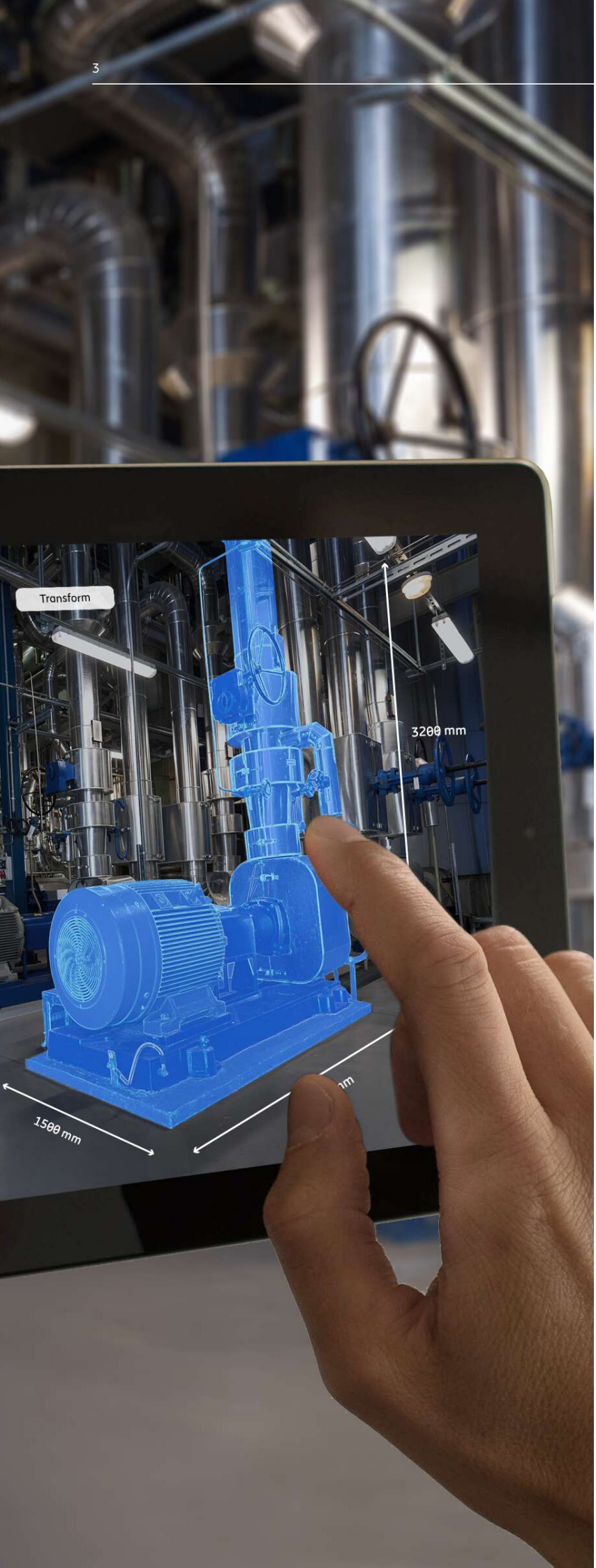
ERICSSON

Implementing Secure IoT Solutions

A systems-based approach to cybersecurity for cellular IoT

May 2021

Contents



Executive summary

Through the next decade, 5G networks will support billions of Internet of Things (IoT) devices that will be the engine for societal transformation enabled by use cases benefiting the public and private sectors, such as Industry 4.0, smart critical infrastructure, connected cars, and enhanced public safety. While great benefits will be realized, IoT also introduces new security risks due to the number of devices, impact of an attack and lack of appropriate security controls. IoT solutions have unique security considerations because the devices are data-centric rather than human-centric. The IoT attack surface is across the entire IoT system, including the individual device profile, scale of devices, network interfaces, IoT application, IoT platform, and shared resources in the cloud. A strong IoT security posture takes zero trust and defense-in-depth approaches by placing security controls across the IoT system at multiple layers, protecting the end-to-end system and data to minimize risk.

The United States National Institute for Standards and Technology (NIST) and other government agencies around the globe have contributed guidelines and best practices for manufacturers and users to secure IoT devices. In addition to the unprecedented size of the attack surface, IoT attack vectors include:

- compromise to the IoT device and system supply chain
- weak device authentication by the network and user authentication by the device
- Distributed Denial of Service (DDoS) attacks against the network or cloud applications
- malware infection of devices, including viruses, bricking, bots and ransomware
- Command and Control (C&C) botnets in which devices target cloud applications and external networks
- unauthorized access to a cloud application leading to data breach

IoT devices should be secure-by-design, but the reality is that market forces pushing for low-cost devices will often require security controls be implemented across the end-to-end IoT system. A secure IoT system has network security and cloud security controls to protect the devices, network and cloud applications, while considering that each system component can be both a target and source of an attack. An end-to-end risk analysis of threats, attack vectors and vulnerabilities of each asset helps to identify the security controls that ensure trust while also protecting IoT system assets, including data. This paper discusses and gives recommendations for security controls on the control and user planes, such as mutual authentication, online and offline monitoring and detection using metadata and logs, and inline traffic behavior analysis. The paper further discusses innovations in 5G, such as network slicing and private networks, that provide opportunities to implement tailored security controls.

Recommendations for securing IoT systems in 5G networks include the following security controls:

- Secure the IoT system end-to-end with a defense-in-depth approach.
- Build a zero trust architecture assuming no trust between devices, network and cloud applications, and the users accessing those assets.
- Use network slicing to provide isolation and tailored security controls.
- Apply cloud security best practices and tools to protect applications and data in the cloud.
- Use a security management solution for security policy configuration and run-time compliance monitoring.

The history of IoT attacks underscores the need to invest in a security posture for the IoT system based upon zero trust and defense-in-depth. The multi-party relationship between the enterprise, service provider and cloud provider requires that security roles and responsibilities are clearly defined along with a multi-lateral agreement addressing the security controls to be deployed and which stakeholder is responsible to implement each control. Changes to risk due to evolving threats, attack vectors and security control technologies should be periodically reassessed by all stakeholders. Governments, network providers, cloud providers, IoT solution vendors, device manufacturers and standards development organizations must work together at a global level to minimize IoT security risks so that IoT's promise for society can be realized.

Introduction

Through the next decade, 5G cellular networks will support billions of Internet of Things (IoT) devices that will be the engine for societal transformation enabled by use cases such as Industry 4.0, smart critical infrastructure, connected cars, improved access to healthcare and enhanced public safety benefiting consumers, public services and the private sector. The U.S. NIST defines the Internet of Things (IoT) as the interconnection of electronic devices embedded in everyday or specialized objects, enabling them to sense, collect, process and transmit data.[1] IoT devices are a diverse class of data-centric "things" that interface to a network, including remote sensors, smart devices, streaming webcams, industrial control systems (ICS), operational technology (OT) and customer premise equipment (CPE) routers, rather than human-centric devices such as smartphones. While great benefits will be realized, IoT also introduces new security risks to confidentiality, integrity and availability due to the number of devices, new use cases, lack of appropriate device security features, and more threat agents. The past decade has witnessed significant internet-based IoT attacks that remind us of the threats and the need to secure IoT systems. A strong IoT security posture takes zero trust and end-to-end defense-in-depth approaches by placing security controls across the IoT system, including the device, network, application and IoT platform, to minimize risk by protecting the system and data at multiple layers. A systems-based risk analysis of threats, attack vectors and vulnerabilities of each asset helps to identify the security controls necessary to ensure mutual trust between device, network, cloud applications and users of those assets, while also protecting those assets from attacks against confidentiality, integrity and availability.

The terminology used in this document aligns with NIST terms and definitions as provided in the Glossary section of this document. IoT security must consider the three principles of the "CIA" triad, which are each defined by NIST as:[2]

- **Confidentiality** — Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity** — Guarding against improper information modification, or destruction, and including ensuring information non-repudiation and authenticity
- **Availability** — Ensuring timely and reliable access to and use of information

1. www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#:~:text=Internet%20of%20Things%20(IoT)
2. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

History of IoT cyberattacks

There have been many IoT attacks over the past 20 years and some of them, shown in Figure 1 below, can be considered as watershed events. These are the Stuxnet attack in 2010, Mirai attack in 2016, VPN Filter attack in 2018, exploits of iLnkP2P vulnerabilities in 2019, Lemon Duck supply chain attack in 2020, the growth of IoT ransomware in 2020, and the Tampa-area water supply attack in 2021.

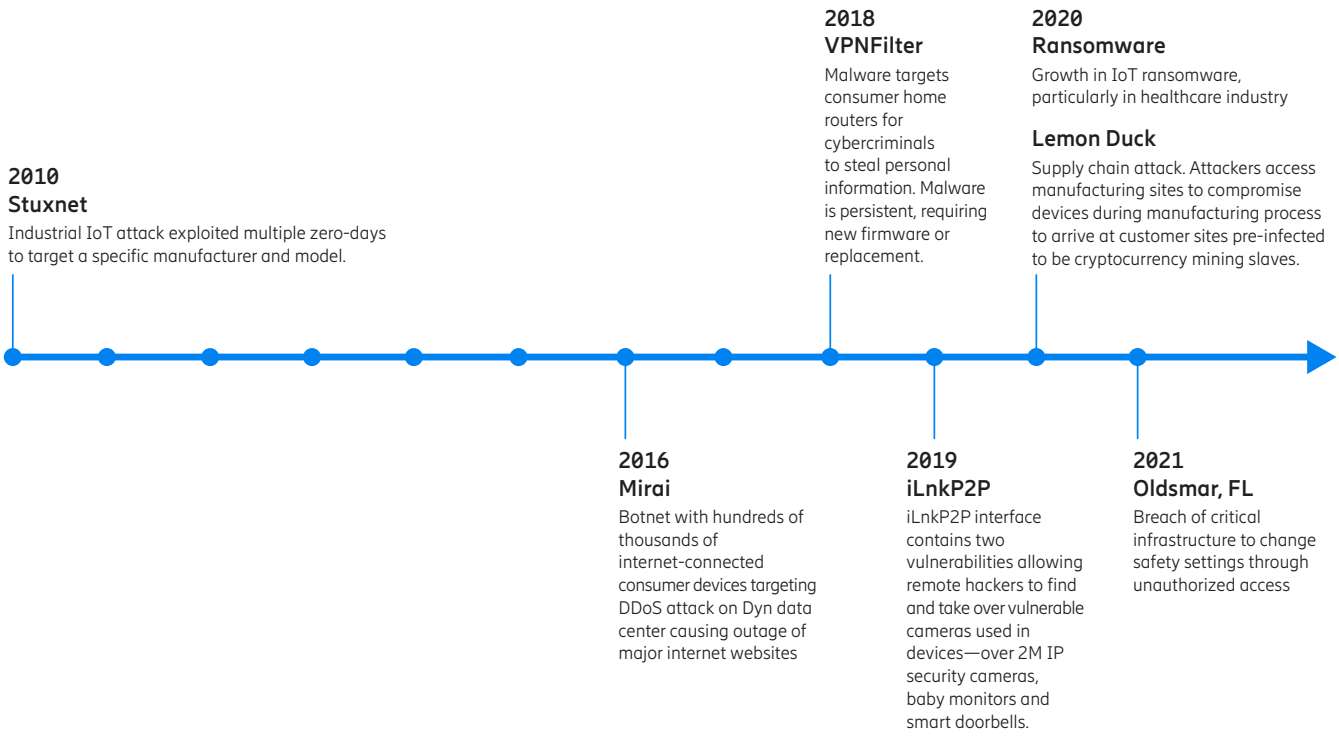


Figure 1. Watershed IoT attacks

The Stuxnet attack in 2010 targeted a specific model of programmable logic controller (PLC) from the manufacturer Siemens to cause misbehavior of processes controlled by the PLC. Stuxnet propagated as a worm and exploited multiple zero-days, an attack that exploits a previously unknown hardware, firmware or software vulnerability,[3] to stealthily move inside a manufacturing facility until it found the intended target, Siemens Step 7 software, where it was able to infect and reprogram the PLC-controlled processes. Many believe that Stuxnet was used to cause failure of spinning centrifuges in Iran's nuclear program in which the processes were controlled to misbehave in a manner to avoid suspicion and the malicious files were hidden so that the infection went undetected for months. Stuxnet is considered the first major IoT attack to target a specific manufacturer and exploit multiple zero-days.

The Mirai Botnet is a self-propagating worm that attacked some high-profile victims in 2016 and 2017. In October 2016, the Mirai botnet infected hundreds of thousands of consumer IoT devices such as IP cameras, home routers and baby monitors using factory default usernames and passwords and unsecure services such as telnet. The attackers used remote Command and Control (C&C) to aim all infected devices around the globe to domain name system (DNS) flood attack a single target, creating a Distributed Denial of Service (DDoS) attack against Dyn, a DNS service provider. This was the first IoT attack to get public attention and press due to the outages of popular websites including Amazon, Github, HBO, Netflix, Paypal, Reddit and Twitter.

The VPN Filter attack infected routers and certain network attached storage devices using malware with a range of capabilities, including spying on traffic being routed through the device, stealing passwords and personal financial data and "bricking" the infected router on command. This attack is unlike most other IoT attacks because it can maintain a persistent presence on an infected device.

In May 2018, many popular home router manufacturers suffered infection resulting

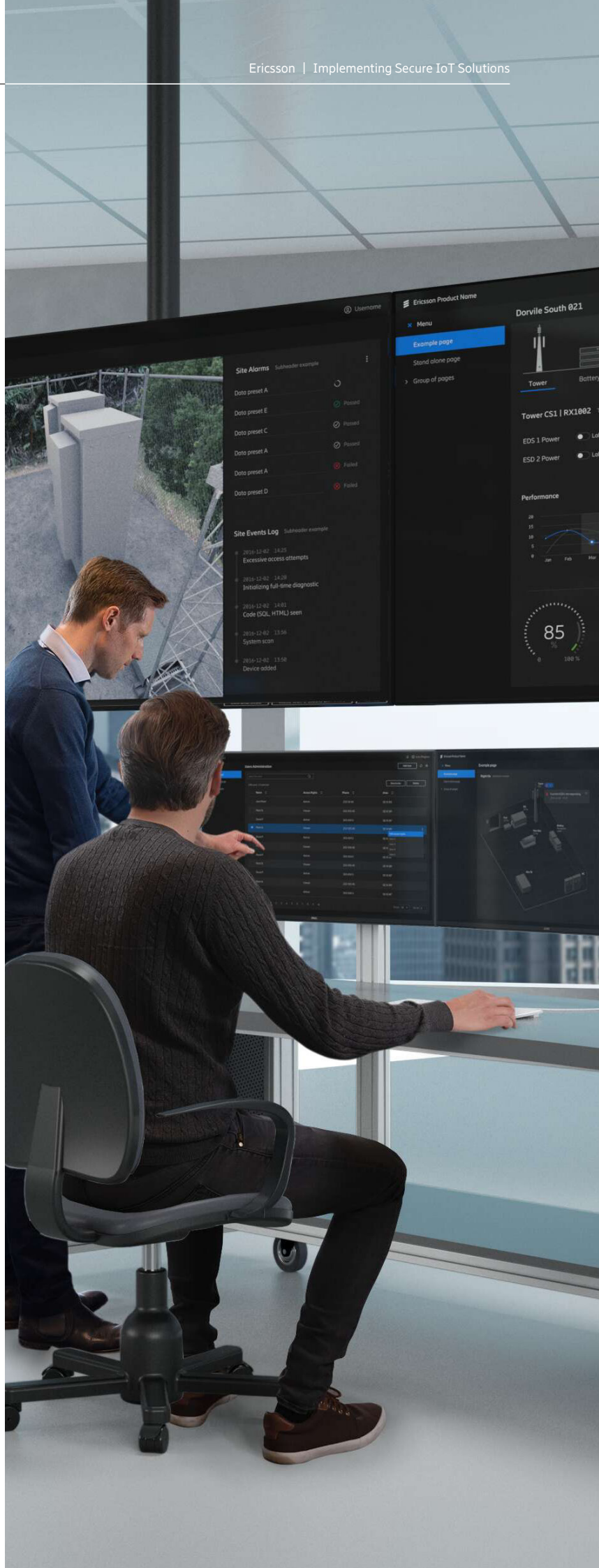
3. https://csrc.nist.gov/publications/detail/nistir/8011/vol-3/final

in an FBI notice[4] with advice to install new firmware, as reboot was insufficient.

iLnkP2P, an IoT device P2P solution, contains two vulnerabilities that allow remote hackers to remotely control cameras on a variety of consumer devices. Over two million IP security cameras, baby monitors and smart doorbell supporting iLnkP2P are at risk to be compromised.

Lemon Duck is an IoT supply chain attack first identified October 2019 that spiked in 2020. It exploits vulnerabilities in Windows 7 embedded devices to convert devices into cryptocurrency mining slaves. Attackers used this malware to break into manufacturing sites and compromise devices during the manufacturing process, resulting in pre-infected devices arriving at the destination. Once connected to a network at the destination, these compromised devices would spread its malware to other devices on that same internal network.

IoT ransomware is different than other ransomware, in which an attacker traditionally targets an IT environment to encrypt data and holds the key until a ransom is paid to decrypt the data. IoT devices typically use forward and forget operation, with limited on-board data storage. Instead of preventing access to data, IoT ransomware attacks "brick" the device, control IoT device function or report false readings. Enterprises can suffer loss of productivity (manufacturing), loss of situational awareness (public safety), impact to health (healthcare) and disruption in basic services (critical infrastructure) until the ransom is paid. In February of 2021, hackers breached the controls of a water supply system in the Tampa, Florida, area with the intention to alter the safety levels of the water.[5] This highlighted the need to secure the IoT system end-to-end, particularly when critical infrastructure is reachable from the internet. Other recent attacks are the Colonial Pipeline ransomware attack[6] and Ubiquiti's potential exposure of user data through a third-party cloud provider.[7]



4. https://us-cert.cisa.gov/ncas/alerts/TA18-145A

5. https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint_Cybersecurity_Advisory_Compromise_of_U.S._Drinking_Treatment_Facility.pdf

6. https://www.forbes.com/sites/rrapier/2021/05/09/the-colonial-pipeline-attack-is-a-major-national-security-incident/?sh=16289e8b23c9

7. https://community.ui.com/questions/possibly-breach/55bc757a-9caf-4889-a2c4-9ad5d8af75ce

IoT use cases

Use cases for IoT will improve healthcare and telehealth, ensure public safety and other mission-critical communications, enable Industry 4.0 including Industrial IoT, smart factories and smart warehousing, deliver energy efficiency and safety with smart grid and smart buildings/homes, bring business efficiencies with monitoring, tracking, remote operation and autonomous robotics, and enhanced digital lifestyles with connected cars, cloud gaming and augmented reality/virtual reality (AR/VR). IoT use cases are defined by requirements for data rate, latency, battery life, coverage, QoS and reliability. 3GPP has specified three services for 5G based upon these requirements: ultra-reliable low latency communication (URLLC) services, enhanced Mobile Broadband (eMBB) and massive Machine Type Communication (mMTC).

There are four types of IoT use cases: Massive IoT, Broadband IoT, Critical IoT and Industrial IoT,[8] as shown in the Table 1 below. Massive IoT uses low-cost devices, including mMTC, NB-IoT and Cat-M, with small data volumes that are useful for metering, tracking and agriculture use cases across a wide coverage area. Broadband IoT, using eMBB, includes IoT services with high data rates, large data volumes, low latency and best effort that is useful for video surveillance and telehealth use cases. Critical IoT (CIoT), using URLLC, includes IoT services with controlled latency, ultra-reliable data delivery and ultra-low latency which are useful for traffic safety and critical infrastructure control use cases. Industrial IoT (IIoT), using eMBB and URLLC, provides IoT services with time-sensitive networking and clock synchronization to enable smart factory and other industrial use cases while also leveraging sub-millisecond latency and highly reliable communications channels.

The security controls required for the use case and the security controls supported in an IoT device can vary. As shown in Table 1, Massive IoT devices may have no security feature support to minimize cost while a Critical IoT device should have strong support of security features to protect its mission or function. When designing security controls for the IoT system, it is necessary to perform threat modeling and a risk assessment to determine the impact of an attack and identify the proper security controls. An IoT device can be included within the authorization boundary of an existing IoT system when it fulfills the appropriate security controls for the system's security impact level. IoT devices that cannot satisfy the requirements for security controls must reside in a separate authorization boundary. Simultaneous use of different types of IoT devices in the IoT system may require the system to have multiple authorization boundaries.

As stated in NIST SP 800-183, "There is no singular IoT and it is meaningless to speak of comparing one IoT to another.... IoT use cases vary from vertical and quality domains (such as transportation, medical, financial, agricultural, safety-critical, security-critical, performance-critical, high assurance, to name a few)."[9] IoT devices should not be treated as all the same and, as a result, risk management must be appropriate for the use case. IoT devices should be secure-by-design, but the reality is that market forces pushing for low-cost devices will often require security controls be implemented across the end-to-end IoT solution. Device classifications and security profiles are necessary to categorize each device type according to its use case, intended function, and classification of the data it processes and stores. This aligns with the recommendation given in the IoT Security Policy Principles from the Council to Secure the Digital Economy (CSDE) to determine the impact of an attack when establishing the proper security controls.[10]

Types of IoT use cases	Use cases	Requirements	Device on-board security capabilities level
Massive IoT	Smart metering, asset management, wearable	Low cost, low power, low throughput, massive numbers	Low
Broadband IoT	Drones/UAV, surveillance video cameras	High throughput, low latency, high data	Moderate
Critical IoT	Automotive, traffic control, safety control	Ultra-reliability, ultra-low latency, very high availability	High
Industrial IoT	Smart grid, smart factory, robotics	Time-sensitive networking, precise indoor positioning	High

Table 1. IoT use cases and typical device security capabilities

8. https://www.ericsson.com/48ff1f/assets/local/reports-papers/white-papers/Cellular_IoT_in_5G_whitepaper_AW.pdf?_ga=2.66249196.39672279.1618936625-565009469.1591360458

9. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

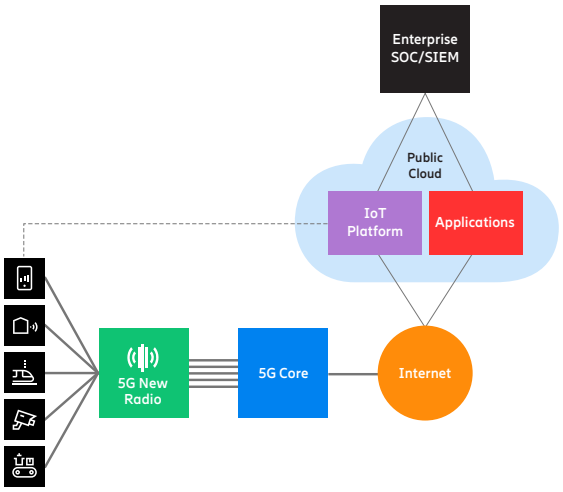
10. https://securingdigitaleconomy.org/projects/iot-security-policy-principles/

IoT cloud deployment models

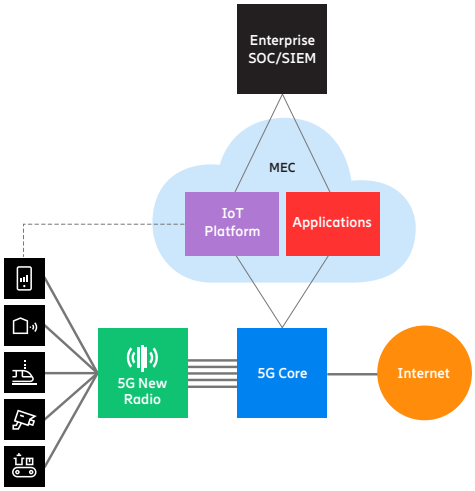
IoT Platforms and applications can be deployed using Software as a Service (SaaS) or Platform as a Service (PaaS) hosted by either a 5G mobile network operator (MNO) or hyperscaler cloud provider (HCP), as shown in Figure 2, using private cloud, public cloud or hybrid cloud models.

The enterprise can deploy the IoT Platform and IoT application in the public cloud or use third-party services operating in the public cloud, as shown in Figure 2(a). MNOs are now utilizing multi-access edge compute (MEC) that brings application resources closer to the IoT device to provide ultra-low latencies to enterprises, as shown in Figure 2(b). The enterprise can deploy in the MNO's MEC the enterprise's IoT Platform and application or use the MNO's IoT services in the MEC. The enterprise can deploy a hybrid model, as shown in Figure 2(c), in which its IoT application, or a third-party IoT application service, is in the public cloud and the IoT Platform is in the MNO network.

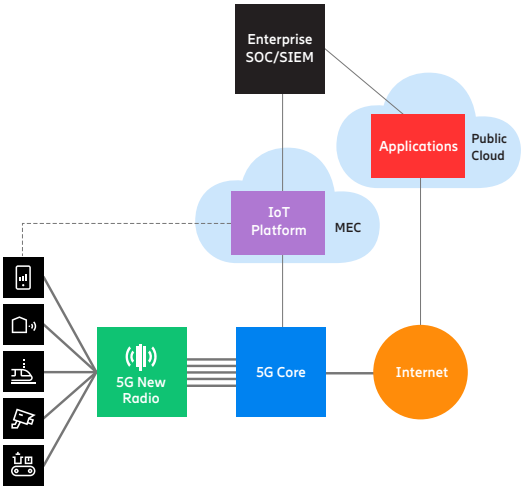
In a zero trust architecture, as defined by NIST SP 800-207, each asset, or network element, is considered a trust zone that requires its own security controls to access that asset and data it may be storing.[11] The multi-party relationship between the enterprise, provider, and cloud provider requires security roles and responsibilities are clearly defined to protect data about the network, enterprise and enterprise's customers. There can be multiple stakeholders at each phase of the data lifecycle: Create, Store, Use, Share, Archive, Destroy. A responsibility matrix with the roles of data owner, controller and processor should be established with consideration for the use case, data subject, personally identifiable information (PII), public safety and business sensitivity. There should be a multi-lateral agreement regarding the security controls to be deployed and which stakeholder is responsible to implement it. The scope of the multi-lateral agreement should include the attack remediation approach, which may include taking the device offline, allow-listing the device to exclusively permitted usage or placing the device into an isolation zone to limit impact while fulfilling primary job function. The risk analysis and recommended security controls are described further in the sections below.



(a) IoT Platform and enterprise application deployed in public cloud



(b) IoT Platform and enterprise application deployed in MNO's MEC



(c) Hybrid model: IoT Platform deployed in MNO network and enterprise application deployed in public cloud

Figure 2. IoT cloud deployment models

11. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

IoT risk analysis

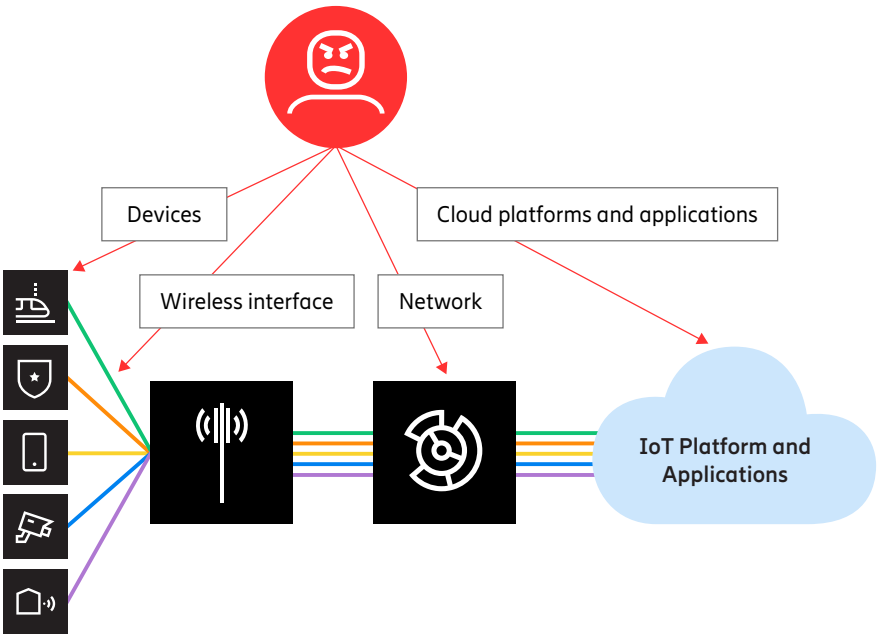


Figure 3. IoT attack surface

The history of IoT attacks underscores the need to systematically invest in an IoT security posture based upon a risk analysis of threats, attack surface, attack vectors and impact in a zero trust architecture in which there is no assumption of implicit trust granted to an asset based upon its location or ownership.[12] Threats to IoT systems from internal and external attackers include device compromise, unauthorized access to the network, attacks on the network control and user planes, cloud-based attacks and access to the management through backdoors.

Attack surface

IoT defense-in-depth is built upon implementation of end-to-end IoT security controls considering separation of the control, user and management planes. The IoT attack surface includes the devices, wireless interface, network, IoT platform, application platform and application that are the components in an IoT system which the attacker can gain access or effect the system. These components, as described below and shown in Figure 3, can be considered an asset for the risk analysis:

- **IoT device** — 'Thing' tethered to the internet that has five primitives: Sensor, Software-based Aggregator, Communication Channel, External Utility and a Decision Trigger.[13] Each IoT device type may have one or more of these primitives.
- **Wireless interface** — An IoT device's network interface that provides data transfer and network control and configuration.
- **Network** — The network side of the wireless interface that handles control signaling between the IoT device and network, referred to as Control Plane, and data transfer between the IoT device and application, referred to as the User Plane.
- **IoT platform** — Provides global connectivity management enabling an enterprise to securely connect and manage IoT devices and the delivery of IoT data from the devices to the application.
- **Application platform** — The compute infrastructure and operating system hosting the IoT application. Multi-tenancy for sharing of compute resources can further expand the attack surface.
- **Application** — The software that manages and processes the data from the IoT devices. Comprises functions like analytics and visualization, process automation, rules engine and decision systems pertinent to a specific IoT vertical.

12. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

Attack vectors

The IoT device authenticates with the network and the result is the device is assigned an IP address that the software running on the device uses to communicate with the IP address used by the cloud application. IoT Attack vectors are shown in Figure 4 below and include the following:

- compromise to the IoT device and system supply chain
- weak user authentication on the management port by the device
- weak mutual authentication between the device and network
- weak mutual authentication between the device and cloud application
- weak user authentication and authorization by the application
- misconfiguration on the device, in the network and in the cloud
- theft or modification of data-in-transit or data-at-rest
- user plane intercept and injection
- unsolicited traffic from the internet destined to the device
- external Distributed Denial of Service (DDoS) attacks against the network or cloud applications
- malware infection of devices, including viruses, bricking, bots and ransomware
- Command and Control (C&C) botnets in which devices target cloud applications
- unauthorized access to a cloud application leading to data breach

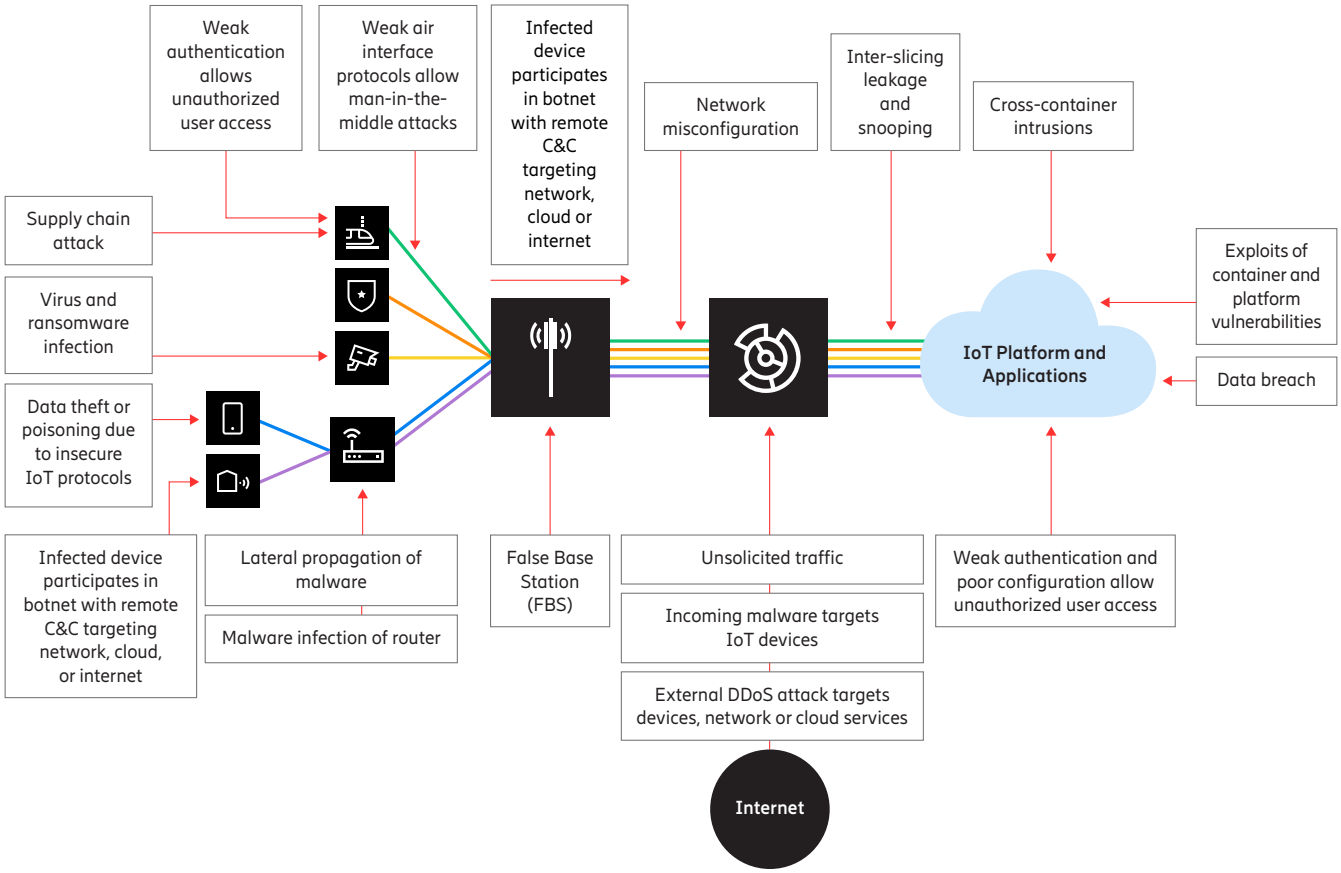


Figure 4. IoT attack vectors

Security controls

IoT defense-in-depth is built upon implementation of end-to-end IoT security controls, as shown in Figure 5, considering separation of the control, user and management planes. The recommended security controls for IoT are not exclusive to IoT solutions and can be applied as security best practices with most wireless solutions. IoT solutions have unique security considerations because the devices are data-centric, rather than human-centric, requiring network-based security controls for end-to-end system protection. IoT system security should be based upon trustworthiness built upon security standards and secure products, networks, operations and management.

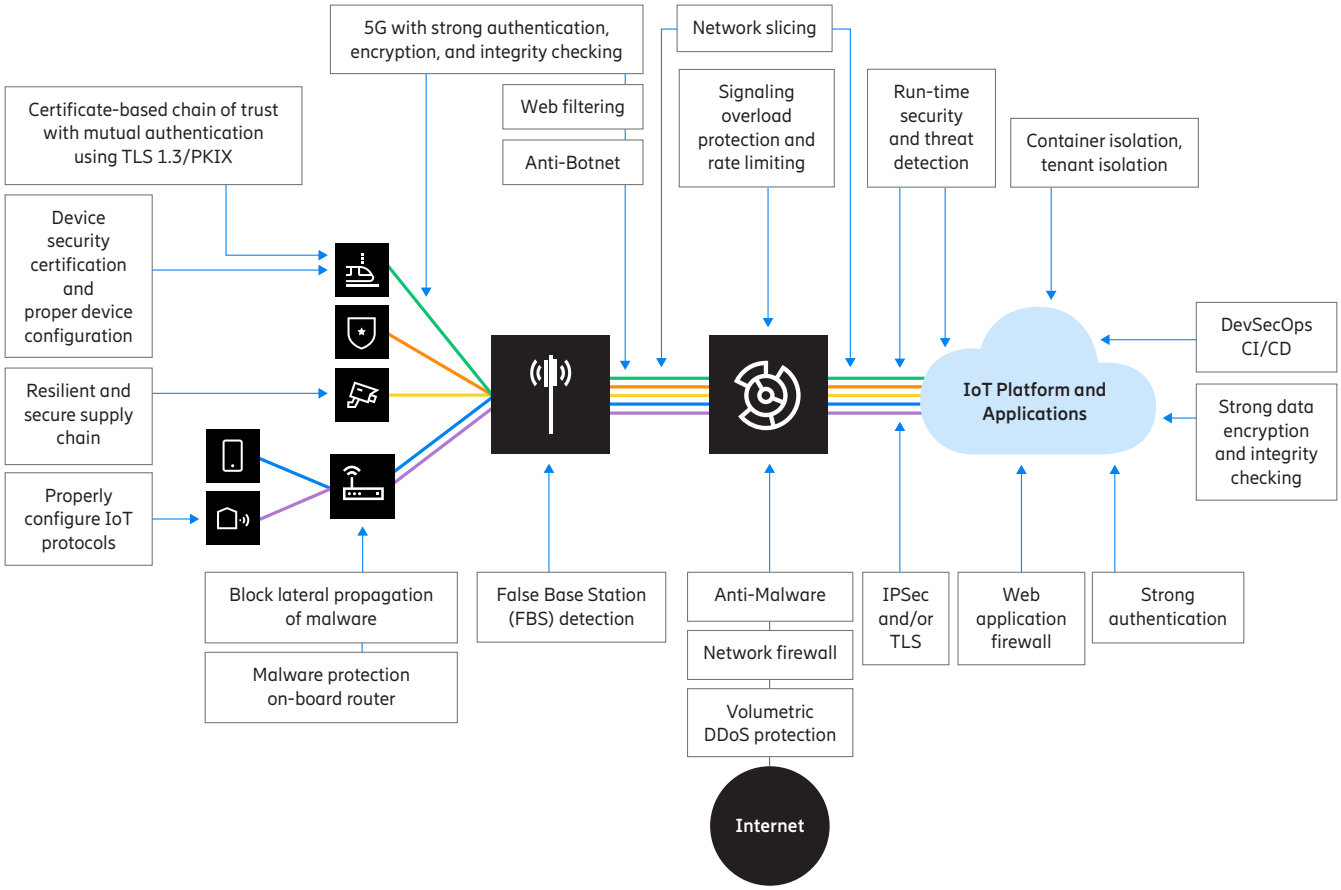


Figure 5. IoT security controls

Risk analysis table

The risk analysis considers threats, vulnerabilities and impact for each asset so that risks to the CIA-triad can be identified and appropriate security controls can be implemented based upon the acceptable risk level. Table 2 provides a high-level IoT risk analysis for each component of the end-to-end solution, treated as an asset in the IoT system. The identified security controls are discussed further in the sections below.

Assets	Threats	Vulnerabilities	Impact	Security controls
Management	Potential backdoor to IoT system	Weak authentication, no encryption, outdated patches	External attacker could take control of IoT system	Strong authentication, encryption, logging
Application	Unauthorized access, application DDoS attack, cross-container intrusion, data breach	Weak authentication, weak encryption, poorly configured firewall	Data theft (confidentiality), data modification (integrity), application failure (availability)	DevSecOps, CI/CD, strong authentication, encryption, application firewall, network slicing, private networks
Application platform	Unauthorized access	Shared resources	Compromised trust stack (confidentiality, integrity, availability)	DevSecOps, CI/CD, tenant isolation, network slicing, private networks
Data	MITM attacks for data in motion, data breach for data at rest	Weak protocols, weak cryptography, weak authentication	Interception of data in transit, loss of sensitive data at rest, and privacy violation (confidentiality), modification to data in transit or at rest (integrity)	Replace deprecated or compromised cipher suites, strong mutual authentication
IoT platform	Unauthorized access	Weak authentication	External or inside attacker is able to execute solution-wide attack (confidentiality, integrity, availability)	Strong authentication, network slicing, private networks
Network – control plane	Untrusted device, massive number of devices, signaling overload	Selection of weak authentication protocol	Network outage, degraded performance (availability)	5G, TLS, firewall, overload protection, rate limiting, network slicing, private networks, IPSec
Network – user plane	Untrusted device, massive number of devices, internal botnet attacks, external DDoS attacks, unsolicited traffic	Selection of weak authentication protocol, poorly configured firewall	Network outage, degraded performance (availability)	5G, TLS, allow and deny listing, firewall, Anti-Botnet, DDoS protection, anti-virus, web filtering, IPS/IDS, network slicing, private networks, IPSec
Wireless interface	Man-In-The-Middle attacks	Selection of weak protocols and cipher suites	Interception of data in transit (confidentiality), loss of network connectivity (availability)	5G, TLS, network slicing, private networks
Device	Unauthorized user access, malware infection, remote control, ransomware, device configuration error, lack of available patches or patches not applied, supply chain attacks	Default passwords, weak authentication, open ports, unused protocols	Data monitoring (confidentiality), loss of device (availability)	Strong authentication, network-based controls, isolation zones, configuration checks, patching, supply chain security

Table 2. IoT risk analysis

Security controls deep-dive

The previous section provided a review of the IoT system risk analysis addressing threats, attack vectors, impacts and security controls. This section provides additional details about the security controls so that the best controls to meet the use case requirements can be selected and implemented.

Secure IoT devices

IoT has an expanded attack surface due to the massive number of devices, forecasted to reach 6 billion cellular connected IoT devices by 2026.[14] Many IoT devices have the flexibility to be used in a variety of disparate use cases, from smart warehouse to public safety, with different levels of security requirements depending upon the use case. IoT devices are considered the "low hanging fruit" to penetrate an IoT solution. Some IoT devices can be more vulnerable than other devices because they were built to perform a specific function at lowest possible cost with limited processing capacity and maximized battery life and, typically, these devices do not have the capabilities to support on-board security functions. Common IoT device vulnerabilities include limited onboard security capabilities, lack of encryption, weak security implementations and configurations, use of factory default or hardcoded usernames and passwords, unsecure interfaces, infrequent patches and software or firmware that is not easily updated. Malicious attacks can exploit IoT vulnerabilities to conduct unauthorized access to data (confidentiality), unauthorized changes to data (integrity) and denial of service (availability). Many of these are listed in Open Web Application Security Project's (OWASP) Top 10 IoT vulnerabilities.[15] IoT security starts with securing the device by implementing the following protections so that it cannot be compromised:

- Devices must implement industry best practices for user/admin authentication to protect against malicious actors gaining remote access to a device.
- Logging and periodic audits of access logs can facilitate proper detection and response, including upgrade of controls.
- As vulnerabilities are identified, it is important that the device firmware and software are upgradeable and the device vendor releases timely patches.
- IoT device vendor provides guidance for device hardening, including:
  - Exposed well-known ports, such as telnet 23/2323 exploited in the Mirai botnet, should be closed.
  - Default passwords should be updated to a strong password that is unique for each device.
  - IoT protocols, such as MQTT and CoAP, should have validated configurations to prevent data theft or poisoning, or use more secure IoT protocols such as LWM2M with DTLS.
- Supply chain security best practices should also be implemented to ensure the device can be trusted.
- NISTIR 8259 recommends that the manufacturer provides users of IoT devices a sourcing statement that, at a minimum, includes the developer of the device's IoT software, the manufacturer of the device's processor and the provider of a cloud-based service used by the device.[16]
- Devices should have upgradeable firmware and software with available security patches. Owners of devices should be aware that the duration of the support contract, including security patches, may not extend to the lifetime of the device.

IoT device certification programs help protect devices and infrastructure by ensuring devices meet a security control baseline. The CTIA IoT device cybersecurity certification program provides an industry baseline for device security on wireless networks that establishes a foundation for secure wireless IoT systems.[17] CTIA represents the U.S. wireless communications industry from carriers and equipment manufacturers to mobile app developers and content creators, and informs standards, industry and regulatory bodies, such as NIST, ATIS and the U.S. FCC CSRIC, on its findings and recommendations. CTIA's IoT device cybersecurity certification process includes verification of the device security features against a set of standard cybersecurity best practices addressing the protection of consumers' information, rigorous password and security management standards and the availability of an over-the-air mechanism for security software updates in a tiered-risk approach to match the requirements of the application. IoT device certification can be performed at an CTIA-accredited Authorized Test Lab (CATL), such as the Ericsson Cybersecurity Testing and Certification program.

14. https://www.ericsson.com/en/mobility-report/dataforecasts/iot-connections-outlook
15. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
16. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
17. https://www.ctia.org/certification-resources

Nations around the globe are proactively addressing IoT device security, including the U.S.'s NIST, EU's ENISA, Japan's METI, China's MIIT, Brazil's Anatel and others. Additional IoT security guidelines are available from the Global System for Mobile Communications Association (GSMA).[18] On Dec. 4, 2020, the United States passed law H.R.1668 Internet of Things (IoT) Cybersecurity Improvement Act that requires specification of minimum information security requirements for managing cybersecurity risks associated with IoT devices, which may be used in low impact, moderate impact, and/or high impact system use cases.[19] The Internet of Things (IoT) Cybersecurity Improvement Act explicitly referenced NISTIR 8259, a family of documents from U.S. National Institute of Standards and Technology (NIST) Cybersecurity for IoT Program team to provide guidance to IoT device manufacturers and users for securing those devices.[20] The foundational document is NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.

Secure wireless interface

IoT devices may connect to applications across the network using cellular, Wi-Fi, Bluetooth or other wireless access technologies. 5G provides global coverage, quality of service, scalability, security, mobility and flexibility to handle the different requirements for a comprehensive range of IoT use cases. As 3GPP has purposely architected each generation of mobile technology to be more secure than the previous, 5G is considered to have the highest level of security. Likewise, IEEE has specified Wi-Fi 6 to have the highest level of security of any version, approaching the level of security in 5G. However, use of public Wi-Fi still poses a risk as Wi-Fi 6 security features are optional and may not be enabled on public Wi-Fi networks. 5G and/or Wi-Fi 6 provide high-speed, low latency and secure communications that can be complementary in a deployment when using an IoT Gateway supporting both Wi-Fi 6 to provide local area device connectivity and 5G to provide the wide area connectivity to applications in the private data center or public cloud. 5G and Wi-Fi 6 can provide encryption and integrity protection of user data with NIST and IANA recommended TLS cipher suites using Advanced Encryption Standard (AES) Galois Counter Mode (GCM) and SHA-256/384. The vendor and provider need to be prepared to replace integrity and/or ciphering algorithms if the current algorithm in use is compromised or deprecated. IoT devices that support only WPA3-Personal will have security less than that of WPA3-Enterprise and 5G. IoT devices that support both WPA3-Personal and WPA3-Enterprise should be securely configured to use WPA3-Enterprise. Bluetooth connections should follow NIST's Guide to Bluetooth Security, SP 800-121.[21]

Data loss prevention and privacy

IoT data in-transit, in-use, and at-rest should be protected to prevent data loss of sensitive information, including confidential information and personally identifiable information (PII), that could impact the enterprise's business, its employees and its customers. Exposure of PII could result in a privacy violation pertinent to a geographic region and industry vertical. For data-in-transit, the risk analysis should inform whether IPSec or (D)TLS is required for the use case and consider device support for IPSec or (D)TLS. Transport layer security (TLS) version 1.2 or 1.3 and Datagram TLS (DTLS) version 1.2 are the most secure and efficient versions of the protocols. For data-in-transit, IPSec and (D)TLS should be used with strong cipher suites to provide end-to-end data confidentiality and integrity that protects sensitive information in the user plane. Any IoT solution should have a privacy impact assessment (PIA) to identify and mitigate privacy risks from data assets, as described in the Ericsson technical paper Privacy in Mobile Networks. Data ownership must be assigned to ensure the appropriate classification and security controls are applied to protect the business and customers. Transfer of data ownership within a cloud environment must also be considered.

18. https://www.gsma.com/iot/iot-security/iot-security-guidelines/
19. https://www.congress.gov/bill/116th-congress/house-bill/1668/text?q=%7B%22search%22%3A%5B%22HR+1668%22%5D%7D&r=1&s=1
20. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
21. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Zero trust

A zero trust architecture makes no assumption of implicit trust granted to an asset based upon its location or ownership. Best industry security practices provide mutual authentication TLS versions 1.2 and 1.3 with public key infrastructure and X.509 (PKIX) certificates signed using current strong cipher suites. 5G and Wi-Fi 6 provide strong mutual authentication with 5G using 5G-AKA, EAP-AKA, and EAP-TLS and Wi-Fi 6 using WPA3 and EAP-TLS. Device attestation with digital signing from a Certificate Authority (CA) establishes a root of trust while TLS with X.509 digital certificates provide a high level of automation and security to ensure only trusted devices are permitted access to a trusted network and application, as shown in Figure 6 below.

To protect the device credentials, hardware security functionality such as Trusted Platform Module (TPM) and Hardware Security Module (HSM) should be used to establish a hardware root of trust. Where TPM is impractical for some IoT devices, a centrally managed root hierarchy can scale to millions of IoT devices. As a further innovation to device hardware security, vendors are providing System on a Chip (SoC) custom-made for mobile networks, with integrated performance, energy efficiency and security enhancements to provide security as a feature of the hardware rather than leaving security to a software feature only. In addition, electronic fuses (eFuses) prevent tampering and access to crypto keys as a further zero trust enhancement.

Embedded SIM (eSIM) and embedded Universal Integrated Circuit Card (eUICC) can provide enhanced security gained from automatic bootstrapping and remote over-the-air (OTA) provisioning.

3GPP Release 15 standardized non-SIM authentication using certificate-based EAP-TLS authentication for 5G Core (5GC). The non-SIM authentication is useful for non-public networks where IoT devices do not need a subscription. MNOs may use the 5G Equipment Identity Registry (EIR) from a registry service via API to automatically block authentication of fraudulent devices. 3GPP Release 15 also introduces the Subscriber Concealed Identifier (SUCI) that encrypts the Subscriber Permanent Identifier (SUPI) to protect the device identity until authentication is successfully completed in 5G. For a detailed overview of the built-in support for zero trust architecture in 5G and the key 5G security features that enable it, please refer to the Ericsson Technology Review article, Realizing Zero Trust in 5G networks.

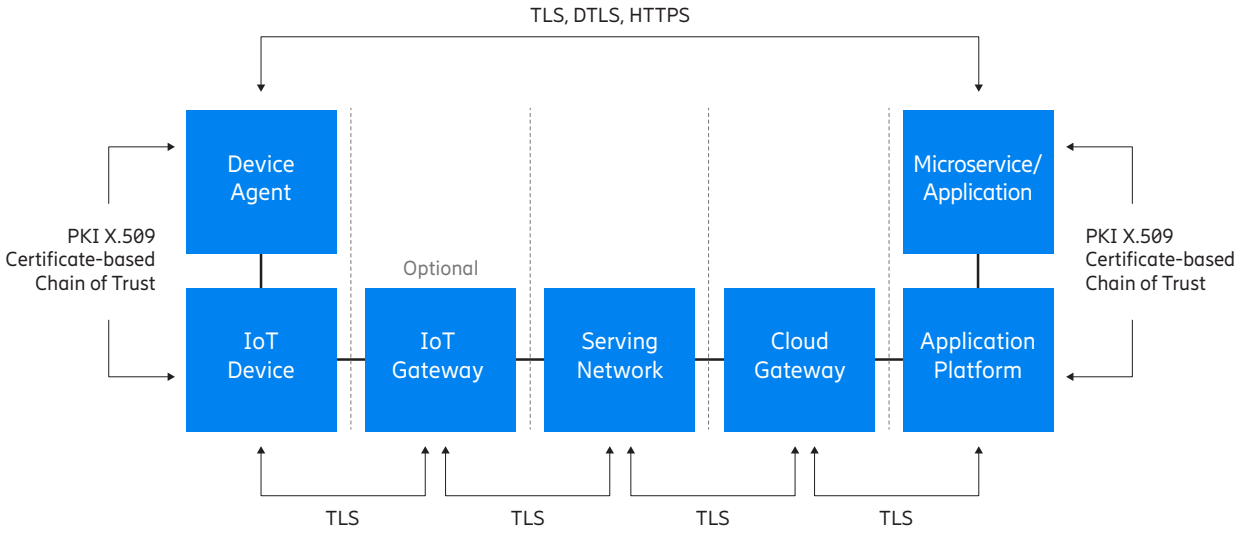


Figure 6. Certificate-based mutual authentication between trust zones

Network-based user plane security

While firewalls at trust boundaries provide some defense against attacks by limiting communication between trusted entities to only permitted IP addresses using only valid protocols on allowed ports, additional security controls are needed on the user plane to effectively mitigate DDoS attacks, botnets and malware infection. Network security functions such as firewalls, volumetric DDOS protection, anti-botnet, antivirus and web filtering can be deployed on the user plane at trust boundaries to provide end-to-end protection as follows:

- Protect devices from attacks sourced from the public internet and cloud.
- Protect the network from attacks sourced from internally attached devices and cloud.
- Protect the cloud from attacks sourced from internally attached devices and the internet.

The massive number of IoT devices makes it a target-rich environment for botnet infection. Botnets are remotely coordinated via a central C&C server to target a victim with an attack on availability of a network or application. Infected devices participating in a botnet attack can overwhelm the serving network from the inside unless mitigated using network-based botnet detection, along with alerting and logging. The network can automatically mitigate a botnet attack by:

- blocking device communication with known C&C IP addresses and URLs
- detecting and blocking use of domain generation algorithm (DGA)
- using anomalous behavior analysis with Artificial Intelligence and Machine Learning (AI/ML) on the user plane to identify and mitigate the attack

IoT devices can be infected with malware in the form of a virus, bricking, botnet or ransomware in the payload on the user plane from external sources or internal lateral propagation. Infected devices can be taken offline if the use case permits. If the use case dictates that the device must stay online, then the anomalous behavior may be mitigated by placing it in an isolation zone or using advanced flow analysis capabilities to allow only permitted behavior. Antivirus using signature-based detection of malicious payloads can prevent malware infection while web filtering can be deployed to provide proactive blocking of attempts to access known malicious websites. The advantage of network-based antivirus and web filtering is that the provider or cloud provider can maintain the virus signature and malicious URL databases to ensure databases are current versus an endpoint-only solution that relies upon the enterprise updating the database on each device, assuming the device is capable of running an on-board security agent.

While the traffic load from a single IoT device may not be significant, an IoT army of bots aimed at a single target can generate an aggregate amount of data that could overwhelm network or cloud resources. Botnet-based DDoS attacks over 1Tbps causing widespread outages have been publicly reported. Inline detection and mitigation functions in the network can be used at the internet edge to prevent volumetric DDoS attacks from the internet, including TCP SYN Floods, UDP Floods and DNS Floods that can attack availability of the network or service. Advances in AI/ML have helped inline DDoS protection and anti-botnet functions achieve accurate near-real-time detection and mitigation with low false positive and false negative rates on high speed links. Other mitigation solutions such as null routing, rate limiting and scrubbing centers can be used on lower speed links.

Secure IoT Gateway
IoT devices may have Wi-Fi connectivity through an IoT Gateway with 3GPP cellular access. The IoT Gateway can support both Wi-Fi 6 to securely provide local area device connectivity and 5G to securely provide wide area connectivity to applications in the private data center or public cloud. Use cases include public transportation, public safety and smart buildings. From the security perspective, the IoT Gateway is both an asset and a control. As an asset, the IoT Gateway must be secured to provide only authenticated access on the management plane and to protect itself from malware infection. It is important that the Gateway is properly configured to ensure there are no unused open ports nor use of default or weak passwords. The Gateway provides security controls for the IoT system through the following capabilities:

- Block anomalous behavior from a device.
- Block non-permitted unsolicited traffic destined for the device.
- Detect and block devices participating in a botnet based upon Indicators of Compromise (IoC) that are identified by real-time threat intelligence and/or anomaly detection.
- Detect and block lateral propagation of malware between devices at Layer-2 and across VLANs.
- Detect and block malware from passing through the wide-area network to devices.
- Detect and block devices from accessing known malicious websites and IP addresses.
- Rate-limit traffic to a device to prevent targeted DDoS attacks.

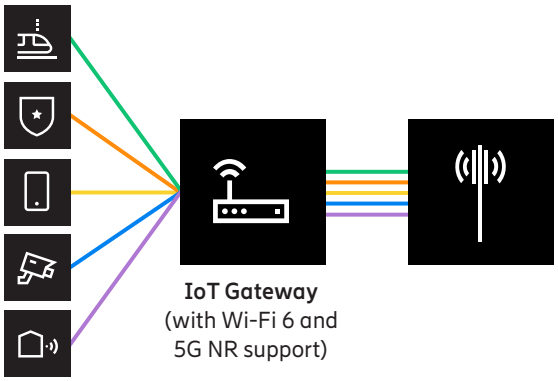


Figure 7. IoT Gateway for secure 5G NR access

5G network slicing and private networks
IoT security is built upon a foundation of network security design best practices, such as network separation and segmentation, to isolate infections and attacks so that impact is minimized and contained. 5G network slicing provides isolated logical networks, as shown in Figure 8, to enable services with diverse requirements on the same 5G network. Cloud-native technologies and network automation have enabled each network slice to be customized to meet the use case and customer requirements. Dynamic resource management enables each slice to meet QoS and SLA requirements, but network slices also provide inherent security advantages as end-to-end isolation ensures properly configured resources dedicated to one slice cannot be consumed by another slice and traffic cannot be intercepted or spoofed by another slice. In addition, each slice can be architected to provide tailored security controls to match the customer and use case. Implementation of physically separated slices can provide further network segmentation and private networks using directly licensed 5G spectrum provide further isolation and tailoring of security controls.

The Single Network Slice Selection Assistance Information (S-NSSAI) identifies a network slice in 5G. 3GPP Release 16 further enhances the security offered by network slicing with the addition of the Network Slice Specific Authentication and Authorization (NSSAA) that provides enhanced per-slice specific authentication and authorization of UEs based upon subscription information from the Unified Data Manager (UDM) and the slice policy to prevent an unauthorized device from connecting to the network slice. As with any security control, proper configuration of network slicing is required to ensure adequate separation, authentication and authorization aligned with the risk analysis for the use case. An end-to-end network slice includes partitioning of the RAN, which is described further in Ericsson blogpost Highlights of Key End-to-End Network Slicing Capabilities.

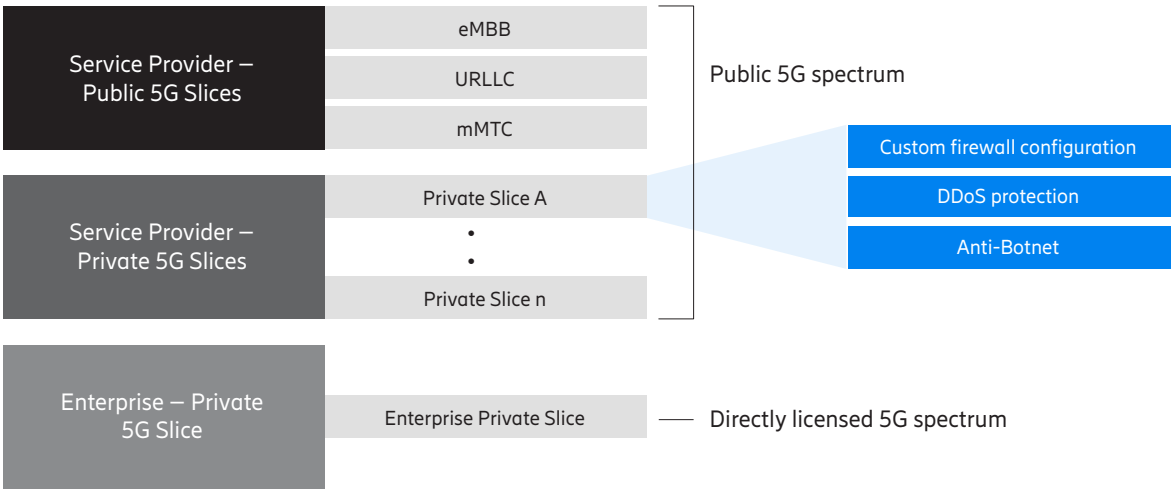


Figure 8. Secure 5G network slicing

Securing cloud platforms and applications

IoT platforms and applications can be deployed in a central cloud or multi-access edge compute (MEC). In an IoT ecosystem, including the enterprise, MNO and HCP, it is the responsibility of all three to ensure that appropriate security controls are applied in the cloud, including:

- mutual authentication: Using certificates in a public key infrastructure and strong ciphers
- Multi-Factor Authentication (MFA): To ensure secure user access to functions in the network and cloud
- container security: Tenant isolation, container isolation, container firewall, image scanning for known vulnerabilities, and run-time security
- network-based perimeter security: Anti-Malware, Web Application Firewall (WAF), and volumetric DDOS protection
- secure configuration: To maintain login credentials, disable unused protocols and close unused ports

Containers provide isolation benefits inherited from the Linux operating system, such as Cgroups to partition and limit access to different processes, Seccomp to limit actions that can be taken by processes, and mandatory access controls (MAC). However, containers are still at risk from rogue processes that bypass isolation to access other containers sharing the same resources, a container being deployed with a known or unknown vulnerability, and container or management platform misconfiguration. Container security includes DevSecOps, as currently being addressed by the NIST DevSecOps project for cloud-native applications, to reduce, mitigate, and prevent recurrence of vulnerabilities.[22] In addition to container security, a strong cloud security program also includes logging/alerting, multi-factor authentication (MFA), patch management, data encryption, Cloud Security Posture Management (CSPM) to identify risks and threat detection and response using AI, ML and anomaly detection. The IoT platform should be hardened at the control, user and management planes with a focus on the assets being managed and how each asset type can potentially be misused to cause a loss or modification of visibility or control within the IoT system.

These security considerations for cloud deployments also apply to vRAN, Cloud RAN or O-RAN used for an IoT system. O-RAN can be leveraged for IoT deployments, but the O-RAN architecture expands the attack surface to introduce additional attack vectors. O-RAN's security risks should be addressed during network implementation according to the recommendations provided in the Ericsson technical paper Security Considerations of Open RAN.

22. https://csrc.nist.gov/Projects/devsecops

Secure IoT management

IoT security management's mission is to provide automated security policy configuration compliance and security threat and attack detection and response initiation. The zero trust principle includes continuous vigilance in proactively reducing the threat surface especially in the cellular automated and optimized workload placement across distributed data centers in a multi-domain, multi-technology and multi-vendor environment. In such a dynamic environment, manual procedures are insufficient.

Automation of security controls requires the existence of security mechanisms within the components. Security controls accessible on the management plane should include strong authentication, encryption and event logging. Secure IoT systems are built upon a foundation of strong identity and access management (IAM) for the device, application and IoT platform with strong authentication using authorization boundaries, multi-factor authentication and digital certificates; for instance, default passwords and passwords in clear text should never be used. In the cellular network context, policies related to generic best practices include:

- restricting invalid login attempts policy
- session management policy
- password management policy
- Command-line interface (CLI) authentication policy
- audit logging policy
- encryption policies

The security management and orchestration function is an independent function that monitors and controls the network asset security mechanisms on the management plane to provide automated real-time security policy configuration compliance, AI/ML-based attack analysis and PKI certificate management. Depending upon the deployment model, the enterprise may be responsible for the end-to-end security of the IoT system, in which case the security management function also provides near real-time aggregation and prioritization to enable the enterprise's Security Information and Event Manager (SIEM) to have visibility and control inside the MNO's network.

Secure IoT operations

Telecom networks are evolving and will be increasingly used for new industry use cases and new deployment scenarios. At the same time security risks are increasing due to end-point vulnerabilities, complexity in critical network infrastructures, and the usage of virtualization and cloud and application technologies with shared capabilities. Instead of current spot-like management of security threats, there is increasing demand for enhanced security visibility and control with adaptive security management automation solutions. These types of solutions provide a comprehensive framework for identifying security risks in a managed context maintaining the desired protection level, detecting known and unknown threats, identifying weaknesses in the system, and responding in a timely manner to the identified threats based on risk evaluation. These solutions provide evidence mechanisms for the security measures that assess the progress towards the target security risk tolerance.

One of the biggest concerns in launching IoT services is security. To address this concern, it is necessary to detect attacks in near real-time and to respond with appropriate actions swiftly. Active response helps to shorten the incident containment with a high degree of automation as closed-loop and expert-assisted response mechanisms. Risk and trust orchestration glues together protection, detection and response functionalities and transforms security-event-driven operations into risk-driven operations ensuring risks are kept within tolerance boundaries.

It is essential that a security baseline assessment is executed before taking a security management automation solution into use. The purpose of the assessment is to evaluate risks for the managed context, to understand the attack surface relevant for the context and to evaluate automation impact to the existing operational processes and procedures. A security risk management framework, such as NIST SP800-37, should be the basis for the assessment.[23] The assessment gives input for the risk-driven security policy selection in the security management platform, gives essential input on how attack detection capabilities could be initially configured in the security management platform and gives indication on which of the operational processes may need to be re-engineered due to introduction of automation and closed-loop response activities.

23. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Recommendations

The complexity and impact of IoT attacks is evolving. Attacks on IoT systems can exploit vulnerabilities to degrade performance, cause denial of service, steal information, compromise individuals or remotely control device behavior. Enterprises can suffer loss of productivity (manufacturing), loss of situational awareness (public safety), impact to health (healthcare) and disruption in service (critical infrastructure). While IoT device security is a critical component of an IoT security posture, it alone cannot ensure a secure IoT solution. Device classifications and security profiles are necessary to categorize each device type according to its use case, intended function, and classification of the data it processes and stores. An end-to-end systems-based approach should implement zero trust and defense-in-depth across the entire IoT attack surface, including devices, networks, cloud applications and platforms. It is recommended that an IoT security posture include the following security controls:

- Use secure IoT devices from a trusted supplier, but do not assume trust. Devices should comply with NIST, or other national or industry guidelines, and have a recognized IoT security certification. Device configuration should be validated to ensure it is secure for use in production.
- Use 5G. It is designed to provide secure IoT use cases by enabling many of the security controls needed for IoT security.
- Use an IoT Gateway for Wi-Fi 6 capable IoT devices to access the 5G network. The gateway can provide security controls closer to the devices, but it is also an asset that must be protected.
- Assume zero trust. IoT solutions should be part of a zero trust architecture (ZTA). Identify Authorization Boundaries and use strong authentication on every solution component and on every interface. DTLS 1.2, TLS 1.2 or TLS 1.3 should be used for mutual authentication and protection of data in transit.
- Use network-based security controls on the user plane to provide the IoT system additional protection against internal attacks from connected devices, external attacks from the public internet and attacks from the cloud. Network-based security controls can provide protection from botnets and DDoS attacks targeting availability.
- Use network slicing to provide isolation and tailored security controls. Private networks provide further isolation and tailoring.
- Use cloud security best practices and tools to protect applications and data in the cloud.
- Use a security management solution for enhanced visibility into the threat landscape as well as for security policy configuration and continuous compliance monitoring.
- The IoT solution should have a privacy impact assessment (PIA) to identify and mitigate privacy risks to data assets.
- The multi-party relationship between the enterprise, service provider and cloud provider requires that security roles and responsibilities are clearly defined along with a multi-lateral agreement addressing the security controls to be deployed and which stakeholder is responsible to implement it. Changes to risk due to evolving threats, attack vectors and security control technologies should be periodically reassessed by all stakeholders.

Conclusions

Securing the end-to-end IoT system is a team sport—individual mandates, device guidelines or technology implementations alone will not achieve the goal of a robust, secure and available ICT infrastructure that incorporates the forecasted growth of new IoT devices and use cases. A strong IoT security posture uses zero trust principles and an end-to-end defense-in-depth approach to place security controls across the IoT system to minimize risk. IoT device, network and cloud providers offer the technological capabilities to secure IoT systems, but market incentives, harmonized standards and legislative actions to reduce the friction of best practices for secure implementations require careful balance to improve security while not slowing innovation. Governments, the information and communications technology (ICT) industry, device manufacturers and standards development organizations (SDOs) must work together at a global level to minimize IoT security risks so that IoT's promise for society can be realized.

Author biographies

Dr. Brenda Connor has been with Ericsson since 1994 and is providing thought leadership in 4G/5G ecosystems for secure enterprise and mission-critical, and Industrial IoT use cases.

Business model innovator, security expert and data scientist passionate about scalable go-to-market approaches that benefit from IoT data-driven outcomes requiring secure and reliable data delivery and insights.

Connor is a change maker for the Networked Society, where every individual and every industry is enabled to reach its true potential. Proven track record of building successful solutions for real-time Command & Control and vertical use cases including a defense-in-depth and zero trust security approach based on NIST Cybersecurity Framework and Industrial Control Systems guidelines.

Scott Poretsky is Director for Security, Network Product Solutions, North America. He has over 25 years of experience in telecommunications security design, engineering, and thought leadership for global service providers, government, and enterprises. Scott is Ericsson's voting member at the O-RAN Alliance's Security Focus Group (SFG) and represents Ericsson in industry-government collaborative cybersecurity working groups including NSTAC, FCC CSRIC and DHS ICT SCRM. He also represents Ericsson at the CSCC 5G Committee and CTIA CSWG and is Advisory Board Chair for the IEEE ComSoc's CQR technical committee. Scott is a recipient of the Ericsson MANA Networks 2020 Gold PRIDE Award for External Customer Satisfaction.

Glossary (NIST definitions)

Asset
A major application, general support system, high impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems. (https://csrc.nist.gov/glossary/term/asset)

Attack
An intentional or inadvertent attempt to exploit a vulnerability in order to violate confidentiality, integrity, availability security objectives. Attacks vary widely. Some involve exploitation of a single vulnerability using a single attack vector, while others involve multiple vulnerabilities and multiple attack vectors, or even a single vulnerability and multiple attack vectors. [NIST SP 800-154]

Attack Surface
The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. [NIST SP 800-160 Vol.2]

Attack Vector
A segment of the entire pathway that an attack uses to access a vulnerability. Each attack vector can be thought of as comprising a source of malicious content, a potentially vulnerable processor of that malicious content, and the nature of the malicious content itself. An example of an attack vector is a network service with inherent vulnerabilities (processor) used maliciously (content) by an external endpoint (source). [NIST SP 800-154]

Authorization Boundary
A discrete, identifiable information technology asset (such as, hardware, software, firmware) that represents a building block of an information system. [NIST SP 800-53]

Availability
Timely, reliable access to data, information, and systems by authorized users. [SP 800-171]

Confidentiality
Assurance that information is not disclosed to unauthorized individuals, processes or devices. [SP 800-171]

Control
The management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. Ultimately an organization's security relies on a combination of people, processes and technology. [NIST SP 800-154]

Defense-in-depth
The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. [NISTIR 8183]

Information Owner
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination and disposal. [NIST 800-53]

Impact Level
The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high. [NIST SP 800-30]

Integrity
A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. [NIST SP 800-171]

Internet of Things (IoT)
'Things' tethered to the internet that has five primitives: Sensor, Software-based Aggregator, Communication Channel, External Utility, and a Decision Trigger. [NIST SP 800-183]

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, and the nation. [NIST SP 800-154]

Risk Analysis
The process of identifying, estimating and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. [https://csrc.nist.gov/glossary/term/risk_analysis]

Risk Mitigation
Reduces a risk to an acceptable level. [NIST SP 800-154]

Security Control Baseline
The set of minimum security controls defined for a low-impact, moderate-impact or high-impact information system that provides a starting point for the tailoring process. [NIST SP 800-53]

Security Posture
The security status of an organization's networks, information, and systems based on information assurance resources (such as, people, hardware, software, policies) and capabilities in place to manage the defense of the organization and to react as the situation changes. [NIST SP 800-137]

Threat
Any circumstance or event with the potential to intentionally or unintentionally adversely impact organizational operations and assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST SP 800-154]

Trust
A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with assurance that the entity and its identifier are genuine. [NIST SP 800-152]

Glossary (cont.)

Vulnerability
Any trust assumption involving people, processes or technology that can be violated in order to exploit a system. Types of vulnerabilities include software flaw vulnerability, security configuration issue vulnerability, software feature misuse vulnerability. [NIST SP 800-154]

Zero-day
An attack that exploits a previously unknown hardware, firmware or software vulnerability [NISTIR 8011, vol. 3]

Zero Trust
An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (that is, local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. [NIST SP 800-207]

Zero Trust Architecture (ZTA)
Uses zero trust principles to plan industrial and enterprise infrastructure and workflows. [NIST SP 800-207]

Acronyms

AES	Advanced Encryption Standard
AI/ML	Artificial Intelligence/Machine Learning
C&C	Command and Control
CATL	CTIA-accredited Authorized Test Lab
Cat-M	Category-Machines
CI/CD	Continuous Integration/Continuous Development
CIoT	Critical IoT
CLI	Command line interface
CoAP	Constrained Application Protocol
CP	Control Plane
CSDE	Council to Secure the Digital Economy
CTIA	Cellular Telecommunications Industry Association
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
eMBB	enhanced Mobile Broadband
eSIM	embedded Subscriber Identity Module
GCM	Galois Counter Mode
HCP	Hyperscaler Cloud Provider
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICT	Information and Communications Technology
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPSec	Internet Protocol Security
LWM2M	Lightweight Machine to Machine
mMTC	massive Machine Type Communication
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrowband Internet of Things
NIST	National Institute of Standards and Technology
NR	New Radio
NSSAA	Network Slice Specific Authentication and Authorization
OTA	Over the Air
OWASP	Open Web Application Security Project
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure with X.509
PLC	Programmable Logic Controller
RAN	Radio Access Network
SDO	Standards Development Organization
SIEM	Security Information and Event Manager
SIM	Subscriber Identity Module
S-NSSAI	Single-Network Slice Selection Assistance Information
SoC	System on a Chip
SUCI	Subscriber Concealed Identifier
SUPI	Subscriber Permanent Identifier
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSN	Time Sensitive Networking
UDM	Unified Data Manager
UP	User Plane
urLLC	ultra-reliable Low Latency Communication
ZTA	Zero Trust Architecture

References

NIST

NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
Joint Task Force, National Institute of Standards and Technology, U.S. Department of Commerce. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST SP 800-121, Guide to Bluetooth Security
Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L. and Scarfone, K., (2017). NIST Special Publication 800-121 Revision 2: Guide to Bluetooth Security. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Ross, R. Pillitteri, V, Dempsey, K., Riddle, M., Guissanie, G., (2020). NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. National Institute of Standards and Technology. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST SP 800-183, Network of 'Things'
Voas, J., (2016). NIST Special Publication 800-183, Networks of 'Things'. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

NIST SP 800-207, Zero Trust Architecture
Rose, S., Borchert, O., Mitchell, S., Connelly, S., (2020). NIST Special Publication 800-207, Zero Trust Architecture. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NIST, NISTIR 8011, vol. 3, Automation Support for Security Control Assessments: Software Asset Management
Dempsey, K., Goren, N., Eavy, P., Moore, G. (2018). NISTIR 8011 Vol. 3, Automation Support for Security Control Assessments: Software Asset Management. National Institute of Standards and Technology. Available at: https://csrc.nist.gov/publications/detail/nistir/8011/vol-3/final

NIST, NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers
Fagan, M., Megas, K.N., Scarfone, K., Smith, M. (2020). NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

CISA (Cybersecurity & Infrastructure Security Agency)

I-052518-PSA, May 25, 2018., https://us-cert.cisa.gov/ncas/alerts/TA18-145A
US FBI. (2018). Alert (TA18-145A): Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide. Available at: https://us-cert.cisa.gov/ncas/alerts/TA18-145A

Department of Justice, Cybersecurity & Infrastructure Security Agency, United States Environmental Agency, Multi-State ISAC. (2021) Compromise of U.S. Water Treatment Facility. Available at: https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint_Cybersecurity_Advisory_Compromise_of_U.S._Drinking_Treatment_Facility.pdf

CTIA

CTIA (no date). CTIA-Certification Resources, Certification Resources. Available at: https://www.ctia.org/certification-resources (Accessed: May 24, 2021).

CSDE (Council to Secure the Digital Economy)

Council to Secure the Digital Economy (CSDE) (2021) IoT Security Policy Principles Policy Considerations Building on the C2 Consensus on IoT Device Security Baseline Capabilities. Available at: https://securingdigitaleconomy.org/projects/iot-security-policy-principles/

GSMA

GSMA (no date) GSMA IoT Security Guidelines and Assessment | Internet of Things, gmsa.com. Available at: https://www.gsma.com/iot/iot-security/iot-security-guidelines/ (Accessed: May 24, 2021).

Ericsson

Anneroth, M., Casella, D., Eriksson, H., Mattsson, K. (2019) Privacy in mobile networks – How to embrace privacy by design. Available at: https://www.ericsson.com/en/reports-and-papers/white-papers/privacy-in-mobile-networks

Brännеby, A., Nazari, A., Hogan, M., Kuhlins, C., Zaidi, A. (2020) Cellular IoT in the 5G era. Available at: https://www.ericsson.com/48ff1f/assets/local/reports-papers/white-papers/Cellular_IoT_in_5G_whitepaper_AW.pdf?_ga=2.66249196.39672279.1618936625-565009469.1591360458

References (cont.)

Cybersecurity Testing and Certification (no date) ericsson.com. Available at: https://www.ericsson.com/en/portfolio/digital-services/transform-business/device-and-network-testing/device-and-application-verification/cybersecurity-testing-and-certification (Accessed: May 24, 2021).

Ekstrand, M. (2019) "Highlights of key end-to-end network slicing capabilities," ericsson.com, 3 May. Available at: https://www.ericsson.com/en/blog/2019/5/highlights-of-key-end-to-end-network-slicing-capabilities (Accessed: May 24, 2021).

Jason S. Boswell, Poretsky, S. (2020) Security considerations of Open RAN: Ensuring network radio systems are open, interoperable, and secure by design. Available at: https://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf

IoT Connections Outlook (2020). Available at: https://www.ericsson.com/en/mobility-report/dataforecasts/iot-connections-outlook

Olsson, J. et al. (2021) "A Zero-Trust Architecture for Telecom," Ericsson Technology Review, 12 May, p. 12. Available at: https://www.ericsson.com/49a20a/assets/local/reports-papers/ericsson-technology-review/docs/2021/zero-trust-and-5g.pdf

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com

www.ericsson.com

SE-126 25 Stockholm, Sweden
Telephone +46 10 719 00 00

May 2021