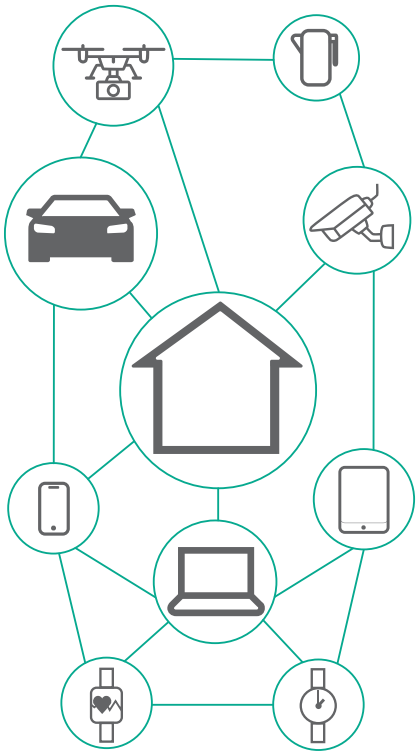
Kaspersky®
IoT Security

# Security as a priority for IoT development

Then there is the industrial internet of things (IIoT), which can form the basis of an urban ecosystem or an industrial facility. Cybercriminals gaining access to systems controlling traffic, street lighting, water supplies and sewerage, emergency notifications, air quality, fire safety and automatic deliveries could lead not only to financial losses running into millions of dollars but also damage the environment, be harmful to people's health or even fatal.



In the modern world, we are surrounded by billions of devices from the internet of things (IoT). Industrial robots and refrigerators that can order food, self-driving cars or a home that identifies ways to save electricity – all of these are now a reality.

Security solutions have usually been associated with protecting personal data. But now, in the IoT age, security is necessary to preserve personal space, the right to confidentiality and privacy and sometimes to protect the health and even the lives of ordinary citizens. Threat actors remotely connecting to surveillance cameras, taking control of smart homes, deactivating or disabling the autopilot in a car, stealing someone's identity and/or personal data, and hacking wearable medical devices such as pacemakers are just some of the threats that IoT users have already encountered or may encounter in the future.

At the same time, the internet of things and its related technologies have already become an integral part of modern society. The IoT provides tremendous opportunities for the development of device manufacturing, including hardware and software, telecommunication services as well as the integration market. A lack of trust in IoT solutions among end users, however, could block or seriously hamper implementation of these opportunities. That's why comprehensive security of IoT solutions should be a priority for all parties interested in its development.

## Threats to the internet of things

In late 2016, a successful attack was launched against the home routers of a European provider. The culprit was a specifically developed version of the Mirai worm that turned the compromised devices into an army of bots which then participated in major DDoS attacks[1]. (One such attack was launched against the DNS provider Dyn and led to disruptions in the operation of Twitter, Amazon, Spotify, GitHub, CNN, Netflix and Visa services in 2016.) A year later, a more sophisticated worm called IoTroop/Reaper became widespread. In early 2018, an international botnet consisting of MikroTik, Ubiquity, Cisco, ZyXEL, TP-Link routers, web cameras, smart TVs and other IoT devices attacked several companies in the financial sector; all these devices were allegedly infected with IoTroop/Reaper. More than 13,000 devices from 139 countries around the world participated in the attack[2,3]. According to analysts, IoTroop/Reaper is capable of infecting over a million devices[4].

Having analyzed the incidents associated with the Mirai and IoTroop/Reaper attacks, we have concluded that users had no idea their home devices had been compromised and were part of a huge botnet.

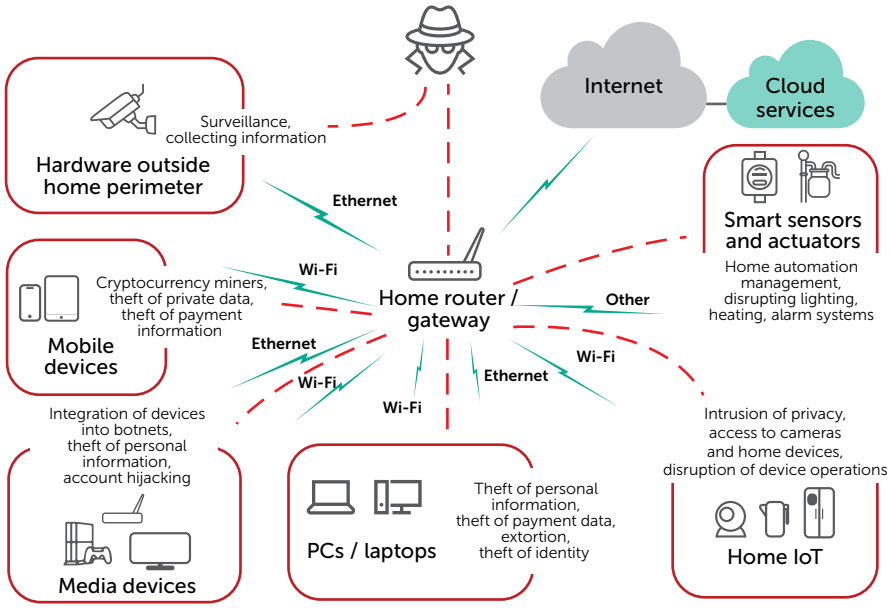
The manufacturers of IoT endpoints and telecommunication equipment often ignore the basic principles of cybersecurity: hardware does not control firmware integrity, devices are provided with preset passwords, including administrator passwords, network security configurations are weak, while obsolete and/or vulnerable software versions are used. Device software is not always updated, meaning devices run for years without updates and remain vulnerable to cybercriminal activity. It's just a matter of time before these devices are attacked.

So, strange as it may seem, the main source of threats to the IoT is the IoT itself – its complex infrastructure and technologies combined with its rapid development.

1 https://securelist.com/ddos-attacks-in-q4-2016/77412/
2 https://www.recordedfuture.com/mirai-botnet-iot/
3 https://www.securityweek.com/financial-services-ddos-attacks-tied-reaper-botnet
4 https://research.checkpoint.com/iotroop-botnet-full-investigation/

It's worth noting that users are often unaware of the network activities of certain home networked devices such as TVs, baby monitors, washing machines, etc., with users assuming they are only connected to the service provider's servers, e.g., their TV only has access to the digital TV or streaming provider. However, in reality devices often connect to several other servers so they can send and receive telemetry, process voice commands, receive updates, etc.

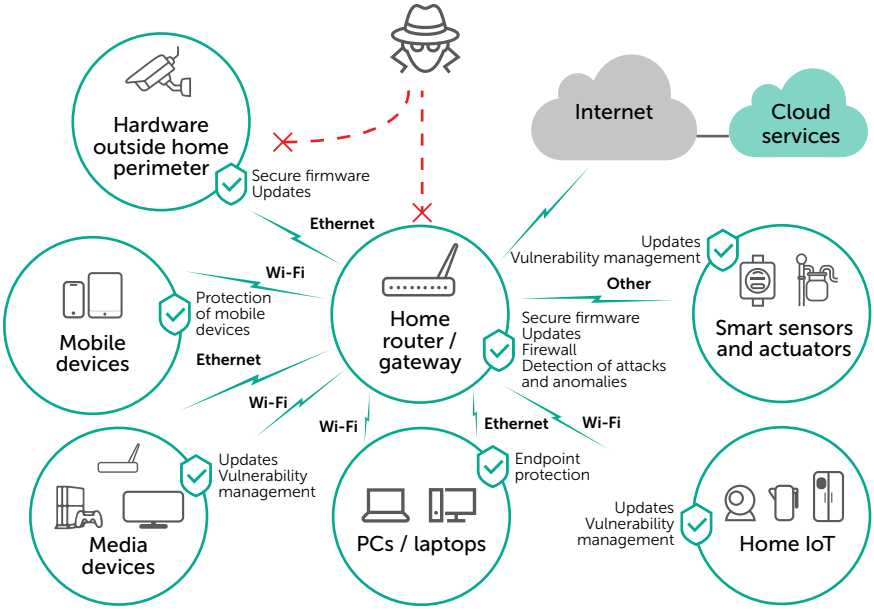
The complexity of IoT infrastructure provides ample opportunities to carry out various types of attacks. Data sent by threat actors can be easily concealed in the large number of network requests; when a device or a service implements a large number of features, there is a very good chance some of them may turn out to be vulnerable.




## Who's responsible for protecting the internet of things?

Concerted efforts by the following parties are required to ensure a secure IoT:

- End device manufacturers;
- Telecom device manufacturers;
- Vendors of the basic hardware for IoT and telecom devices;
- Telecom service providers;
- Application service providers in the IoT sphere;
- System integrators working in the sphere of IoT and connected devices.




The business needs of all the aforementioned parties mean they have an interest in the secure and predictable behavior of endpoint devices. The more that each party works to maintain the consumer's trust in the quality of their solutions and services, the more reliable the implementation of endpoint devices.

Trust is based on guarantees that the vendor – be it of a solution, part of a solution or an integrator – is making an effort within their area of responsibility to avoid incorrect behavior by devices and to prevent attacks against IoT infrastructure. This sort of vendor has a solid reputation which, in the long run, will help them retain and secure the corresponding segment of the market.

**Kaspersky OS**

KasperskyOS is based on a reliable microkernel that implements the only way of communicating. This lightweight microkernel can be used on various platforms. Application design is based on a component model that makes secure development easy and elegant. KasperskyOS is designed with security in mind and remains secure during its whole lifecycle.

**KSS for Linux:**

- Provides the means to implement a security policy relevant to an application area;
- Encloses applications in Linux containers;
- Provides communication channels between those containers;
- Manages containers, secures communication channels and enforces preconfigured security policies;
- Provides a set of ready components, such as secure service to remotely manage the system, audit/logging, secure storage;
- Can be extended to a customized security policies mode;
- Provides the means to securely update core KSS/ Linux components: crypto libraries, certificates, keys and other security-related data (it can also be integrated with a full device firmware update).

**Secure Boot**

Secure Boot starts at the device boot stage before the operating system. Secure Boot checks the digital signature of the firmware to be booted. If the digital signature is correct (issued by a trusted source and the firmware is not modified), Secure Boot starts decrypting the firmware image. Successful decryption means the image was encrypted using the trusted key pair. If both steps were completed successfully, the firmware image will boot. If one of the steps fails, Secure Boot will try to boot the previous firmware image or switch to maintenance mode.

**Secure Update**

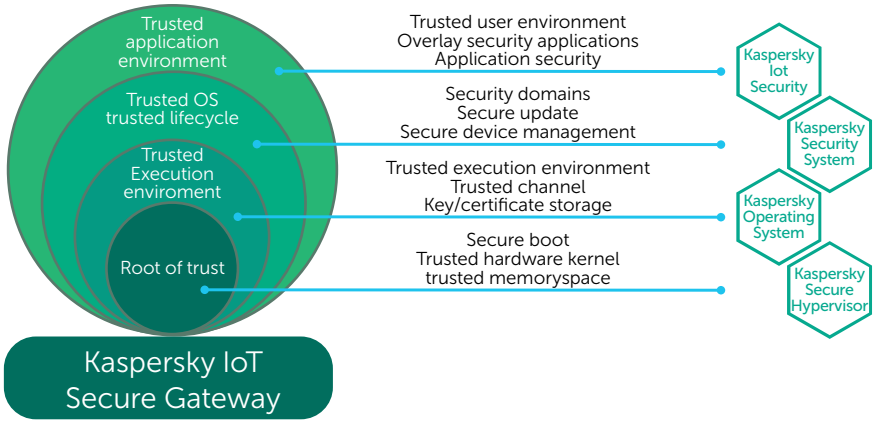
It works as follows:

1. Management console issues download command
2. Update downloader retrieves update image
3. Downloader stores the image in temporary update storage and seals it.
4. Data from storage is passed to data verifier
5. Verifier checks image and authorizes it if it passes check
6. Authorized image goes to updater

# Trusted internet of things

## Device-level trust

Assuring secure operation of IoT devices is based on a chain of trust. The initial point of trust is chosen depending on the required level of security assurance; where top-level assurances are required, it is chosen at the hardware level. With Kaspersky Lab's technologies and solutions, a protected device can be built by implementing the root of trust at any level.




## Infrastructure-level trust

By using Kaspersky Security Network (KSN), Kaspersky Lab's intelligent cloud-based automated service for analyzing depersonalized data, we can not only detect incidents and anomalies in the customer's infrastructure but also, with the customer's consent, prevent them. These intelligent services provide an instant response and protection from the very latest threats emerging anywhere in the world. Another advantage is that all Kaspersky Lab products can be united into a single control and management system, reducing maintenance and hardware expenses, as well as hardening the security of devices using other Kaspersky Lab products (endpoint protection, protection against advanced threats and targeted attacks, industrial protection, management of security threats, etc.). All this ensures a secure and reliable infrastructure where the risk of cyberthreats is minimal.

# Kaspersky Lab technologies for IoT device protection

**Kaspersky OS**
KasperskyOS is a secure operating system for embedded connected devices with specific cybersecurity requirements. KasperskyOS creates an environment where a vulnerability or bad code is no longer a big deal.

**Kaspersky Security System**
Kaspersky Security System (KSS) is a security policy verdict computation engine. It works in conjunction with KasperskyOS (or can be embedded into Linux-based firmware) that enforces KSS verdicts.

**Secure Boot**
Secure Boot allows an IoT device to verify the integrity and authenticity of the firmware image before booting using cryptographic methods. It can utilize secure hardware key storage and detect whether the firmware image is damaged or altered.

**Secure Update**
Secure Update uses cryptographic methods to ensure the integrity and authenticity of firmware updates. The Secure Update feature works together with Secure Boot and ensures firmware is only updated from correctly signed and encrypted images from trusted sources.

### Web filtering

Kaspersky Web Filter is a technology which provides protection from phishing, malicious websites and inappropriate content.

With Kaspersky Web Filter you can classify websites according to dozens of pre-defined categories, allowing you to:

- Protect users and the network by blocking phishing and malicious websites
- Control web usage and reduce corporate traffic
- Increase employee productivity: reduce the time spent on non-work-related activity by restricting access to non-productive sites such as social networks and online games
- Enforce parental control for children by blocking inappropriate content

### Parental control

Parental control makes it possible to track a child's online activity, protect them from undesirable contacts, block access to inappropriate content and games, manage app downloads, supervise communications on social media and prevent undesirable third-party access to the child's private data.

### Machine Learning-based protection

ML protection utilizes not only the gateway system resources but also uses Kaspersky Security Network Cloud ML to learn fast and make split-second decisions. The decisions are also based on the experience of other devices and services using Kaspersky Lab products.

ML features enable operation with both raw traffic and the values extracted from it that characterize the device's physical behavior.

### Secure Audit

Secure Audit is a Kaspersky OS feature called to recognize, record and store audit logs and provide guarantees that log entries cannot be altered. Secure Audit can utilize blockchain technology for distributed and secured log management.

### Linux Application Control

Before executing a new binary file, Application Control calculates its hash and connects to Kaspersky Security Network to receive the reputation trust level and security recommendations for the application. If the hash matches malicious code in KSN Database, Application Control will prevent the code from executing on the device. This technology can prevent infections of IoT devices with malware like Mirai or Bashlite and can be used on devices running Linux-based operating systems.

### Web filter/Parental control

Depending on the device's intended use, web filtering (corporate or industrial devices) or parental control (personal devices) technologies can be added to its firmware.

### Machine learning-based protection

To ensure customer networks are protected in the best possible way, we designed the Machine Learning (ML) protection mechanism, which can also be implemented in network devices (gateways or routers). ML is used to discover all network devices via passive and active analysis, understand their behavior, make a profile of each device and detect when something in the network is not functioning as intended. For example, ML can detect when a device has been hacked or is infected by malware and tries to send unusual data, or normal data to an unusual destination. ML technologies also make it possible to detect stealth malicious activity and data transfers concealed in normal traffic.

### ML asset discovery

ML-based asset discovery technology can discover, categorize and organize all the assets in the protected network automatically. Using special fingerprint technology, our solution detects the type of device, maker's name and model (and even firmware version) by simply analyzing specific parts (metadata) of the network traffic

### ML device behavior analysis

Once assets in the network are discovered and categorized, a specific profile is created describing the overall (healthy) network behavior of the asset. Such profiles describe how a specific device with the current firmware is behaving in the customer's network.

### ML anomaly detection

The use of ML-based asset discovery and device profiling technologies help detect any anomaly in IoT/IIoT devices. ML-based anomaly detection logs malware and botnet activities, the device's involvement in DDoS attacks, firmware exploitation, mining activities, device hijacking, etc.

## Conclusion

Kaspersky Lab's technologies make it possible to build a secure internet of things, irrespective of whether the device and firmware are designed from scratch or security features need to be integrated into existing software components. Kaspersky Lab's solutions can be customized to the customer's specific software and hardware platform. With Kaspersky Lab technologies, telecom providers and manufactures of IoT and IIoT devices can build secure solutions that fully comply with the business needs and security requirements of today's threat landscape

**www.kaspersky.com**



KasperskyOS®-based products: os.kaspersky.com/products/
Kaspersky Lab, Moscow, Russia: www.kaspersky.com
Cyber Threats News: www.securelist.com

#kasperskyos
#truecybersecurity