IoT Network Audit Checklist

IoT Security Lab, IIIT Allahabad with the support and funding of C3iHub, IIT Kanpur

Layers	Requirement	Applicability (Yes/No)	Applied (Yes/No)
Device Security Requirements [Responsible entity (Manufacturer/User) is given in bracket]			
Physical Security	**A1.**Monitoring Physical Access: The publicly placed devices should be monitored through the surveillance systems. [User]		
	A2. Hard Cover: The device should not be easily connectable and no open interfaces. Also, device should not be vulnerable to the natural elements. [Manufacturer and User]		
	A3. Access Alert: Device should give an alert if there is an unauthorized physical access or a power interruption (with the help of secondary power). For example, if someone connects the USB or other interface with the device, the alert should be generated or sent to the next device in the hierarchy. [Manufacturer]		
	A4. Disable Debugging module: The debugger such as UART, etc. should be disabled or erased or given controlled access before supplying the product.[Manufacturer]		
Data Security	**B1.**Securely store credentials: The credentials of the device should be hashed with a salt and stored. [Manufacturer and User]		
	B2. Securely store sensitive data: The sensitive data of user should be encrypted using standard algorithms and stored. 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 need to know basis. [Manufacturer (if it is firmware part) and User]		
	B4. Data Integrity: Users should have provision to verify the integrity of the data. [Manufacturer (if it is firmware part) and User]		
	B5. Data Availability: Data should be available in case of any failure such as network and power. [Manufacturer]		
	B6. Data Validation: The incoming data should be examined before using. [User]		
	B7. Non-Disclosure of Device's Sensitive Data: The device should not disclose any sensitive data such as password, keys, ports that are open, OS type, and battery percentage and baud rate to unauthorized users. [Manufacturer and User]		
Network Security Hardware Security	**C1.**Secure Protocols: It is mandatory to establish a secure tunnel between the device and receiver before transmitting/receiving the data. Also, restrict the downgrading of the protocols. [Manufacturer and User in case of own application installation]		
	C2. Necessary Network Interfaces and Services Only: The device		

	should run only the necessary network services and interfaces such as Wireless, Wired and Bluetooth. [Manufacturer and User]		
	C3. Restricted Data Flow: Control the incoming packets to avoid the Denial of Service attack, etc. The device should have firewall to control the data flow. [Manufacturer and User]		
	C4. Secure Remote Access: The device can be accessed only through the secure mode and authenticated using the password/key. [Manufacturer and User]		
	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 in the boot log of the device. [Manufacturer]		
	D4. No Access to Hardware: Device should have the sensing capability to control data leakage due to any external access. For example, attackers can access firmware, etc. using Serial Peripheral Interface (SPI), Joint Test Action Group (JTAG), Inter-Integrated Circuit (I2C), and UART. [Manufacturer]		
Software Security	**E1.**Secure Update Mechanism: The application or system software or firmware should be updated securely on demand. The update may be Over the Air (OTA), local, etc. Lack of update mechanism and use of out-dated components should be avoided. [Manufacturer and User]		
	E2. Easy Update Mechanism: The manufacturer should provide the easy update mechanism of the application or system software and firmware. [Manufacturer]		
	E3. Easy Installation Mechanism: The manufacturer should provide the easy install mechanism of 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 the proper 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 run only the necessary software services. [Manufacturer and User]		
Management Security	**F1.**Default or weak passwords: Devices should not use the default, hardcoded or weak password. Manufacturer should ensure that at the first access, the default password gets modified to a strong password and a password life time is defined in the		

	password policy. [Manufacturer and User]		
	F2. Unique Password: Administrator should ensure the unique password for all devices in the network. [User]		
	F3. Multi Factor Authentication: In required, device should support the multi factor authentication. [Manufacturer and User]		
	F4. Need Only Services: The device should run only 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, functionality of the devices, etc. [User]		
	F6. Unique Identification of Devices: The devices in 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 provision should be in the device to bring it back to the default settings or do factory reset, in case the data or software is at risk or user wants to clean the data. [Manufacturer]		
	F8. Security Team: The manufacturer should provide 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 any external module such as network connection should not affect the device process and device should be in position to send the data later and device should reset to safer state in case of any malware. [Manufacturer]		
	F10. Activity Log: The device should have the activity log facility for the future auditing. The log should not include sensitive data. [Manufacturer and User]		
	F11. Remote Storage: The user should have the option to choose the remote storage [Cloud] or local storage. User should not be forced to use the remote storage. [Manufacturer]		
Life Cycle Management	**G1.** Supply Chain Security: The device should not be tampered throughout the manufacturing to delivery process. The cryptography hash of the software/firmware components can be used to verify the device integrity. [Manufacturer]		
	G2. Device Decommissioning: The user data should be erased completely before the disposal of the device. The device can have the factory reset option or wipe-out tools can be used. [Manufacturer and User]		
	G3. Quality Check: The manufacturer should ensure implementation of the security requirements (including security verification third party libraries and softwares) before the release		

	of products from the manufacturing unit. [Manufacturer]		
	G4. Regular Vulnerability Scanning: The device should be regularly scanned for the presence of any vulnerability and identified vulnerabilities should be fixed. [User]		
Application Programming Interface (API) Security			
	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]		
Communication Layer Security			
Communication Layer	**N1**.Authentication and Authorization: Only authorized devices should join the network using single or multi-factor authentication. Device to Device Authentication is required. [Administrator]		
	N2. Secure Protocols**:** As defined in the IoT Device Auditing guidelines.		
	N3.Secure Routing: The devices should communicate only with the authorized devices and secure routing pathways ~~only~~. [Administrator]		
	N4. Device asset management: The devices that are part of the network to be identified and recorded. Create a solid device identity scheme and revoke access for unauthorized devices. [Manufacturer and Administrator]		
	N5.Network Segmentation: The IoT network should be segmented according to the security requirement to control access and prevent the spreading of security breaches. Also, segmentation should be done between the enterprise network and IoT network [Administrator]		
	N6. Traffic Monitoring and Analysis: Monitor the network traffic for suspicious activity using intrusion detection and prevention technologies. Network traffic analysis can identify and address security threats. The gateway should analyze the traffic. [Administrator]		
	N7. Secure Configuration of Network Devices: The devices that are in the network such as routers, switches and firewalls should be configured securely. [Administrator]		
	N8. Disconnect IoT Device: The device that is not in use should be disconnected from the network [Administrator]		

Mobile Application Security Requirements			
Mobile Application	**I1.**Authorized Users: The IoT device should be accessed through authorized mobile application users. [Manufacturer]		
	I2. Multi-Factor Authentication: The application should be accessed through multi-factor authentication for the first time and as and when required. [Manufacturer]		
	I3.Secure Storage: The application should store the data that are accessed from the IoT device in encrypted form. The necessary secret keys should be encrypted and stored using the password or the keys can be derived from the Trusted Platform Module (TPM). [Manufacturer]		
	I4.Unauthorized Data Access: The data should not be accessible to unauthorized personnel in case of device loss or tampering of the devices. [Manufacturer]		
	I5. Data Validation: The input data to the application should be validated before passing to the IoT devices. [Manufacturer]		
	I6. Expiry Time for the Data: The user should have the provision to define the expiry time for the data if any fetched from the IoT device and stored on the Mobile or other devices. [Manufacturer and User]		
	I7. Secure configuration Management: Only authorized users through the application can access the configuration interface of the IoT device. Enforce Strong Authentication over configuration management access. [Manufacturer and User]		
	I8. Erasure of the Data: The data should be erased securely when the mobile device is no longer used. [Manufacturer and User]		
Cloud Usage Security Requirements			
Cloud Security	**J1.**Secure Communication: The communication between the IoT device and the Cloud should be through the standard secure communication protocol. No data should be shared in the plain format that is using HTTP, FTP, etc. [Manufacturer and User]		
	J2.Secure Storage: The data that is shared and stored in the Cloud should be encrypted using standard protocols at the IoT device end. [Manufacturer and User]		
	J3.Authorized Access: Only authorized users should access the IoT device data from the Cloud. [Manufacturer]		
	J4.Cloud Option: The user should be given the option to choose the Cloud or Local storage instead of forcing to use the Cloud. [Manufacturer]		
	J5. Deletion of Data: The authorized user should have the provision to delete the data that is stored in the Cloud on requirement. [Manufacturer]		
	J6. Anonymised Data: The data that is stored in the Cloud should be anonymized for ensuring 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 IoT device should be validated before processing it. [Manufacturer and User]		
	J9. Product Related Service: The Product-related API keys to		

	specific IoT applications are not installed on non-authorized devices. The API Keys should not be hardcoded on the devices. [Manufacturer]		
	J10. Secure Remote Configuration: The device can be configured using the Cloud only through secure protocols such as SSH. [Manufacturer]		
	J11. Outage Resilience: The IoT device should perform its function even if the Cloud service is not available. [Manufacturer]		

Note: If anything seems missed out kindly point it out.