				DoS - UE
						Identity related attacks

References:

[Threat modeling framework for mobile communication systems]

[MITRE ATT&CK® Matrices for Mobile]

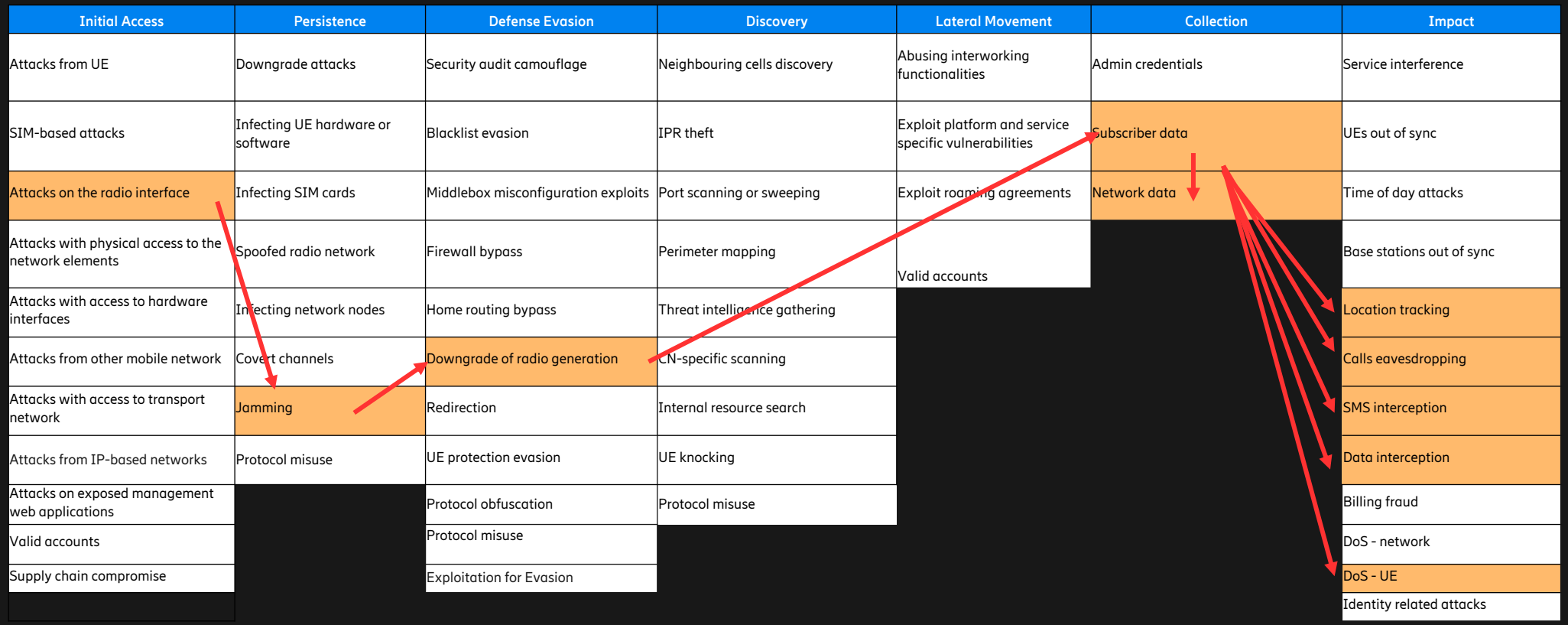
Use Case: Rogue Base Stations



- Rogue base stations impersonates a legitimate cell, luring subscribers to connect to it.

- The objective of an attacker could be to:
  - Collect subscriber identities.
  - Track subscriber location.
  - Eavesdrop calls, SMS and data.
  - Collect radio configuration.

Mapping to the Matrix: Rogue Base Stations

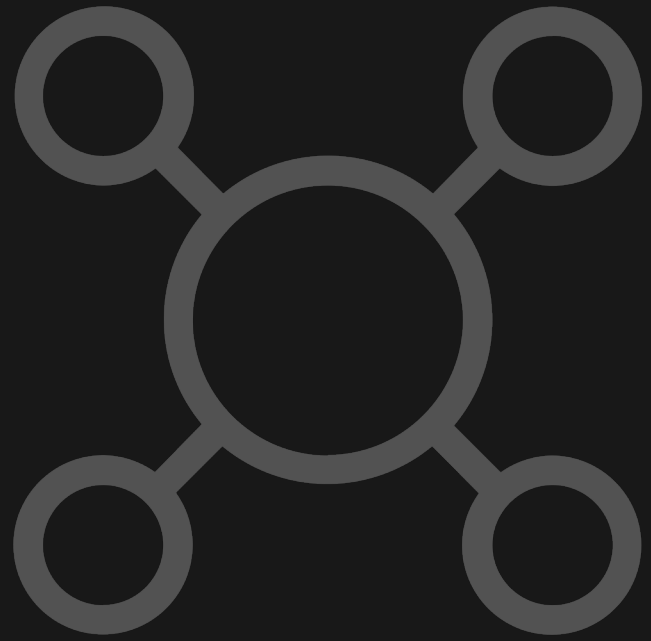


Initial Access	Persistence	Defense Evasion	Discovery	Lateral Movement	Collection	Impact
Attacks from UE	Downgrade attacks	Security audit camouflage	Neighbouring cells discovery	Abusing interworking functionalities	Admin credentials	Service interference
SIM-based attacks	Infecting UE hardware or software	Blacklist evasion	IPR theft	Exploit platform and service specific vulnerabilities	Subscriber data	UEs out of sync
Attacks on the radio interface	Infecting SIM cards	Middlebox misconfiguration exploits	Port scanning or sweeping	Exploit roaming agreements	Network data	Time of day attacks
Attacks with physical access to the network elements	Spoofed radio network	Firewall bypass	Perimeter mapping	Valid accounts		Base stations out of sync
Attacks with access to hardware interfaces	Infecting network nodes	Home routing bypass	Threat intelligence gathering			Location tracking
Attacks from other mobile network	Covert channels	Downgrade of radio generation	CN-specific scanning			Calls eavesdropping
Attacks with access to transport network	Jamming	Redirection	Internal resource search			SMS interception
Attacks from IP-based networks	Protocol misuse	UE protection evasion	UE knocking			Data interception
Attacks on exposed management web applications		Protocol obfuscation	Protocol misuse			Billing fraud
Valid accounts		Protocol misuse				DoS - network
Supply chain compromise		Exploitation for Evasion				DoS - UE
						Identity related attacks

To be discussed

- Is telecom too limiting?

- How about techniques targeting transport networks?
  - MAC-spoofing
  - IP-spoofing
  - DNS-spoofing
  - Rogue DHCP server
  - ARP-spoofing
  - 802.1Q attacks
  - Etc.



What's next? We'd appreciate your feedback!

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

or get in touch with me at

jonathan dot olsson at ericsson dot com

Survey closes Friday May 22nd

https://www.ericsson.com/en/security