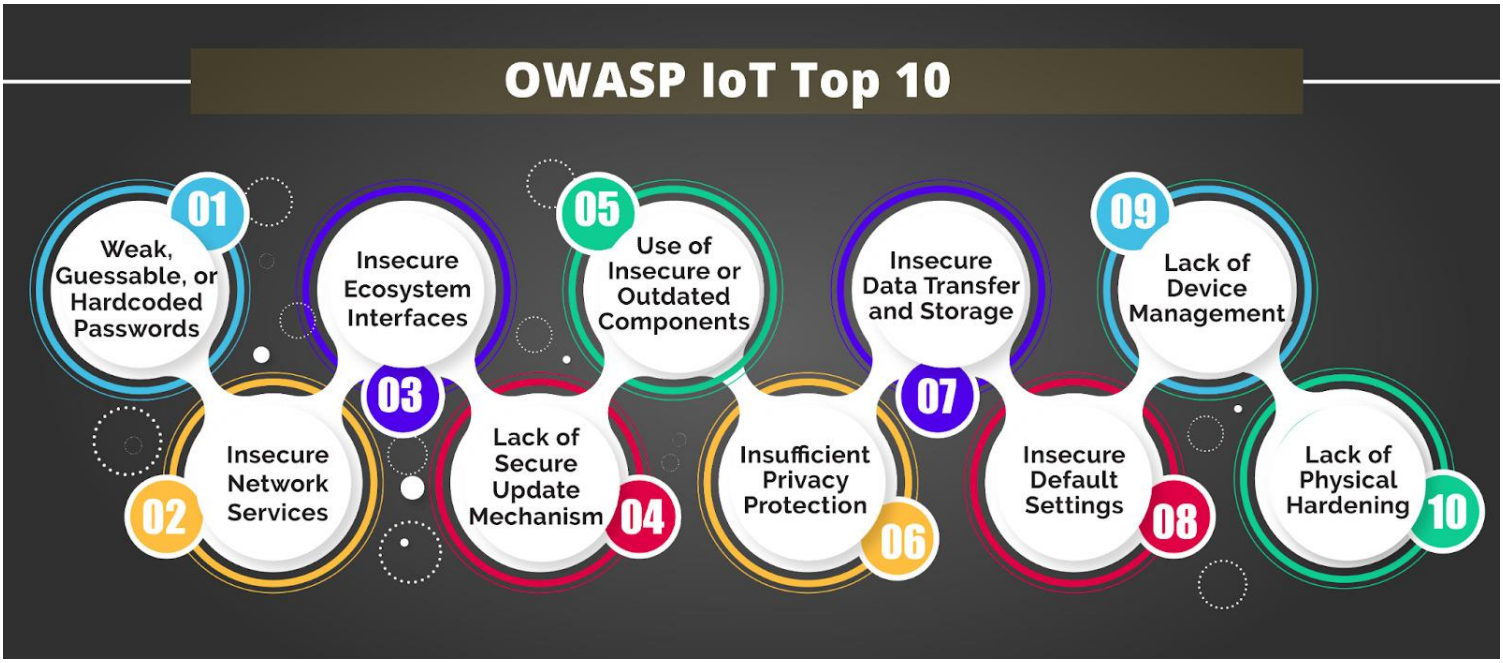
# OWASP Top 10 for IoT

The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.




## 1. Weak, guessable or hard coded passwords

IoT devices with weak default passwords are prone to cyber attacks. IoT device manufacturers must pay attention to password settings while launching the device. Either the device doesn't allow the users to change the default password or the users prefer not to change it even if they can. Moreover, a successful attempt to gain unauthorized access into one device leaves others in the system vulnerable as IoT devices often share the same default passwords.

**Examples** of weak, guessable, or hardcoded passwords include:  admin/admin, user/password, root/toor

To combat the first vulnerability listed by OWASP, manufacturers must take the following steps:

- Every device must have a unique set of credentials
- Disable weak passwords
- Removing backdoors created during debugging

## 2. Insecure network services

Network services running within the device can pose a threat to the security and integrity of the system. These, when exposed to the internet, provide unauthorized remote access and data leak. Attackers can successfully compromise the security of an IoT endpoint by taking advantage of the weaknesses present in the network communication model.
**Examples** of insecure network services can include : telnet , FTP ,UPnP

To prevent threats arising from insecure network services, manufacturers should:

- Use secure protocols like HTTPS, sFTP, and SSH
- Disable non-essential ports and services that provide remote access
- Keep IoT devices on a separate network

## 3. Insecure ecosystem interfaces

There are several interfaces like web interface, the backend API, the cloud, and the mobile interface that enable smooth user interaction with the device. However, lack of proper authentication, poor encryption and data filtering can adversely impact the security of IoT devices.

**Examples** of an insecure ecosystem are the Insecure web interface, Insecure mobile app,Insecure cloud interface, Insecure API

To address insecure interfaces, the following tips are useful:

- Adhering to the principle of least privilege
- Block public access to S3 bucket
- Strong authentication of IoT endpoints

## 4. Lack of secure update mechanisms

The inability of the device to securely update is the fourth vulnerability in the list. No firmware validation, unencrypted transfer of data, absence of anti rollback mechanisms, lack of security update notifications are the reasons for compromised security of IoT devices.

For secure delivery of updates to IoT devices, manufacturers must:

- Only implement updates that are digitally signed
- Implement anti-rollback mechanisms
- Secure and verify access to updates

## 5. Use of insecure or outdated components

This implies the use of third party hardware or software that have risks associated with it and threatens the security of the entire system. The industrial internet of things (IIoT) is particularly affected by systems that are difficult to update and maintain. Such vulnerabilities can be leveraged to launch an attack and disrupt the smooth functioning of the device.
**Examples** of deprecated or insecure software components can include : OpenSSL, LibreSSL, Bouncy Castle

IoT manufacturers are advised to :

- Refrain from legacy technologies
- Ensure continuous tracking of hardware and software components
- Immediately replace any of the components that turn obsolete

## 6. Insufficient privacy protection

IoT devices may have to store and retain sensitive information of users to function properly. However, these devices often fail to offer a secure storage which leads to leakage of critical data when hacked by cyber criminals. In addition to devices, the manufacturer's databases are also prone to attacks. An encrypted traffic is still prone to threats as there have been instances where passive observers could also extract information.

**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.

Consumer privacy is one of the key concerns that need to be addressed with the following measures:

- Limit the storage of personal data on devices
- Frame a data protection policy for your organization
- Prepare an incident response plan to combat any breach of security in the future

## 7. Insecure data transfer and storage

The lack of encryption while handling sensitive data either during transmission, processing or at rest is an opportunity for hackers to steal and expose data. Encryption is must wherever transfer of data is involved.

**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 role-based access.
- Not verifying the integrity of stored data, resulting in possible tampering or corruption

To ensure maximum protection of data, IoT manufacturers need to implement the following for complete security:

- Ensure encryption at all levels
- Strictly utilize secure channels like HTTPS, sFTP and SSH
- Opt for one-time-use keys that aren't stored in the device

## 8. Lack of device management

This refers to the inability to effectively secure all the devices on the network. It exposes the system to numerous threats. Irrespective of the number of devices involved or their size, each one of them needs to be protected against data breach.

**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.

There is an increased risk of attacks if there are several devices with weak security functioning within the same system. The following steps must be implemented for flawless device management.

- Secure decommissioning, endpoint quarantine and blacklisting
- Integrate devices with asset management, bug tracking and patch management systems
- Build an interface that is flexible and seamlessly integrates with other systems

## 9. Insecure default settings

The existing vulnerabilities in the default settings expose the system to an array of security issues. It might be fixed passwords, inability to keep up with the security updates and presence of outdated components.

**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

The following 3 tips can enable IoT manufacturers to thwart the risks associated with weak default settings:

- Use only secure default settings
- Grant users permission to change default passwords
- Prompt users to change their default passwords compulsorily

# 10. Lack of physical hardening

Lack of physical hardening can easily help users with malicious intent to gain remote control over the system. Failure to remove debug ports or removal of the memory card can expose the system to attacks owing to lack of physical hardening.

**Examples** of a lack of physical hardening can include:

- 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

To counter physical threats to IoT devices, manufacturers should:

- Understand how a user may modify the device
- Proactively anticipate what damages any user may inflict on the device
- Devise solutions and build an IoT device that can withstand all the possible attacks

## The Future of the OWASP IoT Top 10

The team has a number of activities planned to continue improving on the project going forward.

Some of the items being discussed include:

- Continuing to improve the list on a two-year cadence, incorporating feedback from the community and from additional project contributors to ensure we are staying current with issues facing the industry.
- Mapping the list items to other OWASP projects, such as the ASVS, and perhaps to other projects outside OWASP as well.
- Expanding the project into other aspects of IoT—including embedded security, ICS/ SCADA,etc.
- Adding use and abuse cases, with multiple examples, to solidify each concept discussed.
- Considering the addition of reference architectures, so we can not only tell people what to avoid, but how to do what they need to do securely.