ISASecure®

Securing Private 5G networks in manufacturing using penetration testing

Case Study

Palindrome Technologies
ASSURANCE | TRUST | CONFIDENCE
21 Roszel Road, Suite 105, Princeton, NJ 08540
info@palindrometech.com
www.palindrometech.com

Q: Why did the forklift operator at the 5G-enabled manufacturing plant get a promotion?

A: Because he always knew how to lift …

the security standards.”

Since its inception in 2005,

Palindrome Technologies has earned a reputation as a trusted provider of cybersecurity services for top organizations spanning complex telecommunications networks to high assurance environments.

We bring a meticulous discipline to cybersecurity through applied research, scientific analysis, and rigorous testing.

With an unwavering commitment to excellence, we enable clients to operate with confidence in a hostile cyberspace.

Visit palindrometech.com.

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)

NIST Guidance on 5G security

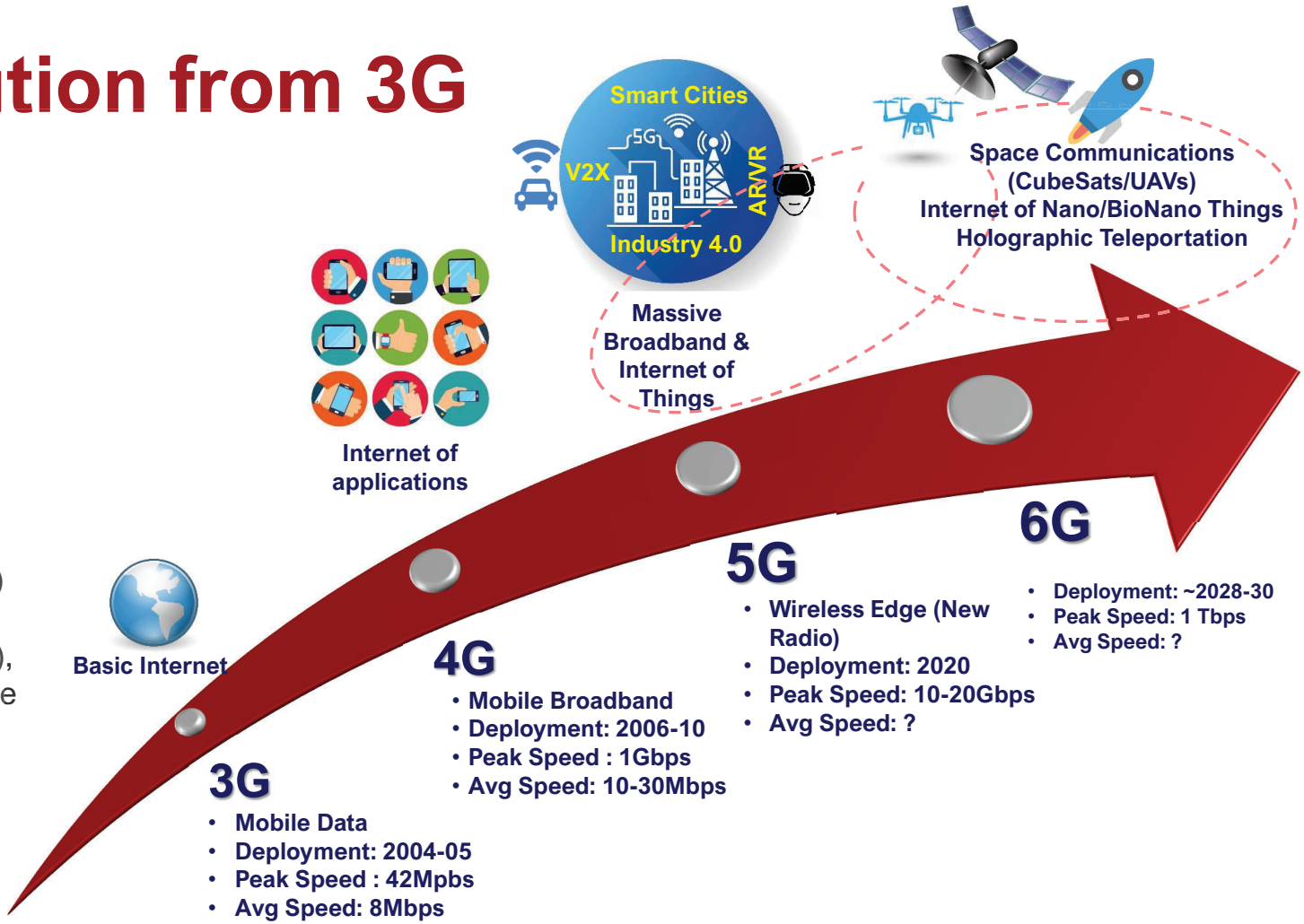
"*The 5G standards do not specify cybersecurity protections to deploy on the underlying information technology (IT) components that support and operate the 5G system. This lack of information increases the* ***complexity*** *for organizations planning to leverage 5G*."

[5G Security, NIST SPECIAL PUBLICATION 1800-33B, 2022]

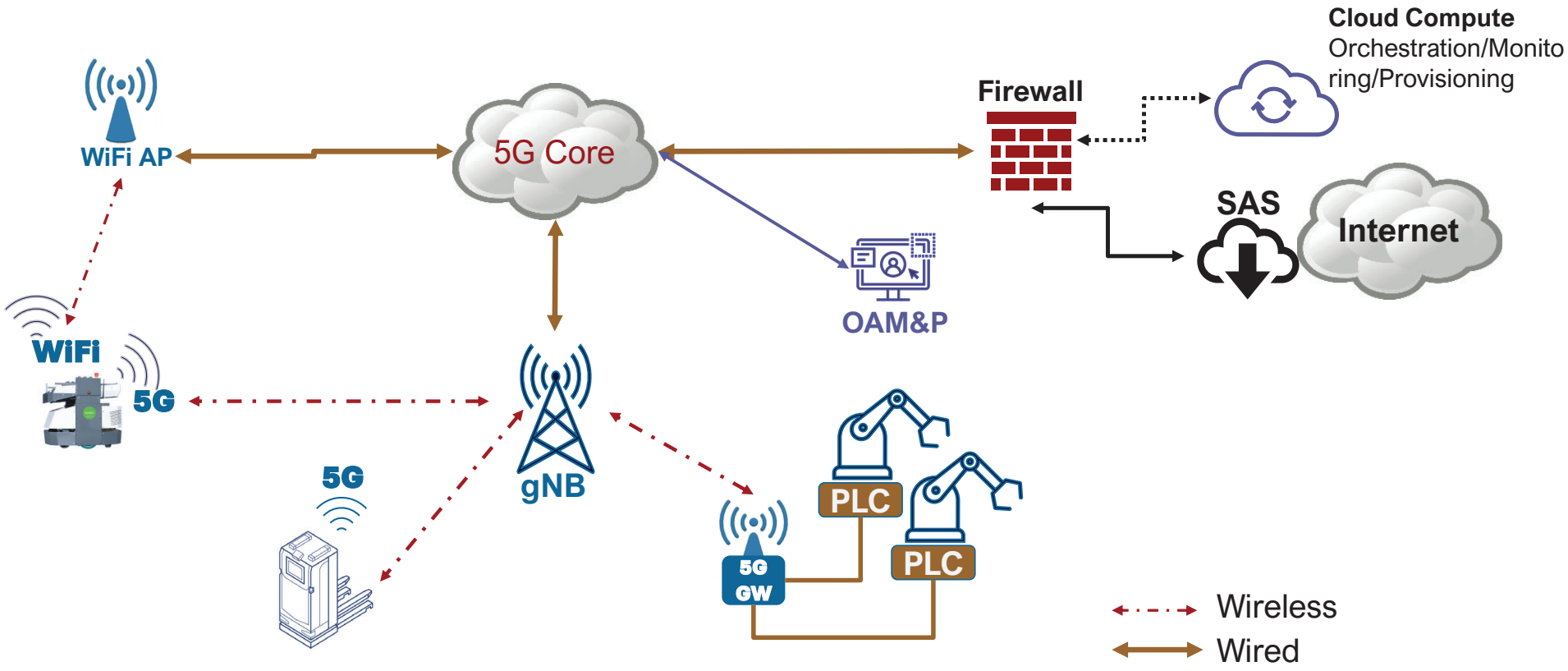
Cellular Evolution from 3G

International Mobile Telecommunications Vision

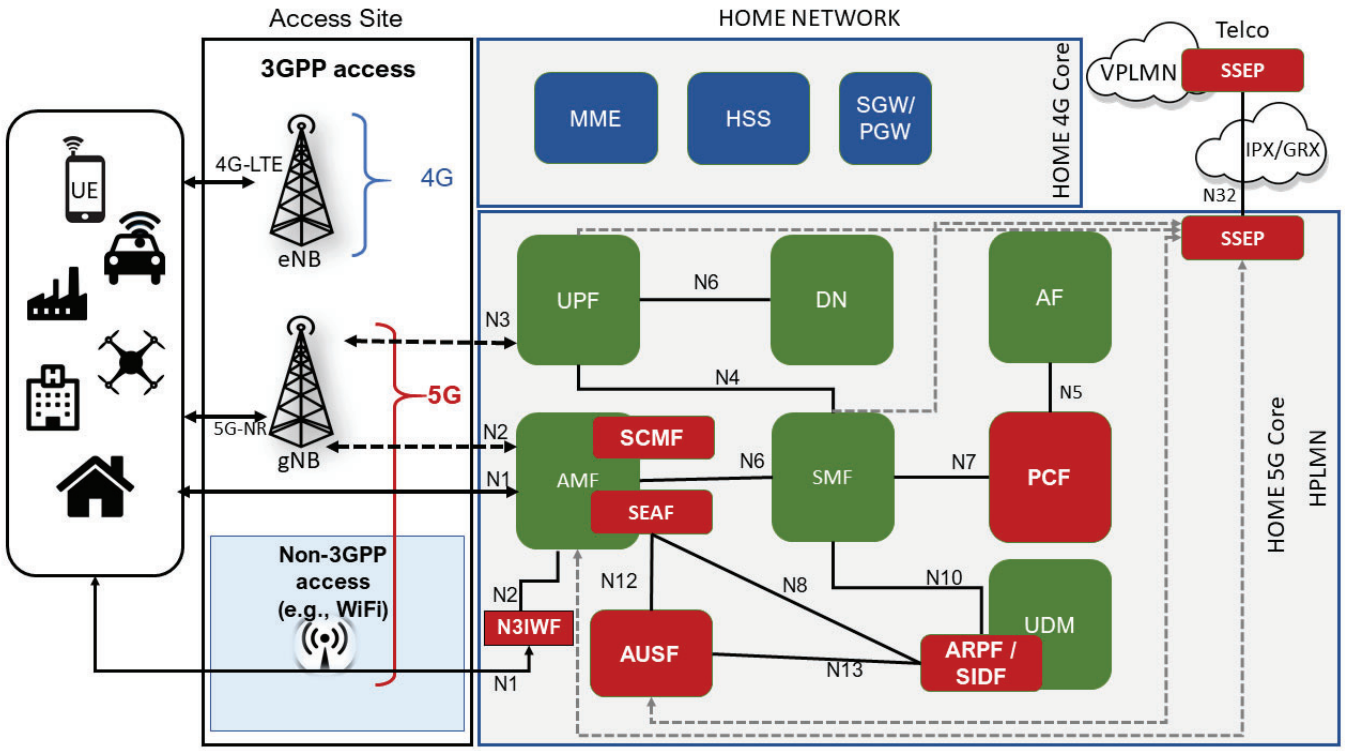
- Three usage scenarios that distinguish 5G from fourth generation (4G)
  1. Enhanced Mobile Broadband (**eMBB**)
  2. ultra-reliable, low-latency communications (**URLLC**)
  3. massive Machine-Type Communications (**mMTC**), also referred to as massive Internet of Things (mIoT)



5G in manufacturing (simplified view)



5G Core - Architecture



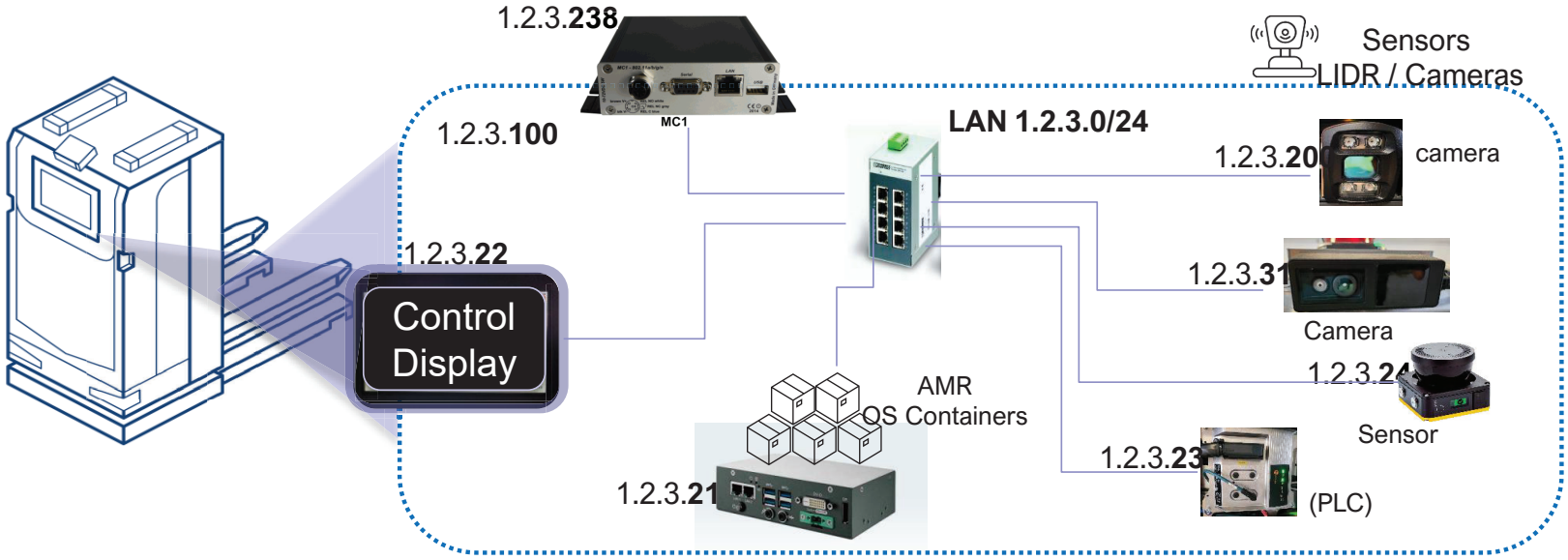
5G Core Network Elements / Functions

- **AMF**; Access and Mobility Management Function
- **UPF**; The User Plane Function
- **UDM**; Unified Data Management
- **SMF**; Session Management Function
- **PCF**; Policy Charging Function
- **AUSF**; Authentication Server Function
- **N3IWF**; N3-Inter-Working Function
- **SSEP**; Security Edge Protection Proxy

- Decoupled architecture
- Components are Virtualized Functions
- Multiple API's
- NEF / SEPP expose core

Autonomous Ground Vehicle (AGV) local net

Connected devices may operate their own LAN



Security Challenges in Industrial Automation and Control Systems (IACS)

- Legacy Systems
- Increased Connectivity
- Critical Infrastructure
- Supply Chain Vulnerabilities
- Hardware-Level Vulnerabilities
- Difficulty in Patching and Updates

Security Challenges Introduced by 5G for IACS

Integrating 5G into IACS environments introduces a new set of security challenges:

- Expanded Attack Surface
- Network Slicing Attacks
- Decentralized Security
- Increased Reliance on Software
- Radio Interface Security
- Integration with Untrusted Networks
- Real-time Requirements
- Evolving Threat Landscape

Security Analysis and Testing Process

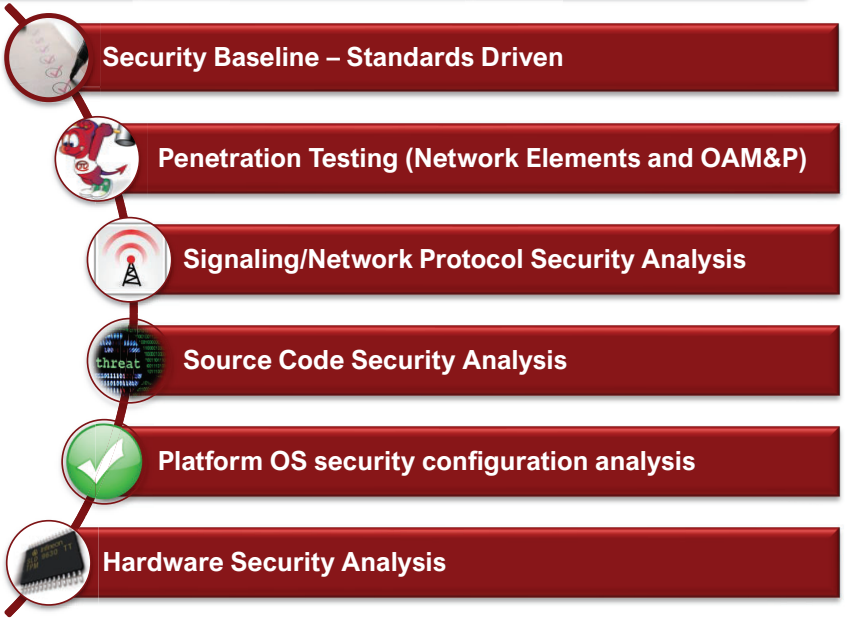
Objective: demonstrate that security assurance principles and best practices have been implemented properly.

- Verification
- Categorization
- Prioritization

Scope Definition → Threat Modeling → Evaluation → Results Analysis → Final Report

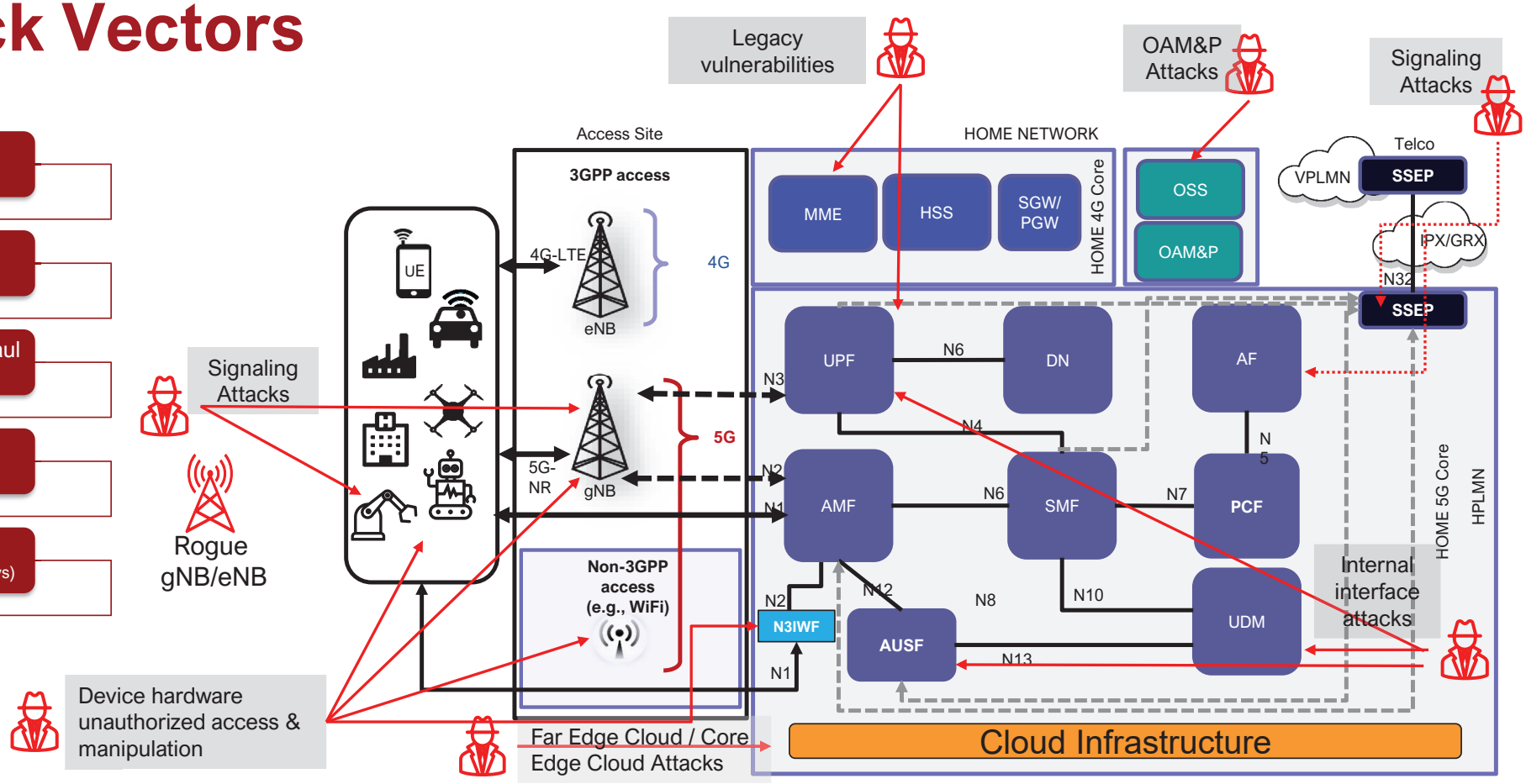
- Product Team
- Product(s) in scope
- Objectives
- Requirements
- Timeline

- Identify applicable Threats
- Categorize and Prioritize
- Develop Threat Model
- Develop Test Strategy



Attack Vectors

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



Attack examples

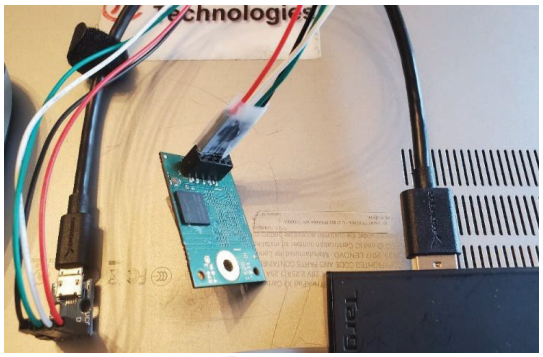
- Hardware
- RAN attacks - Rogue base station (eNB/gNB)
- Administration, Management and Provisioning interfaces

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

5G OAM&P Application (SQL Injection)

- `/api/csv/subscriber` module contains sensitive data

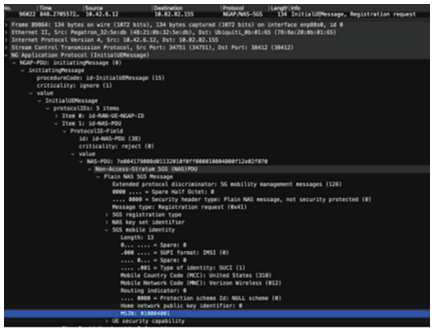
```
HTTP/1.1 200 OK
Content-Type: text/csv; header=present; charset=UTF-8
Content-disposition: attachment;filename=subscriber.csv
Content-Length: 42388

"id","admin_state","sub_type","imsi","tmsi","ptmsi","imei","msisdn","authorised","privilege_level","sip_client_attachment"
,"mno_attachment","local_ps_attachment","mno_ps_attachment","lac","previous_lac","tac","domain","ki","sip_username","sip_passw
ord","auth_algorithm","ciphering_algorithm","cell_id","name","additional_info","call_forward_unconditional","call_forward_on_b
usy","call_forward_on_no_answer","call_forward_on_out_of_reach","call_forward_condition_time","welcome_sms_sent","sip_profile_
id","mt_sip_profile_id","user_portal_username","last_mwi","opc","topc","measurement_record_interval","priority","dl_ambr","ul_
ambr","mno_cs_activity_time","mno_ps_activity_time","classmark1","nas_encryption","local_cs_activity_time","local_ps_activity_
time","last_call_divert_status","short_network_name","call_divert_sms_prefix","wifi_enabled","record_measurements","vlr_numbe
r","msc_number","sgsn_number","hlr_number","mme_number","hss_host","hss_realm","mme_host","mme_realm","aaa_host","aaa_realm","s
ip_client_detach_time","telephony_allowed","emergency_calls_allowed","mt_sms_allowed","mo_sms_allowed","visitor","digest_aka_s
upported","terminate_pdp_context_req","force_camping","subscription_profile_preference_id","csg_ids","cag_data","ran_type","en
odeb_id","t31324","t31412","gnb_id","odb_all_packet_services_barred","odb_all_out_calls_barred","odb_out_int_calls_barred","od
b_out_int_calls_hplmn_barred","non_3gpp_ip_access_allowed","active_imsi","active_msisdn","csi_profile_id","iab_operation_allow
ed","smsf_number","smsf_host","smsf_realm","ipsmgw_host","ipsmgw_realm"
1,2,"data_only","315010005001092","","","354392700003612","551092",1,0,"DETACHED","DETACHED","DETACHED","DETACHE
D",0,0,50,"127.0.0.1","#d13OACtB5vbzj2POSBzGBRvP3b2Bwaf6f0fLuYvhQBmraW","","###$Ti+ahShFJo7CBuIfLXG5ow==","milenage","best",16
1,"CLEAR-TEXT-SIP-PASSWORD","Prod","","","","",0,0,1,0,"",0,"#/aF4elidQLI7CuzSF2YgR/j4Br/o5
iEUuundbCFlJVlUAidVPQ/cuj/gQ4Ro","###$Ti+ahShFJo7CBuIfLXG5ow==",1,0,500000,500000,"","",0,1,"","",0,"","",1,0,"","","","","","
","","","","","","",1,1,1,1,0,0,0,0,0,"","",3,0,0,0,10,0,0,0,0,1,"","",0,0,"","","","",""
```

5G Signaling – Selected Vulnerabilities

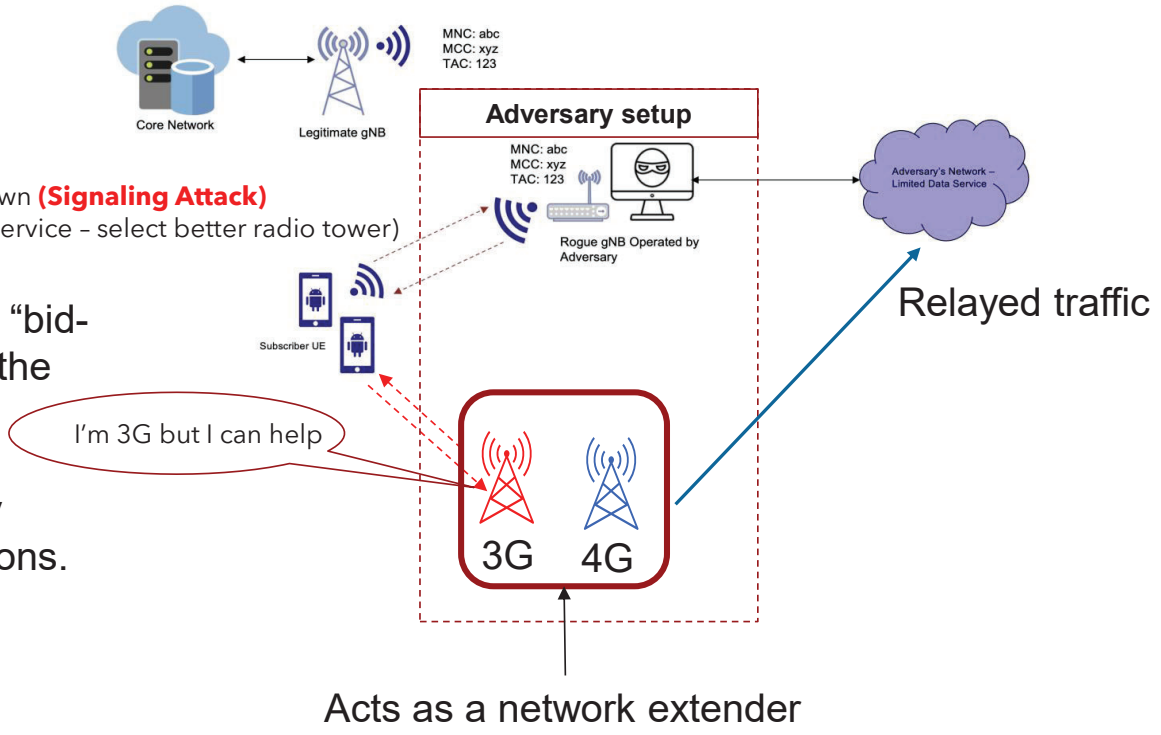
- RAN signaling
  - No Data Confidentiality & Integrity Protection from gNB to SeGW - HIGH
  - No Ciphering & Integrity of User Data based on Security Policy sent by the SMF – HIGH
  - Rogue gNB can anchor with 5G core without authentication / verification

Rogue gNB – standalone (Sting Ray)

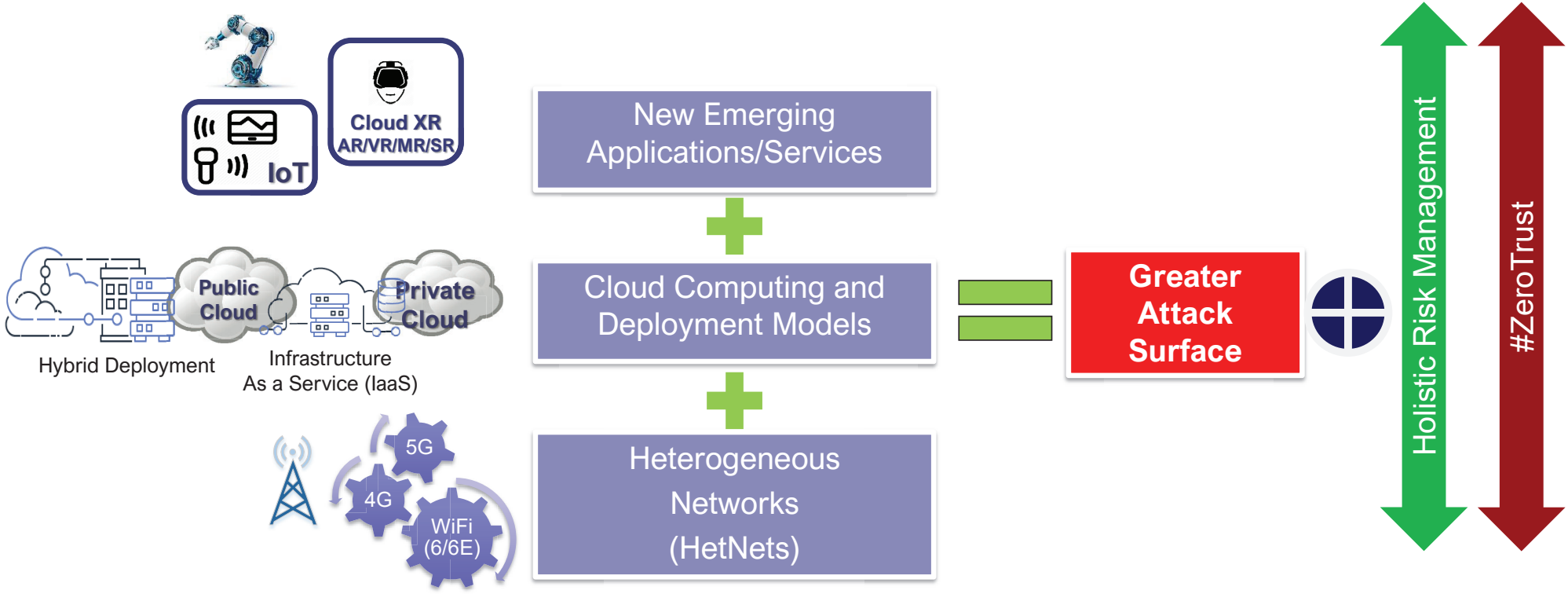
- Ability to capture IMSI
- Obtain location information
- UE service disruption



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.



Securing Complexity in Private 5G Enterprise

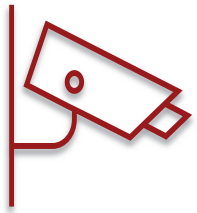


6 ways ISA 62443 Secures Private 5G Devices

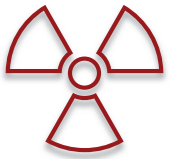
1. **Secure Device Development**
   - *Ensures devices connected to private 5G networks are built with security in mind, covering secure design, coding, testing, and vulnerability management.*
   - *Mandates security capabilities like authentication, encryption, and secure communication, which are essential for 5G devices.*

2. **Network Segmentation and Access Control**
   - *Supports robust network segmentation to isolate critical devices from less secure zones within a 5G network.*
   - *Implements role-based access control and identity management, reducing the risk of unauthorized access.*

6 ways ISA 62443 Secures Private 5G Devices

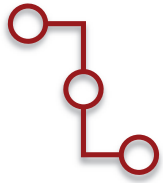


3. **Security Monitoring and Incident Response**
   - *Provides guidelines for continuous monitoring and rapid incident response, crucial for real-time 5G communication environments.*
   - *Ensures that devices can detect and report security breaches quickly.*



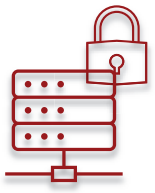
4. **Risk Management and Threat Modeling**
   - *Establishes a structured approach to identify and mitigate risks, aligning with the dynamic threat landscape of 5G.*
   - ***Encourages periodic security assessments and vulnerability management.***

6 ways ISA 62443 Secures Private 5G Devices



5. Supply Chain and Device Integrity

- *Focuses on securing the entire lifecycle of devices, from manufacturing to deployment, ensuring supply chain integrity.*
- *Mandates measures to prevent tampering and unauthorized firmware updates.*



6. Cryptography and Secure Communications

- *Requires robust encryption for data in transit and at rest, aligning well with security requirements for 5G networks.*

Addressing Security Challenges in Private 5G

- Security by Design (authentication, authorization, encryption)
- Defense-in-Depth
- Zero Trust Architecture
- Network Segmentation
- Vulnerability Management
- Supply Chain Security
- Compliance with Standards and Frameworks
- Security Awareness and Training

5G Threat Domains – Top 10
(from field analysis)

1. Hardware (edge devices - UE, IoT devices, gNB/eFemtos/extenders)
2. RAN Signaling
3. 5G Core Signaling
4. Network Slicing
5. Network Peering Functions – Security Edge Protection Proxy (SEPP)
   - *Partner networks*
6. Network Exposure Function (NEF)
7. Network Infrastructure (fronthaul/mid-haul/backhaul)
8. Virtualization / Cloud Infrastructure / MEC (Multi-access Edge Computing)
9. Management and Network Orchestration Applications (MANO/OAM&P/OSS)
10. Software Supply Chain (SBOM)

Securing Private 5G – Summary Areas

Threat Modeling

- How does 5G and MEC impact my operations and infrastructure?
- Consider equipment and infrastructure Threats (e.g., hardware, software, cloud)
- Threats associated with the type of applications/services (e.g., APIs, protocols, mobile apps)

Security Requirements

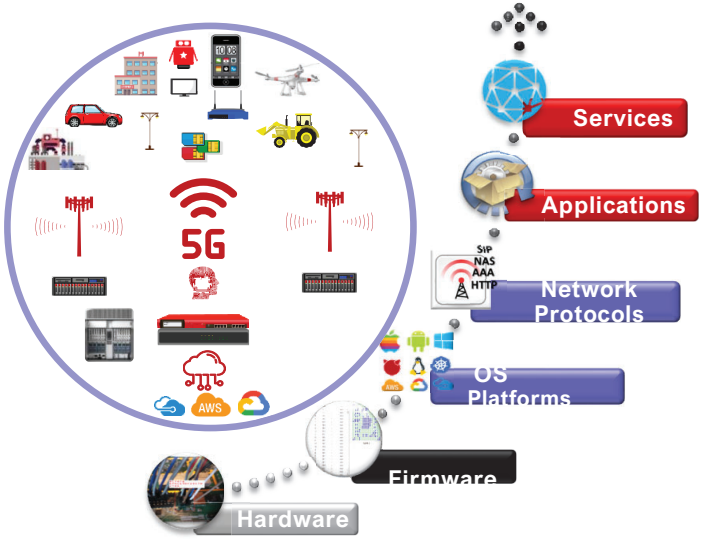
- Leverage relevant industry standard and best practices for your implementation
- Security Requirements Definition
  - ➢Augmented network (my data resides in the cloud which extends my virtual network footprint)

Validation

- Initial pre-deployment evaluation
- Continuous Security Analysis / Penetration Testing

Monitoring

- Continuous Monitoring
- Network / Cloud
- Device



5G and Device Security - Frameworks and Standards

- **DHS CISA**
  - *National Strategy to Secure 5G*
  - *Framework to Conduct 5G Testing*
- **GSMA**
  - ***Future Networks***
  - ***NESAS*** *(**Network Equipment Security Assurance Scheme**)*
- **FCC** CSRIC VII Report on Risk to 5G from Legacy Vulnerabilities and Best Practices for Mitigation. (June 10, 2020)
- **NIST**
  - *5G Security*
  - *Cloud Security Reference Architecture*
  - *General Access Control Guidance for Cloud Systems*
  - *Zero Trust Architecture*
- **ISASecure**
  - *ISASecure® Certifications - ICS Cybersecurity Standards & Assurance*

Thank you!
Q & A

If you would be interested in a free t-shirt email at:
peter.thermos@palindrometech.com

Supplemental Material

Industry Accreditations and Certifications (1 of 2)

ISO 17025 Accredited Testing Lab for:
- IMS Security Assurance
- LTE Security Assurance
- Network Security Assurance
- Web Application Security Testing

FCC IoT Cybersecurity Labeling Program (IoT Labeling Program)
- Cybersecurity Label Administrator (CLA)
- Testing Lab

- ISO/IEC 17065 accredited third-party certification body (CB)
- Cyber security test lab

- Medical Device Cyber Security Certification
- IoT Sensor Cyber Security Certification

Industry Accreditations and Certifications (2 of 2)

GSMA Accredited Testing Lab:

- IoT Security Assurance Testing Lab
- NESAS - Network Equipment Security Assurance Scheme Testing Lab

CTIA Accredited Testing Lab:

- IoT Security Assurance Testing Lab

HITRUST Authorized CSF Assessor

Cloud Security Alliance - Trusted Cloud Consultant

Palindrome Technologies
Impart Assurance, Instill Trust and Inspire Confidence

- Trusted Cybersecurity Services Provider since 2005
- Science to the art of cybersecurity
  - *Applied research, scientific analysis, and rigorous testing*
- Keen expertise for High-Assurance environments and complex communication networks
- Secure emerging technologies, empowering our clients to operate with confidence in an insecure world

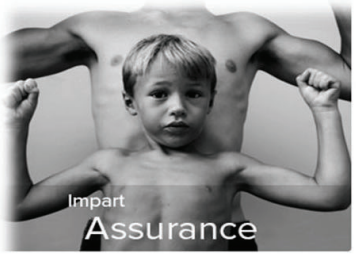
5G Threat Vectors

Policy and Standards	• Open Standards • Optional Controls
Supply Chain	• Counterfeit Components • Inherited Components
5G System Architecture	• Software Configuration • Network Security • Network Slicing • Legacy Communications Infrastructure • Multi-Access Edge Computing • Spectrum Sharing • Software Defined Networking

Source: DHS-CISA

Vision

To *secure* emerging technologies, *empowering* our clients to operate with *confidence* in an insecure world.



Assurance

We consider ourselves as a transparent extension of our customer's operations where we strive to impart Assurance in their processes, services and products by offering professional expertise and advice.

Trust

We use our expertise to help our customers to instill Trust in their infrastructure, services and client relationships.

Confidence

Helping establish Assurance and Trust to our customer operations, bolster their Confidence (and in turn their client's) and help them focus on growing their business with integrity and reliability.