element14
AN AVNET COMMUNITY

May 2021

The Top Trends in IoT Security for 2021

Table of Contents

Top Trends in IoT Security for 2021

element14 is a Community of over 750,000 makers, professional engineers, electronics enthusiasts, and everyone in between. Since our beginnings in 2009, we have provided a place to discuss electronics, get help with your designs and projects, show off your skills by building a new prototype, and much more. We also offer online learning courses such as our Essentials series, video tutorials from element14 presents, and electronics competitions with our Design Challenges.

Billions of IoT-enabled devices are already active across the globe, and that number is predicted to grow steadily. But the security of these devices is sometimes lacking, allowing malicious actors to steal data and hijack systems. This eBook will feature recent IoT security trends.

element14 Community Team

The Top Trends in IoT Security for 2021

CHAPTER 1 Introduction

The **Internet of Things (IoT)** is a cluster of numerous interconnected objects, services, devices, and humans that communicate and share information to accomplish actions in diverse applications. IoT solutions offer meaningful insights and data to individuals and businesses. The IoT has several implementation domains like transportation, distribution, agriculture, energy production, and healthcare. The benefits, however, are tempered by their vulnerability to cyber-attacks. Recent research has revealed that 90 percent of consumers are concerned about IoT device security; thus, IoT developers must ensure the confidentiality and integrity of IoT solutions and data while diminishing cybersecurity risks. This eBook discusses IoT security-related issues and highlights future trends in IoT security.

CHAPTER 2 IoT Structures and Security-Related Threats

The following IoT security threat categories must be factored in during any IoT system development:

Confidentiality Breach: It occurs when a third party can access sensitive information without the subscriber's consent.

Theft of Service: It occurs when security weaknesses in implemented protocols fall prey to hackers, who then illicitly gain unauthorized access.

Data Integrity: It occurs when an unsanctioned user acquires deployed devices or drops unwanted messages inside the network. Hackers may target sensor-attached IoT nodes to disrupt plant production, for example.

Availability: Hackers use a "Denial of Service" attack, in which a device's network is flooded with random requests from connected nodes to overflow a server or a cloud application and, ultimately, crash it.

Industrial IoT devices are vulnerable to cyber threats like Man-in-the-middle, distributed denial of service (DDoS), device hijacking, and permanent denial of service (PDoS). The intention behind such attacks is to destroy IIoT infrastructure. Attacks on industrial control systems (ICSs), including programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and human-machine interfaces (HMIs) disrupt productivity and hamper service delivery across multiple industries. The adoption of complex and powerful IP-based devices (for example, sophisticated microprocessors) comes with increased risk.

Many wearables preserve unencrypted data on their local device. There is often no password or PIN protection and zero biometric security. User authentication is not required to access data recorded on a wearable, and sensitive data can be easily accessed. Wearable devices wirelessly connect to tablets or smartphones, using protocols like Bluetooth, Wi-Fi, and NFC, thus creating another entry point. These wireless communications are vulnerable to a continuous brute-force attack.

Automotive vehicles continue to advance and discard older technologies for newer, safer, and more efficient ones. Robust cybersecurity underpins such new connected services – overriding nearly all cybersecurity challenges that once blighted connected transport. Standard strategies employed to infiltrate automotive IoT solutions involve vulnerabilities in peer authentication, endpoint integrity hiatus, practical cryptographic tampering, the absence of partition between non-critical and critical applications, software application flaws, and business logic fragility.

IoT has rapidly found traction in healthcare. Medical diagnoses are a major chunk of hospital bills. IoT enables healthcare professionals to access a patient's medical history, vitals, and lab results. The technology enables either on-site access or remotely via smartphones or tablets. Risks are endemic when it comes to data gathering from devices specially engineered for IoT use. Device storage is particularly vulnerable during network transmission and also inside the cloud.

Sleep tracking devices measure heart rates and movements, and users benefit from quality sleep. These products, however, come with security issues like privacy and security vulnerabilities. Downloaded third-party apps contaminate sleep tracking software and code them into malware, enabling hackers to access the device remotely. Since most IoT sleep-tracking devices communicate over public networks, the adversary can execute various attacks, such as Botnets and Denial of Service (DoS), to intercept that communication channel. A data breach may also happen, as bad actors may remotely access the cloud-stored data. This is done by compromising the data via malicious software.

CHAPTER 3 Algorithms Used in IoT Security

A few standard algorithms for IoT Security implementation include:

RSA: An asymmetric encryption algorithm calculated using two randomly chosen prime numbers requiring public and private keys. The public key encrypts the message, which is again decrypted by the private key.

Advanced Encryption Standard (AES): A substitution-permutation network (SPN) dependent symmetric key block cipher algorithm. Uses three fixed 128-bit block ciphers cryptographic key sizes (128, 192, 256-bits).

Secure Hash Algorithm (SHA): The SHA accepts data input and generates the message digest or hash. SHA-0 and SHA-1 utilize 16-Bit hashing, and SHA-2 involves two functions set with respective 256-bit and 512-bit technologies. This algorithm accepts any size data and resolves it to a specific, predefined size string. The resulting string is termed a “Hash,” and the hash function application process to random inputs is termed “hashing.”

Elliptic Curve Digital Signature Algorithm (ECDSA): This is used for message authentication. A private key is used to sign a simple message, and any receiver who has the sender’s public key can trace the message to its sender.

Elliptic Curve Password Authenticated Key Exchange by Juggling (ECJPAKE): A password-authenticated key agreement protocol without Public Key Infrastructure (PKI) authentication. An authenticated and private channel is established on top of an insecure network, exclusively based on a shared password.

Cyclic Redundancy Check (CRC): Frequently used to detect and correct errors in storage devices and digital communication networks. Short data bytes pad blocks of data based on the polynomial division balance of their content. The CRC bytes on the receiver side are recalculated from received data and then compared with received CRC. The received data are discarded or corrected if there is a non-match.

CHAPTER 4 Error Correction and Cryptography

Error Detection and Correction methods preserve data integrity, especially during transfers. Parity bit check, Polar Codes, CRC check, and Hashing are a few popular techniques used. Data security focuses on encryption to encipher or decipher data. Cryptography can be symmetric or asymmetric, depending on the case.

Symmetric cryptography: in this setup, the same key is shared between the sender and the receiver. Key sharing poses a security risk when shared between the communicating factions. The Hellman key exchange technique is a secure method to exchange keys over a potentially insecure channel before communication.

Asymmetric or public-key cryptography: in this setup, a pair of public and private keys are used. Both keys are mathematically related, yet different. The sender uses the receiver’s public key to encrypt the data. Only the receiver’s private key, which is never shared, can decrypt the encrypted data. Public key cryptography is frequently used for authenticity.

CHAPTER 5 Security at the Edge

Easily accessible edge (node) devices must be physically protected to bar communication port access or firmware interference. Anyone with physical access to hardware during manufacture, installation, or even deployment may threaten security. UARTs and other device-debugging interfaces are easily compromised and must be secured against unlawful access. A few recent controllers and processors offer exclusive encryption/decryption engines. Some IoT devices utilize processors with operating systems support, making OS-level security crucial. ICs are vulnerable to key capture, malware injection, and counterfeiting during distribution and production.

Security ICs create a barrier that separates vital processes from the IoT application software, in order to function in a safe environment. They integrate nonvolatile memory into the IC to manage and transport the keys securely.

Products like A71CH and A1006 are examples of Security ICs. NXP's A71CH Trust Anchor utilizes a "plug and trust" approach vis-a-vis its microcontrollers, to locally save the secret keys for asymmetric cryptography solutions. The A1006 is a tamper-proof authenticator IC and comes with a private key and the corresponding certificate accommodating the Public Key, customer's product fields, a unique identifier, and usage. The static keys are unique for every A1006. The ECDSA key, based on the SHA-224 digest and NIST P-224 curve hash with the client's chosen certificate authority, digitally signs the certificates.

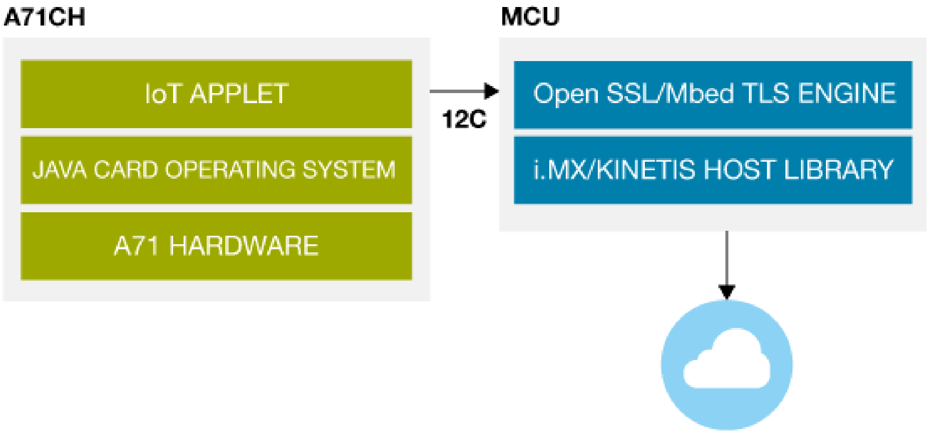


Figure 1: A71CH block diagram (Image Source: NXP Semiconductors)

CHAPTER 6 Gateway Security

Connected End nodes with no IP connection in a personal area network (PAN) cannot directly transmit data to the cloud or web servers. As a result, these nodes require gateways that route the traffic to connect the PAN to the Internet. However, this ceases to be an issue if Ethernet or Wi-Fi are used to connect the devices. Since the gateway uses a UDP or TCP/IP to connect these servers, the communication must be protected. The following protocols find use in gateway-server secured communication:

HTTP/HTTPS

The Hypertext Transfer Protocol (HTTP) refers to an application layer protocol active on client-server models. Since standard HTTP traffic utilizes plain text, anyone with the right tools or physical access can acquire the packet's information. HTTPS, a more secure version of HTTP, was developed to eliminate such issues. The advanced versions use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt all traffic. The client uses an X.509 certificate issued by the server, and this certificate usually contains the public encryption key. Only the private key, which is never disclosed by the server, can decrypt the data. HTTP is vulnerable to distributed denial-of-service (DDoS) bombardment. The attacker uses POST or HTTP GET calls from internet connected or interconnected devices to swarm the server with traffic. The attacker can also execute a man-in-the-middle (MITM) attack forcing the server to SSLV3 and effectuate the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack. This vulnerability is found in the Cipher Block Chaining Mode.

MQTT

Message Queuing Telemetry Transport (MQTT) refers to an ISO-standard publish-subscribe messaging protocol. It tasks on top of TCP/IP, and its operation requires a broker to be implemented on the cloud server. MQTT depends on SSL or payload encryption and TLS. The TLS is reviewed if users or network nodes are authenticated by password and username authentication. If constrained resources discourage TLS, then the user may use MQTT to encrypt the transmitted payload. Authentication credentials may also be encrypted by the use of hashing or any other encryption method.

COAP

Constrained Application Protocol (COAP) is a lightweight RESTful protocol, particularly for M2M communication for IoT applications. COAP security uses Datagram Transport Layer Security (DTLS), and by default, uses 3072-bit RSA equivalent keys.

CHAPTER 7 Communication Security

IoT end nodes utilize wireless technologies. Since air is the data transmission medium, any individual inside the Wi-Fi hotspot/modem/Access Point range may try to eavesdrop, making these nodes highly vulnerable.

Wi-Fi

Wi-Fi, a wireless Local Area Networking technology, operates on a 2.4GHz or 5.8GHz ISM band based on 802.11 standards. It has evolved with multiple security protocols to offer secure and seamless user connectivity. Security options include WEP (Wired Equivalent Privacy), EAP (Extensible Authentication Protocol), and WPA (Wi-Fi Protected Access).

LORA/LORAWAN

LoRa refers to a long-range, low-power wireless communication technology utilizing the LPWAN ISM band. It is well suited for battery-powered IoT end nodes. LoraWAN refers to a media access control layer protocol specification for managing communication among LoRa nodes and gateways. The gateways use IP connectivity to connect to cloud services, and nodes send data to different gateways.

LoRa utilizes two-layer encryption:

- A distinct 128-bit Network Session Key split between the network server and end-device

- A distinct 128-bit Application Session Key (AppSKey) divided end-to-end at the application level

All keys and authentication use the AES algorithm. Network and application-level encryption enable full private data transmission. Even the network operator cannot access it. Keys are activated during commissioning or production through modified Over the Air (OTAA) or Activated by Personalization (ABP). OTAA is more secure than ABP, as the keys are negotiated during the joining process.

An EUI-64 based DevEUI global unique identifier and 128-bit AppKey accompany a LoRaWAN device and are used during device authentication. Two AES-128 session keys, AppSKey and NwkSKey, are generated from the AppKey, and they encrypt traffic between servers and nodes. AppSKey encrypts and decrypts the application payloads, and NwkSKey verifies packet integrity and authenticity.

Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) targets battery-operated devices and is recognized as a Personal Area Network (PAN) technology. It shares the 2.400–2.4835 GHz ISM frequency band with classical Bluetooth.

Security Mode 1: This mode uses encryption to administer security and has four levels:

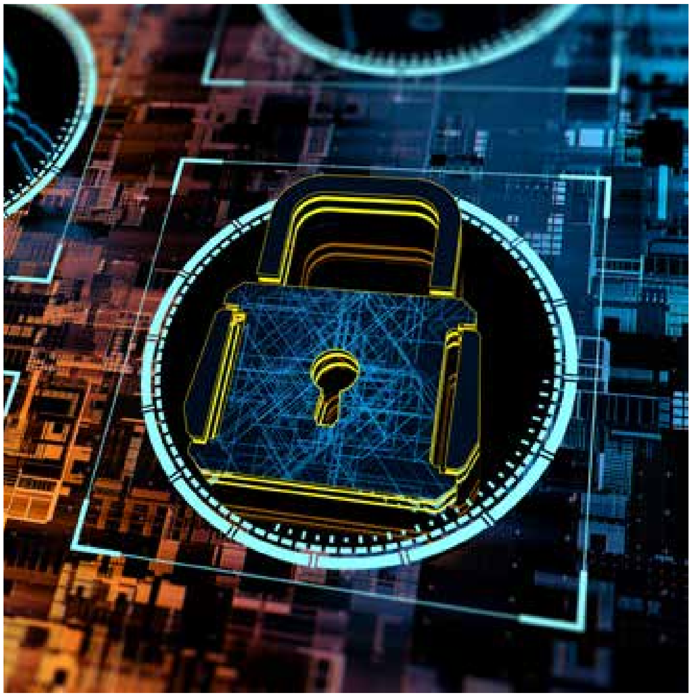
- Level 1 – Zero Security (No encryption and no authentication)
- Level 2 - Unauthenticated with encryption
- Level 3 - Authenticated partnering (pairing) with encryption
- Level 4 - Authenticated LE Secure Connections partnering (pairing) with encryption

Security Mode 2: This mode uses data signing to enforce security and has two levels:

- Level 1 - Unauthenticated pairing or partnering with data signing
- Level 2 - Authenticated pairing or partnering with data signing

SIGFOX

The LPWAN, ultra-narrowband Sigfox uses 868 and 902 MHz ISM frequencies. A distinct symmetrical authentication key is dispatched with all Sigfox Ready devices. Messages from or to the device hold a cryptographic token computed from the authentication key, verifying the message's origin and data integrity. The authentication key is stored locally in the end device and is unique for every Sigfox-ready instrument.



VPN and SSL encryption is used to communicate between the Sigfox base station and the Sigfox cloud. A message originating from the Sigfox end nodes carries a distinct signature produced from a locally stored key. This unique signature underlines the message's authenticity. This message also has an individual packet number, which saves that network from message replay. When it transmits from the end node, the message is transmitted thrice in three distinct frequencies to ensure message delivery to the Sigfox cloud. Such an arrangement also forbids jamming, as the transmission is of random frequency.

Thread

Designed for smart home use, Thread is an IPV6-based 6LoWPAN communication technology. ECJPAKE is a primary security measure in the NIST P-256 elliptic curve Thread Network. The Diffie-Hellmann elliptic curve algorithm finds use as a key agreement and Schnorr signatures as NIZK (Non-Interactive Zero-Knowledge) proof mechanism to authenticate the two peers. The NIZK also establishes a shared secret between them based on a passphrase.

ZIGBEE

ZigBee applies the IEEE 802.15.4 described security model, inclusive of access control to network devices (authentication), message integrity checks (MICs), encryption (symmetric-key cryptography), and confirmation of the safety of transmitted frames. ZigBee's symmetric key cryptography utilizes three distinct types of keys for peer-to-peer communication:

Master Key: Pre-installed by manufacturers on the device.

Link Key: Restricted to nodes and utilized to encrypt all point-to-point communication data at the application level and confined to the nodes. This key is separate for each communication node pair and minimizes master key distribution risk in the network.

Network Key: Used at the network level and known to all the nodes in the network.

Z-Wave

Z-Wave is a low-power RF communication technology targeted towards Smart Home products or Home Automation for low latency and small data packets. It supports mesh networking.

The Z-Wave Alliance launched the S2 Security framework as a substitute for their primary S0 with an enhancement in the key exchange mechanism. The S2 framework utilizes an Elliptic Curve Diffie-Hellman (ECDH) algorithm for key exchange. It utilizes an AES algorithm to produce all the keys.

Near Field Communication (NFC)

NFC technology works at the 13.56MHz frequency and supports up to 420kbps data transfer speed and a low communication range (<10cm). It is integrated into devices and used for pairing and authentication for contactless payment processes. NFC manufacturers may use any encryption algorithm to manage security attacks.

CHAPTER 8 Cloud Level Security

IoT devices tether to web services operating on cloud networks or assigned servers. It is of paramount importance to maintain the safety of private data kept in applications, databases, and servers when designing IoT applications.

Many service providers set up secured servers as a Software-As-A-Service (SAAS) or Platform-As-A-Service (PAAS). SaaS offers the software on a license basis to end-users, whereas PaaS is a total development and deployment environment located in the cloud.

Since servers are frequently installed in physically inaccessible data centers, system admins use SSH (Secure Shell) to link to remote servers. SSH keys established on public-key cryptography ensure secure communication. SSL or TLS are employed with exposed web services. All server traffic gets encrypted, thus circumventing man-in-the-middle attacks.

VPNs secure the connection among machines and show the connections as a private local network, thus adding an extra security layer.

CHAPTER 9 IoT Security Trends for 2021

2020 was, by any measure, a disruptive year. The sheer unpredictability of the COVID-19 pandemic forced organizations to pivot, change, and adapt. Here are some of the leading IoT security trends happening today.

1. Keeping Computing Private

Classified computing requires a trusted ecosystem where organizations can fearlessly share data in undocumented environments. Private, secure computing frequently involves three technologies that shield data during its use. Confidential computing creates a careful data processing environment. Privacy-aware machine learning (ML) enables decentralized data analytics and processing. Cryptographic techniques like homomorphic encryption help third parties synthesize encrypted data, and the encrypted result is returned to the owner of that data. The data is securely enclosed through encryption, and only the data owner can access it.

2. CSPM: The Way to Effortless Compliance

Organizations use Cloud Security Posture Management (CSPM) for automatic GDPR, HIPAA, and CCPA compliance. This versatile tool automates a broad range of cloud security management issues, including different cloud infrastructures. Companies frequently use CSPM tools to identify risks and mitigate them.

3. Distributed Cloud

The Distributed Cloud accommodates privacy laws that dictate data housing in specific geographical areas. It offers public cloud options to several physical addresses. The public cloud company maintains services and, when required, physically implements them. The company can evolve to satisfy growing user needs. Distributed cloud assists low-latency contexts and reduces data costs.

4. Location-independent Functions

Location-agnostic operations enable proper administration of distributed infrastructure spread across multiple business services. They are designed to help employees and support customers. Organizations enjoy seamless remote access through passwordless, multifactor authentication. Security perimeters are achieved through secure access service edge (SASE), zero-trust security, and identity.

5. Zero Trust Cybersecurity

Contrary to popular perception, zero trust cybersecurity is not an assortment of technologies but rather an evolving security culture. An individual’s identity dictates that person’s customized security perimeter. This is applicable for specific devices, as well. A granular and secure approach calls for effective, robust authentication and authorization. This is achieved by centralizing policy orchestration and distributing policy enforcement.

6. Time Tested Cloud PKI

Public key infrastructure (PKI), a security tool, is used by numerous organizations. It is complex, and secure facilities are needed to administer it. PKI also needs dedicated, trained personnel for smooth operation. However, the introduction of IoT, DevOps, and Cloud and their subsequent popularity has changed PKI’s role in the industry.

7. Endpoint Management

Organizations need proper endpoint management solutions, as cybercriminals may use them to enter corporate networks without permission. A good solution imports multiple benefits, such as remote workforce protection, management of endpoint environments, and automated compliance and provisioning.

8. Responsible AI

Artificial Intelligence (AI) is a potentially disruptive, powerful technology. Its apparently limitless applications raise multiple concerns like workforce displacement, privacy loss, potential biases during decision-making, and the absence of control over robots and automated systems. Responsible AI eliminates such concerns.

It promises (and delivers) accountable, ethical, and transparent usage of AI technologies compatible with user expectations, societal laws, and organizational values. Responsible AI fosters innovation in organizations to realize AI's transformative potential.

Want to learn more about IoT security and other related topics? Visit our **IoT page** here.

element14
AN AVNET COMMUNITY

300 S. Riverside Plaza, Suite 2200
Chicago, IL 60606

www.element14.com/community

Facebook.com/e14Community
Twitter.com/e14Community