Protection of the internet of things in smart cities based on Kaspersky Cyber Immunity approach

Kaspersky IoT Infrastructure Security

The smart city concept involves the integration of multiple information and communication technologies. These include systems for the internet of things (IoT) that manage municipal infrastructure, such as transportation, healthcare, residential and public utilities, and security systems. Implementation of the smart city concept enables real-time analysis of data collected from thousands of residential and non-residential facilities. This reduces resource consumption, optimizes the cost of maintaining utility systems and makes it possible to communicate with residents in near real time.

This increased level of automation and rapid integration of information technologies in municipal infrastructure substantially increases the risks associated with cyberattacks on city facilities. To mitigate these risks, Kaspersky offers **Kaspersky IoT Infrastructure Security**, a comprehensive solution for building secure smart city systems.

kaspersky

KasperskyOS

Cloud-based management system tasks

- Remote monitoring of residential meters and utility systems
- Optimization of system maintenance costs
- Reduction in resource consumption
- Improved response time to accidents and incidents
- Quality control of residential and public utility maintenance

Municipal cloud-based management system

It is practically impossible to manually gather and analyze data received from several thousand residential and non-residential facilities without a cloud-based management system. Without a platform for the centralized collection of data from these facilities, they cannot be efficiently managed and there is no way to get an accurate picture of the city-wide status of public utilities.

A solution that enables a unified control platform is based on technologies of the internet of things. Each year these technologies are being used more and more actively in city infrastructures, and this hasn't gone unnoticed by cybercriminals.

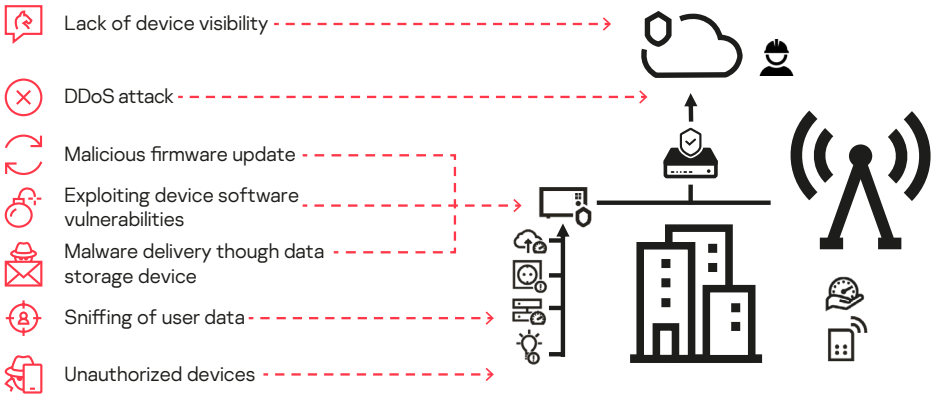
The importance of smart city infrastructure security

Smart cities are evolving faster than the tools used to protect them, thereby leaving a large gap for cybercriminals to exploit. Unfortunately, the development of unified standards for cybersecurity of the internet of things is still in its infancy. Meanwhile, the market is being constantly bombarded with more and more new IoT solutions, many of which don't even meet basic information security requirements.

The threat model typical for the internet of things is also applicable to a smart city infrastructure.

On-site sensors and controllers provide:

- Collection of power supply data: phase voltage, current frequency, current strength
- Collection of water supply data: hot/cold water consumption, temperature and pressure in water pipeline
- Collection of heat supply data: heat-transfer fluid temperature upstream and downstream of automated control node, heat-transfer fluid temperature upstream of consumer supply point, thermal energy consumption
- Collection of climate control data in building entrances: temperature, lighting, humidity, CO2 level, noise level
- Operation of elevators, opening of shaft doors
- Operation of intercom systems
- Triggering of fire alarm systems
- Triggering of access control systems



The functioning of critical municipal structures and the many human lives reliant on them may depend directly on the security of the internet of things. For example, if a hacker is able to gain access to a fire alarm system, first responders may not be notified of a fire in time.

Implementation details

A number of monitored sensors are deployed at each facility. Most of the sensors transmit data via the Modbus RTU protocol with an RS-485 interface.

Hot/cold water supply sensors transmit data via the LoRa wireless protocol.

Data from the access control system (ACS) sensors is transmitted to the controller through a digital input/output (DI/DO) module.

After the data is collected by the controller, KISG 1000 enables secure data transfer to the cloud over a GSM channel.

Administration of all gateways within the network is carried out with the help of Kaspersky Security Center.

Solution

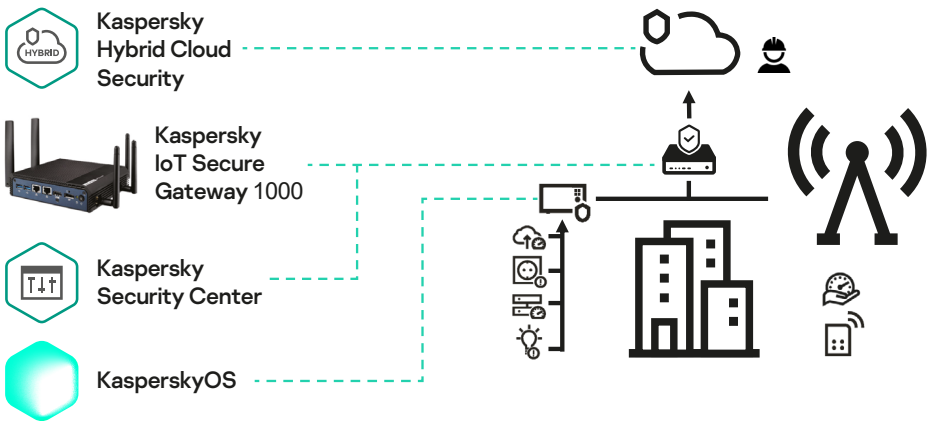
A residential building is equipped with systems that monitor the consumption of resources and manage electricity and water supply. The meters inside apartments are connected over the wireless protocol known as LoRaWAN. Physical security of the systems is provided through remote-access video surveillance systems, physical locks, motion detectors and door sensors. Information security is provided by Kaspersky solutions.

Kaspersky IoT Secure Gateway (KISG) 1000 is a Cyber Immune gateway based on the secure **KasperskyOS** operating system. It not only has its own built-in protection against cyberattacks but also helps to ensure the security of the entire IoT infrastructure. The Kaspersky Security Center platform is used to centrally manage and monitor KISG 1000 events. Together, these two products form the comprehensive solution **Kaspersky IoT Infrastructure Security**.

Controllers running **KasperskyOS** are installed as PLCs in the control center platform.

At the cloud level, protection is provided by **Kaspersky Hybrid Cloud Security**. This is an integrated solution that provides automated protection of hybrid cloud infrastructure and prevents vulnerabilities (including zero-day threats) from being exploited by malware.

Kaspersky's approach to IoT security



Kaspersky Cyber Immunity is a new approach to developing inherently secure solutions based on KasperskyOS. These solutions are protected from the majority of cyberattacks, including those that are currently known as well as future attack threats, and will perform their critical functions even in hazardous environments.

KasperskyOS is an operating system that is employed in areas with high security requirements, such as smart cities, transportation, industry, electric power sector, the public sector and others. It helps ensure the confidentiality and integrity of data and protects against data spoofing.

Functions of Kaspersky IoT Secure Gateway 1000

Data gathering	Gateway protection	IoT infrastructure protection	Monitoring
Aggregate data collected from sensors and transmit it over cellular networks and Ethernet. Work with cloud systems using the MQTT protocol.	Security at the operating system kernel level. Safe downloading and updating.	Firewall for protection against unauthorized access. Intrusion detection and prevention technology (IDS/IPS).	Detection and categorization of devices. Notification of the administrator when new devices are connected.

Roles of KISG 1000 in the protection of video surveillance systems

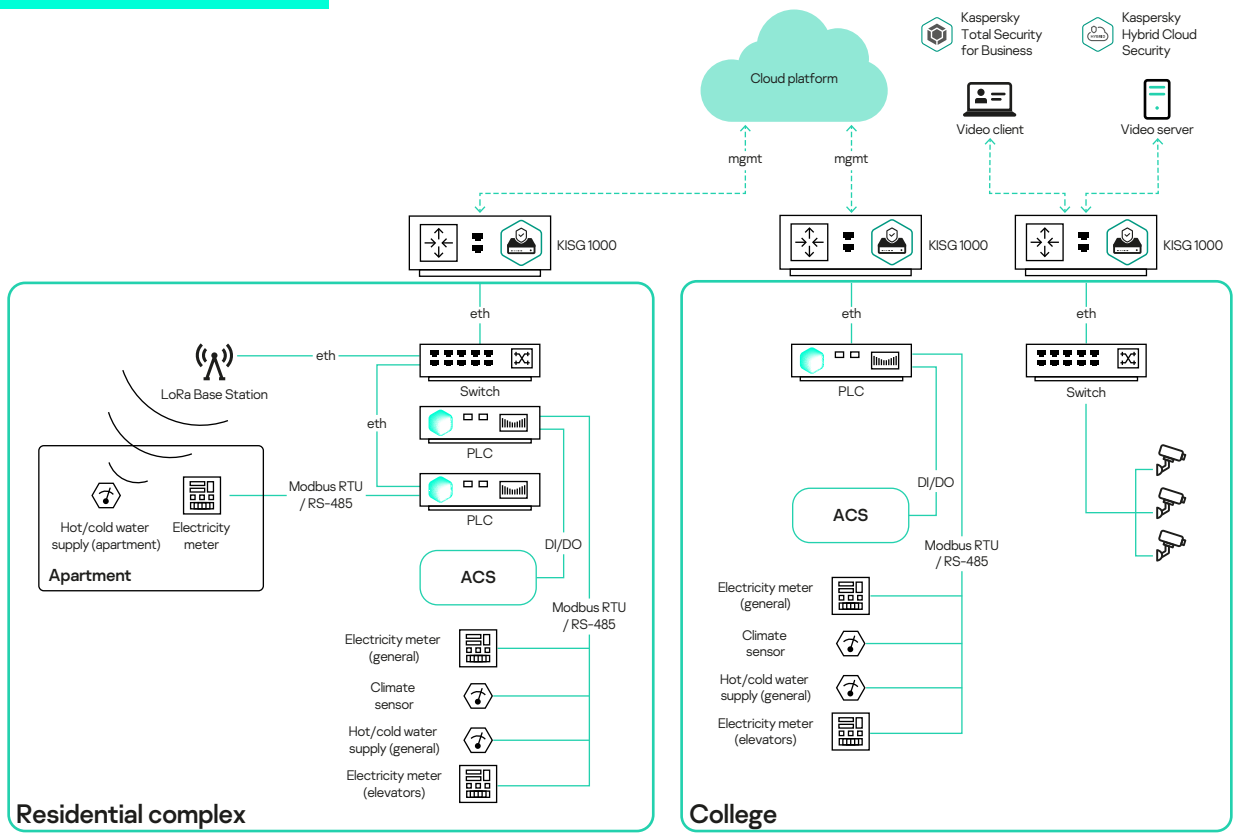
- Blocks all unauthorized interactions between the video server and cameras
- Prevents attacks launched from cameras
- Blocks attempts to attack cameras from a video server or video client
- Provides notifications when an unauthorized device appears in the local network (which could also indicate a camera has been replaced)
- Provides notifications if a camera is disabled

In a smart city infrastructure, video surveillance systems perform security and monitoring functions. State-of-the-art video cameras are smart and highly functional devices that are also vulnerable to hacker attacks just like other devices on the internet of things.

The Kaspersky approach to protecting local and cloud-based video surveillance systems includes the following:

- **Kaspersky IoT Infrastructure Security**
  - **Kaspersky IoT Secure Gateway 1000**
  - **Kaspersky Security Center**
- **Kaspersky Hybrid Cloud Security**
- **Kaspersky Total Security for Business**, a protective solution not only for endpoints and servers, but also for other nodes of the corporate network

Protection of smart city systems with Kaspersky technologies



KasperskyOS

Kaspersky IoT Infrastructure Security

Learn more on os.kaspersky.com

www.kaspersky.com