IoT and Big Data Security

Abdullah Al Mahmud
Lecturer
Daffodil International University

What is IoT Security

IoT security refers to the protective measures and technologies used to safeguard connected devices and networks in the Internet of Things (IoT). These devices can range from simple household items like smart thermostats and security cameras to complex industrial tools.

Why is IoT Security Important?

Data Privacy: Many IoT devices collect personal information, which can include sensitive data. Effective security measures prevent this data from being accessed or misused by unauthorized parties.

Infrastructure Security: In many cases, IoT devices are part of critical infrastructure systems, such as energy grids or water supply systems. Compromises in IoT security could lead to disruptions in these essential services.

Economic Impact: Security breaches can lead to significant financial losses due to theft of intellectual property, manipulation of data, and the cost of restoring systems to normal operations.

IoT security challenges

Weak Authentication and Authorization

- **Issue**: Many IoT devices come with simple or default usernames and passwords that are easy to guess or are widely known, making them vulnerable to unauthorized access. Additionally, some devices lack robust mechanisms to manage who has the rights to access and control them.
- **Impact**: This can lead to unauthorized access, where attackers could take control of devices, manipulate their functionalities, or access sensitive data.

Lack of Encryption

- **Issue**: Encryption is critical for protecting data in transit and at rest, yet many IoT devices do not encrypt their data. This makes the information they send and store susceptible to interception and misuse.
- **Impact**: Without encryption, data such as personal information, business data, and even control commands can be read and altered by attackers, leading to privacy breaches and manipulation of device operations.

Vulnerabilities in Firmware and Software

- **Issue**: IoT devices often operate on firmware that may not be regularly updated or patched, leaving known vulnerabilities unaddressed. The software on these devices can also be outdated or have inherent flaws due to poor design or implementation.
- **Impact**: These vulnerabilities can be exploited by cybercriminals to gain unauthorized access, disrupt device functionality, or use the devices as entry points into wider networks.

Insecure Communications

- **Issue**: Many IoT devices communicate over networks without any security measures in place, such as secure protocols (e.g., HTTPS, TLS). This exposes their communications to potential eavesdropping or interception by malicious actors.
- **Impact**: Insecure communications can lead to data being intercepted during transmission. Attackers could gain sensitive information or even alter communications to issue unauthorized commands to IoT devices.

Difficulty in Patching and Updating Devices

- **Issue**: IoT devices often have limited interfaces for updates or require manual interventions to install patches. Some may not even have the capability to be updated remotely, or manufacturers may cease support for older devices.
- **Impact**: The inability to easily update devices means that once vulnerabilities are discovered, they may remain unpatched, leaving devices perpetually at risk. This makes maintaining long-term security for IoT devices challenging and increases the risk of successful cyber attacks.

How to protect IoT systems and devices

1. Design Phase Integration

- Security by Design: Introduce IoT security during the design phase of device development. This involves enabling security by default, using the most recent operating systems, and choosing secure hardware.
- IoT developers should continually assess cybersecurity vulnerabilities throughout each stage of development, not just during the design phase

2. Cryptographic Measures

- Secure client-server connections by the encryption and decryption of private messages. This ensures the confidentiality and integrity of data transmitted between devices.

3. Network Security

- Networks provide a huge opportunity for threat actors to remotely control IoT devices. Because networks involve both digital and physical components, on-premises IoT security should address both types of access points. Protecting an IoT network includes ensuring port security, disabling port forwarding and never opening ports when not needed; using antimalware, firewalls, intrusion detection systems and intrusion prevention systems; blocking unauthorized IP addresses; and ensuring systems are patched and up to date.

How to protect IoT systems and devices

4. API security:

APIs are the backbone of most sophisticated websites. They enable travel agencies, for example, to aggregate flight information from multiple airlines into one location. Unfortunately, hackers can compromise these channels of communication, making API security necessary for protecting the integrity of data being sent from IoT devices to back-end systems and ensuring only authorized devices, developers and apps communicate with APIs. T-Mobile's 2018 data breach exposed the consequences of poor API security. Due to a leaky API, the mobile giant exposed the personal data of more than 2 million customers, including billing ZIP codes, phone numbers and account numbers.

5. Patch management and continuous software updates.

It's critical to provide a way to update devices and software either over network connections or through automation. Having a coordinated disclosure of vulnerabilities is also important for updating devices as soon as possible. Consider end-of-life strategies as well.

How to protect IoT systems and devices

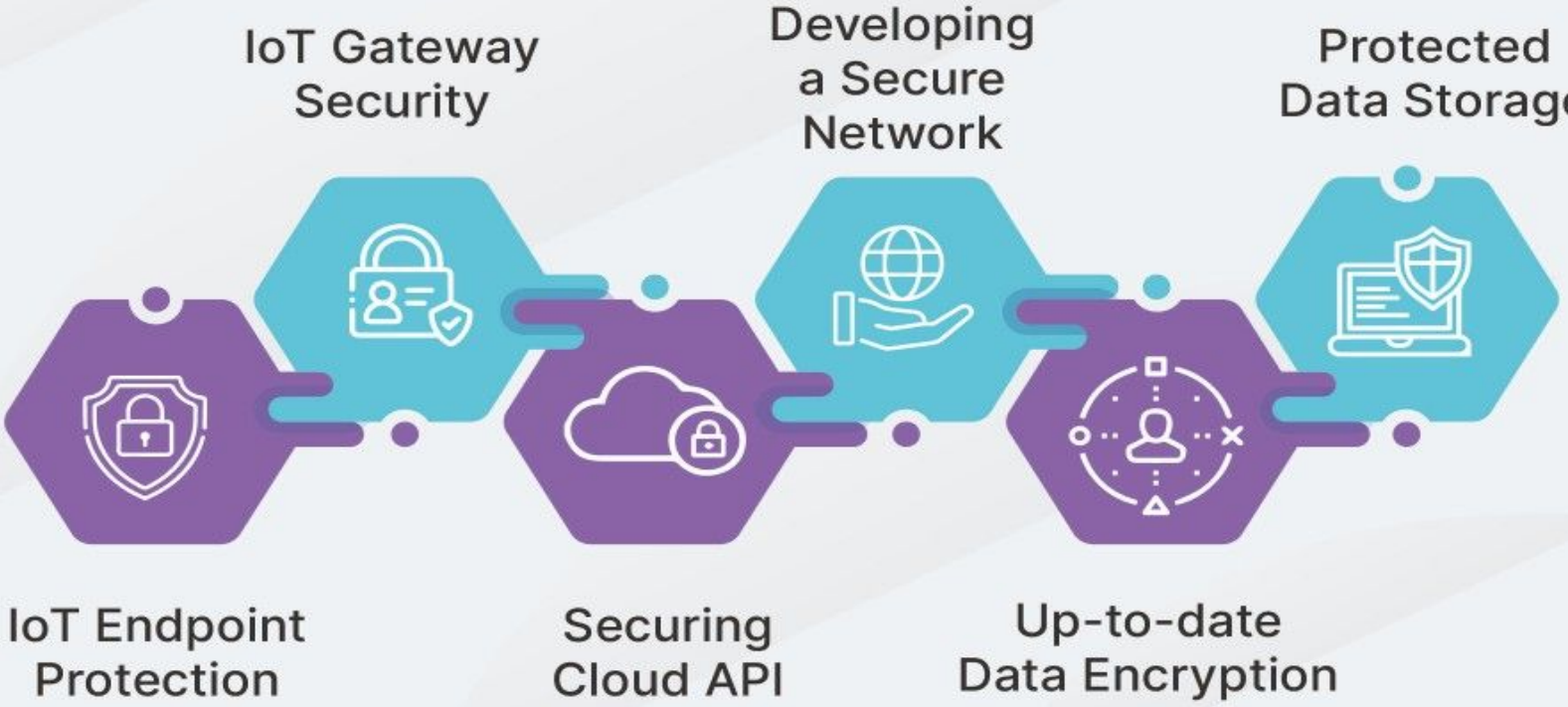
6. Organizational and Consumer Education

- **Training**: Continuously train security teams on new IoT and operational system security challenges.
- **Consumer Awareness:** Educate consumers about IoT security risks and the importance of security measures like changing default credentials and applying updates.
- **Zero-Trust and MFA:** Implement and automate zero-trust policies, requiring continual verification and authorization of all users. Use multifactor authentication (MFA) to enhance access security.

7. Machine learning (ML).

ML technology can be used to secure IoT devices by automating the management and scanning of devices throughout the entire network. Since every device connected to the network is scanned, it stops assaults automatically before IT teams are alerted. That's what happened in 2018 when Microsoft Windows Defender software stopped a Trojan malware attack in 30 minutes.

IoT Security Key Recommendations



Thank You