IOT Security & Forensics

Name: Vinayak Bhagwat

Course: M.Sc. Cyber Security

Enrolment number:104CTMSCS2122002

IoT OWASP 10

01. Weak, Guessable, or Hardcoded Passwords

One of the most common security risks that can affect IoT devices is weak or easily guessed passwords. Many IoT devices come with factory-default passwords that are either easy-toguess, publicly available, or unchangeable. This is the case for most IoT devices with a web interface. Hardcoded Passwords, also known as embedded credentials, are plain-text passwords or other secrets in the very source code of the device firmware. If an attacker gains access to the source code, they will have access to all of the passwords and secrets used by the device. Examples of weak, guessable, or hardcoded passwords include the following:

- admin/admin
- guest/guest
- user/password
- rot/toor

Use of:

- Easily brute-forced
- Publicly available
- Unchangeable credentials including backdoors in firmware or client software that grants unauthorized access.

02. Insecure Network Services

Insecure or unneeded device network services exposed to the public Internet can lead to the compromising of the

confidentiality, integrity, and availability of their information. IoT security that is often compromised through default passwords can lead to these devices being used by botnets, which can execute attacks such as Distributed Denial-of-Service (DDoS), data theft, or ransomware.
Unneeded or insecure network services running on the device itself, especially:

- Those exposed to the internet
- Any that compromise the confidentiality, integrity/ authenticity, or availability of information
- Any service that allows unauthorized remote control

Examples of insecure network services can include the following:

- Telnet
- FTP
- UPnP

03. Insecure Ecosystem Interfaces

An ecosystem of interfaces can be defined as any communication interface used by the device that is not part of the device itself.

Insecure interfaces in the ecosystem outside the device:

- Web
- Backend API
- Cloud
- Mobile

Common Issues:

- Lack of authentication
- Lack of authorization
- Weak password/encryption
- Lack of input & output filtering

04. Lack of Secure Update Mechanism

The lack of any secure update mechanism, software and firmware updates can be subject to the unauthorized modification of a system, system component, its intended behaviour, or data, either at the source or in transit.
Lack of ability to securely update the device.

- Lack of firmware validation on device
- Lack of secure delivery (un-encrypted in transit)
- Lack of anti-rollback mechanisms
- Lack of notifications of security changes due to update

2016 Carnegie Mellon University Study, On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle.

- Observations: insecure firmware updates and downloads
- Researchers were able to make arbitrary firmware modifications and maliciously update remote firmware.

05. Use of Insecure or Outdated Components Use of deprecated or insecure software components/libraries that could allow the device to be compromised.

Deprecated or insecure software components/libraries, as listed below, could lead to the overall compromise of the device:

- Insecure customization of operating system platforms
- Third-party software libraries from a compromised supply chain
- Third-party hardware components from a compromised supply chain

Components of a software with known vulnerabilities that have not yet been patched should be avoided until they can be updated. Examples of deprecated or insecure software components can include the following:

- OpenSSL

- LibreSSL
- Bouncy Castle

06. Insufficient Privacy Protection

Users' personal information stored within the device or within the ecosystem being used insecurely, improperly, or without permission. Privacy protection is a critical compliance risk for many standards, including the following:

- GDPR, or General Data Protection Regulation, which requires businesses to protect the personal data and privacy of European Union (E.U.) citizens for transactions occurring within their member states.
- PCI-DSS, or the Payment Card Industry Data Security Standard, which requires any business processing, storing, or transmitting credit card information to protect cardholders' data.

Examples of insufficient privacy protection can be a security vulnerability due to insecure local data storage or even the unauthorized collection and storage of personal data.

2017 Cornell University Study

A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic "We examine four IoT smart home devices [...] and find that their network traffic rates can reveal potentially sensitive user interactions even when the traffic is encrypted"

https://arxiv.org/abs/1705.06805

07. Insecure data transfer & storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

Examples of insecure data transfer and storage can include the following:

- Sending data over an unsecured network connection without encryption.
- Storing data in an unencrypted database or file.
- Failing to properly restrict access to sensitive data based on a need-to-know or rolebased access.
- Not verifying the integrity of stored data, resulting in possible tampering or corruption.

"The Espressif ESP8266 chipset makes three-dollar 'Internet of Things' development boards an economic reality. According to the popular automatic firmware-building site node MCUbuilds, in the last 60 days there have been 13,341 custom firmware builds for that platform. Of those, only 19% have SSL support, and 10% include the cryptography module." https://hackaday.com/2017/06/20/practical-iot-cryptography-on-the-espressif-esp8266/

08. Lack of device management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities. Examples of a lack of device management can include the following:

- Failing to track or monitor devices.
- Not having the ability to remotely update or patch devices.
- Lack of visibility into devices and their configurations.
- Inability to properly decommission a device when it is no longer needed, resulting in orphaned devices that could still be used to access sensitive data or networks.
- Not having systems in place to detect and respond to security incidents.

We haven't solved this for non-IoT environments yet.

- 25% still rely on Excel spreadsheets to track assets

- 56% verify asset location only once a year, while 10-15% verify only every five years
- Staff spends 10+ hours weekly to resolve data accuracy issues
- Nearly 66% of IT managers have an incomplete record of their IT assets

09. Insecure default settings

Devices or systems launched with insecure default settings or that cannot be made more secure by restricting operators from changing them. Examples of insecure default settings include default passwords that are either well-known or easily guessed, the use of hardcoded or easily guessable default administrative credentials, or the lack of proper access control mechanisms, such as not requiring strong authentication for administrator accounts. These may include:

- Bad filesystem permissions
- Exposed services running as root

10. Lack of physical hardening

Lack of physical hardening measures, allowing potential attackers to obtain sensitive information that could be leveraged to launch a future remote attack or to take local control of the device.

Examples of a lack of physical hardening can include the following:

- Not using tamper-resistant hardware.
- Using easily guessable or default passwords for physical access control mechanisms, such as locks and keys.
- Failing to properly protect devices from unauthorized physical access, resulting in possible tampering, theft, or destruction of the device.
- Easily Available Debug Port Discovery