CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

IoT Security

Video summary

- What is IoT
- Elements of IoT Network
- Patching IoT Vulnerabilities
- IoT Security and Privacy Requirements
- MiniSec

The Internet of Things (IoT)

- IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors
  - IoT is a dominant theme enabling new forms of communication between people and things, and between things themselves
- The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system
- The IoT is primarily driven by deeply embedded devices
  - These devices are low-bandwidth, low-repetition data capture, and low data-usage appliances that communicate with each other and provide data via user interfaces
  - Embedded appliances, such as high-resolution video security cameras, video VoIP phones, and a handful of others, require high-bandwidth streaming capabilities

Evolution

With reference to the end systems supported, the Internet has gone through roughly four generations of deployment culminating in the IoT:	Information technology (IT)	PCs, servers, routers, firewalls, and so on, bought as IT devices by enterprise IT people, primarily using wired connectivity
	Operational technology (OT)	Machines/appliances with embedded IT built by non-IT companies, such as medical machinery, SCADA, process control, and kiosks, bought as appliances by enterprise OT people, primarily using wired connectivity
	Personal technology	Smartphones, tablets, and eBook readers bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity
	Sensor/actuator technology	Single-purpose devices bought by consumers, IT and OT people exclusively using wireless connectivity, generally of a single form, as part of larger systems

It is the fourth generation that is usually thought of as the IoT, and which is marked by the use of billions of embedded devices

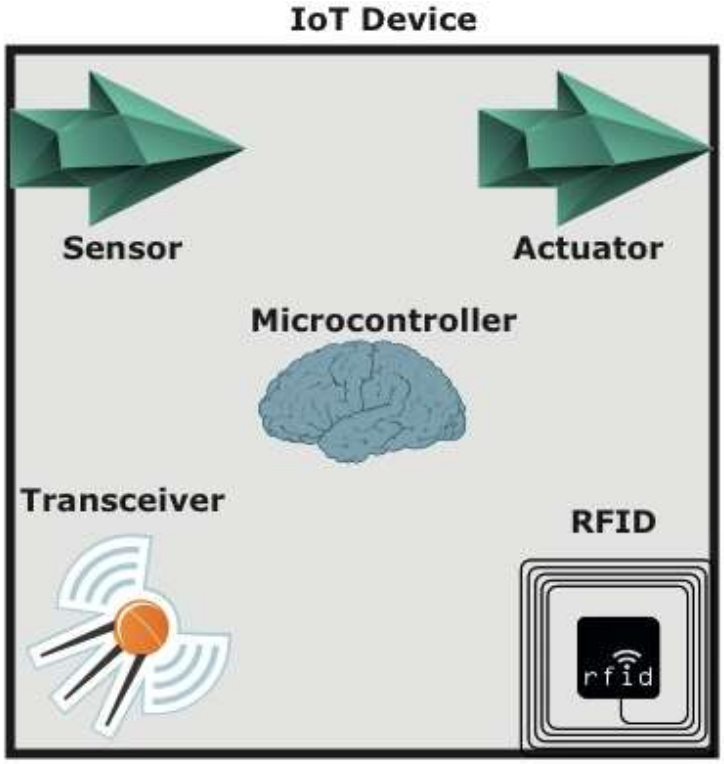


Figure 13.8 IoT Components

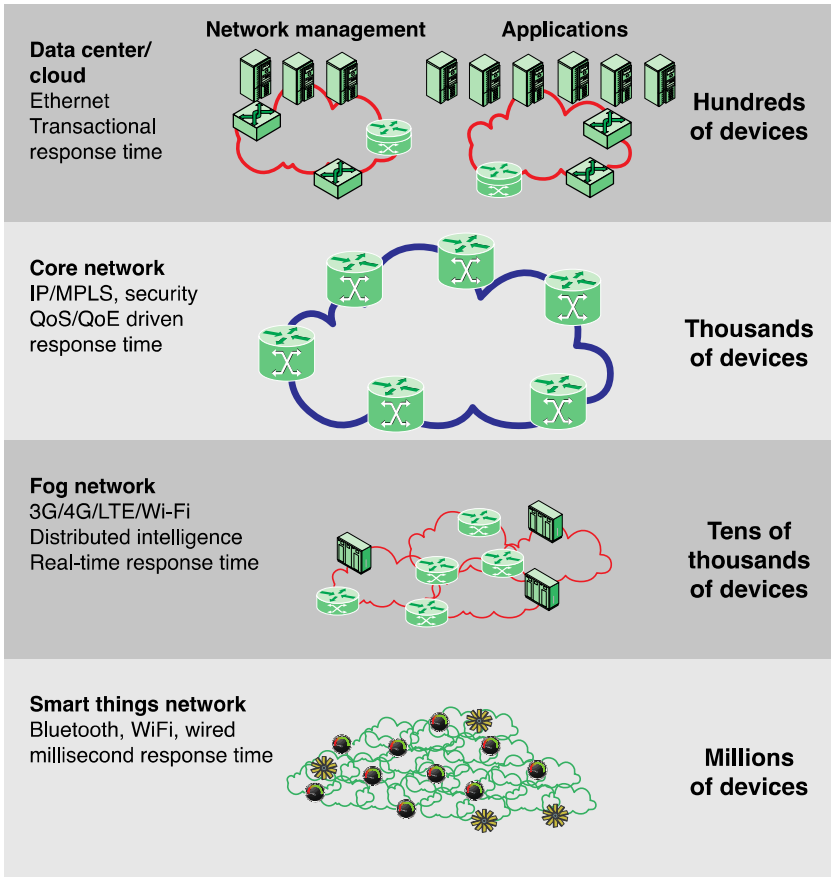


Figure 13.9 The IoT/Cloud Context

Fog

- ✓ The term *fog computing* is inspired by the fact that fog tends to hover low to the ground, whereas clouds are high in the sky

- ✓ Fog computing addresses the challenges raised by the activity of thousands or millions of smart devices, including security, privacy, network capacity constraints, and latency requirements

Fog

- In many IoT deployments, massive amounts of data may be generated by a distributed network of sensors
- Rather than store all of that data permanently in central storage accessible to IoT applications, it is often desirable to do as much data processing close to the sensors as possible
- The purpose of what is sometimes referred to as the edge computing level is to convert network data flows into information that is suitable for storage and higher-level processing
- The following are examples of fog computing operations:

Core

- The *core network,* also referred to as a *backbone network,* connects geographically dispersed fog networks as well as providing access to other networks that are not part of the enterprise network
- Typically the core network will use very high-performance routers, high-capacity transmission lines, and multiple interconnected routers for increased redundancy and capacity

	Cloud	Fog
Location of processing/storage resources	Center	Edge
Latency	High	Low
Access	Fixed or wireless	Mainly wireless
Support for mobility	Not applicable	Yes
Control	Centralized/hierarchical (full control)	Distributed/hierarchical (partial control)
Service access	Through core	At the edge/on handheld device
Availability	99.99%	Highly volatile/highly redundant
Number of users/devices	Tens/hundreds of millions	Tens of billions
Main content generator	Human	Devices/sensors
Content generation	Central location	Anywhere
Content consumption	End device	Anywhere
Software virtual infrastructure	Central enterprise servers	User devices

Table 13.4
Comparison of Cloud and Fog Features

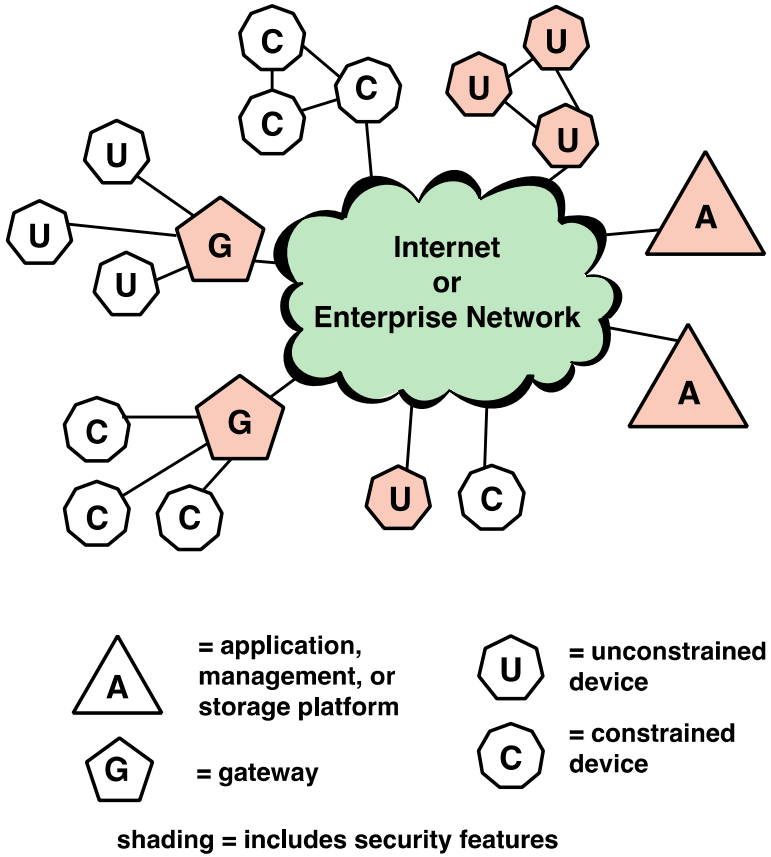
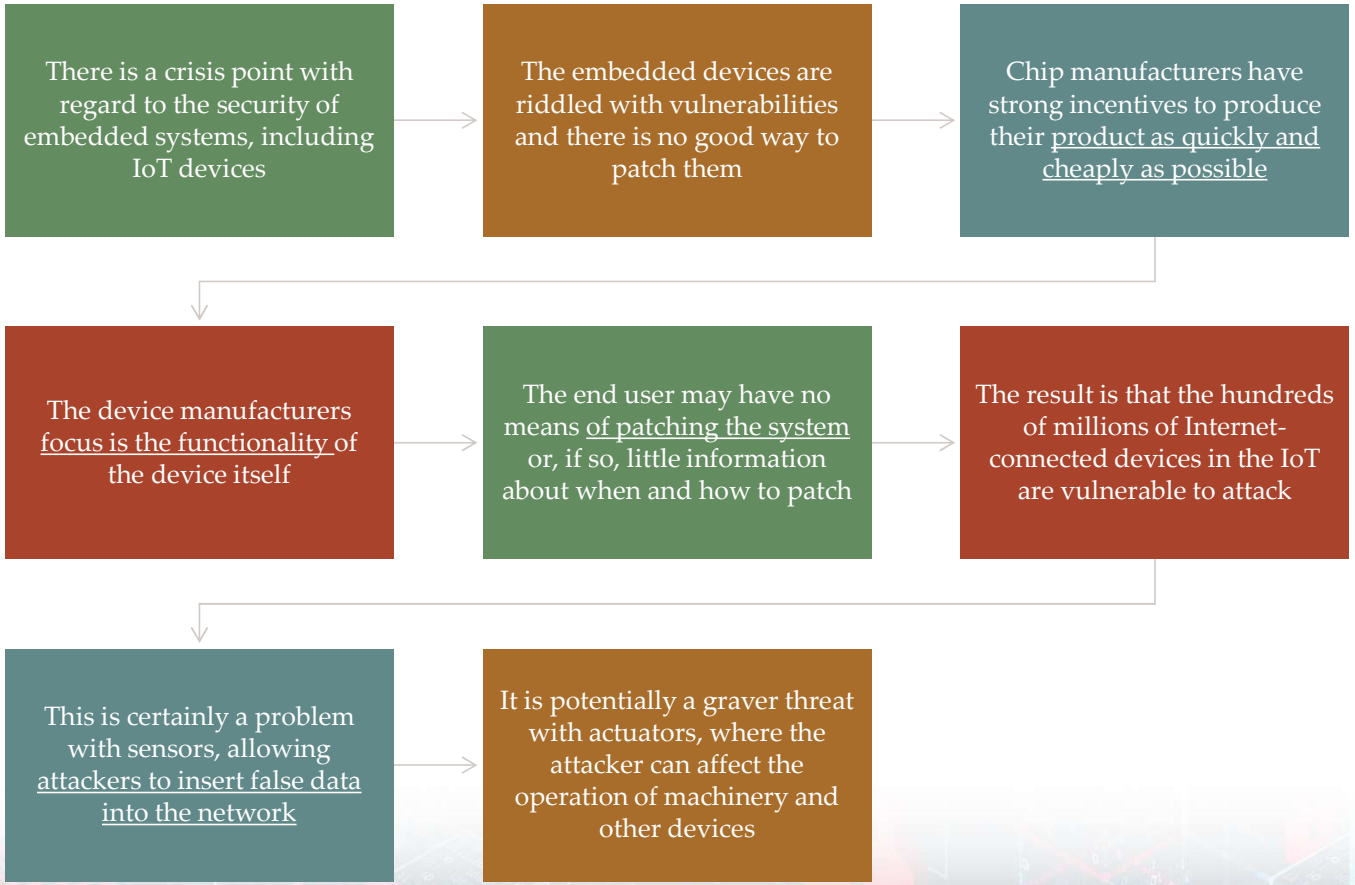


Figure 13.10 IoT Security: Elements of Interest

Patching Vulnerability



IoT Security and Privacy Requirements

- ITU-T Recommendation Y.2066 includes a list of security requirements for the IoT

- The requirements are defined as being the functional requirements during capturing, storing, transferring, aggregating, and processing the data of things

- The requirements are:

  - ✓ Communication security
  - ✓ Data management security
  - ✓ Service provision security
  - ✓ Integration of security policies and techniques
  - ✓ Mutual authentication and authorization
  - ✓ Security audit

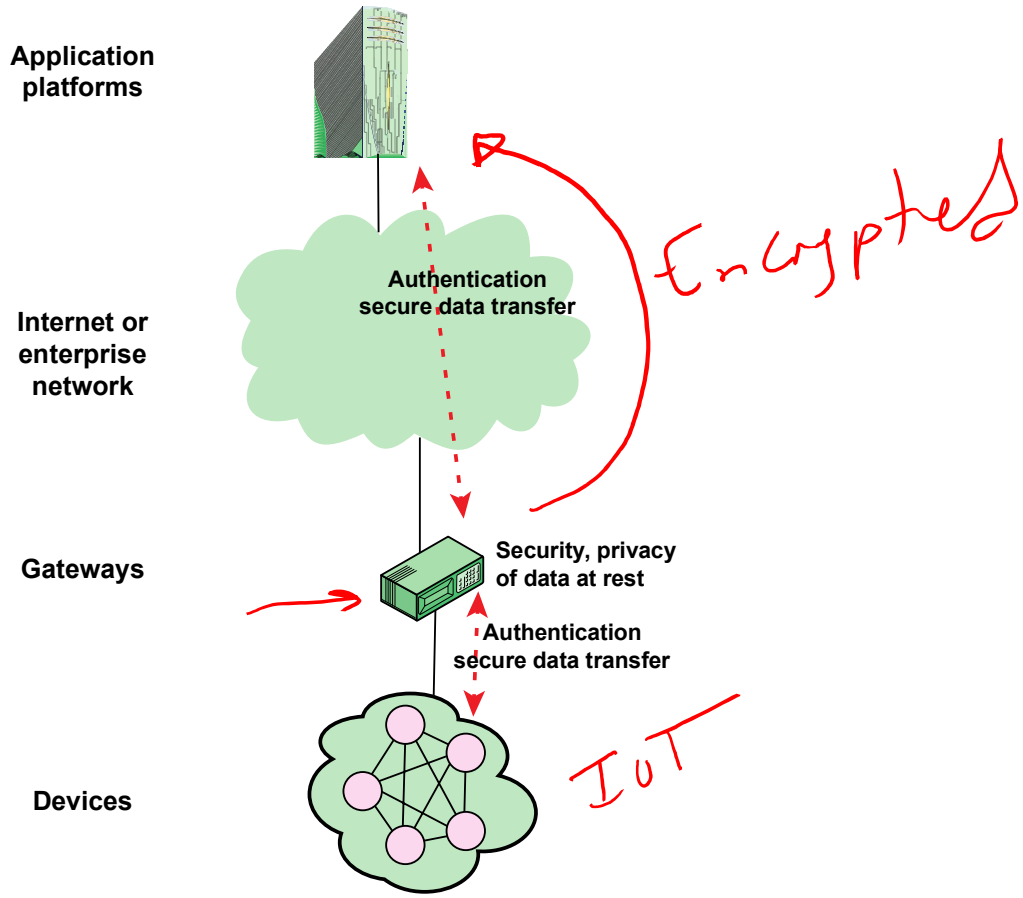


Figure 13.11 IoT Gateway Security Functions

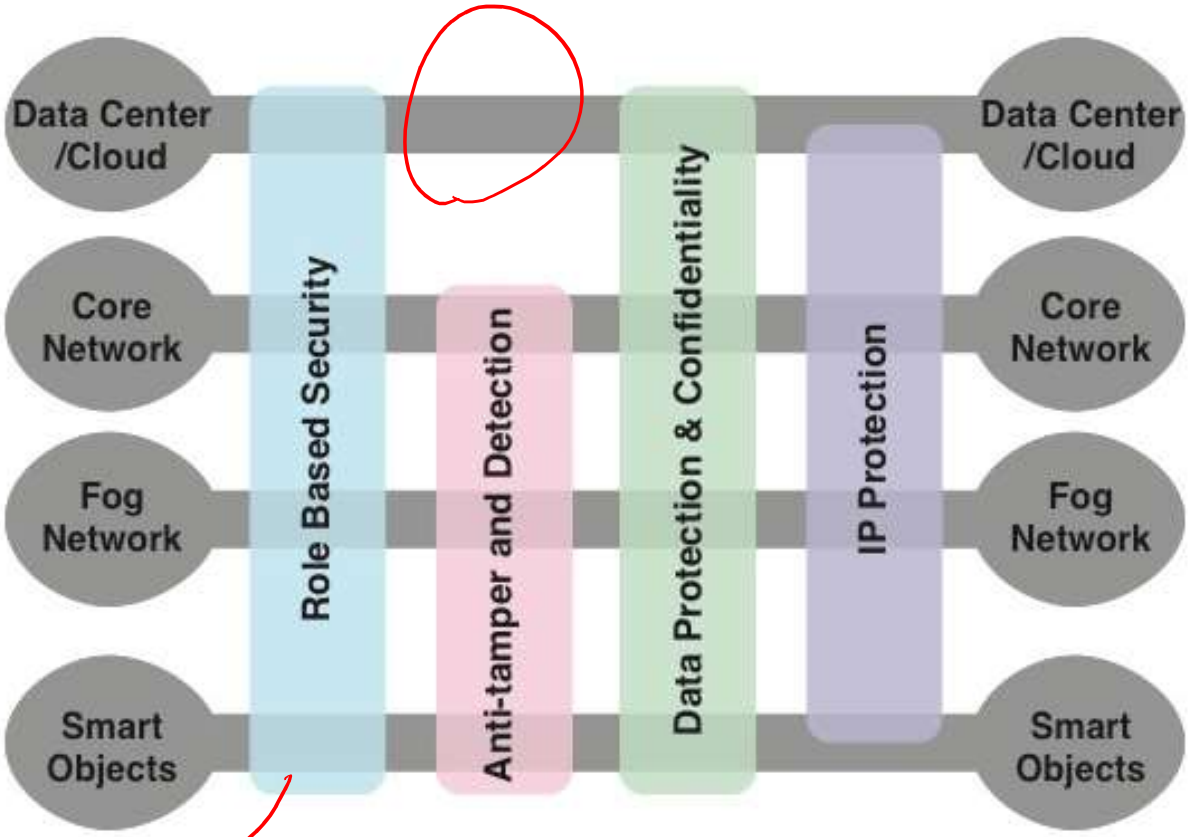


Figure 13.12 IoT Security Environment

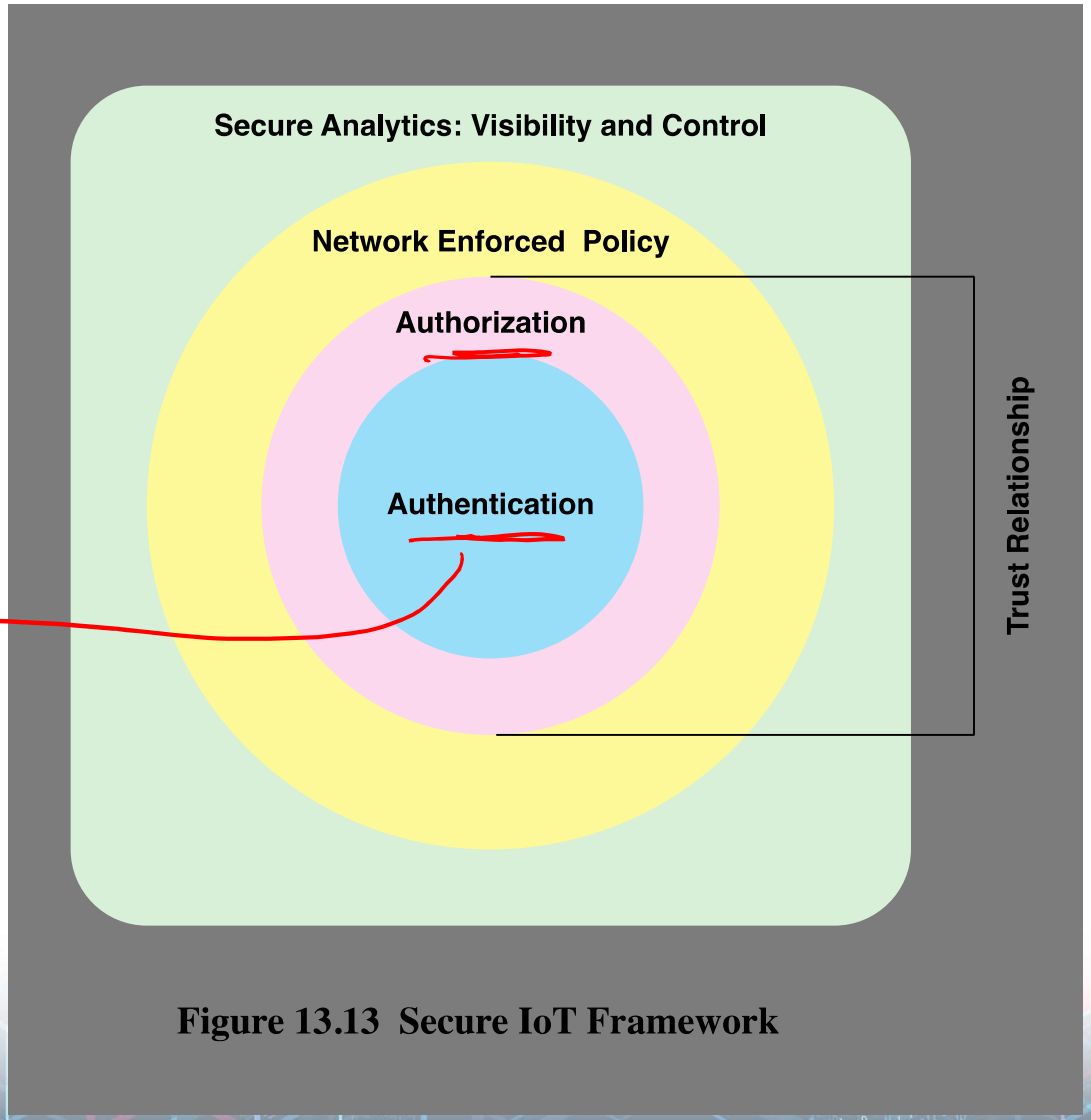


Figure 13.13 Secure IoT Framework

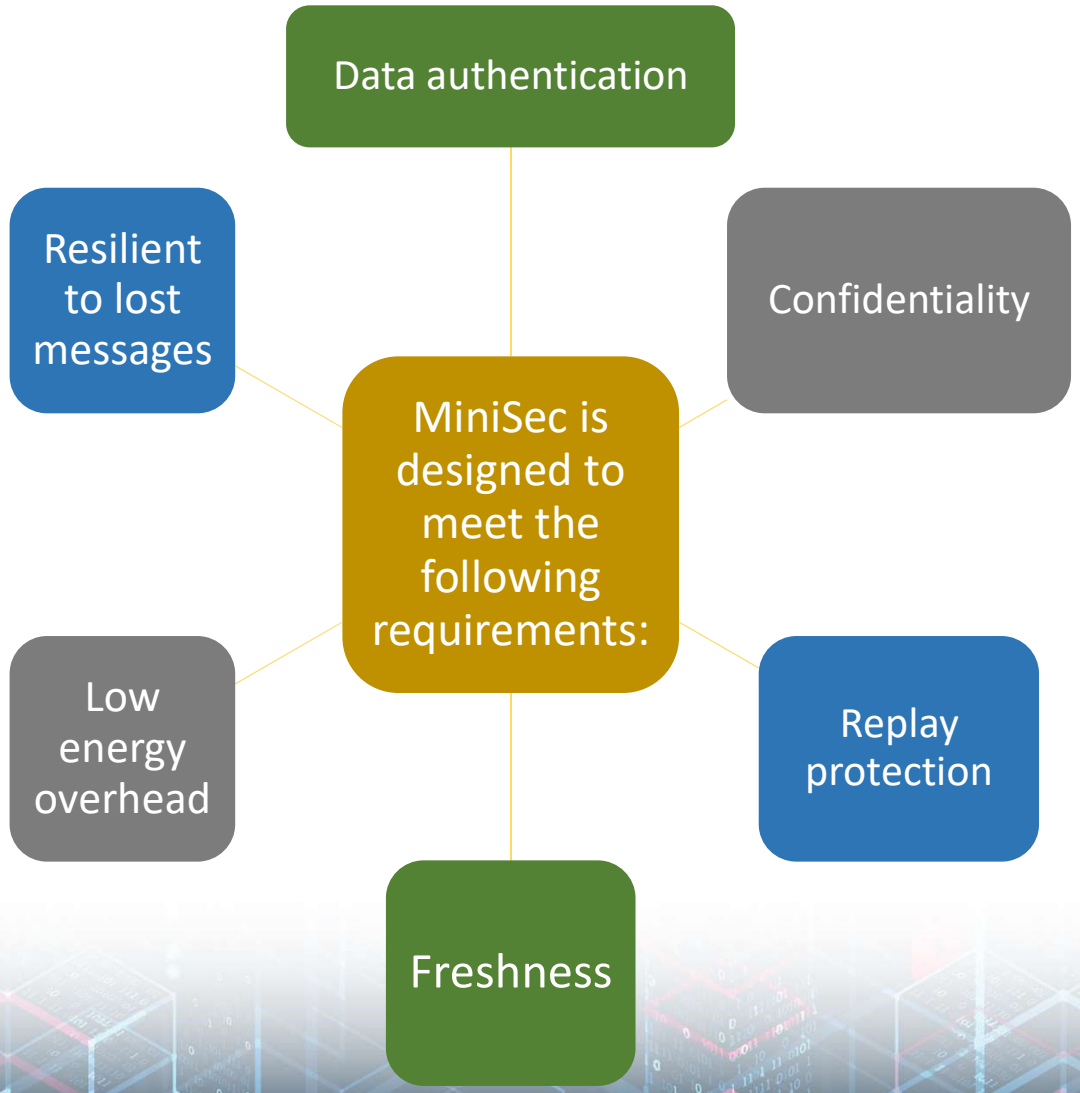
MiniSec

- MiniSec is an open-source security module that is part of the TinyOS operating system

- It is designed to be a link-level module that offers a high level of security, while simultaneously keeping energy consumption low and using very little memory

- MiniSec provides confidentiality, authentication, and replay protection

MiniSec


Data authentication
Resilient to lost messages
Confidentiality
MiniSec is designed to meet the following requirements:
Low energy overhead
Replay protection
Freshness

Video summary

- What is IoT
- Elements of IoT Network
- Patching IoT Vulnerabilities
- IoT Security and Privacy Requirements
- MiniSec