6G Security Considerations

IEEE Industry Connection Open RAN Meeting
June 17, 2025

Palindrome Technologies
ASSURANCE | TRUST | CONFIDENCE

National Cybersecurity Strategy

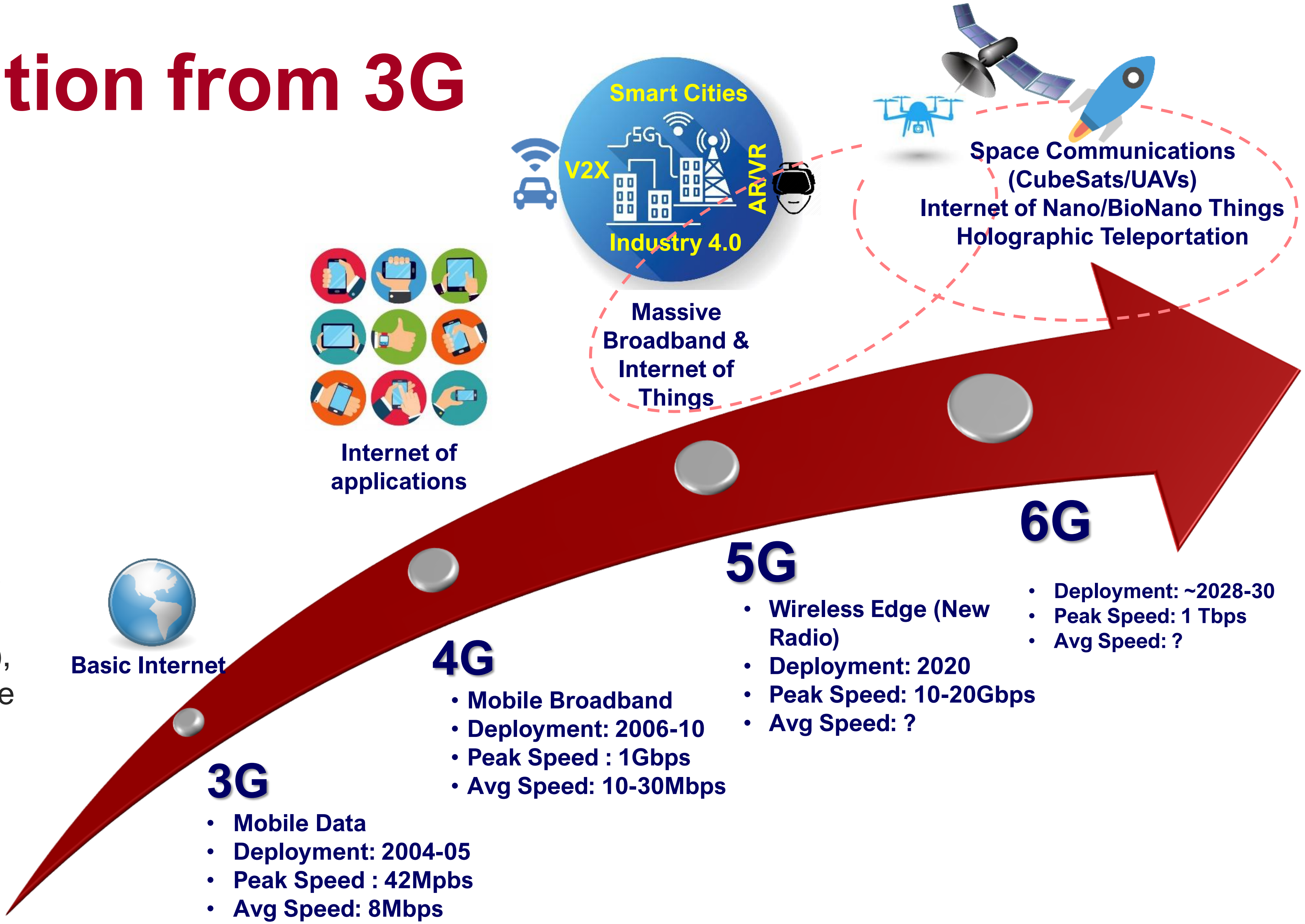
The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever more **complex** and **interdependent systems**, dramatic shifts in the coming decade will unlock new possibilities for human flourishing and prosperity while also multiplying the systematic risks posed by insecure systems (*)

(*) National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

Cellular Evolution from 3G

International Mobile Telecommunications Vision

- Three usage scenarios that distinguish 5G from fourth generation (4G)
  1. Enhanced Mobile Broadband (**eMBB**)
  2. ultra-reliable, low-latency communications (**URLLC**)
  3. massive Machine-Type Communications (**mMTC**), also referred to as massive Internet of Things (mIoT)



Basic Internet

3G

- Mobile Data
- Deployment: 2004-05
- Peak Speed : 42Mpbs
- Avg Speed: 8Mbps

Internet of applications

4G

- Mobile Broadband
- Deployment: 2006-10
- Peak Speed : 1Gbps
- Avg Speed: 10-30Mbps

Massive Broadband & Internet of Things

5G

- Wireless Edge (New Radio)
- Deployment: 2020
- Peak Speed: 10-20Gbps
- Avg Speed: ?

Space Communications (CubeSats/UAVs)
Internet of Nano/BioNano Things
Holographic Teleportation

6G

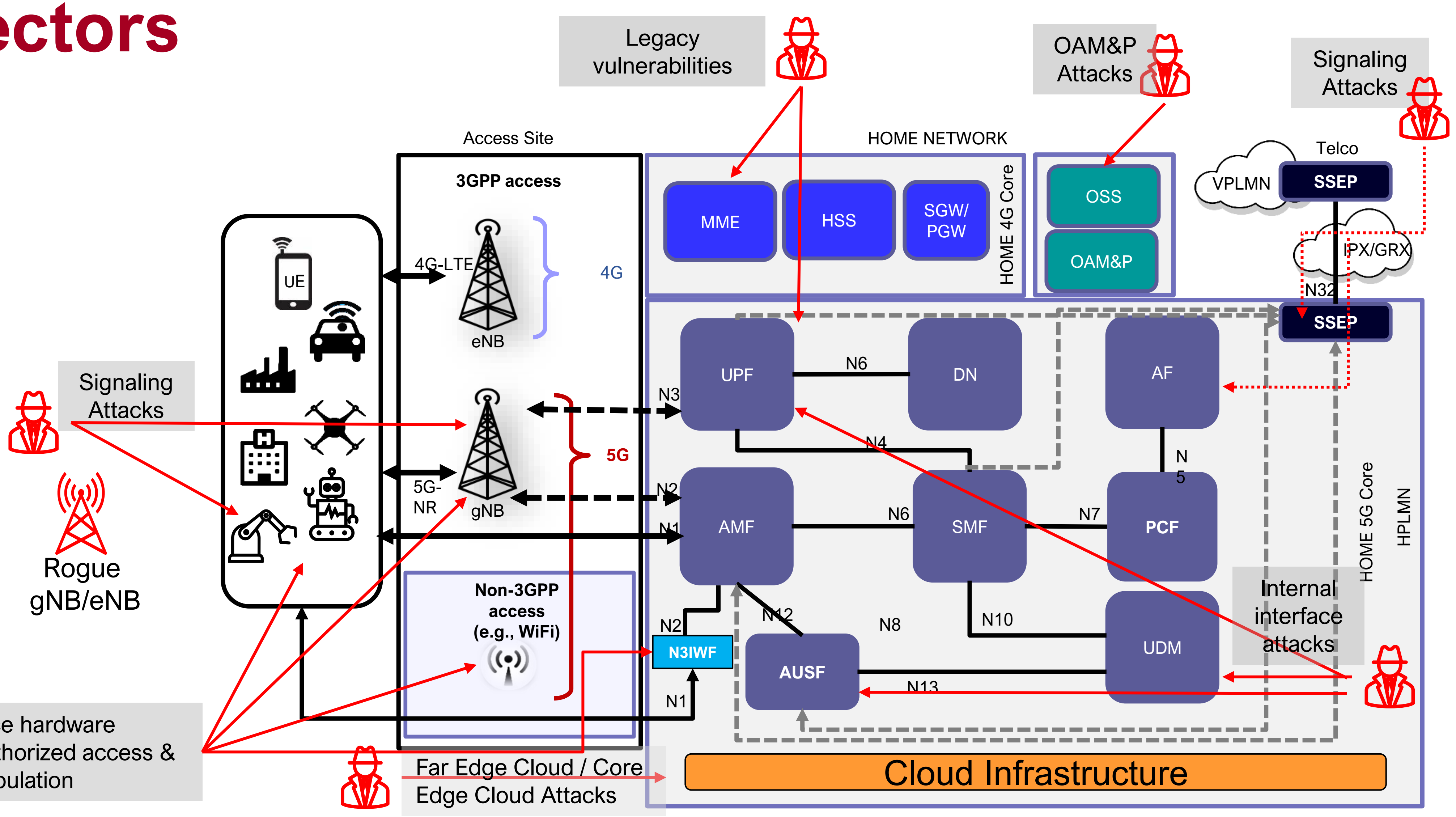
- Deployment: ~2028-30
- Peak Speed: 1 Tbps
- Avg Speed: ?

GSMA - RAN Threats

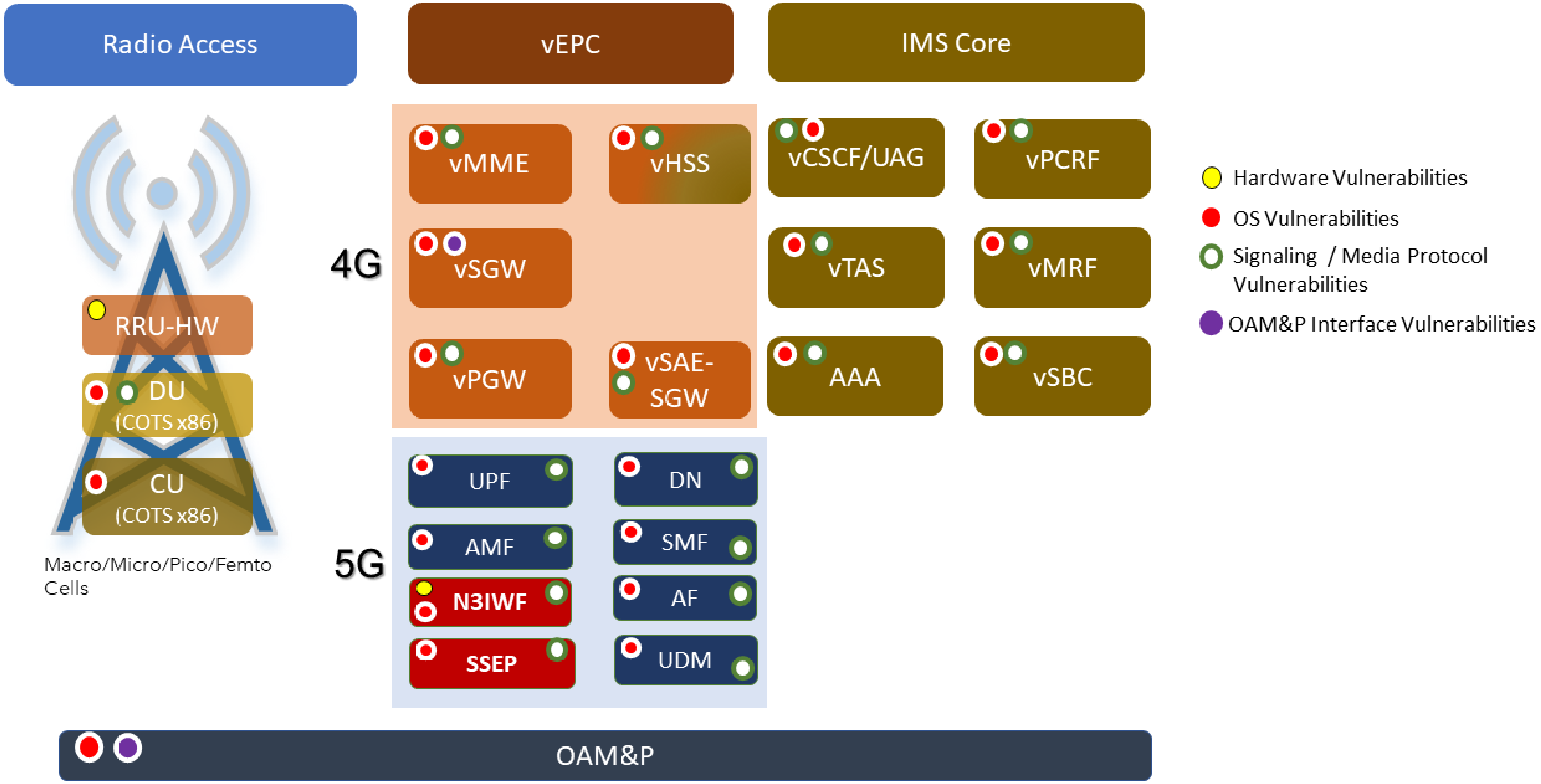
- IMSI catching
- DoS attack against mobile device
- 5G/4G/3G to 2G downgrade
- DoS attack against the network
- SMS spam
- Passive eavesdropping
- Impersonating calls and texts
- Active eavesdropping
- Radio jamming
- Breaking LTE on Layer 2
- FBS enabled LTE billing compromise
- Privacy attacks using side channel information
- 5G authentication vulnerabilities
- LTE FBS enabled DoS, location data and broadcast alert spoofing
- LTE impersonation attacks
- VoLTE eavesdropping
- 4G and 5G user location tracking
- GPRS encryption cryptanalysis
- Hijacked TCP connection eavesdropping

Attack Vectors

- Application
- Signaling
- Transport/Backhaul Network
- Cloud/OS
- Device Hardware (e.g., AGV, 5G gateways)

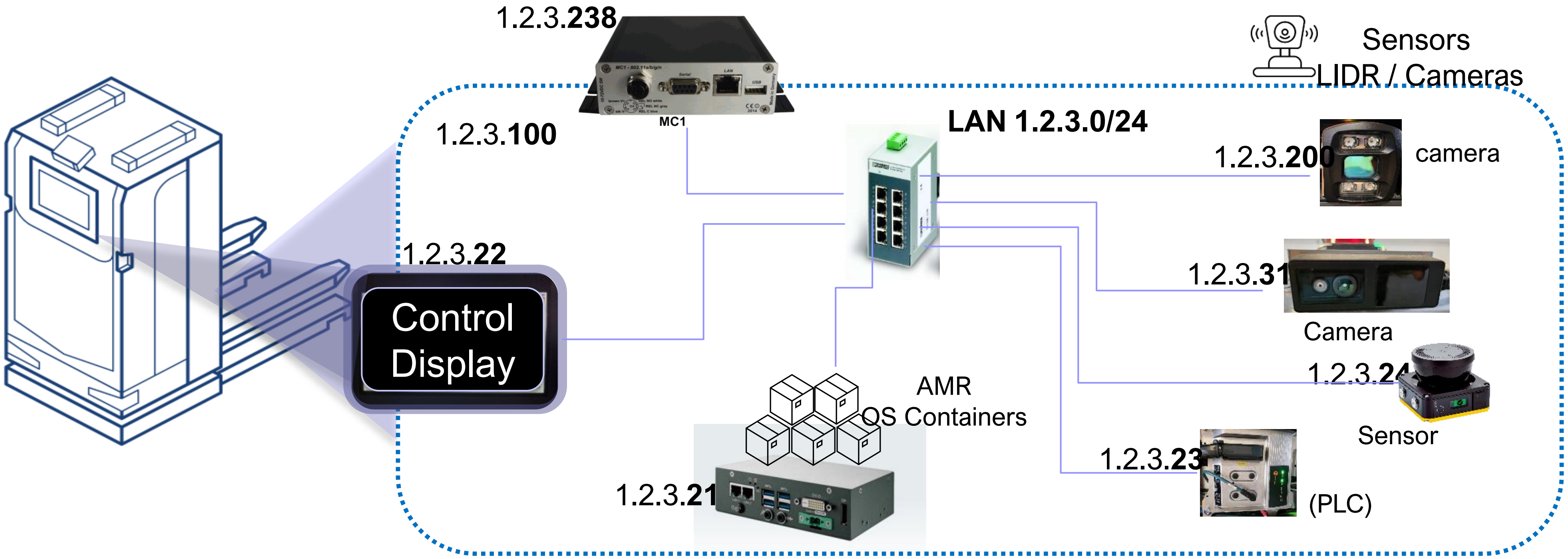


Lessons from 4G/5G security testing



Autonomous Ground Vehicle (AGV) local net

Connected devices may operate their own LAN

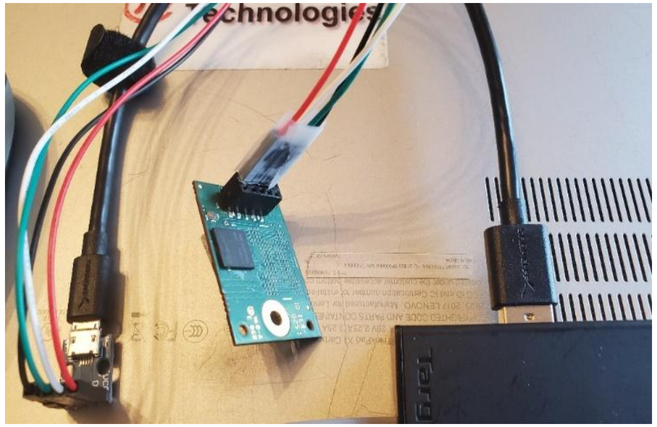


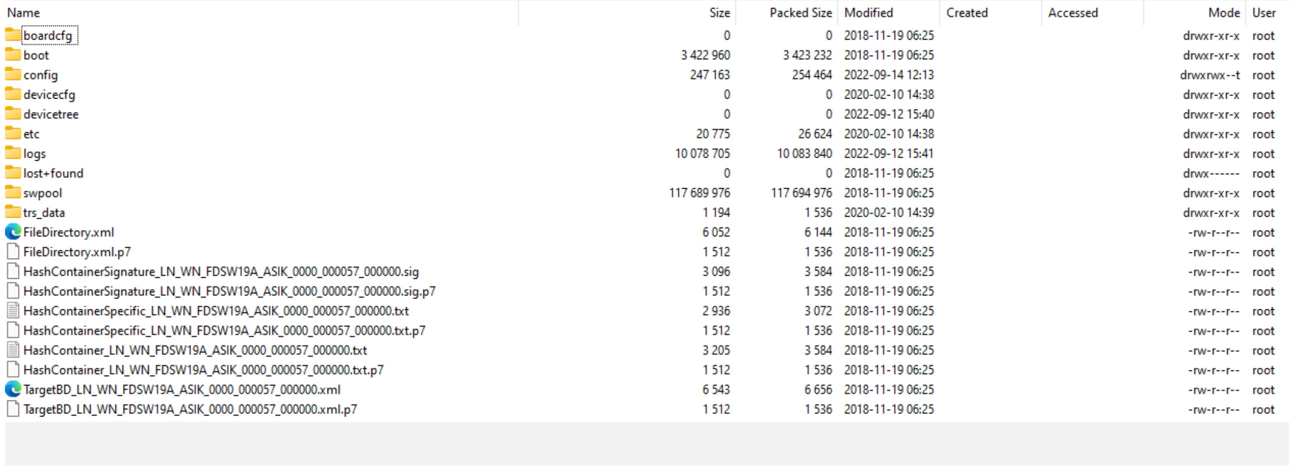
Hardware attacks (5G Gateway)

- Embedded hardware (e.g., UART, JTAG, EEPROM)
- eMMC extraction/manipulation
- Service maintenance port access (RJ45, USB, HDMI)
- SIM/UICC
  - □ *UICC based web browser compromise*
  - □ *UICC credential theft*

Simjacker: an attack which affects some SIM/UICCs that contain web browsers such as the S@T browser. A commonly-used security setting can allow code to be executed when received in SMS messages from any source. The exploit makes use of commands to report a user's location (CellID) or device identity (IMEI) to the attacker's device, without user interaction or knowledge. The exploit could also be used to commit fraud (sending SMS/making calls), or perform other actions such as opening a specific site on the device's web browser. Zero-security level should be used for Pull messages to protect against this attack.

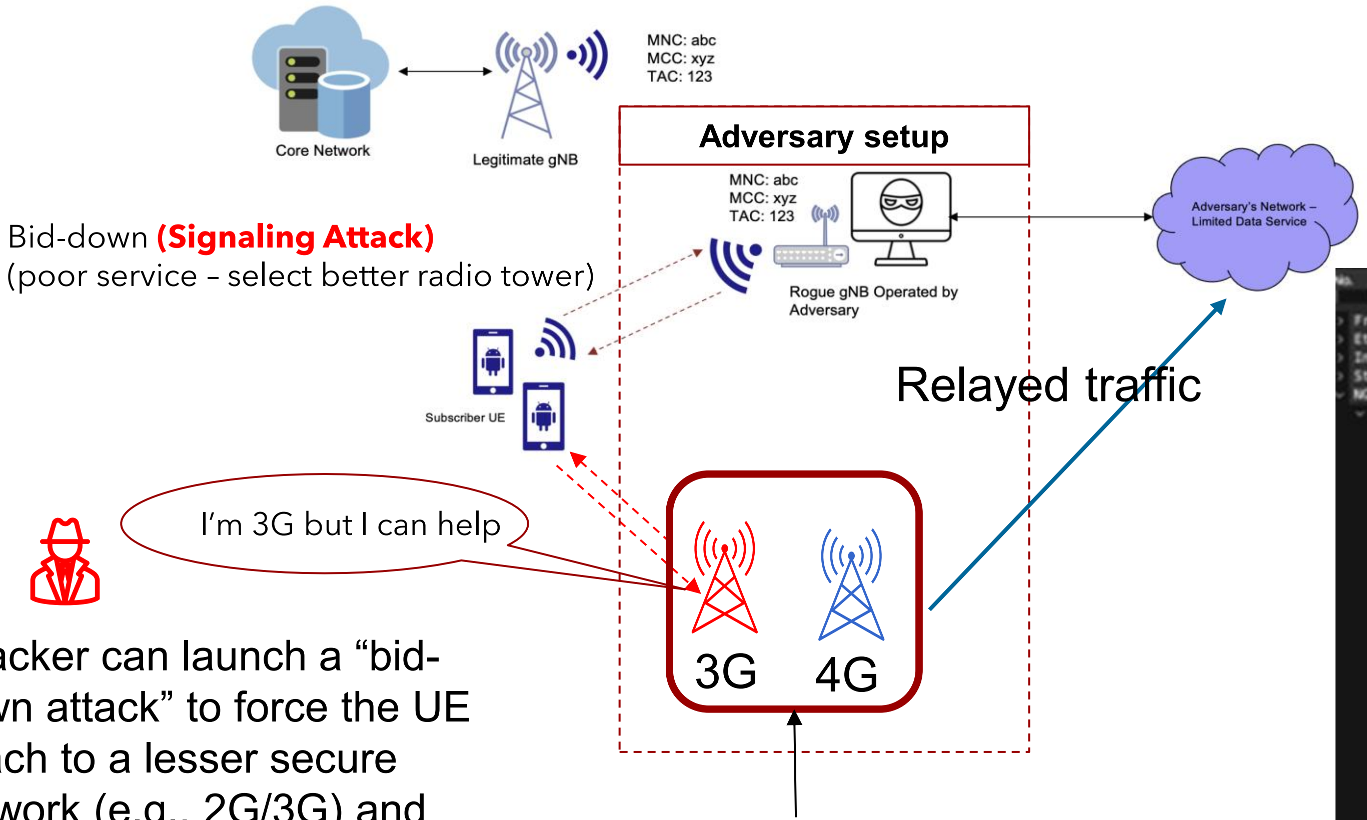
eMMC extraction and manipulation





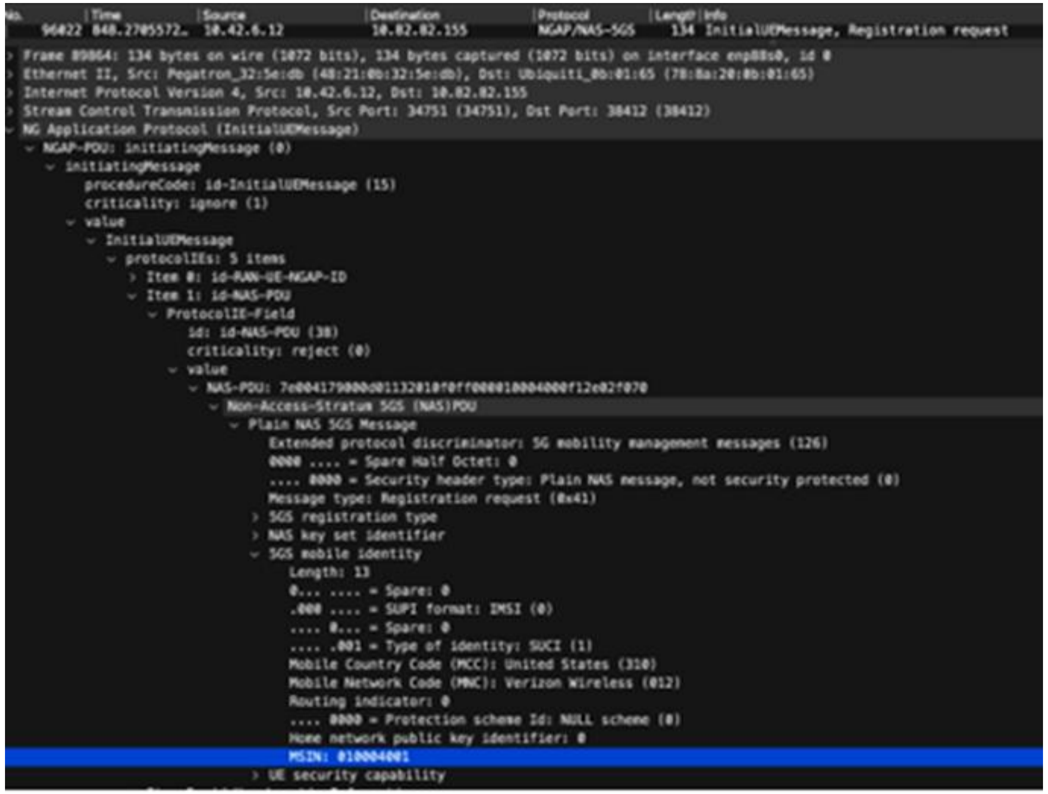
Name	Size	Packed Size	Modified	Created	Accessed	Mode	User
boardcfg	0	0	2018-11-19 06:25			drwxr-xr-x	root
boot	3 422 960	3 423 232	2018-11-19 06:25			drwxr-xr-x	root
config	247 163	254 464	2022-09-14 12:13			drwxrwx--t	root
devicecfg	0	0	2020-02-10 14:38			drwxr-xr-x	root
devicetree	0	0	2022-09-12 15:40			drwxr-xr-x	root
etc	20 775	26 624	2020-02-10 14:38			drwxr-xr-x	root
logs	10 078 705	10 083 840	2022-09-12 15:41			drwxr-xr-x	root
lost+found	0	0	2018-11-19 06:25			drwx------	root
swpool	117 689 976	117 694 976	2018-11-19 06:25			drwxr-xr-x	root
trs_data	1 194	1 536	2020-02-10 14:39			drwxr-xr-x	root
FileDirectory.xml	6 052	6 144	2018-11-19 06:25			-rw-r--r--	root
FileDirectory.xml.p7	1 512	1 536	2018-11-19 06:25			-rw-r--r--	root
HashContainerSignature_LN_WN_FDSW19A_ASIK_0000_000057_000000.sig	3 096	3 584	2018-11-19 06:25			-rw-r--r--	root
HashContainerSignature_LN_WN_FDSW19A_ASIK_0000_000057_000000.sig.p7	1 512	1 536	2018-11-19 06:25			-rw-r--r--	root
HashContainerSpecific_LN_WN_FDSW19A_ASIK_0000_000057_000000.txt	2 936	3 072	2018-11-19 06:25			-rw-r--r--	root
HashContainerSpecific_LN_WN_FDSW19A_ASIK_0000_000057_000000.txt.p7	1 512	1 536	2018-11-19 06:25			-rw-r--r--	root
HashContainer_LN_WN_FDSW19A_ASIK_0000_000057_000000.txt	3 205	3 584	2018-11-19 06:25			-rw-r--r--	root
HashContainer_LN_WN_FDSW19A_ASIK_0000_000057_000000.txt.p7	1 512	1 536	2018-11-19 06:25			-rw-r--r--	root
TargetBD_LN_WN_FDSW19A_ASIK_0000_000057_000000.xml	6 543	6 656	2018-11-19 06:25			-rw-r--r--	root
TargetBD_LN_WN_FDSW19A_ASIK_0000_000057_000000.xml.p7	1 512	1 536	2018-11-19 06:25			-rw-r--r--	root

Rogue gNB – standalone (Sting Ray)


Core Network
Legitimate gNB
MNC: abc
MCC: xyz
TAC: 123
Adversary setup
MNC: abc
MCC: xyz
TAC: 123
Rogue gNB Operated by Adversary
Adversary's Network – Limited Data Service
Bid-down (Signaling Attack)
(poor service – select better radio tower)
Subscriber UE
Relayed traffic
I'm 3G but I can help
3G
4G
Acts as a network extender

- Ability to capture IMSI
- Obtain location information
- UE service disruption

Attacker can launch a "bid-down attack" to force the UE attach to a lesser secure network (e.g., 2G/3G) and ultimately eavesdrop conversations.



```
No.    Time            Source        Destination    Protocol      Length Info
 96022 848.2705572…  10.42.6.12    10.82.82.155   NGAP/NAS-5GS    134 InitialUEMessage, Registration request
> Frame 89864: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface enp88s0, id 0
> Ethernet II, Src: Pegatron_32:5e:db (48:21:0b:32:5e:db), Dst: Ubiquiti_0b:01:65 (78:8a:20:0b:01:65)
> Internet Protocol Version 4, Src: 10.42.6.12, Dst: 10.82.82.155
> Stream Control Transmission Protocol, Src Port: 34751 (34751), Dst Port: 38412 (38412)
v NG Application Protocol (InitialUEMessage)
  v NGAP-PDU: initiatingMessage (0)
    v initiatingMessage
        procedureCode: id-InitialUEMessage (15)
        criticality: ignore (1)
      v value
        v InitialUEMessage
          v protocolIEs: 5 items
            > Item 0: id-RAN-UE-NGAP-ID
            v Item 1: id-NAS-PDU
              v ProtocolIE-Field
                  id: id-NAS-PDU (38)
                  criticality: reject (0)
                v value
                  v NAS-PDU: 7e004179000d01132010f0ff00001000400f12e02f070
                    v Non-Access-Stratum 5GS (NAS)PDU
                      v Plain NAS 5GS Message
                          Extended protocol discriminator: 5G mobility management messages (126)
                          0000 .... = Spare Half Octet: 0
                          .... 0000 = Security header type: Plain NAS message, not security protected (0)
                          Message type: Registration request (0x41)
                        > 5GS registration type
                        > NAS key set identifier
                        v 5GS mobile identity
                            Length: 13
                            0... .... = Spare: 0
                            .000 .... = SUPI format: IMSI (0)
                            .... 0... = Spare: 0
                            .... .001 = Type of identity: SUCI (1)
                            Mobile Country Code (MCC): United States (310)
                            Mobile Network Code (MNC): Verizon Wireless (012)
                            Routing indicator: 0
                            .... 0000 = Protection scheme Id: NULL scheme (0)
                            Home network public key identifier: 0
                            MSIN: 010004001
                        > UE security capability
```

6G Security considerations

1. Physical layer security (i.e., spectrum sharing attacks, jamming)
2. **Signaling/User-plane security and privacy**
3. 6G sensing and security implications
4. Hetnets (e.g., WiFi-evolution/5G/6G) security concerns
5. AI/ML Security considerations
6. User and Device Identity Management
7. **Zero trust adoption for RAN and 6G Core components**
8. Non terrestrial networks
9. **Supply Chain**; will have to adopt to new paradigms for security assurance with greater OEM accountability and requirements for product security assurance and certification (e.g., CTIA, IEEE 2621, GSMA-NESAS)
10. Tangential Technologies
    - □ *Distributed ledger technology (DLT)*
    - □ *Visible light communication (VLC)*
    - □ *Quantum computing*

Security Challenge - Signaling

6G will feature a **hyper-dense ecosystem** of devices, leading to an explosion in signaling traffic. This sheer volume, combined with increased **protocol complexity** and software-defined interfaces, creates a massive attack surface.

1

6G Signaling Integrity and Confidentiality (1of2)

- **Signaling Plane Attacks (not exhaustive list)**
  - □ **Signaling Message Manipulation and Replay Attacks**
    - **Message Impersonation**: Malformed Signaling Messages, Traffic Amplification
    - **Message Replay**: valid authentication signaling or modify authorization tokens to gain unauthorized access to network resources or sensitive services.
    - **Message Injection: Falsify Control Information for New Capabilities (**e.g., Inject false control data for RIS, leading to suboptimal or malicious beamforming.)
  - □ **Traffic analysis and Eavesdropping**
    - **Impact on User Privacy**: If signaling encryption is weak, improperly implemented, or compromised at a network node, it can expose highly precise user location and inferred activities.

6G Signaling Integrity and Confidentiality (2of3)

- **Signaling Plane Attacks (not exhaustive list)**
  - □ **Leakage of Network Control and Security Parameters**
    - (e.g,. intercepting critical network topology information, slice configuration details and potentially revealing operational parameters of slices dedicated to critical industries, security keys or pre-keying material, parameters for AI models used in network management, or control instructions for sensitive network functions.)
    - Information collected from signaling messages (e.g., device capabilities, active services, security algorithms/policies) can be invaluable for attackers in planning more sophisticated and targeted subsequent attacks.
  - □ **Disrupt Network Orchestration:** Send crafted messages to MANO components or AI controllers, potentially leading to incorrect network configurations, resource misallocation, or even cascading failures if AI models are fed manipulated signaling telemetry.

6G Signaling Integrity and Confidentiality (3of3) (continued)

- **"Harvest Now, Decrypt Later":** Even if signaling messages are encrypted with current strong algorithms, their capture by adversaries poses a long-term risk, as future advancements (e.g., quantum computing) could break this encryption, exposing sensitive 6G operational and user data years later.

Security Challenge – Network Complexity

The future network is a **complex** mesh of diverse devices, AI-driven functions, and integrated sensing and communication technologies which introduces a vast and **dynamic attack surface** which necessitates a paradigm shift towards a Zero Trust Architecture (ZTA).

2

6G Zero Trust: A Paradigm Shift for Next-Generation Security

- **What is Zero Trust (ZT) in 6G?**
  - □ *An evolution of security principles, moving away from perimeter-based trust.*
  - □ *Assumes no implicit trust for any entity (users, devices, network functions, applications) inside or outside the network.*
  - □ *Crucial for the highly dynamic, disaggregated, and AI-driven 6G environment. (Derived from general ZT principles and the complexity implied for future networks).*

ZTA = Trust NOTHING, verify EVERYTHING

6G Zero Trust: A Paradigm Shift for Next-Generation Security

Core Principles for 6G Zero Trust: (Inspired by NIST SP 800-207 referenced in the 5G document)

- **Never Trust, Always Verify**
  - Explicitly verify every access request, regardless of origin.
- **Assume Breach**
  - Design the system assuming attackers are already present or will inevitably penetrate defenses.
- **Least Privilege Access**
  - Grant only the necessary permissions for a specific task and time.
- **Micro-segmentation**
  - Divide the network into small, isolated zones to contain threats.
- **Comprehensive Data Governance & Security Analytics**
  - Continuously monitor and analyze all network activity for threats. (Extrapolated from KI#1's focus on data exposure for monitoring)

6G Zero Trust: A Paradigm Shift for Next-Generation Security

- **Why ZT is Critical for 6G:**
  - □ ***Massive*** *increase in* ***connected devices*** *and diverse service requirements.*
  - □ ***Complex interactions*** *between AI-driven components and virtualized functions.*
  - □ ***Expanded attack surface*** *due to new technologies (e.g., integrated sensing & communication, immersive multimedia applications, massive amount of smart devices, open programable API’s).*

Enabling 6G Zero Trust: Key Considerations & Foundational Enablers

- **Continuous & Automated Security Monitoring:**
  - □ ***Comprehensive Data Exposure:*** *Define what security-relevant data (e.g., from NFs, APIs, slices) needs to be collected and exposed for real-time evaluation.*
  - □ ***AI-Powered Analytics:*** *Utilize advanced AI/ML for threat detection, anomaly identification, and predicting potential attacks from vast data streams. (Logical extension for 6G).*
  - □ ***Standardized Data Formats:*** *Facilitate interoperability and automated processing of security data.*

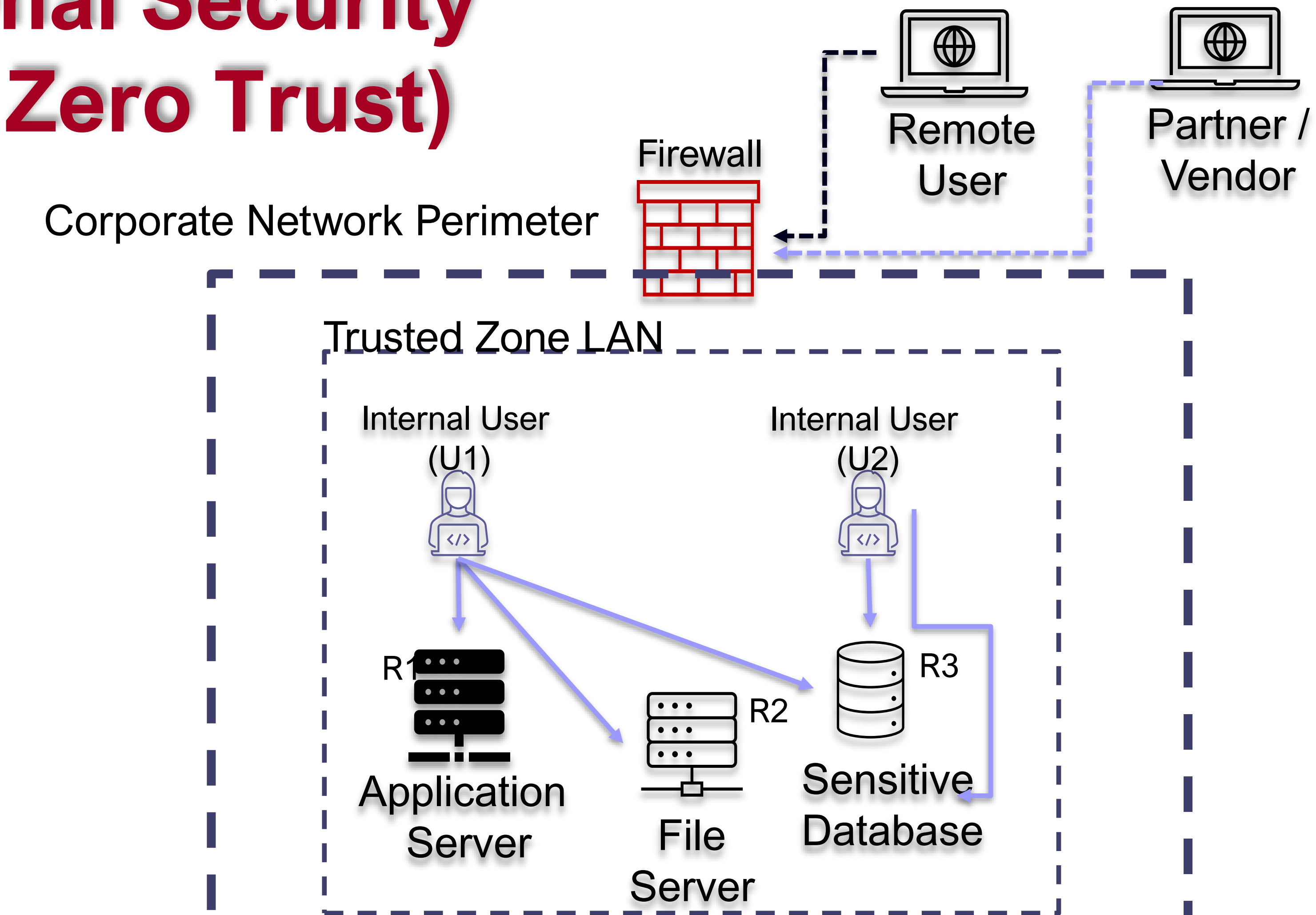
Enabling 6G Zero Trust: Key Considerations & Foundational Enablers

- **Dynamic & Adaptive Policy Enforcement:**
  - □ ***Intelligent Policy Decision Points (PDPs)***
    - Dynamically assess trust levels and make access control decisions based on real-time risk posture.
  - □ ***Agile Policy Enforcement Points (PEPs)***
    - NFs, NRF-equivalents, or SCP-equivalents in 6G must be capable of enforcing granular policies swiftly based on PDP instructions.
  - □ ***Automated Response***
    - Enable rapid, automated responses to detected threats to minimize impact.

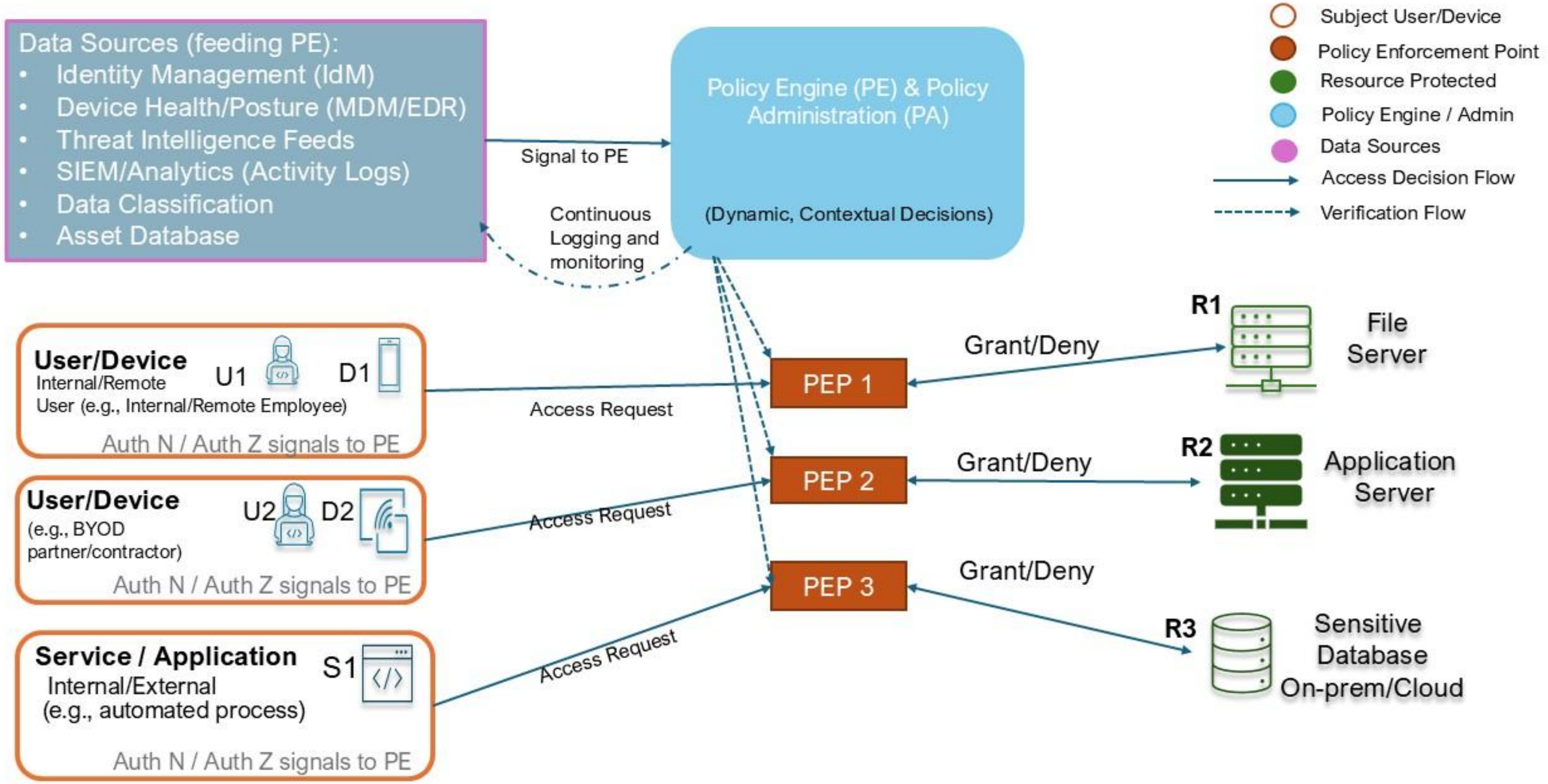
Enabling 6G Zero Trust: Key Considerations & Foundational Enablers

- **Secure Identity & Access Management (IAM) for Everything:**
  - □ *Robust authentication and authorization for all entities (NFs, UEs, services, AI models).*
  - □ *Consideration for new types of identities in a 6G ecosystem.*
- **Resilience and Adaptability:**
  - □ *Design for resilience against sophisticated attacks, including those leveraging AI.*
  - □ *Mechanisms for self-healing and adaptive security postures.*

Traditional Security (Before Zero Trust)



Zero Trust Architecture



Data Sources (feeding PE):
- Identity Management (IdM)
- Device Health/Posture (MDM/EDR)
- Threat Intelligence Feeds
- SIEM/Analytics (Activity Logs)
- Data Classification
- Asset Database

Policy Engine (PE) & Policy Administration (PA)

(Dynamic, Contextual Decisions)

Signal to PE

Continuous Logging and monitoring

User/Device U1 D1
Internal/Remote User (e.g., Internal/Remote Employee)
Auth N / Auth Z signals to PE

User/Device U2 D2
(e.g., BYOD partner/contractor)
Auth N / Auth Z signals to PE

Service / Application S1
Internal/External
(e.g., automated process)
Auth N / Auth Z signals to PE

Access Request

Access Request

Access Request

PEP 1

PEP 2

PEP 3

Grant/Deny

Grant/Deny

Grant/Deny

R1 File Server

R2 Application Server

R3 Sensitive Database On-prem/Cloud

○ Subject User/Device
● Policy Enforcement Point
● Resource Protected
● Policy Engine / Admin
● Data Sources
→ Access Decision Flow
⇢ Verification Flow

ZTA = Trust NOTHING, verify EVERYTHING

Security Challenge – Supply Chain

The 6G ecosystem will be built on a complex, global, and **multi-vendor supply chain**, making it a prime target for attack. Vulnerabilities can be introduced at any stage, from design and manufacturing to deployment and maintenance.

3

Securing the 6G Future: A Resilient Supply Chain and Through Validation

- The 6G Landscape: Amplified Interconnectivity & Risks
  - □ ***Vast Attack Surface***
    - 6G will connect an unprecedented number of diverse devices (IoT, IIoT, wearables, autonomous systems), significantly increasing potential entry points for attackers.
  - □ ***Complex Supply Chains***
    - Global and multi-tiered supply chains for 6G components (hardware, software, AI models) create vulnerabilities to **tampering, counterfeiting**, and **insertion of malicious elements**.

Securing the 6G Future: A Resilient Supply Chain and Through Validation

- The 6G Landscape: Amplified Interconnectivity & Risks
  - □ ***AI-Driven Dynamics***
    - While AI enhances 6G capabilities, it also introduces new security challenges, including adversarial AI attacks and the need to secure AI models themselves throughout their lifecycle.
  - □ ***Data-Centricity***
    - Massive data flows in 6G raise critical concerns regarding data privacy, integrity, and confidentiality

Key Focus Areas for 6G Supply Chain Security

- **Secure Software Development Lifecycle (SSDLC)**
  - □ *Ensuring security is integrated from the design phase.* ***NIST SP 800-204, Security Guidelines for the Software Supply Chain, provides detailed guidance.***
- **Hardware Integrity**
  - □ *Protecting against counterfeit components and hardware Trojans.* ***NISTIR 8276, Key Practices in Software and Hardware Supply Chain Risk Management, addresses hardware considerations.***
- **Software Bill of Materials (SBOM)**
  - □ *Transparency into software components to manage vulnerabilities.* ***NIST plays a leading role in promoting SBOM adoption and standards.***
- **Continuous Monitoring & Response**
  - □ *Adapting to evolving threats throughout the product lifecycle.* ***NIST emphasizes continuous monitoring and incident response as critical elements of cybersecurity (NIST CSF)***

Leveraging Standards for 6G Device & Product Security

- **Building on Proven Frameworks for 6G Assurance**
  - □ *Ensuring device and product security in the 6G era requires leveraging and adapting established security assurance schemes and standards, with strong consideration for NIST's comprehensive guidance on supply chain risk management*
- **ISA/IEC 62443: Securing Industrial Control Systems (IACS) & Critical Infrastructure**
  - □ *Provides a comprehensive framework for the cybersecurity lifecycle of industrial automation and control systems, crucial as 6G integrates with critical infrastructure and manufacturing (IIoT).*
  - □ *Specifies security requirements for product suppliers and secure product development lifecycle processes, including third-party component management. Testing against these standards ensures components and systems meet defined security levels,* ***consistent with NIST's emphasis on supplier security in the supply chain (NIST SP 800-161).***

Leveraging Standards for 6G Device & Product Security

- **Building on Proven Frameworks for 6G Assurance**
  - □ ***IEEE 2621: Advancing IoT Device Security (initially for Medical Devices) (NISTIR 8397)***
    - Establishes a framework for IoT device security evaluation programs, defining assurance levels and test requirements. Its principles of lab-based testing for security functional requirements can be adapted for a broader range of 6G IoT devices. **NISTIR 8397, Security Considerations for the Healthcare Sector, highlights the importance of device security, aligning with IEEE 2621.**
    - Emphasizes evaluation by authorized testing labs to assess compliance with security requirements, promoting a baseline of security for connected devices, **a practice supported by NIST for independent verification.**

Leveraging Standards for 6G Device & Product Security

- **Building on Proven Frameworks for 6G Assurance**
  - □ ***FCC IoT Cyber Trust Mark: Enhancing Consumer IoT Security (NISTIR 8429)***
    - This U.S. voluntary cybersecurity labeling program for consumer IoT products helps consumers identify secure devices. It relies on accredited labs testing against NIST-defined cybersecurity criteria. **NISTIR 8429, Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products, directly underpins this FCC initiative.**
    - Central to the program, third-party labs verify that products meet the required cybersecurity standards before they can bear the "U.S. Cyber Trust Mark," providing a visible indicator of security assurance that can be extended to consumer-facing 6G devices, **demonstrating the practical application of NIST guidelines through independent assessment.**

Leveraging Standards for 6G Device & Product Security

- **Building on Proven Frameworks for 6G Assurance**
  - □ ***NESAS (Network Equipment Security Assurance Scheme): Ensuring Telecom Equipment Integrity (Aligned with NIST SP 800-161)***
    - Developed by GSMA and 3GPP, NESAS provides an industry-defined security assurance framework for network equipment. It assesses both vendor development/lifecycle processes and the security of network equipment itself. **NESAS aligns with the principles outlined in NIST SP 800-161 regarding supply chain security for critical infrastructure.**
    - Relies on independent security test laboratories and auditors to evaluate equipment against defined security requirements and assess vendor processes. This will be vital for the core infrastructure components of 6G networks

Why Security Testing is Non-Negotiable

- **Objectivity & Impartiality**
  - □ *Independent verification provides unbiased assessment of security claims and product robustness, free from vendor bias.* ***NIST promotes independent assessment as a key element of risk management (e.g., NIST CSF, Identify, Protect, Detect, Respond, Recover).***
- **Expertise & Specialization**
  - □ *Cyber labs possess specialized tools, knowledge, and methodologies to conduct in-depth security evaluations that may be beyond the capabilities of individual manufacturers.*
- **Building Ecosystem Trust**
  - □ *Verifiable security credentials foster confidence among consumers, enterprises, and governments, facilitating technology adoption and interoperability.* ***NIST's focus on trust and transparency in the supply chain underscores the importance of verifiable security (e.g., NIST SP 800-161).***
- **Proactive Vulnerability Discovery**
  - □ *Rigorous testing helps identify and mitigate vulnerabilities before products are widely deployed, reducing the risk of large-scale breaches.* ***This aligns with NIST's proactive risk management approach***

The Path Forward for 6G Security Assurance

- **Harmonization & Evolution**
  - □ *Adapting and potentially harmonizing aspects of these standards to address the unique scale, complexity, and AI-integration of 6G*
- **Global Collaboration**
  - □ *International cooperation in developing and recognizing third-party testing and certification schemes for 6G*
- **Dynamic Assurance**
  - □ *Moving towards continuous assessment models to address the evolving threat landscape and software-defined nature of 6G*

Drop me an email if you would like a T-Shirt and share your passion for security ;-)

Q & A

peter.thermos@palindrometech.com
www.palindrometech.com