IoT Network Security Audit Guidelines

Version 1.0

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 certification agencies.

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

Table of Contents

1. Introduction

IoT devices are connected to a network to fulfill the user's desired task. The IoT network has different layers of operations to connect the input from the physical world to the end user or for autonomous decisions. Table 1 shows the IoT network stack with the different layers, their possible operations or components and security requirements.

Table 1. IoT Network Stack

Layers	Activities/Components	Security Requirements
Application and Processing Layer	Applications (Mobile or Desktop)	Provided in this document
	Cloud Services	
Communication Layer	Connectivity	
Perception Layer	Devices	Refer our Guidelines: IoT Device: Layer Wise Security Audit Guidelines, version 2.0, October 2023

2. Communication/Network Layer Security Requirements

In order to achieve secure communication, the IoT network must meet the following security requirements:

N1. Authentication and Authorization: Only authorized devices should join the network using single or multi-factor authentication. Device-to-Device Authentication should be implemented. [Administrator]

N2. Secure Protocols: As defined in our IoT Device Auditing Guidelines.

N3. Secure Routing: Devices should communicate only with the authorized devices and through the secure routing pathways. [Administrator]

N4. Device Asset Management: The devices that are part of the network should be identified and logged. A robust device identity scheme should be implemented and access to unauthorized devices should be revoked. [Manufacturer and Administrator]

N5. Network Segmentation: The IoT network should be segmented according to the security requirements to control access and to contain the security breaches. Segmentation should also performed between the enterprise network and IoT network [Administrator]

N6. Monitor and Analyze Network Traffic: Monitor the network traffic for suspicious activity using intrusion detection and prevention technologies that helps to identify security threats. The network gateway should analyze the traffic. [Administrator]

N7. Secure Configuration of Network Devices: Network devices such as routers, switches and firewalls should be configured according to the security baselines, to provide only necessary services. [Administrator]

N8. Disconnect IoT Device: Disconnect the device that has not been used for a specified period of time from the network. [Administrator]

N9. Client Isolation: Interaction between IoT devices should be allowed according to the requirement and should be restricted otherwise.

3. IoT Mobile Application Security Requirements

The secure mobile application development requirements are detailed below, which should also be followed for any IoT-related mobile application development as well:

DI1. No hardcoded Credentials: The application should not have any hardcoded credentials other than the public keys. [Application Developer]

DI2. No default or Weak Passwords: The user of the mobile application should not be allowed to use the default or weak passwords. This applies to access to both the mobile application and the device. [Application Developer and Users]

DI3. Secure Communication: The mobile application should access the IoT device using secure protocols such as TLS. [Application Developer]

DI4. Secure Application Development: The application should be developed and deployed using the secure coding practices. [Application Developer]

DI5. Easy Update: It should be easy for the users to perform secure updates of the applications. [Application Developer]

DI6. Credential Exposure: Credentials should not be exposed when connecting to the networks. [Application Developer]

DI7. Limit Failed Login Attempts: The user should be restricted from making infinite failed login attempts to identify the correct credentials and provision should be made secure password reset. [Application Developer]

In addition to the above secure application development requirements, the IoT device manufacturer should ensure that the IoT device mobile application meets the following security requirements in order to protect the IoT devices and the data:

I1. Authorized Users: The IoT device should be accessed by authorized mobile application users. [Manufacturer]

I2. Multi-Factor Authentication: The application should be accessed through multi-factor authentication at the first time and on demand. [Manufacturer]

I3. Secure Storage: The application should store the data accessed by the IoT device in encrypted form. The necessary secret keys should be encrypted with a strong password provided by the user. These keys should be securely stored and accessible after authentication, or, the keys can be derived from the Trusted Platform Module (TPM). [Manufacturer]

I4. Prevent Unauthorized Data Access: In the event of loss, damage, or tampering with the mobile device, data stored on the mobile device should be inaccessible to unauthorized persons. [Manufacturer]

I5. Data Validation: Data entered into the application should be validated before being passed to the IoT devices. [Manufacturer]

I6. Data Expiry Time: The user should be able to set the expiry time for the data, when data is retrieved from the IoT device and stored on the mobile or other devices. [Manufacturer and User]

I7. Secure Configuration Management: The configuration interface of the IoT device should only be accessible to authorized users through the mobile application. [Manufacturer and User]

I8. Data Erasure: The IoT device data (if any) should be securely erased from the mobile device used to interact with IoT device when the mobile device is no longer in use. [Manufacturer and User]

4. Cloud Security Requirements

The IoT devices have limited storage and computing capabilities. Since so many devices are connected to the Cloud or third-party storage for data processing, Cloud Security is an important aspect of the IoT security. The manufacturer or user of the IoT devices should ensure that the following Cloud Security requirements are met for the IoT network:

J1. Secure Communication: Communication between the IoT device and the Cloud should be via standard secure communication protocol. No data should be exchanged in the plain format using unsecured communication protocols like HTTP, FTP, etc. [Manufacturer and User]

J2. Secure Storage: Data stored in the Cloud should be encrypted using standard algorithms. [Manufacturer and User]

J3. Authorized Access: Only authorized users should access the IoT device data from the Cloud. [Manufacturer]

J4. Option to choose Cloud storage: The user should be given the option to choose between Cloud and Local storage, rather than being forced to use the Cloud. [Manufacturer]

J5. Deletion of Data: The authorized user should be able to delete the data that is stored in the Cloud, if necessary. [Manufacturer]

J6. Anonymized Data: Data stored in the Cloud should be anonymized to ensure privacy. [Manufacturer]

J7. Authentic Connection: The IoT device should connect to the Cloud service using a strong authentication mechanism. [Manufacturer and User]

J8. Command and Data Validation: The command and data flow between the Cloud and the IoT device should be validated before processing. [Manufacturer and User]

J9. Product Related Service: The product-related API keys for specific IoT applications should not be installed on unauthorized devices. Also, the API Keys should not be hardcoded into the devices. [Manufacturer]

J10. Secure Remote Configuration: The device configured via the Cloud should only use secure protocols, such as SSH. [Manufacturer]

J11.Outage Resilience: The IoT device should be able to perform its function even if the Cloud service is unavailable. [Manufacturer]

References

- https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 [Last accessed on 24/11/2023]
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf [Last accessed on 24/11/2023]
- https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security [Last accessed on 24/11/2023]
- https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf [Last accessed on 25/11/2023]
- https://www.isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf [Last accessed on 25/11/2023]
- https://tec.gov.in/public/pdf/M2M/Security%20by%20Design%20for%20IoT%20Device%20Manufacturers.pdf [Last accessed on 25/11/2023]
- https://tec.gov.in/pdf/M2M/Code%20of%20Practice%20for%20Securing%20Consumer%20Internet%20of%20Things%20(IoT)%20TEC%2031318_2021_after.pdf [Last accessed on 25/11/2023]

- 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 25/11/2023]
- https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf [Last accessed on 25/11/2023]
- 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.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pdf [Last accessed on 27/09/2023]
- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 [Last accessed on 24/08/2022]
- 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://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf [Last accessed on 04/06/2024]

APPENDIX

Appendix – I. Comparison of Security Guidelines

Table A compares the different IoT security guidelines or standards with respect to our security requirements. Table A documents the missing and unclear security requirements of the existing guidelines and standards.

Table A. Comparison of Security Guidelines

	Network Security Requirements Available	Mobile Application Security Requirements Available	Cloud Security Requirements Available
OWASP 2018	N1, N3, N4, N5, N7, N8, N9	I1, I3, I4(P), I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J8(P), J9, J10, J11
NIST 8259A	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J4, J6, J8(P), J9, J10(P)
UK government's Code of Practice for consumer IoT security	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I6, I7(P)	J1, J2, J3, J4, J6, J7, J8, J9, J10, J11
CIS Critical Security Internet of Things Security Companion to the CIS Critical Security Controls (Version 6)	N2, N3, N6, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
ISA/IEC 62443	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
TEC 31318:2021	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I6, I7(P)	J1, J2, J3, J4, J6, J7, J8, J9, J10, J11
IMDA IoT Cyber Security Guide V1	N1, N2, N3, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
IoTSF Secure Design Best Practice Guides, Release 2 November 2019	N1, N2, N3, N4, N5, N6, N7, N8, N9	I6, I7(P), I8	J4, J5(P), J6, J8(P), J9 J10(P), J11(P)
DSCI IoT SECURITY GUIDE August 2022	N2, N3, N4(P), N9(P)	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
Secure by design Internet of Things – IoT Cyber Security Advice	N1, N2, N3, N4, N6	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
ENISA Good Practices for Security of IoT - Secure Software Development Lifecycle November 19, 2019	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J4, J5, J6, J8(P), J9
NTRA, Egypt IOT Cyber Security Framework	N3(P), N5, N8, N9	I1, I2, I6, I8	J4, J5, J6, J11
National Cyber	N1(P), N3, N4, N6, N7(P),	I2(P), I3, I4(P), I5, I7	J1, N4, J5, J6, J8(P), J9,

Security Authority, Saudi Arabia Cybersecurity Guidelines for Internet of Things (Draft) (CGIoT-1:2023)	N8, N9		J10, J11
Singapore Computer Society Recognising IoT Security Issues: 12 Ways You Can Protect Your Devices	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
IEEE Internet of Things (IOT) Security Best Practices, 2017	N3, N4, N6, N7, N8, N9	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
Industrial Internet Consortium IoT Security Maturity Model: Description and Intended Use Version 1.1 2019-02-15	N1(P), N2, N3, N5, N6, N7, N8, N9(P)	I1, I2, I3, I4, I5, I6, I7, I8	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11
Australian Cyber Security Center (ACSC) Code of Practice Securing the Internet of Things for Consumers, 2023	N1, N2, N3, N4, N5, N6, N7, N8, N9	I1, I6, I7(P)	J1, J2, J3, J4, J6, J7, J8, J9, J10, J11