Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

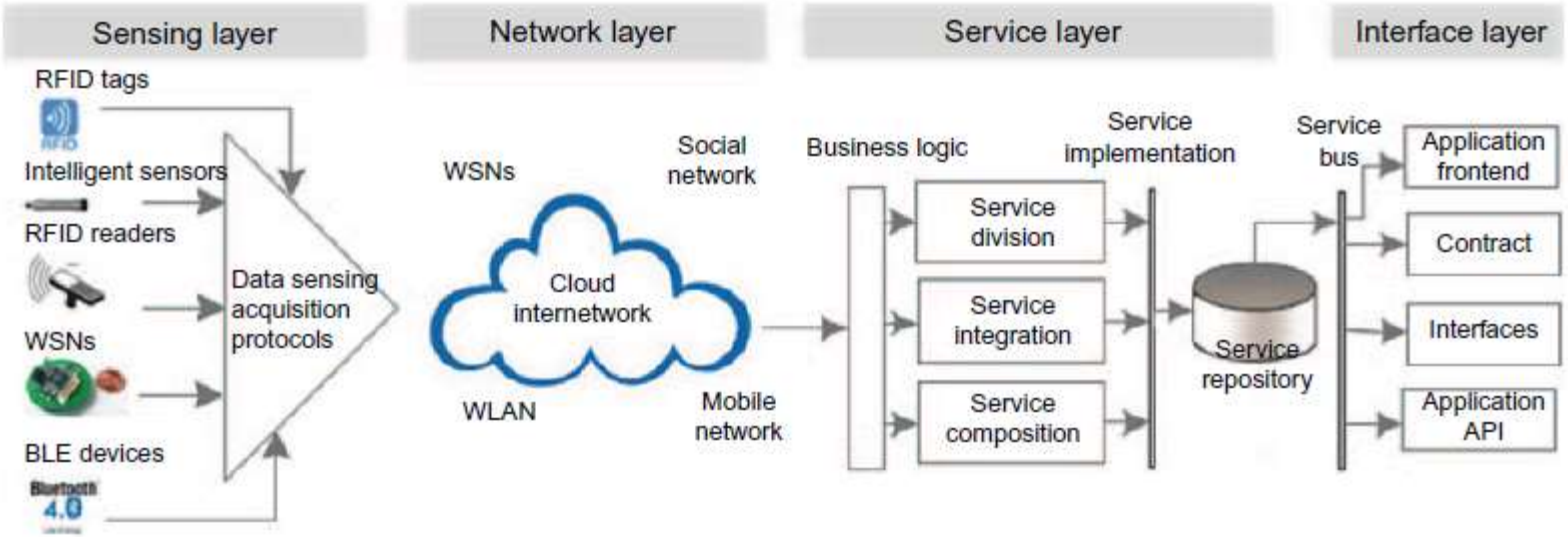
<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture: IoT Security

Requirements, Reference Guidelines, Vulnerabilities, Security Framework Features and Implementation Methods

Source Disclaimer: Content for some of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

RECAP: IoT Layers: A Security Perspective

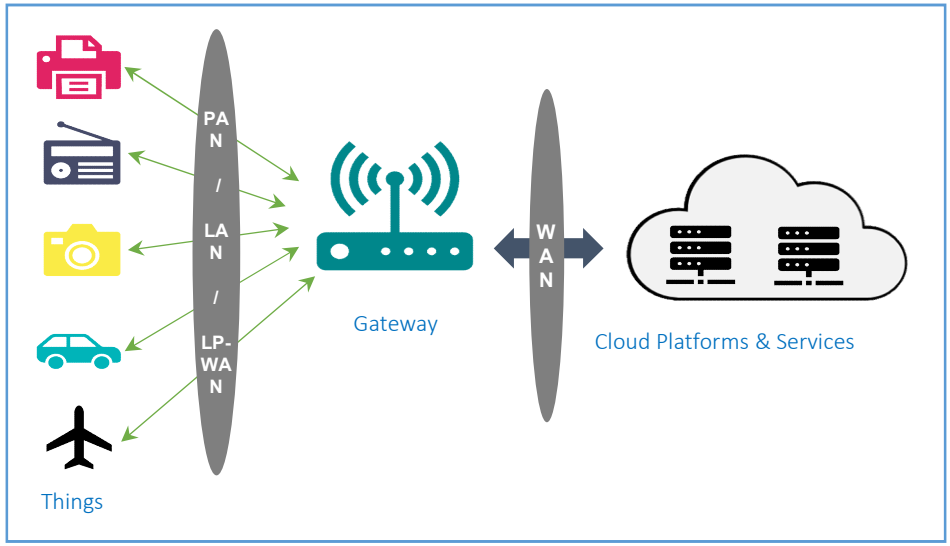


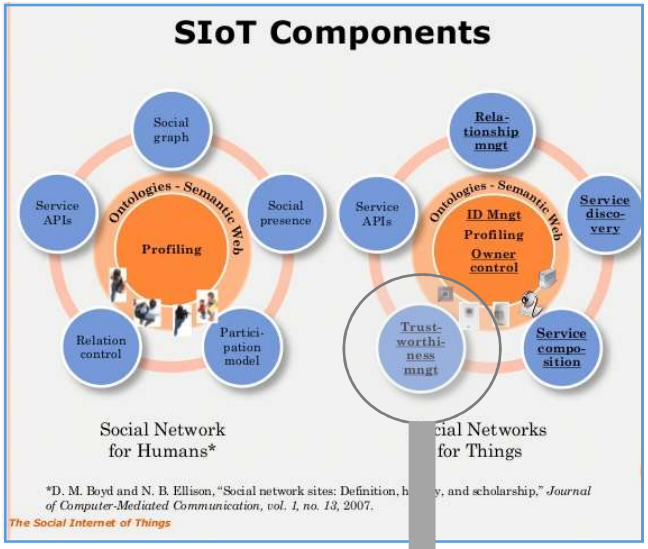
Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

RECAP: IoT Architectures – The Evolving Landscape!

CENTRALIZED ⟷ DISTRIBUTED

Architecture Evolution





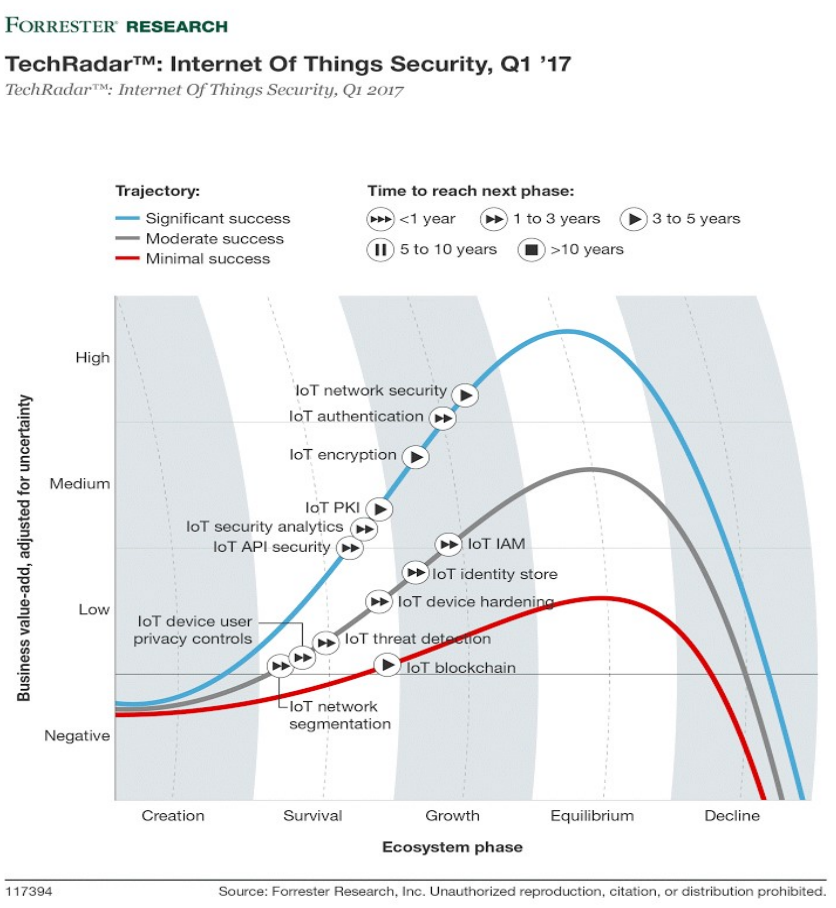
Cloud Computing ⟷ Machine-to-Machine | Internet of Vehicles | Internet of Energy | Internet of Sensors

- *"The way to secure the Internet of Things is to allow the self-organizing migration of services away from a central cloud alone and into local infrastructure ecosystems where they can act independently"* - https://www.scmagazineuk.com/doriot-project-secure-internet-things/article/1590701

RECAP: IoT Security: Involved Domains

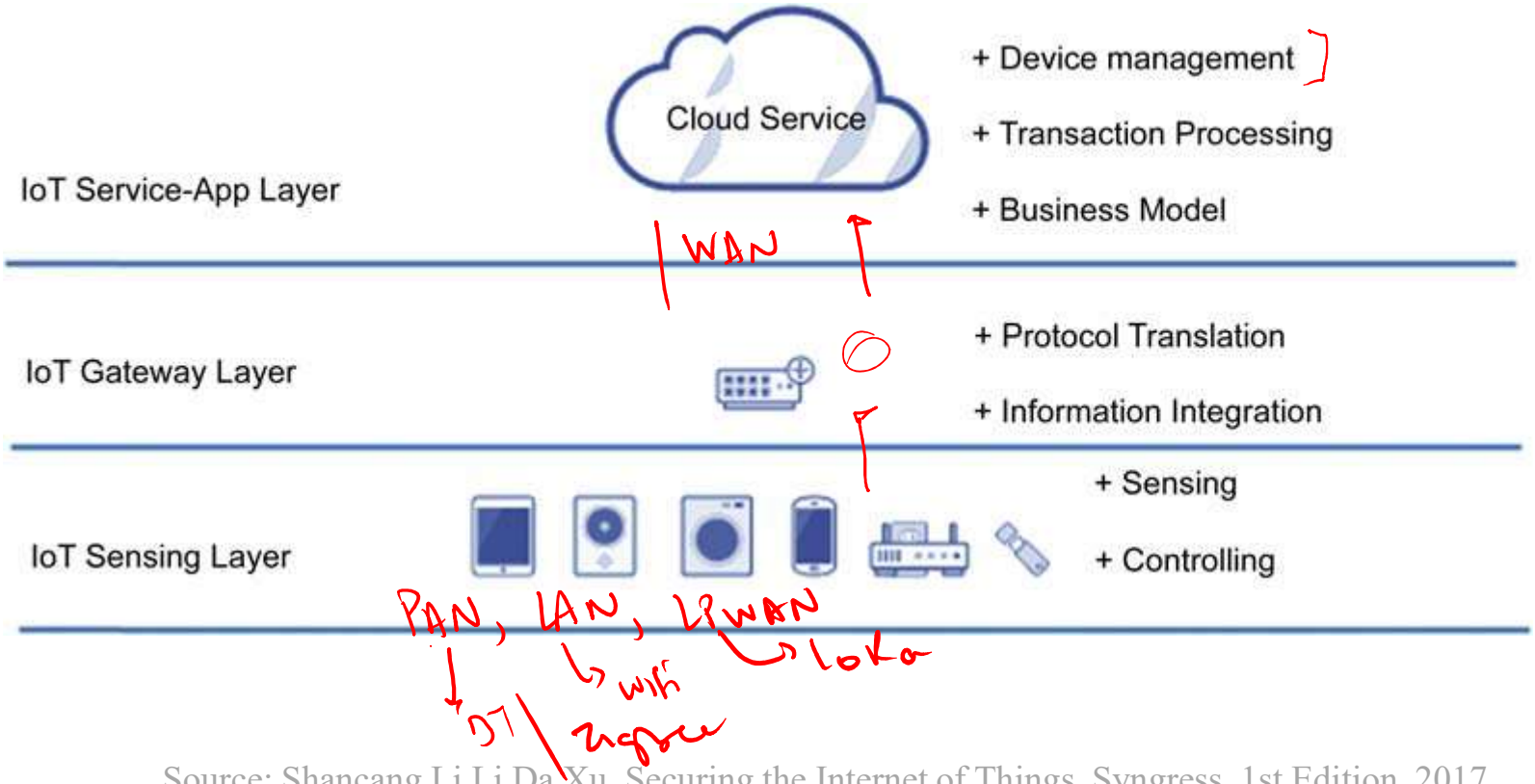
"Cyber security is also a moveable feast - what is deemed secure today may not be tomorrow" – IoTSF

- Device Security (aka Sensing Layer)
  - Securing the IoT Device
  - **Challenges**: Limited System Resources
- Network Security (aka Network Layer)
  - Security the network connecting IoT Devices to Backend Systems
  - **Challenges**: Wider range of devices + communication protocols + standards
- Cloud/ Back-end Systems Security (aka Service and Interface Layer)
  - Securing the backend Applications from attacks
  - Firewalls, Security Gateways, IDS/IPS
- Mutual Authentication (Across Layers)
  - Device(s) ←→ User(s)
  - Passwords, PINs, Multi-factor, Digital Certificates
- Encryption (Across Layers)
  - Data Integrity for data at rest and in transit
  - Strong Key Management Processes



IoT Security Requirements

Example of a Simple IoT System / Solution

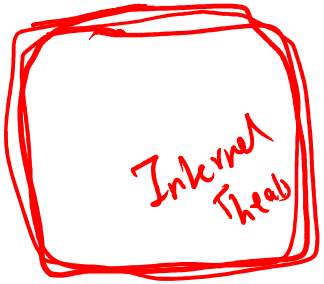


Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

Security Requirements for IoT Systems

- IoT introduces large quantities of new devices that will be deployed
- Each connected device could be a potential doorway into the IoT infrastructure or personal data → **Data Security** happens to be the biggest challenge even in IoT Systems → Data-centric Security Approaches

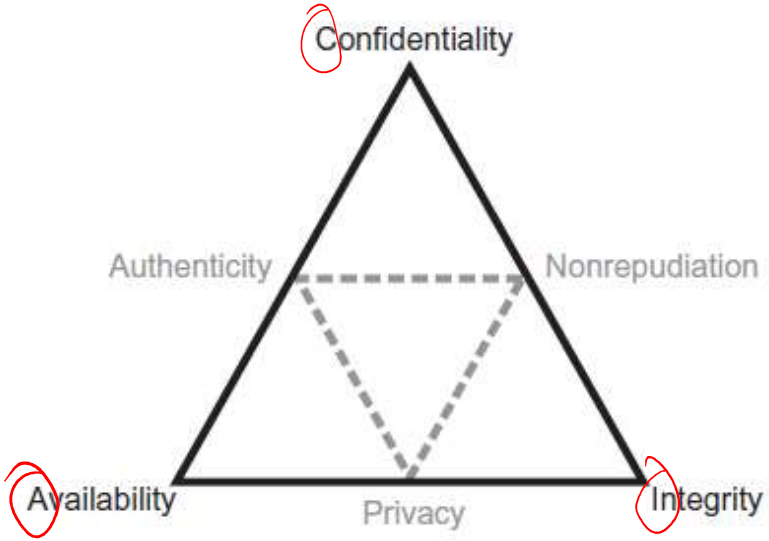
- Security Requirements for IoT systems are handled via a combination of:
  - Sensing Layer Security
  - Network Layer Security
  - Service (& Interface) Layer Security



CIA - Triad

IoT Data Security

- For IoT Data Security, the main security requirements are addressed from six aspects, as shown in the figure



- **Confidentiality**—data is secured to authorized parties
- **Integrity**—data is trusted
- **Availability**—data is accessible when and where needed
- **Nonrepudiation**—service provides a trusted audit trail
- **Authenticity**—components can prove their identity
- **Privacy**—service does not automatically see customer data

Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

Sensing Layer Security

- This layer of the framework is characterized as the intersection of people, places, and things
  - These things can be simple devices like connected thermometers and light bulbs, or complex devices such as medical instruments and manufacturing equipment
- For security in IoT to be fully realized, it must be designed and built into the devices themselves. This means that IoT devices must be able to
  - prove their identity to maintain authenticity
  - sign and encrypt their data to maintain integrity, and
  - limit locally stored data to protect privacy
- The security model for devices must be strict enough to prevent unauthorized use, but flexible enough to support secure, ad hoc interactions with people and other devices on a temporary basis
- Physical security is another important aspect for devices
  - This creates the need to design tamper resistance into devices so that it is difficult to extract sensitive information like personal data, cryptographic keys, or credentials
- Lastly, devices must support software updates to patch vulnerabilities and exploits

Network Layer Security

- This layer of the IoT framework represents the connectivity and messaging between things and cloud services
- Communications in the IoT are usually over a combination of private and public networks, so securing the traffic is obviously important.
- This is probably the most understood area of IoT security, with technology like TLS/SSL encryption ideally suited to solve the problem.
- The primary difficulty arises when you consider the challenges of cryptography on devices with constrained resources. E.g. 8-bit microcontrollers with limited RAM. For example:
  - an Arduino Uno takes up to 3 min to encrypt a test payload when using RSA 1024 bit keys
  - however an elliptical curve digital signature algorithm with a comparable RSA key length can encrypt the same payload in 0.3 s.
  - This indicates that device manufactures cannot use resource constraints as an excuse to avoid security in their products
- Another security consideration for the network layer is that many IoT devices communicate over protocols other than WiFi
  - This means the IoT gateway is responsible for maintaining confidentiality, integrity, and availability while translating between different wireless protocols, from Z-Wave or ZigBee to WiFi for example.

Service Layer Security

- This layer of the framework represents the IoT management system and is responsible for onboarding devices and users, applying policies and rules, and orchestrating automation across devices
- Access control measures to manage user and device identity and the actions they are authorized to take is critical at this layer
- To achieve nonrepudiation, it is also important to maintain an audit trail of changes made by each user and device so that it is impossible to refute actions taken in the system
- Big Data Challenges:
  - providing clear data use notification so that customers have visibility and fine-grained control of the data sent to the cloud service
  - keeping customer data stored in the cloud service segregated and/or encrypted with customer-provided keys, and
  - when analyzing data in aggregate across customers, the data should be anonymized

IoT Security:
Reference Guidelines

Guidelines for Secure System Engineering

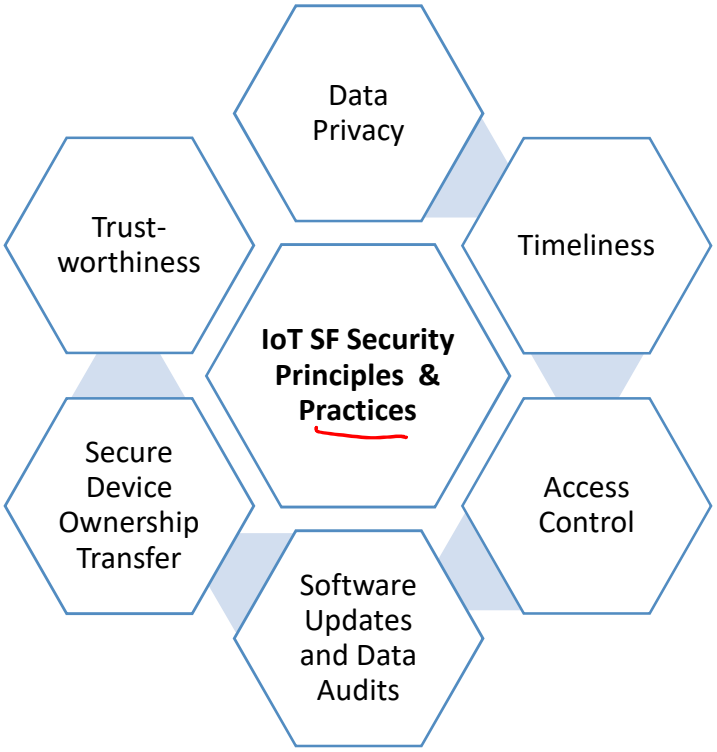
- Forrester Research: "***There is no single, magic security bullet that can easily fix all IoT security issues***"

- IoT Security Foundation
  - Establishing Principles for Internet of Things Security

  » Does the data need to be private?
  » Does the data need to be trusted?
  » Is the safe and/or timely arrival of data important?
  » Is it necessary to restrict access to or control of the device?
  » Is it necessary to update the software on the device?
  » Will ownership of the device need to be managed or transferred in a secure manner?
  » Does the data need to be audited?

- Do not re-invent the wheel – rely on reusing existing cyber security principles and practices

  "the underlying principles that inform good security practices are well established and quite stable" – IoT SF



NIST GUIDANCE ON INTERNET OF THINGS

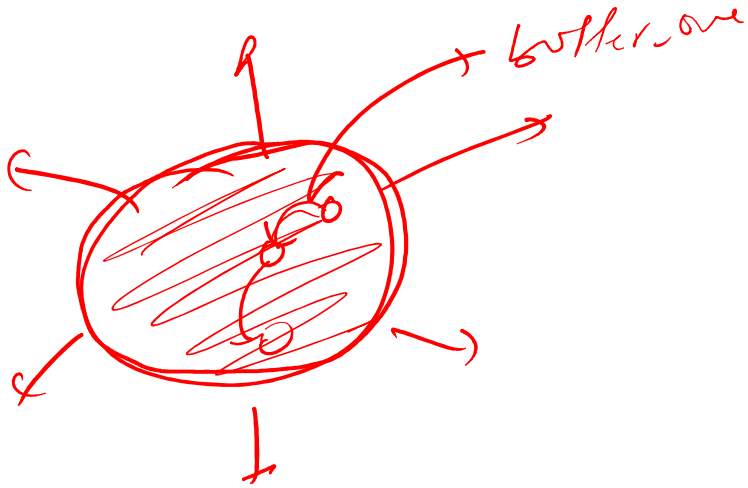
- NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers
  - Intended for a wide range of IoT devices, but only those that are newly developed
  - It is not meant to be a retroactive *band-aid* for devices already out on the market!
- The guidance provides six clear steps that manufacturers should follow, which are further separated into two phases:
  - ***Pre-Market:*** before the device is sold
  - ***Post-Market:*** after the device is sold
- Because over half of the recommendations are specifically for a manufacturer to perform before releasing their product, NISTIR 8529 cannot be applied to IoT devices already on the market
  - Four pre-market activities (1–4) and two post-market activities (5–6) for IoT manufacturers to address cybersecurity in IoT devices
    - Activity 1: Identify expected customers and define expected use cases.
    - Activity 2: Research customer cybersecurity goals.
    - Activity 3: Determine how to address customers' goals.
    - Activity 4: Plan for adequate Support of customers' goals.
    - Activity 5: Define approaches for communication to customers.
    - Activity 6: Decide what & how to communicate to customers.

Source(s): https://risk3sixty.com/2020/08/17/securing-iot-devices-with-nistir-8259/
https://www.mwe.com/insights/nist-guidance-on-internet-of-things/

NISTIR 8259A

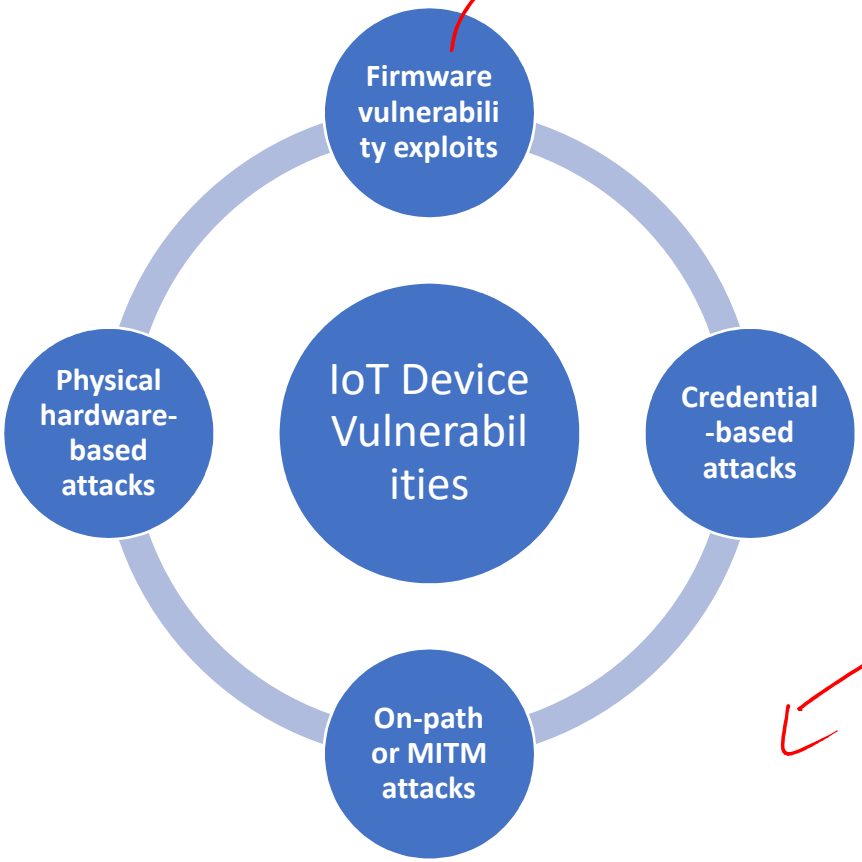
- NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline provides six capabilities, cross-referenced with applicable industry and federal standards, as a default for minimally securable IoT devices.
  - Device identification: The IoT device can be uniquely identified logically and physically.
  - Device configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
  - Data protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
  - Logical access to interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
  - Software update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.
  - Cybersecurity state awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

Source(s): https://www.mwe.com/insights/nist-guidance-on-internet-of-things/



IoT Security:
Current Vulnerabilities

IoT Device Vulnerabilities



IoT Device Vulnerabilities (2)

- Firmware vulnerability exploits
  - For the majority of IoT devices, the firmware is essentially the operating system or the software underneath the OS
  - Most IoT firmware does not have as many security protections in place
  - Often the vulnerabilities in the firmware cannot be patched

- Credential-based attacks
  - IoT devices come with default administrator usernames and passwords
  - Well-known, or simple to guess, and often, not very secure
  - In some cases, these credentials cannot be reset
  - Often, IoT device attacks occur simply because an attacker guesses the right credentials

Source: https://www.cloudflare.com/en-in/learning/security/glossary/iot-security/

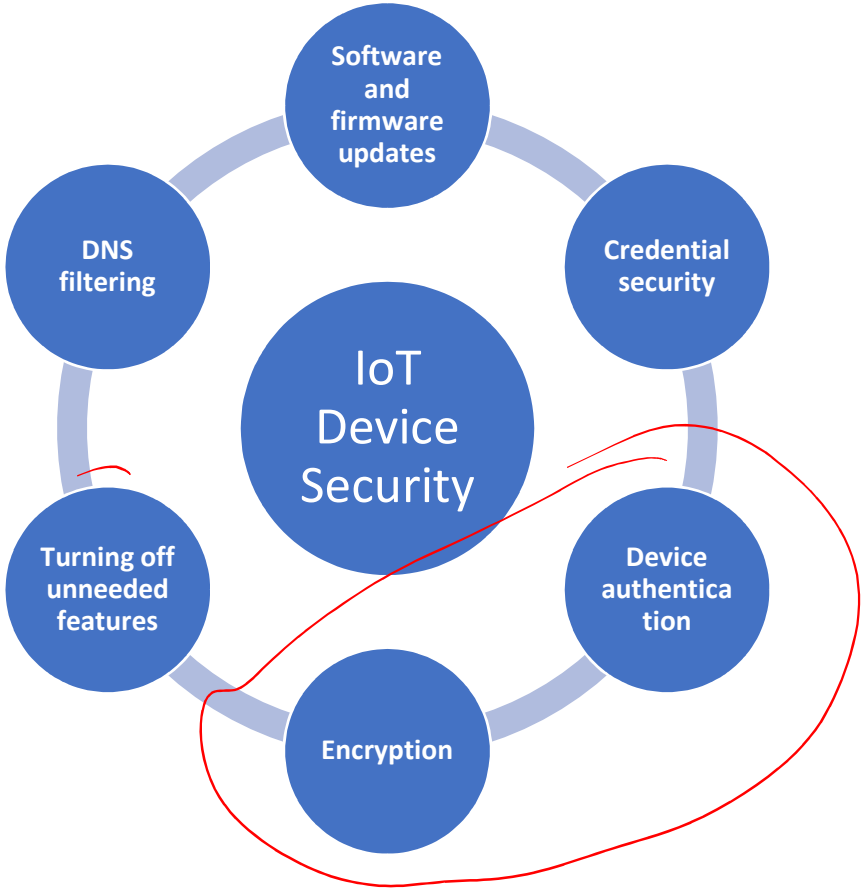
IoT Device Vulnerabilities (3)

- On-path attacks (or Man-in-the-Middle attacks)
  - IoT devices are particularly vulnerable to such attacks because many of them do not encrypt their communications by default
  - On-path attackers position themselves between two parties that trust each other and intercept communications between the two
  - MITM attacks can also happen by Impersonation, where a malicious node sets up two sessions (with device and server), impersonating and relaying messages between them

- Physical hardware-based attacks
  - Many IoT devices, like IoT security cameras, stoplights, and fire alarms, are placed in more or less permanent positions
  - An attacker having physical access to an IoT device's hardware can steal its data or take over the device
    - They could do this by accessing programmatic interfaces left on the circuit board, such as JTAG and RS232 serial connectors
    - Some microcontrollers may have disabled these interfaces, but could still allow direct reads from the attached memory chips if the attacker solders on new connection pins
  - This approach would affect only one device at a time, but a physical attack could have a larger effect if the attacker gains information that enables them to compromise additional devices on the network

Source: https://www.cloudflare.com/en-in/learning/security/glossary/iot-security/

Common Measures to overcome Device Vulnerabilities



Device Security (1)

- Software and firmware updates:
  - IoT devices need to be updated for vulnerability patch or software update
- Credential security:
  - IoT device admin credentials should be updated if possible.
  - It is best to avoid reusing credentials across multiple devices and applications — each device should have a unique password
- Device authentication:
  - IoT devices connect to each other, to servers, and to various other networked devices. Every connected device needs to be authenticated to ensure they do not accept inputs or requests from unauthorized parties
- Encryption:
  - Prevents on-path attacks.
  - Encryption must be combined with authentication to prevent MITM attacks. Otherwise, the attacker could set up separate encrypted connections between one IoT device and another, and neither would be aware that their communications are being intercepted.

Source: https://www.cloudflare.com/en-in/learning/security/glossary/iot-security/

Device Security (2)

- Turning off unneeded features:
  - Most IoT devices come with multiple features, some of which may go unused by the owner
  - Even when features are not used, they may keep additional ports open on the device
  - The more ports an Internet-connected device leaves open, the greater the attack surface — often attackers simply ping different ports on a device, looking for an opening
  - Turning off unnecessary device features will close these extra ports.
- DNS filtering:
  - DNS filtering is the process of using the Domain Name System to block malicious websites
  - Adding DNS filtering as a security measure to a network with IoT devices prevents those devices from reaching out to places on the Internet they should not (i.e. an attacker's domain)

Source: https://www.cloudflare.com/en-in/learning/security/glossary/iot-security/

IoT Security Framework

IoT Security Framework

At the heart of the IoT Security Framework are the following key functions:

- Authentication
- Authorization
- Access Control
- (*Apart from the obvious function – Encryption!*)

We discuss these functions in the following slides.

Authentication

- At the heart of the framework is the authentication layer, used to provide and verify the identity information of an IoT entity
- When connected IoT/ M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device
- The way to store and present identity information may be substantially different for the IoT devices (as against human credentials, like username/password, etc)
  - Device identifiers include RFID, shared secret, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware based root of trust
  - Establishing identity through X.509 certificates provides a strong authentication system. However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates
  - There exists opportunities for further research in defining smaller footprint credential types and less compute-intensive cryptographic constructs and authentication protocols (***aka*** *Lightweight Cryptography*)

Authorization

- The second layer of this framework is authorization that controls a device's access (to network services, back-end services, data etc)
  - This layer builds upon the core authentication layer by leveraging the identity information of an entity
  - With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information
- Trust relationships can sometimes also be formed in absence of Authorization techniques, and is necessary in some conditions
  - E.g in the absence of a common Authentication and Authorization framework
  - Or, for latency sensitive applications, e.g. those built using the distributed M2M or SIoT architectures