Internet of Things (IoT) Overview & Security Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39052/

IoT Security Best Practices

1. Maintain Up-to-Date Firmware:	Always maintain your IoT devices' firmware and software up-to-date. Manufacturers frequently publish security fixes to fix flaws.
2. Make Use Of Strong Passwords:	Create robust passwords for each IoT device and change them frequently. Do not use default or simple passwords.
3. Implement Encryption:	For data transfer between IoT devices and servers, implement encryption. End-to-end encryption should be used, and powerful encryption methods like AES should be used.
4. Regulate Network Access:	Regulate how much network access IoT devices have. To prevent unwanted access, use virtual private networks (VPNs) and firewalls.
5. Implement Two-Factor Authentication:	When logging into IoT networks, devices, and data, use two-factor authentication.
6. Implement Access Control Techniques	to limit access to IoT devices based on identities, roles, and permissions.
7. Track and Analyze IoT Traffic:	Track and examine IoT device traffic to and from the devices to look for unusual or suspicious activity. To recognize and stop assaults, employ intrusion detection and prevention systems (IDS/IPS).
8. Use Secure Protocols:	To communicate data between IoT devices and servers, use secure protocols like HTTPS, TLS, and SSL.
9. Segment IoT networks from the main network	to stop lateral attacker movement in the event of a breach. Utilize network segmentation strategies like VLANs and subnets.

IoT Security Best Practices (cont)

10. Educate Users:	Inform users of safe device usage and IoT security recommended practices. Show them how to spot questionable activity and report it.
11. Disable unneeded Services:	To lessen the attack surface on IoT devices, disable any unneeded services or protocols.
12. Regularly verify your security protocols	including vulnerability scanning, penetration testing, and security audits.
13. Use Trustworthy IoT Devices:	Only use trustworthy IoT devices from recognized manufacturers. Before buying, do your research on the gadgets to make sure they adhere to privacy and security standards.
14. Safely Store Data:	Use encryption and access control techniques to safely store IoT data, including backups and archives.
15. Secure Key Management with HSM	Implement Hardware Security Modules (HSMs) for secure key management in IoT devices. Use HSMs to generate, store, and protect cryptographic keys used for encryption, decryption, and digital signatures. HSMs provide a tamper-resistant environment for key storage, preventing unauthorized access or extraction of keys.

IoT data security is essential for protecting the integrity and safety of IoT networks and devices. To reduce risks, IoT security needs regular monitoring, updates, and enhancements. You can defend your devices, data, and infrastructure from cyber threats by being watchful and taking a proactive approach.

Comparison between device SDKs and embedded SDKs

Feature	Device SDKs	Embedded SDKs
Definition	Collection of software libraries and tools for devices	Software development tools for embedded systems
Hardware platform	Specific devices or hardware platforms	Embedded systems or microcontrollers
Abstraction Level	Higher-level APIs and services	Low-level access to hardware peripherals and interfaces
Functionality	Device integration, data collection, device management	Firmware development, low-level software
Development environment	Integration with popular development environments	Specialized development environments
Use Cases	Smart devices, IoT devices, hardware peripherals	Embedded systems, microcontrollers, real-time systems

Microcontrollers boards

Arduino:	is a publicly available electronics platform providing a range of microcontrollers and development boards, featuring an accessible programming interface and a user-friendly development environment.
Raspberry Pi:	a widely used single-board computer that functions as a microcontroller and operating system combined.
ESP8266:	due to its low power consumption, this compact and affordable Wi-Fi microcontroller is frequently used in Internet of Things (IoT) devices.
The ESP32:	a well-known microcontroller with Bluetooth and Wi-Fi integrated in that offers improved functionality.
STM32:	Microcontrollers in the STM32 family are frequently used in industrial and commercial IoT applications because of their toughness and robustness.

Microcontrollers boards (cont)

PIC:	a family of microcontrollers that are well-liked in IoT and embedded systems due to their low power needs and usability.
Atmel:	is a family of microcontrollers that is frequently utilized in IoT applications because of its great performance and low power requirements.
NXP LPC:	a collection of microcontrollers that are frequently used in Internet of Things applications and feature integrated peripherals and communication interfaces.
Texas Instruments MSP430:	a collection of ultra-low-power microcontrollers that are typically seen in battery-powered Internet of Things gadgets.
Nordic Semiconductor nRF52:	a collection of high-performance, low-power microcontrollers used commonly in Internet of Things (IoT) applications that require wireless connections.

Network Topologies

Star Topology:	IoT devices are connected to a central hub.
Mesh Topology:	IoT devices are connected to each other in a decentralized network.
Bus Topology:	IoT devices are connected to a common data transmission line.
Ring Topology:	IoT devices are connected in a circular network.
Tree Topology:	IoT devices are connected in a hierarchical network.
Hybrid Topology:	Combines two or more topologies to form a more complex network.

https://www.geeksforgeeks.org/types-of-network-topology/

Cloud platforms for IoT

AWS:	A complete suite of cloud computing services, encompassing IoT services, designed to empower developers in creating, deploying, and overseeing IoT applications.

Cloud platforms for IoT (cont)

Microsoft Azure:	is a comprehensive cloud computing platform offering a wide array of services to facilitate the development, testing, deployment, and management of IoT applications.
Google Cloud Platform (GCP):	A suite of cloud computing services that empower developers to create, test, and deploy IoT applications using Google's robust infrastructure.
IBM Watson IoT:	A cloud-based service that empowers developers with the capabilities to construct, oversee, and analyze IoT applications efficiently.
Oracle IoT:	A cloud-based service that enables developers to effectively build and manage IoT applications utilizing Oracle's advanced infrastructure.
ThingWorx:	A platform designed to simplify the creation and deployment of IoT applications, providing tools for seamless device connectivity, efficient data management, and intuitive dashboard creation.
Salesforce IoT:	A platform tailored for seamless integration and management of IoT devices and data within the Salesforce ecosystem.
Siemens MindSphere:	A cloud-based platform specifically developed for industrial IoT applications, equipped with robust tools for data analytics, machine learning, and predictive maintenance.
Cisco IoT Cloud Connect:	A cloud-based platform providing management services for connectivity of IoT devices, ensuring secure and scalable communication between devices.

Cloud platforms for IoT (cont)

GE Predix:	A cloud-based platform offering tools for data analytics, machine learning, and predictive maintenance to facilitate the construction and deployment of industrial IoT applications.
SAP Leonardo IoT:	A cloud platform that provides a wide range of tools for data processing, analytics, and machine learning to help developers build and deploy effective IoT applications.
PTC ThingWorx:	A cloud-based platform tailored for building and deploying industrial IoT applications that provides tools for device connectivity, data processing, and visualization.
Alibaba Cloud IoT:	A cloud-based platform offering a range of services for IoT applications, including device management, data processing, and analytics.
Baidu Cloud IoT:	A chinese cloud-based platform equipped with tools for device connectivity, data processing, and analytics, along with machine learning and AI services.
Particle:	An IoT cloud platform that facilitates the construction and administration of IoT applications, offering a suite of tools for seamless device connectivity, efficient data processing, and insightful analytics.
AWS IoT Greengrass:	A cloud-based platform empowering IoT applications with edge computing capabilities, allowing data processing and analysis to occur at the network's edge for improved efficiency and responsiveness.

Real-time operating systems (RTOS)

Mbed OS:	An open-source RTOS for IoT devices, supporting multiple communication protocols.
NuttX:	A lightweight and portable open-source RTOS for resource-constrained IoT devices.
RIOT:	An open-source RTOS optimized for low-power consumption and diverse communication protocols in IoT.
CMSIS--RTOS:	An open-source RTOS with a standardized API for microcontrollers in IoT devices.
eCos:	An open-source RTOS for embedded systems and IoT devices with support for various architectures.
Contiki:	An open-source RTOS with broad communication protocol support, including IPv6, for IoT.
FreeRTOS:	An open-source RTOS widely used in IoT devices with support for multiple architectures.
ThreadX:	A commercial RTOS with a small memory footprint and efficient context switching for resource-constrained IoT devices.
Zephyr:	An open-source RTOS for IoT devices with limited resources, supporting multiple architectures.
Nucleus RTOS:	A commercial RTOS with low latency, high throughput, and real-time performance for industrial automation and automotive applications.
VxWorks:	A commercial RTOS with high reliability, real-time performance, and multi-architecture support for critical IoT applications.
Micrium OS:	A commercial RTOS with fast context switching and a low memory footprint for low-power IoT devices.

Critical applications that demand real-time performance might benefit from RTOS in the IoT by getting predictable and deterministic response times. They are employed in healthcare, automotive, and industrial automation, and because they feature low-power modes, they are perfect for use in IoT devices that run on batteries. In IoT systems, RTOS is crucial for quick and dependable processing.

IoT standards and protocols

802.11 (Wi-Fi):	A standard for wireless local area networks that are widely used in IoT applications
Zigbee:	is a widely used low-power wireless protocol for industrial and home automation applications.
Z-Wave:	For low-power Internet of Things devices, this wireless protocol is used in home automation applications.
LoRaWAN:	is a low-power, long-range wireless protocol that's widely used in Internet of Things applications like smart cities and smart agriculture.
Sigfox:	a commonly used wide-area, low-power network protocol for IoT applications like asset tracking and environmental monitoring.
CoAP (Constrained Application Protocol):	A lightweight protocol for IoT devices that are designed for use in constrained environments such as smart homes and industrial automation.
MQTT (Message Queuing Telemetry Transport):	A protocol for lightweight messaging between IoT devices and servers.
HTTP (Hypertext Transfer Protocol):	A protocol that is widely used in IoT applications for communication between devices and servers over the internet.
OPC UA (Open Platform Communications Unified Architecture):	A standard for communication between industrial automation devices.
KNX (Konnex):	a standardized protocol for home automation that facilitates communication between devices produced by various manufacturers.

IoT standards and protocols (cont)

Bluetooth:	A wireless protocol that is widely used in IoT applications for short-range communication between devices.
NFC (Near Field Communication)	A wireless protocol widely employed in IoT applications to enable contactless communication between devices. It allows for secure and convenient data exchange over short distances.
Thread	Thread An IPv6-based wireless protocol optimized for low-power IoT devices. It finds extensive usage in home automation applications, providing reliable and efficient connectivity for smart devices within a network.
UDP (User Datagram Protocol):	A protocol that is widely used in IoT applications for lightweight, real-time communication between devices.
DMX512 (Digital Multiplex):	A protocol that is widely used in stage lighting and architectural lighting applications.
LWM2M:	A standard for managing IoT devices over the internet.
DDS-XRCE:	A standard for real-time communication between IoT devices in extremely resource-constrained environments.
IEC 61400-25:	A standard for communication between wind turbines and grid management systems.
ISO 15118:	A standard for communication between electric vehicles and charging infrastructure.
IPSO :	A standard for defining data models and communication protocols for smart IoT devices.

IoT standards and protocols (cont)

MQTT-SN:	A version of MQTT that is designed for use in wireless sensor networks.
OPC UA PubSub:	A protocol for real-time communication between industrial automation devices.
AMQP:	A protocol for message-oriented middleware that is used in IoT applications for reliable, asynchronous communication.
BLE (Bluetooth Low Energy):	A wireless protocol that is widely used in IoT applications for short-range communication between devices.
ISA100 Wireless:	A standard for wireless communication in industrial automation applications.
WirelessHART:	A wireless protocol that is widely used in process automation applications.
Modbus:	A protocol for communication between industrial devices.

IEEE standards PDF

Actuators

Electric motors are devices that utilize electrical energy to rotate objects and are extensively utilized in various applications such as robotics, industrial automation, and HVAC systems.

Solenoid valves are employed in numerous applications to regulate the flow of fluids or gases. They find usage in systems such as irrigation systems, pneumatic systems, and HVAC systems.

Piezoelectric actuators are devices that convert electrical energy into mechanical motion. They have diverse applications in activities such as scanning probe microscopy, nanopositioning, and micropositioning.

Hydraulic actuators generate mechanical motion using hydraulics and are commonly found in heavy-duty equipment like construction tools, industrial machinery, and aerospace applications.

Pneumatic actuators utilize compressed gas or air energy to create mechanical motion, enabling control over the final control elements.

Shape memory alloys (SMAs) are employed as actuators in various fields, including robotics and medical equipment, owing to their ability to change shape in response to temperature or electrical stimulation.

Actuators (cont)

Electroactive polymers (EAPs) find application as actuators in soft robotics and biomimetic systems, simulating the mobility and flexibility of natural muscles.

Shape-memory polymers (SMPs): Because they can adapt to changes in temperature, they are used as actuators in a variety of fields, including aerospace, robotics, and smart textiles.

Electrostatic actuators: in order to manipulate particles and regulate movement, they are used in microelectromechanical systems (MEMS) and microfluidics.

Thermal bimorph actuators are used in many MEMS and sensor-related applications.

Sensors

Temperature sensors are commonly utilized in a variety of applications, including home automation, HVAC systems, and food storage, to accurately assess the temperature of their immediate surroundings. Thermocouples, RTDs (resistance temperature detectors), and thermosiphons are among the examples of temperature sensors frequently employed in these contexts.

Pressure sensors find widespread use in industrial automation, automotive, and medical devices, where monitoring the pressure of gases or liquids is crucial. Optical, capacitive, and piezoresistive sensors are just a few examples of pressure sensors utilized in these applications.

Humidity sensors play a significant role in HVAC systems, building automation, and environmental monitoring systems by measuring the moisture content in the air. Capacitive humidity sensors, resistive humidity sensors, and thermal conductivity sensors are among the various types of humidity sensors employed in these domains.

Accelerometers are extensively utilized in the automotive, aerospace, and industrial automation sectors for monitoring acceleration or vibration. Capacitive and MEMS (Micro-Electro-Mechanical Systems) accelerometers are examples of such sensors commonly employed in these industries.

Light sensors: photodetector devices that detect light are known as light sensors. Photodiodes, photoresistors, phototransistors, and photovoltaic sensors are typical varieties of light detectors. Applications like mobile device light detection can make use of these components.

Gas sensors are essential for the identification of various gases in environmental monitoring, industrial automation, and medicinal applications. Carbon monoxide, oxygen, and hydrogen sensors are just a few of the sensors that are frequently used in these sectors.

Sensors (cont)

In robotics, consumer electronics, and automotive applications, **magnetic sensors** are frequently utilized because they can monitor a magnetic field's strength and direction. Magnetoresistive, Hall-effect, and fluxgate sensors are some types of sensors.

Gyroscopes are common in robotics, virtual reality, and navigation. They are sensors that measure angular velocity. MEMS gyroscopes, fiber optic gyroscopes, and ring laser gyroscopes are a few examples.

Comparison between sensors and actuators

Feature	Sensor	Actuator
Function	Detect and measure physical or environmental changes	Control or manipulate physical systems
Input	Physical or environmental changes	Electrical or other types of energy
Output	Electrical signals or data	Mechanical motion
Importance	Important for data collection and monitoring systems	Essential for control and automation systems
Interconnectivity	Often networked with other sensors or devices	Controlled by sensors or other devices
Power requirements	Generally low power	Generally high power

Firmware Over-the-Air (FOTA) updates

IoT devices can have their firmware updated remotely through a wireless network using firmware over-the-air (FOTA) upgrades without physical access or user intervention, ensuring that the devices are safe and current.

GPS modules

Adafruit Ultimate GPS Breakout:	A GPS module that provides accurate location data for IoT devices, with support for various communication protocols.
u-blox NEO-M8N GPS Module:	A compact and high-precision GPS module with low power consumption, ideal for use in IoT devices.
SparkFun GPS-RTK2 Board:	A GPS module that supports real-time kinematic (RTK) positioning, providing centimeter-level accuracy for IoT applications.

GPS modules (cont)

GlobalTop Gms-u1LP GPS Module:	A low-power GPS module with fast time-to-first-fix and low power consumption, ideal for use in battery-powered IoT devices.
SIMCom SIM33EAU GPS Module:	A GPS module with low power consumption and support for various communication protocols, making it ideal for use in IoT devices.
Quectel L76-L GPS Module:	A high-sensitivity GPS module with low power consumption and support for multiple satellite systems, making it ideal for use in IoT devices.

GPS modules in IoT provide real-time location data for assets, vehicles, and people. They enable tracking and monitoring in the logistics, transportation, and healthcare industries. GPS modules are essential for accurate and reliable location information in IoT systems.