TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.
Internet of Things (IoT) can be described as the next industrial and human lifestyle revolution. Depending on who you talk to, IoT is defined in different ways, and it encompasses many aspects of segmentation—from connected homes and cities, to connected cars and healthcare interfaces, to the devices that track an individual’s behavior and use the data collected for future services. In general, IoT refers to the use of sensors and communication technology embedded into physical devices that enable them to be tracked and controlled over the Internet. Because of IoT, billions of things—and people—may be able to communicate with each other. Gartner, Inc. forecasts that 20.8 billion connected things will be in use worldwide by 2020.¹

IoT solutions require advanced communication platforms and cloud solutions that facilitate seamless integration of devices, networks, gateways, applications, and services. This means there is a wide range of exposure to potential vulnerabilities with multiple attack surfaces, creating a hackers’ playground.

As for security, IoT will face severe challenges for the following reasons:

1. IoT devices do not have enough computing power required for sophisticated security protection
2. Communication through the Internet is easily hijacked by man-in-the-middle attacks
3. Data in the cloud is practically a treasure trove for attackers

Therefore, a full range of security protection across devices, gateways, and the cloud is a necessary countermeasure.

This document will focus on IoT device security, using the device lifecycle to explain what we can do to address issues regarding confidentiality, authenticity, availability, and integrity of data.

The Way We See the IoT World

From our point of view, IoT is not just something hooking up to the Internet, but a combination of various technologies including sensors, hardware processors, communication protocols, data storage/analysis methods, smart applications, intelligent service offerings, and mobile/web interfaces. The whole picture of the IoT world involves six main steps:

1. Capturing of data using sensors
2. Processing of captured data
3. Connecting the data to the network/gateway
4. Decision-making based on the analysis of the data to turn it into valuable information
5. Using the information to improve productivity for smart applications
6. Using the various aspects of new intelligence services which benefit segmentation

![Figure 1. The six steps of IoT technology and service](image-url)
Figure 1 gives more details about the IoT world using the Six Layers model. Listed below are the steps on how IoT devices receive, process, and use data.

1. In the data sensors layer, different sensors collect data for different purposes. These sensors include proximity sensors, magnetometers, gyroscopes, altimeters, and others.

2. The raw data is then processed before it is sent out to the Internet by an MCU (Microcontroller Unit), MPU (Microprocessor Unit), or other data processors in the second layer.

3. In the data connection layer, there are several different protocols which can be used in IoT communication or M2M (machine-to-machine) communication such as ZigBee, Bluetooth, NFC, RFID, Wi-Fi, Z-wave, etc.

4. In the fourth layer, data goes out to the cloud through an IoT gateway, router, or 4G network for storing data analysis. It then turns the data into valuable information for the next layer to use.

5. The fifth layer is where the data is plugged into smart applications such as smart buildings, homes, cars, and so on.

6. The final layer is the service layer, where alternative intelligence services can be created and offered to the public or specific domain focus areas for benefits. These benefits include increased productivity, energy savings, and improved air quality, among others.

Besides these six-layer data transformation stages, mobile apps and web apps also play a very important role in the IoT world. This is because a lot of IoT devices use either mobile apps or web apps as the management console for the interaction.

Another aspect that has triggered this IoT boom is the concept Industry 4.0. It is described as the latest revolution in manufacturing, powered by IoT technology and smart factories.

![Figure 2. Industrial manufacturing advancement leading to Industry 4.0](image-url)
IoT Security

By looking at the digital world’s ever-changing threat landscape—from disablement to data breaches and ransomware—we can see that most attacks are aimed at data, and are executed with extensive preparation. The adoption of new technology also creates new avenues attackers can target and abuse.

![Current threat landscape in the IoT ecosystem](image)

Since there are various attack surfaces available for attackers, protection needs to be considered at three different layers:

- **Edge protection**: Ensures device, mobile app, and web app integrity to prevent devices from becoming attack entry points
- **Network protection**: Secures communication channels to prevent man-in-the-middle attacks
- **Cloud protection**: Assures data privacy and prevents data leakage

### IoT Device Security Risks

From a security point-of-view, IoT devices have security challenges for the following reasons:

1. **Hardware limitations and cost factors**
   - Due to cost considerations, IoT devices have too many hardware constraints which do not allow for any kind of sophisticated security implementation.
   - As a result, communications do not use encryption in device-to-device, device-to-Internet, and Internet-to-user interfaces (like mobile apps, for instance).
2. Hardware hacking and device identity
   - Since many IoT devices are available in the market, it is easier for attackers to familiarize themselves with exploiting the hardware and their weaknesses.
   - Because most device information is stored in the cloud, faking a device’s identity will be relatively easy.

3. Closed system security patch difficulty
   - A lot of closed systems are using open source libraries with potential vulnerabilities, making it more dangerous for those closed systems to connect to the Internet without proper security patch methods.
   - In contrast to multi-purpose computer devices like PCs, IoT devices cannot install or deploy security software after they have been shipped to the market. This means the only way to fix the issue is to go through firmware updates.

Typical Attacks in the IoT World

From several hacking case studies, we found out that typical attacks would be carried out through the following methods:

![Figure 4. Common attack scenarios on IoT devices](image-url)
IoT Device Security Guidelines

Trend Micro realizes that the design philosophy for IoT device security is completely different from that of other computing systems. Signature-based blacklisting solutions are not suitable for IoT devices due to hardware limitations. Instead, ensuring device integrity, confidentiality, identification, and operation continuity will be vital in IoT security implementation. To design appropriate security measures, we need to examine device lifecycles and make sure these security measures are truly protecting the device.

Device Life Cycle

Unlike multi-purpose computers such as PCs, IoT devices are generally more like single-purpose computers. The first life cycle, for example, includes four steps:

1. **Boot-up**: The device loads the firmware and starts to work as defined.
2. **Initialization**: Once boot-up is completed, the system reads the configuration, establishes connections, syncs up data, etc.
3. **Operation**: The device performs its designed purpose continually.
4. **Update**: New firmware is installed, the device reboots, and then starts to load the new firmware.

![IoT device lifecycle diagram](image)

The device should complete its previous life cycle before starting the next life cycle every time the firmware is updated. Eventually, the device will be retired for whatever reason. When it does, it reaches the end of the device life cycle called termination.
IoT Device Security Guidelines in Device Life Cycle

We are going to use one life cycle to explain what kind of security features should be in place at each step.

1. **Boot-up**
   - **Firmware integrity check:** To ensure that firmware has not been modified or tampered by others, the best method is to implement an integrity check by embedded checksum or secure password.
   - **Secure boot:** Encrypt firmware with PKI or public/private certification to secure the whole boot-up process.

2. **Initialization**
   - **AAA protection**
     - Use proper encryption to avoid user/device hijack.
     - Default account credentials appear in many IoT devices. It’s best to have an activation process which requires end-user to change default password.
   - **Key/Certification protection:** Use a KMS (Key Management System) or CMS (Certification Management System) to protect encryption/decryption keys, or store those keys in a TPM (Trusted Platform Module).
   - **Communication protection:** The communication between device and device, device and the Internet, or device and user interface (through mobile apps or web apps) should be encrypted (HTTPs, AES 128, 256, and others).
   - **Identity protection:** To prevent a fake identity within the communication group, it is necessary to make sure the communicated object is certified. A KMS or CMS can also play an important role here.

3. **Operation**
   - **AAA protection**
     - Remove all backdoor debug user accounts. From several studies, we have found out that many IoT devices keep those accounts for debugging purposes in the system and that increases the chances of penetration.
     - During the operation stage, the IoT device may still associate with new devices, users, and clouds, for example; add new monitor sensors for a connected home, or creating additional user account for home member, so account protection is still needed in this stage.
   - **Monitoring:** The device should implement knowledge to detect abnormal operations and, if such operations occur, provide a warning to the backend or end user.
• **Integrity check**: Run-time integrity checks can prevent the device from being compromised during operation. Leveraging cloud technology to have two-way integrity checks will be the most effective way.

• **Risk management**: Use a method like virtual patching or a host IPS to reduce risk before Firmware Over-the-Air (FOTA) triggers.

4. **Update**

• **Secure FOTA (Firmware Over-the-Air)**: Before the FOTA trigger, the new firmware needs to be encrypted and checked to make sure the next lifecycle will be performing a secure boot up again.

Figure 6. Security protocol for each step of a device life cycle
Trend Micro implements a full range of protection concept to secure the IoT: cloud, network, and edge.

1. **Data Sensors**
   - Proximity
   - Magnetometer
   - Gyroscope
   - Altimeter
   - Orientation
   - Accelerometer
   - Temperature
   - Pressure

2. **Data Processing**
   - Hybrid MCU/MPU
   - MCU
   - Network Processor
   - MPU

3. **Data Connection**
   - Zigbee
   - Bluetooth
   - NFC
   - RFID
   - iBeacon
   - Z-Wave
   - GloWPAN/CoRE
   - WiFi
   - GPS
   - Weave

4. **Software Information**
   - Support platform
   - Cloud computing
   - Big data

5. **Smart Applications**
   - Smart homes
   - Smart lighting
   - Smart cars
   - Smart farms
   - Smart buildings
   - Smart grid
   - Smart energy
   - Smart health
   - Smart tags
   - Smart cities

6. **Intelligence Services**
   - Asset tracking
   - Efficient transportation
   - Environmental protection
   - Building automation
   - Remote healthcare
   - Intelligent navigation
   - Air quality control
   - Supply chain automation
   - Remote appliance

---

Figure 8. Trend Micro IoT full-range protection deployment

---

Figure 9. Trend Micro full-range protection features block diagram
Figure 9 shows the full range of Trend Micro IoT security solutions. Since this document focuses on IoT device security, the following contains the detailed feature list in the edge layer protection (Secure Endpoint).

![Secure Endpoint/Hub SDK - IoT](image)

**Secure Endpoint/Hub SDK - IoT**

**Risk assessment**
- System anomaly detection
  - Static integrity check (File system)
  - Dynamic integrity check (CPU/memory status)
- Process anomaly detection
  - Dynamic integrity check (Code flow control)
  - Dynamic integrity check (App whitelisting)
- Network anomaly detection
  - IP/timing frequency/bandwidth
- System vulnerability scanning

**System protection**
- Network and data protection
  - CMS / KMS
- Self protection (system hardening)
  - Application whitelist (Access control)
  - Host IPS (Virtual path)
- Storage protection
  - Anti-malware (VSAPI)

Figure 10. Trend Micro full-range Secure Endpoint features block

To fit in the device life cycle, Trend Micro works with platform providers to focus on the device initialization stage and operation stages. Edge SDK provides two main features:

1. **Risk assessment**
2. **System protection against hacking and intrusion across the IoT device lifecycle**

![Trend Micro focus](image)

**Trend Micro focus**
- Reduced attack surface
- Health/risk check
- Block attack attempts

![Platform provider](image)

**Platform provider**
- Secure boot
- Firmware integrity check

![Boot up](image)

**Boot up**
Device is loading up the firmware and starts to work as defined.

![Initialization](image)

**Initialization**
Boot up completed; system will read configuration, establish connection or sync up data.

![Operation](image)

**Operation**
Device performs its designed purpose continually.

![Update](image)

**Update**
New firmware arrives; device reboots and then starts to load new firmware.

Next cycle

Figure 11. Trend Micro focus in IoT device life cycle
TREND MICRO™
Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers’ and partners’ needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.