IoT security | IoT device security

IoT security is the practice of protecting Internet of Things (IoT) devices from attack.

What is IoT security? | IoT device security

Internet of Things (IoT) devices are computerized Internet-connected objects, such as networked security cameras, smart refrigerators, and WiFi-capable automobiles.

IoT security is the process of securing these devices and ensuring they do not introduce threats into a network.

Anything connected to the Internet is likely to face attack at some point. Attackers can try to remotely compromise IoT devices using a variety of methods, from credential theft to vulnerability exploits.

Once they control an IoT device, they can use it to steal data, conduct distributed denial-of-service (DDoS) attacks , or attempt to compromise the rest of the connected network.

IoT security can be particularly challenging because many IoT devices are not built with strong security in place — typically, the manufacturer's focus is on features and usability, rather than security, so that the devices can get to market quickly.

IoT devices are increasingly part of everyday life, and both consumers and businesses may face IoT security challenges.

What attacks are IoT devices most susceptible to?

Firmware vulnerability exploits

All computerized devices have firmware, which is the software that operates the hardware.

In computers and smart phones, operating systems run on top of the firmware; for the majority of IoT devices, the firmware is essentially the operating system.

Most IoT firmware does not have as many security protections in place as the sophisticated operating systems running on computers.

And often this firmware is rife with known vulnerabilities that in some cases cannot be patched.

This leaves IoT devices open to attacks that target these vulnerabilities.

Credential-based attacks
Many IoT devices come with default administrator usernames and passwords. These usernames and passwords are often not very secure — for instance, "password" as the password — and worse, sometimes all IoT devices of a given model share these same credentials.

In some cases, these credentials cannot be reset.

Attackers are well aware of these default usernames and passwords, and many successful IoT device attacks occur simply because an attacker guesses the right credentials.

On-path attacks
On-path attackers position themselves between two parties that trust each other — for example, an IoT security camera and the camera's cloud server — and intercept communications between the two.

IoT devices are particularly vulnerable to such attacks because many of them do not encrypt their communications by default (encryption scrambles data so that it cannot be interpreted by unauthorized parties).

Physical hardware-based attacks
Many IoT devices, like IoT security cameras, stoplights, and fire alarms, are placed in more or less permanent positions in public areas.

If an attacker has physical access to an IoT device's hardware, they can steal its data or take over the device.

This approach would affect only one device at a time, but a physical attack could have a larger effect if the attacker gains information that enables them to compromise additional devices on the network.

How are IoT devices used in DDoS attacks?

Malicious parties often use unsecured IoT devices to generate network traffic in a DDoS attack.

DDoS attacks are more powerful when the attacking parties can send traffic to their target from a wide range of devices.

Such attacks are harder to block because there are so many IP addresses involved (each device has its own IP address).

One of the biggest DDoS botnets on record, the Mirai botnet , is largely made up of IoT devices.

What are some of the main aspects of IoT device security?

Software and firmware updates

IoT devices need to be updated whenever the manufacturer issues a vulnerability patch or software update.

These updates eliminate vulnerabilities that attackers could exploit.

Not having the latest software can make a device more vulnerable to attack, even if it is outdated by only a few days.

In many cases IoT firmware updates are controlled by the manufacturer, not the device owner, and it is the manufacturer's responsibility to ensure vulnerabilities are patched.

Credential security

IoT device admin credentials should be updated if possible.

It is best to avoid reusing credentials across multiple devices and applications — each device should have a unique password.

This helps prevent credential-based attacks.

Device authentication

IoT devices connect to each other, to servers, and to various other networked devices.

Every connected device needs to be authenticated to ensure they do not accept inputs or requests from unauthorized parties.

For example, an attacker could pretend to be an IoT device and request confidential data from a server, but if the server first requires them to present an authentic TLS certificate, then this attack will not be successful.

For the most part, this type of authentication needs to be configured by the device manufacturer.

Encryption

IoT device data exchanges are vulnerable to external parties and on-path attackers as they pass over the network — unless encryption is used to protect the data.

Think of encryption as being like an envelope that protects a letter's contents as it travels through the postal service.

Encryption must be combined with authentication to fully prevent on-path attacks.

Otherwise, the attacker could set up separate encrypted connections between one IoT device and another, and neither would be aware that their communications are being intercepted.

Turning off unneeded features

Most IoT devices come with multiple features, some of which may go unused by the owner.

But even when features are not used, they may keep additional ports open on the device in case of use.

The more ports an Internet-connected device leaves open, the greater the attack surface —often attackers simply ping different ports on a device, looking for an opening.

Turning off unnecessary device features will close these extra ports.

DNS filtering

DNS filtering is the process of using the Domain Name System to block malicious websites.

Adding DNS filtering as a security measure to a network with IoT devices prevents those devices from reaching out to places on the Internet they should not (i.e. an attacker's domain).

What is mutual TLS (mTLS)?

Mutual Transport Layer Security (mTLS) is a type of mutual authentication, which is when bothsides of a network connection authenticate each other.

TLS is a protocol for verifying the server in a client-server connection; mTLS verifies both connected devices, instead of just one.

mTLS is important for IoT security because it ensures only legitimate devices and servers can send commands or request data.

It also encrypts all communications over the network so that attackers cannot intercept them.

mTLS requires issuing TLS certificates to all authenticated devices and servers.

A TLS certificate contains the device's public key and information about who issued the certificate.

Showing a TLS certificate to initiate a network connection can be compared to a person showing their ID card to prove their identity.