IoT Device: Layer-Wise Security Audit Guidelines

Version 2.0

July 2024

IoT Security Research Centre/Lab, IIIT Allahabad

Funded by
C3iHub, IIT Kanpur &
Department of Science and Technology,Government of India

Request for Comments

Audience

This document will be useful for the Manufacturers, Users and for the certification agencies.

Send the suggestions/corrections to venkat@iiita.ac.in

Table of Contents

1. Introduction

The Internet of Things (IoT) is an application of the network that allows the devices capable of sensing, transmitting, and receiving to communicate to collect and exchange data, issue the commands, control the devices, etc. IoT is used in many applications such as manufacturing industry, health, and smart transportation. While the IoT is increasingly being used to automate various activities, the security of IoT is a major concern. Security issues arise in the individual IoT devices, their interaction protocols, and the distributed applications running over an IoT. The security issues with IoT devices can be in the software, firmware, hardware, and the protocols used. They can also be due to a lack of cyber hygiene practices. The actors responsible for exposing users of IoT devices and applications to security risk are:

- End Users – Lack of awareness, Carelessness, Laziness, Cost-cutting intent
  - Uses the default or weak credentials
  - Devices placed in public places allow attackers to capture the traffic (where users are required to place the device in a public place)
  - Failure to report known or identified vulnerabilities/attacks
  - Purchasing IoT devices based on cost, ease and efficiency rather than security
  - Improper configuration of device, failure to update software/firmware
- Administrators – Lack of awareness, Carelessness, Laziness, Cost-cutting intent
  - Uses the default or weak credentials
  - Devices placed in public places allow attackers to capture the traffic (where users are required to place the device in a public place)
  - Failure to report known or identified vulnerabilities/attacks
  - Purchasing IoT devices based on cost, ease and efficiency rather than security
  - Improper configuration of device, failure to update software/firmware
  - Not following the security standards
- Manufacturers – No Mandate, No awareness, Carelessness, Cost-cutting intent
  - Not providing easy update mechanisms for software/firmware
  - No security vulnerability reporting team
  - Not forcing users for strong security such as changing the default password and restricting the weak passwords
  - Not hardening the device configuration
  - Using insecure protocol or algorithm
  - Failure to comply with the security requirements or security standards
  - Failure to maintain business continuity and therefore support for users
  - Failure to report vulnerabilities
- Agencies – Non-Availability, Lack of Pre-preparation
  - No standards for the manufacturer and administrators
  - Not providing the required awareness to the users
  - No tracking of the manufacturers and products
  - No security vulnerability reporting of the products

2. Security Requirements

For an IoT application to be considered secure, the devices must meet the following security requirements. In the following, "user" refers to both the administrator and the end user:

A. Physical Security: IoT devices placed in public places may be physically accessed by attackers and need to be protected.

A1.Monitoring Physical Access: The publicly placed devices should be monitored by the surveillance systems. [User]

A2. Hard Cover: The device should not be easy to connect and should not have open interfaces. The device should not be vulnerable to the natural elements. [Manufacturer and User]

A3. Access Alert: The device should give an alert if there is unauthorized physical access or a power interruption (using secondary power). For example, if someone connects the USB or other interface to the device, the alert should be generated or sent to the next device in the hierarchy. [Manufacturer]

A4. Disable the Debugging module: The debugger such as UART, etc. should be disabled or erased or given controlled access before shipping the product. [Manufacturer]

B. Data Security: The sensitive data stored in the devices should not be accessible to the unauthorized users.

B1. Secure storage of credentials: The credentials of the device should be hashed with a salt and stored. [Manufacturer and User]

B2. Securely store sensitive data: The user's sensitive data should be encrypted and stored using standard algorithms. The key should be derived from the Trusted Platform Module (TPM). [Manufacturer and User]

B3. Need to know data: Data should be accessed only by the authorized users and on a need-to-know basis. [Manufacturer (if it is firmware part) and User]

B4. Data Integrity: Authorized users should have the means to verify the integrity of the data. [Manufacturer (if it is firmware part) and User]

B5. Data Availability: Data should be available for access in the event of any failure such as network and power (with secondary power). [Manufacturer]

B6. Data Validation: Incoming data should be verified or validated before use. [User]

B7. Non-Disclosure of Device's Sensitive Data: The device should not disclose any sensitive data such as password, keys, open ports, operating system type, and battery level and baud rate to unauthorized users. [Manufacturer and User]

C. Network Security: Network traffic carrying sensitive data should be kept confidential, either using a secure or non-secure protocol with encryption.

C1. Secure Protocols: It is mandatory to establish a secure tunnel (e.g. SSL) between the device and the recipient prior to transmitting/receiving the data. The downgrading of the protocols must also be restricted. [Manufacturer and User in case of own application installation]

C2. Necessary Network Interfaces and Services Only: The device should only run the necessary network services and interfaces such as wireless, wired and bluetooth. [Manufacturer and User]

C3. Restricted Data Flow: Controlling the incoming packets to avoid the Denial-of-Service attack, etc. is essential. The device should have a firewall to control the data flow. [Manufacturer and User]

C4. Secure Remote Access: The device can only be accessed in secure mode (eg. SSH) and authenticated with the password/key. [Manufacturer and User]

D. Hardware Security: The devices can have the TPM or similar controllers to prevent the boot virus, etc.

D1. Secure Boot: Ensure the secure boot of the system using TPM or other modules. [Manufacturer]

D2. Side Channel Attack: The hardware should be resistant to the side channel attack. [Manufacturer]

D3. No sensitive data leakage in Boot Log: No sensitive data such as password and key shall be leaked in the boot log of the device. [Manufacturer]

D4. No Access to Hardware: The device should have the detection capability to control data leakage due to any external access. For example, attackers can access firmware, etc. via Serial Peripheral Interface (SPI), Joint Test Action Group (JTAG), Inter-Integrated Circuit (I2C), and UART. [Manufacturer]

E. Software Security: Updated and secure software/firmware must be used in the IoT devices. No vulnerable applications, operating systems, firmware, drivers and interfaces should be used.

E1. Secure Update Mechanism: The application or system software or firmware should be securely updated on demand. The update may be Over the Air (OTA), local, etc. Lack of update mechanism and use of obsolete components should be avoided. [Manufacturer and User]

E2. Easy Update Mechanism: The manufacturer should provide the easy update mechanism for the user to update the application or system software and firmware. [Manufacturer]

E3. Easy Installation Mechanism: The manufacturer should provide an easy installation mechanism for the user to install the application or system software and firmware. [Manufacturer]

E4. Software Integrity: No unauthenticated software should be installed/used in the device. [Manufacturer and User]

E5. Privilege Control: The operating system should have appropriate privilege control to access the services. [Manufacturer and User]

E6. Secure Default Settings: All secure settings should be enabled by default. For example, the UDP echo and Chargen should be disabled. [Manufacturer]

E7. Necessary Software Services Only: The device should only have and run the necessary software services. [Manufacturer and User]

F. Management Security: Hardening by having only required software on the device and need of security management is important.

F1. Default or weak passwords: Devices should not use the default, hardcoded or weak passwords. Manufacturers should ensure that the default password is changed to a strong password on first access and that a password lifetime is defined in the password policy. [Manufacturer and User]

F2. Unique Password: The administrator should ensure the unique password for all devices on the network. [User]

F3. Multi-Factor Authentication (MFA): Device should support the multi-factor authentication. User should enable MFA. [Manufacturer and User]

F4. Need Only Services: The device should only run the required services (applications). For example, the SSH service and packet forwarding service can be disabled. [Manufacturer and User]

F5. Asset Management: The inventory of the devices should be maintained to control the third-party devices intrusion, device functionality, etc. [User]

F6. Unique Identification of Devices: The devices on the network should be uniquely identified without any spoofing. PUF based hardware can be used or user defined random identity can be used. [Manufacturer]

F7. Reset to Default Settings: The device should have the capability to return to default settings or perform a factory reset if the data or software is compromised or the user wishes to wipe the data. [Manufacturer]

F8. Security Team: The manufacturer should provide an easy way for the users to report the security bugs and have the security team to handle the security bugs. [Manufacturer]

F9. Device Resilient to Outages: The failure of an external module such as network connection should not affect the device process and the device should be able to send the data later, and the device should reset to a more secure state in case of any malware. [Manufacturer]

F10. Activity Log: The device should have the ability to log activity for the future auditing. The log should not contain sensitive data. [Manufacturer and User]

F11. Remote Storage: The user should have the option to choose the remote storage [Cloud] or local storage. The user should not be forced to use the remote storage. [Manufacturer]

G. Life Cycle Management: It is necessary that the lifecycle of the device should be defined for users.

G1. Supply Chain Security: The device should not be tampered throughout the manufacturing to delivery process. The cryptographic hash of the software/firmware components can be used to verify the integrity of the device. [Manufacturer]

G2. Device Decommissioning: The user data should be completely erased before disposing the device. The device can be reset to factory defaults or wiping tools can be used. [Manufacturer and User]

G3. Quality Check: The manufacturer should ensure the implementation of the security requirements (including security verification of third-party libraries and softwares) before releasing products from the manufacturing unit. [Manufacturer]

G4. Regular Vulnerability Scanning: The device should be regularly scanned for the presence of vulnerabilities, and any vulnerability found should be fixed. [User]

H. Application Programming Interface (API) Security: It is necessary to protect the device from API attacks that can steal sensitive information or cause a denial-of-service attack.

H1. Data Validation: The data that are handled by the API should be validated before it is used. This can mitigate the SQL injection and other exploits. [User]

H2. Authentication: Strong authentication including the multi-factor method should be used to access the API. [Manufacturer and User]

H3. Secure Data Exchange: The data exchanged through the API should be done through the secure channel. [Manufacturer and User]

H4. Need to Know Data: The API should access the data according to the granted authorisation. [Manufacturer and User]

H5. Configuration Hardening: The API configuration should be secured by default. Only necessary services should be running and error messages should not reveal any sensitive information. [Manufacturer and User]

3. Layers of Device

The IoT device operates at different layers, as shown in Table 1. Each layer of the device has specific tasks, services, or components that are required to achieve the desired security. Possible layer-wise vulnerabilities and threats are presented in Table 1 according to the Open Web Application Security Project (OWASP - 2018) and Mitre EMB3D (2024). In addition, we present the security requirements at each layer according to the various standards and guidelines listed below, along with suggested guidelines from the IoT Security Lab, IIITA.

1. NISTIR 8259A (May 2020) & NIST SP 800-213A (November 2021),
2. European Union Agency for Cyber Security (ENISA)'s Good Practices for Security of IoT - Secure Software Development Lifecycle November 19, 2019 (2019),
3. UK Government Code of Practice for consumer IoT security (2018),

4. IoT Security Maturity Model: ISA/IEC 62443 (August 2023),
5. Telecommunication Engineering Centre (TEC 31318:2021),
6. IoTSF Secure Design Best Practice Guidelines (BPGs) (November 2019),
7. CIS Critical Security Controls (Version 6): IoT Security (October 2015),
8. IMDA IoT Cyber Security Guide V1 (March 2020),
9. DSCI IoT SECURITY GUIDE (August 2022),
10. Australian Cyber Security Centre (ACSC) ACSC Code of Practice Securing the Internet of Things for Consumers, 2023 (2023)
11. National Telecom Regulatory Authority (NTRA), Egypt IOT Cyber Security Framework (October 2022),
12. Singapore Computer Society Recognising IoT Security Issues: 12 Ways You Can Protect Your Devices (~2021),
13. National Cyber Security Authority, Saudi Arabia Cybersecurity Guidelines for Internet of Things (Draft) (CGIoT-1:2023)
14. IEEE Internet of Things (IoT) Security Best Practices, 2017 (2017),
15. Secure by design Internet of Things – IoT Cyber Security Advice (Na),
16. Industrial Internet Consortium’s [IIC] IoT Security Maturity Model: Description and Intended Use (February 2019)

Table 1. IoT Device Layer-Wise Representation and Security Requirements

Layers	Service/Components	OWASP Vulnerabilities [2018]	NIST Security Requirement	ENISA	UK Govern. Requirement	CIS Critical Security Controls (Version 6): IoT Security	IoT Security Maturity Model: ISA/IEC 62443	TEC 31318:2021	IMDA IoT Cyber Security Guide V1	IoTSF Secure Design Best Practice Guidelines (BPGs)	NTRA, Egypt	DSCI and ACSC	IoT Security Research Lab, IIITA
1. Application	Bash, Device Apps	1.Weak, guessable, or hardcoded passwords 3.Insecure ecosystem interfaces 4.Lack of secure update mechanisms 5. Use of insecure or outdated components 6. Insufficient privacy protection 7.Insecure data transfer and storage 9.Insecure	DI – Device Identification DC – Device Configuration LA – Logical Access to Interfaces SU – Software Update DS – Device Security DP –Data Protection	Key Management and Authentication System Software patched for known vulnerabilities Secure Web Interfaces Protect Data against leakages Authorization	No default passwords. Keep software updated. Ensure software integrity. Validate input data. Minimise exposed attack surfaces.	Inventory of Authorized and Unauthorized Software Secure Configuration of Software Email and Web Browser Protections Malware Defences Application Software Security Controlled Access Based on the Need to Know	Identification and authentication control (IAC) System integrity (SI) Timely response to events (TRE) Resource availability (RA). Use control (UC) –can be applied to all layers	No Universal Default passwords Password policy (Revised in Security By Design) Keep software updated Ensure Software Integrity Validate Input Data Make it easy for users to delete user data Make systems resilient to outages	Employ strong cryptography Protect impactful data Enforce proper access controls (Default or Weak Passwords)	Software update policy Software image and update signing Logging Securing Software Update Encryption Application Security Credential Management Network Connections	Device Software Encryption and Key Management for hardware Web User Interface Authentication and Authorization	Ensure Unique Credentials [No duplicated default or weak passwords] Keep software updated. Ensure software integrity. Validate input data. Minimise exposed attack surfaces.	Data Security Software Security Management Security Application Programming Interface Security

		default settings						Device Identity & Strong Credentials (Revised in Security by Design)					
2. Session	MQTT, CoAP	1.Weak, guessable, or hardcoded passwords 2.Insecure network services 4.Lack of secure update mechanisms 5. Use of insecure or outdated components. 6. Insufficient privacy protection 7.Insecure data transfer and storage	DP –Data Protection DC – Device Configuration	Secure Communication Protocols Implement Secure Session Management	No default passwords. Keep software updated. Communicate securely. Minimise exposed attack surfaces. Monitor system telemetry data. Make systems resilient to outages. Validate input data.	Secure Configuration of Software Limitations and Control of Network Ports, Protocols and Services	Data confidentiality (DC) Restricted data flow (RDF)	No Universal Default passwords Keep software updated Ensure Software Integrity Validate Input Data Make systems resilient to outages Examine system telemetry data Password policy (Revised in Security By Design)	Employ strong cryptography Protect impactful data Employ secure transport protocols Enforce proper access controls (Default or Weak Passwords)	Software update policy Software image and update signing Logging Securing Software Update Encryption Application Security Credential Management Network Connections	Device Wired and Wireless Interfaces Authentication and Authorization Encryption and Key Management for hardware	Ensure Unique Credentials [No duplicated default or weak passwords] Keep software updated. Secure Communication [Ensure communication security]. Minimise exposed attack surfaces. Monitor system telemetry data. Make	Software Security Management Security Network Security Data Security

												systems resilient to outages. Validate input data.	
3. Network	Ethernet, Wi-Fi, Bluetooth, Zigbee as well as IP Layer	2.Insecure network services	DS – Device Security DP –Data Protection	Secure Communication Protocols	Communicate securely. Minimise exposed attack surfaces.	Wireless Access Control	Data confidentiality (DC) Restricted data flow (RDF)	Communicate Securely Ensure that Personal data is secure	Employ secure transport protocols	Encryption Network Connections	Device Wired and Wireless Interfaces Authentication and Authorization Encryption and Key Management for hardware	Secure Communication [Ensure communication security]. Minimise exposed attack surfaces.	Network Security
4. Operating System	Linux, Android	4.Lack of secure update mechanisms 5.Use of insecure or outdated components	DC – Device Configuration DS – Device Security LA – Logical Access to Interfaces	Software patched for known vulnerabilities Protect Data against leakages Authoriz	No default passwords. Keep software updated. Ensure software integrity.	Secure Configuration of Software Controlled Use of Administrative Privileges	System integrity (SI) Timely response to events (TRE) Resource availability (RA).	No universal default password Device Identity & Strong Credentials (Revised in Security by	Enforce proper access controls (Default or Weak Passwords)	Software image and update signing Software update policy Logging Securing Software	Device Operating System Device Software Authentication and Authori	Ensure Unique Credentials. Keep software updated. Ensure software integrity.	Software Security Management Security Data Security

		9.Insecure default settings	SU – Software Update	ation				Design) Password policy (Revised in Security By Design)		Update Credential Management Secure Operation System	zation Encryption and Key Management for hardware		
5. Memory	RAM, SSD	6. Insufficient privacy protection 7.Insecure data transfer and storage	DP –Data Protection LA – Logical Access to Interfaces	Secure storage of user credentials Protect Data against leakages	Securely store credentials and security-sensitive data. Ensure that personal data is protected [during the process also]. Make it easy for consumers to delete personal data.	Data Recovery Data Protection	Data confidentiality (DC) Resource availability (RA).	Securely store the sensitive security parameters	Employ strong cryptography Protect impactful data	Encryption Credential Management Classification of Data	Encryption and Key Management for hardware	Securely store credentials and security-sensitive data. Ensure that personal data is protected [during the process also]. Make it easy for consumers to delete personal data.	Data Security
6. Firmware		9.Insecure default settings 4.Lack of secure update mechanism	DC – Device Configuration DS – Device Security	Software patched for known vulnerabilities		Secure Configuration of Hardware and software Inventory of Authorized and		Ensure software integrity		Software image and update signing Software update policy	Device Software Encryption and Key Manage		Software Security

		s 10 Lack of physical hardening				Unauthorized Software				Securing Software Update	ment for hardware		
7. Hardware		10.Lack of physical hardening	DI – Device Identification (Physical)	Physical Protection of Systems Control of Physical Access		Inventory of Authorized and Unauthorized Devices (Physical)	Identification and authentication control (IAC) (Physical)	Boot should fail gracefully (Security By Design)	Establish Root-of-Trust with TPM	Side Channel Attack Physical Security Secure Boot Process Assessing a secure boot process	Device Hardware and Physical Security Encryption and Key Management for hardware		Physical Security Hardware Security

Table 1. IoT Device Layer-Wise Representation and Security Requirements [contd.]

Layers	**Service/Components**	**EMB3D Threat Model**	**Singapore computer Society (~2021)**	**National Cyber Security Authority, Saudi (2023)**	**IEEE (2017)**	**Secured by design**	**IIC (Feb, 2019)**	**IoT Security Research Lab, IIITA**
1. Application	Bash, Device Apps	Application Software Threats	Apply strong cryptography Protect impactful system data Enforce proper access controls Prepare for and safeguard against attacks	Identity and Access Management Email and Messaging services protection Data and Information Protection Cryptography Backup and Recovery Management [including software] Vulnerability Management [Patching]	Use strong authentication Protect sensitive information	Evaluate Settings (Default Settings) Turn on 2 step Verification Change Default Passwords Update Software	Security Enablement	Data Security Software Security Management Security

				Event Logs and Monitoring Management				
2. Session	MQTT, CoAP	Network Threats	Apply strong cryptography Employ secure versions of transport protocol Enforce proper access controls	Identity and Access Management Network Security Management Data and Information Protection Cryptography Vulnerability Management [Patching] Event Logs and Monitoring Management	Use strong authentication Use strong encryption and secure protocols Protect sensitive information	Evaluate Settings (Default Settings) Turn on 2 step Verification Change Default Passwords Update Software	Security Enablement	Software Security Management Security Network Security Data Security
3. Network	Ethernet, Wi-Fi, Bluetooth, Zigbee as well as IP Layer	Network Threats	Apply strong cryptography Employ secure versions of transport protocols	Network Security Management Data and Information Protection Cryptography Vulnerability Management [Patching] Event Logs and Monitoring Management	Use strong encryption and secure protocols Minimize device bandwidth Divide networks into segments			Network Security
4. Operating System	Linux, Android	System Software Threats	Enforce proper access controls	Identity and Access Management Data and Information Protection Backup and Recovery Management Vulnerability Management [Patching] Event Logs and Monitoring Management	Use strong authentication Protect sensitive information	Update the Operating System Evaluate Settings (Default Settings) Change Default Passwords	Security Enablement	Software Security Management Security Data Security

5. Memory	RAM, SSD	-	Apply strong cryptography Protect impactful system data Enforce proper access controls	Identity and Access Management Data and Information Protection Cryptography Backup and Recovery Management	Protect sensitive information		Security Enablement	Data Security
6. Firmware		System Software Threats	Establish hardware root-of-trust	Backup and Recovery Management Physical Security	Provide for firmware updates/patches			Software Security
7. Hardware		Hardware Threats	Establish hardware root-of-trust	Asset Management Physical Security Device Lifecycle Management	Make hardware tamper resistant		Security Enablement	Physical Security Hardware Security

4. Classification of Device

Table 2 classifies the devices into different levels based on the features that are available on them. This classification will be useful in identifying the security requirements for the devices. The general security requirement will not be effective for all the IoT devices. We have considered very low-end devices (sensors) to medium portable devices (mobile and laptop). We know that there are different characteristics or components that a device can have, but not all devices fulfil all characteristics. We categorised devices into levels based on their components and the features/functionality they support.

Table 2. IoT Device Classification Based On Features

Device Level	Cache	Computation (Negligible ignored)	Operating System Enabled (Generic)	Network Support	Remote Access/User Interface	Sensing	Takes Input	Send Data	Control Device	Additional Software Installable	Programming Facility	Secondary Storage	Multi-user	Battery	Application control	Example
0						Yes		Yes (Local)								Digital Humidity and Temperature (DHT), Ultrasonic sensor
1	Yes			Yes		Yes/No	Yes	Yes/No						Yes/No	Yes/No	Headset, Bulb, Fan
2	Yes	Yes		Yes		Yes	Yes	Yes				Yes		Yes/No	Yes	Camera, Watch, Printer, Lock
3	Yes	Yes		Yes	Yes	Yes	Yes	Yes				Yes		Yes/No	Yes/No	Network Devices: Access Point
4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes/No		Mobile, Laptop, etc.

5. Device Level Security Compliance

Table 3 details the compliance with the security requirements for the different levels of devices. The security audit of the device can be performed based on the requirements. The security requirements for a device are based on the components of the device and the function it has. For example, every device needs physical security, whether it is a sensor or a laptop. However, a sensor does not need software security.

Table 3. Security Requirements Compliance for Level of Devices

Security Requirements	Level 0	Level 1	Level 2	Level 3	Level 4
A1	Y	Y	Y	Y	Y
A2		Y	Y	Y	Y
A3		Y	Y	Y	Y
A4		Y	Y	Y	Y
B1				Y	Y
B2			Y	Y	Y
B3		Y	Y	Y	Y
B4			Y	Y	Y
B5		Y	Y	Y	Y
B6		Y	Y	Y	Y
B7		Y	Y	Y	Y
C1		Y	Y	Y	Y
C2		Y	Y	Y	Y
C3		Y	Y	Y	Y
C4					Y
D1			Y	Y	Y
D2		Y	Y	Y	Y
D3		-	Y	Y	Y
D4		Y	Y	Y	Y
E1		Y	Y	Y	Y
E2			Y	Y	Y
E3					Y
E4		Y	Y	Y	Y
E5					Y
E6		Y	Y	Y	Y
E7			Y	Y	Y
F1			Y	Y	Y
F2			Y	Y	Y
F3			Y	Y	Y
F4			Y	Y	Y
F5	Y	Y	Y	Y	Y
F6			Y	Y	Y
F7		Y	Y	Y	Y
F8	Y	Y	Y	Y	Y
F9		Y	Y	Y	Y
F10			Y	Y	Y
G1	Y	Y	Y	Y	Y
G2		Y	Y	Y	Y
G3		Y	Y	Y	Y
G4		Y	Y	Y	Y
H1			Y		Y
H2			Y		Y
H3			Y		Y
H4			Y		Y
H5			Y		Y

Note for H rows: API requirements only apply if the device uses the API.

6. Threat Model

The threat model for auditing the IP-based IoT device is shown in Table 4, along with the risk level, impact layers, and required access to the devices.

Table 4. IP based IoT Device Threats

Sl. No.	Vulnerability	Impact	Risk	Layers	Access
1	Default password	Device Compromise	High	1,2,3,4	Remote
2	Weak/Guessable Password	Account/Device Compromise	High	1,2,3,4	Remote
3	SSH port open	Attempt to compromise	Low	2	Remote
4	Responding to scanners	Attempt to compromise and Denial of Service	Medium	1,2,3,4, 5,6	Remote
5	Plain Text Communication	Disclosure of data during packet sniffing	High	2,3	Remote
6	Using publicly known vulnerable software	Device Compromise	High	All Layers	Remote/ Physical
7	Disclosing OS fingerprint	Attempts to compromise the system using a known vulnerability and targeted	Medium	4	Remote
8	Downgrading Attack	Data Disclosure	High	2,3	Remote
9	Disclosing MAC Id	ARP spoofing possible [No protection Mechanism other than sending an ARP request before sending any data.]	Low	3	Remote
10	Time Synchronization Information Leak	Confidence to the attacker that the attempt will be successful	Medium	2	Remote
11	Firewall Availability disclosure	Attack will be framed accordingly	Medium	1	Remote
12	Plain Storage of Credentials	Account/Device Compromise	High	5	Remote/ Physical
13	Reverse Engineering (Shell)	Device Compromise	High	1	Remote
14	Malicious code/Component injection	Device Compromise	High	1	Remote
15	Hardcoded Password	Accidentally disclosed to third party, resulting in account/device compromise	High	1,2,3,4, 6	Remote/ Physical
16	Outdated Firmware	Publicly known vulnerability will be exploited	High	6	Remote/ Physical
17	FTP Communication	Able to analyze the traffic and obtain confidential data.	High	2	Remote
18	Telnet Communication	Able to analyze the traffic and obtain confidential data.	High	2	Remote
19	Directory Access/Traversal	Unauthorized users can access the sensitive information	High	1,4	Remote
20	Protocol Vulnerability	e.g., Denial of Service in case of Eclipse Mosquitto password setting vulnerability	Medium	2	Remote
21	Side Channel Attack	Sensitive information can be leaked	High	7	Physical
22	Memory Corruption	Buffer overflow attack to extract sensitive data or bypass	High	1,5	Remote

		authentication			
23	ARP Poisoning	Man In the Middle Attack	High	2	Remote
24	Easy Physical Connection	An attacker can insert the USB or other devices to perform the desired activity. [Bootlog capture]	High	7	Physical
25	Illegal forwarding	A device used by the attacker can send data to the manufacturer without the user's knowledge.	High	6	Remote/ Physical
26	Asset Management	Identify all connected devices	-	7	Remote

In addition, the threats presented by the Mitre EMB3D (2024) can be added to the threat list.

References

- https://wwwthinxtreamcom/iot-deviceshtml#Firmware [Last accessed on 21/08/2022]
- https://wwwcisoplatformcom/profiles/blogs/classification-of-iot-devices [Last accessed on 21/08/2022]
- https://nvlpubsnistgov/nistpubs/SpecialPublications/NISTSP800-213A.pdf [Last accessed on 21/08/2022]
- https://www.coderus.com/internet-of-things-iot-security-guide-problems-solutions/ [Last accessed on 23/08/2022]
- https://www.ietf.org/id/draft-ietf-lwig-7228bis-00.html [Last accessed on 24/08/2022]
- https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931460 html [Last accessed on 24/08/2022]
- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 [Last accessed on 24/08/2022]
- https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf [Last accessed on 24/08/2022]
- https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security [Last accessed on 24/08/2022]
- https://owasp.org/www-community/vulnerabilities/ [Last accessed on 24/08/2022]
- https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project [Last accessed on 04/06/2024]
- https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf [Last accessed on 23/03/2023]
- https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf[Last accessed on 12/06/2023]
- https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/08/SMM-62443-Asset-Owner-Product-Supplier-Service-Provider-Mappings-2022-08-16.pdf[Last accessed on 11/09/2023]
- https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf[Last accessed on 25/09/2023]
- https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf [Last accessed on 25/09/2023]
- https://tec.gov.in/pdf/M2M/Framework%20of%20National%20Trust%20Centre%20for%20M2M-IoT%20Devices%20and%20Applications%20TEC%2031188_2022_after.pdf[Last accessed on 25/09/2023]
- https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf [Last accessed on 26/09/2023]

- https://www.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pdf [Last accessed on 27/09/2023]
- https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf[Last accessed on 29/09/2023]
- https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf [Last accessed on 30/09/2023]
- https://kratikal.com/blog/ultimate-guide-to-iot-security-testing/?utm_source=Acumba+mail&utm_medium=Newsletter&utm_campaign=IoT+security+testing [Last accessed on 07/10/2023]
- https://www.isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf [Last accessed on 24/10/2023]
- https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10[Last accessed on 24/11/2023]
- https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/iot-secure-design-guidance-manufacturers [Last accessed on 04/01/2023]
- https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf [Last accessed on 04/06/2024]
- National Telecom Regulatory Authority (NTRA), Egypt, IOT Cyber Security Framework[Last accessed on 14/01/2024]
- https://backend.nca.gov.sa/api/public/cms/files/f93e8453-319c-4f19-861b-0271bf52d64c_Cybersecurity-Guidelines-for-Internet-of-Things-(Draft).pdf [Last accessed on 17/02/2024]
- https://www.scs.org.sg/articles/iot-security-how-to-secure-your-devices [Last accessed on 17/02/2024]
- https://standards.ieee.org/wp-content/uploads/import/documents/other/whitepaper-internet-of-things-2017-dh-v1.pdf [Last accessed on 17/02/2024]
- https://www.securedbydesign.com/internet-of-things/cyber-security-advice [Last accessed on 23/03/2024]
- https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf [Last accessed on 24/04/2024]
- https://emb3d.mitre.org/ [Last accessed on 06/05/2024]

APPENDIX

Appendix – I. Comparison of Security Guidelines

Table A compares the various security guidelines or standards with respect to our security requirements. Table A documents the missing and unclear security requirements in the existing guidelines and standards.

Table A. Comparison of Security Guidelines

Sl. No.	**Standards or Guidelines**	**Physical Security**	**Hardware Security**	**Software Security**	**Data Security**	**Network Security**	**Management Security**	**Life Cycle Management**	**Application Programming Interface (API) Security**
1	NIST 8259A	A1, A3, A4	D1, D2, D3	E6, E7	B3, B6, B7	C2, C3	F2, F4, F8, F9, F11	G4	H1, H2, H3, H4, H5
2	UK government's Code of Practice for consumer IoT security	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F3, F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
3	CIS Critical Security Internet of Things Security Companion to the CIS Critical Security Controls (Version 6)	A1, A2, A3, A4	D2, D3	E1, E2, E3, E7	B3, B4, B6, B7	C4	F2, F3, F6, F7, F9, F11	G1, G2, G3	H1, H2, H3, H4, H5 (**$**)
4	IoT Security Maturity Model: ISA/IEC 62443	A4	D2, D3, D4	E2, E3, E6	B7(P)	-	F7, F8, F9, F11	-	H1, H2, H3, H4, H5
5	TEC 31318:2021	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
6	IMDA IoT Cyber Security Guide V1	A3, A4	D2, D3, D4	E1, E2, E3, E4, E6, E7	B5, B6, B7	C2, C3, C4	F2, F4, F7, F9, F11	G1, G2, G3	H1, H2, H3, H4, H5
7	IoTSF Secure Design Best Practice Guides, Release 2 November 2019	A1, A3	D3	E2, E3, E6	B6, B7	C4	F2, F5, F9, F11	G2, G3, G4	H1, H2, H3, H4, H5
8	DSCI IoT Security Guide August 2022	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
9	Australian Cyber Security Center (ACSC) Code of Practice Securing the Internet of Things for Consumers, 2023	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H1, H2, H3, H4, H5

10	ENISA Good Practices for Security of IoT - Secure Software Development Lifecycle November 19, 2019	A3, A4(P)	D1, D3, D4(P)	E2, E3, E7	B3, B6, B7	C2, C3, C4(P)	F2, F3, F4, F5, F6, F11	-	H1, H2, H3, H4, H5 ($)
11	NTRA, Egypt IOT Cyber Security Framework	A1	-	E2, E3	B7	C3 (P)	F2, F8, F9, F10, F11	G1 (P)	H1, H2, H4, H5
12	Singapore Computer Society Recognising IoT Security Issues: 12 Ways You Can Protect Your Devices	A1,A3, A4(P)	D2, D3, D4(P)	E2, E3, E6, E7(P)	B4, B5, B6, B7	C2(P), C3, C4(P)	F5, F6, F7, F8, F9, F11	G1, G2	H1, H2, H3, H4, H5
13	National Cyber Security Authority, Saudi Arabia Cybersecurity Guidelines for Internet of Things (Draft) (CGIoT-1:2023)	A1,A3, A4(P)	D2, D3, D4(P)	E2, E3, E4, E5, E6, E7(P)	B6, B7(P)	C2, C3, C4(P)	F7, F8, F11	-	H1, H2, H3, H4, H5
14	IEEE Internet of Things (IOT) Security Best Practices, 2017.	A1,A2(P), A3, A4	D2, D3, D4(P)	E1, E2, E3, E4, E5, E6, E7	B3, B4, B5, B6, B7	C2, C4(P)	F4, F5, F6, F7, F8, F9, F10, F11	G1, G3	H1, H2, H3, H4, H5
15	Secure by design Internet of Things – IoT Cyber Security Advice	A1, A2, A3, A4	D1, D2, D3, D4	E1, E3, E4, E5, E7	B1, B2, B3, B4, B5, B6, B7	C1, C2, C3, C4	F2, F5, F6, F7, F8, F9, F10, F11	G1, G2, G3, G4	H1, H2, H3, H4, H5
16	Industrial Internet Consortium (IIC)IoT Security Maturity Model: Description and Intended Use Version 1.1 2019-02-15	A1(P)	D1, D2, D3, D4	E1(P), E2(P), E3, E4, E7	B1, B2, B3 (P), B6, B7	C1, C2, C3, C4	F1, F2, F3, F4, F6, F7, F8, F9(P), F10, F11	G2, G3 (P)	H1, H2, H3, H4, H5

*P – Partial

*$– In general discussed the API Security

API security is not discussed in most guidelines/standards because they may have considered it to be part of software security.