Fakultas Informatika
School of Computing
Telkom University

Internet of Things

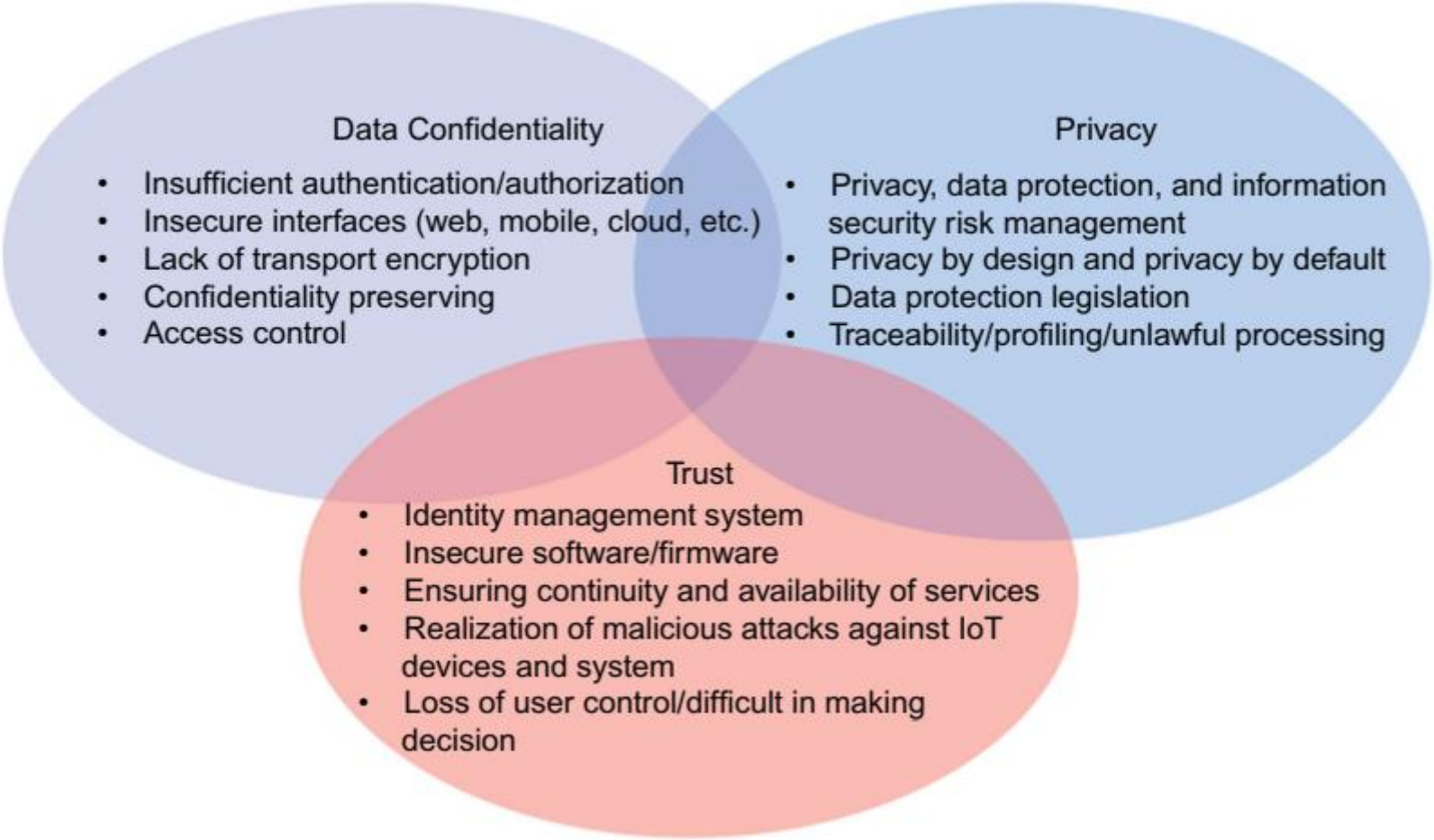
MATERI 11:
IoT Security

What we learn today ...

- Securing the Internet of Things
- Security and Vulnerability in the Internet of Things
- Security Requirements in Internet of Things

Securing the Internet of Things : Security Requirements

Securing the Internet of Things : Security Requirements



Securing the Internet of Things : Security Requirements

Table 1.1 Top Ten Vulnerabilities in IoT

Security Concerns	Interface Layer	Service Layer	Network Layer	Sensing Layer
Insecure web interface	√	√	√	
Insufficient authentication/ authorization	√	√	√	√
Insecure network services		√	√	
Lack of transport encryption		√	√	
Privacy concerns		√	√	√
Insecure Cloud interface	√			
Insecure mobile interface	√		√	√
Insecure security configuration	√	√	√	
Insecure software/firmware	√		√	
Poor physical security			√	√

Securing the Internet of Things

Security challenge in IoT are

- Authenticate to multiple networks securely;
- Ensure that data are available to multiple collectors;
- Manage the contention between the data access;
- Manage privacy concerns between multiple consumers;
- Provide strong authentication and data protection;
- Maintain availability of the data or the service;
- Allow for evolution in the face of unknown risks.

Secrecy and secret-key management

- The IoT devices communicate with other it has eavesdropping threat.
- Because IoT devices has many sensitive data, then secrecy needs to be held.
- The challenge :
  - Lightweight
  - Heterogeneous

Authentication and Authorization Devices

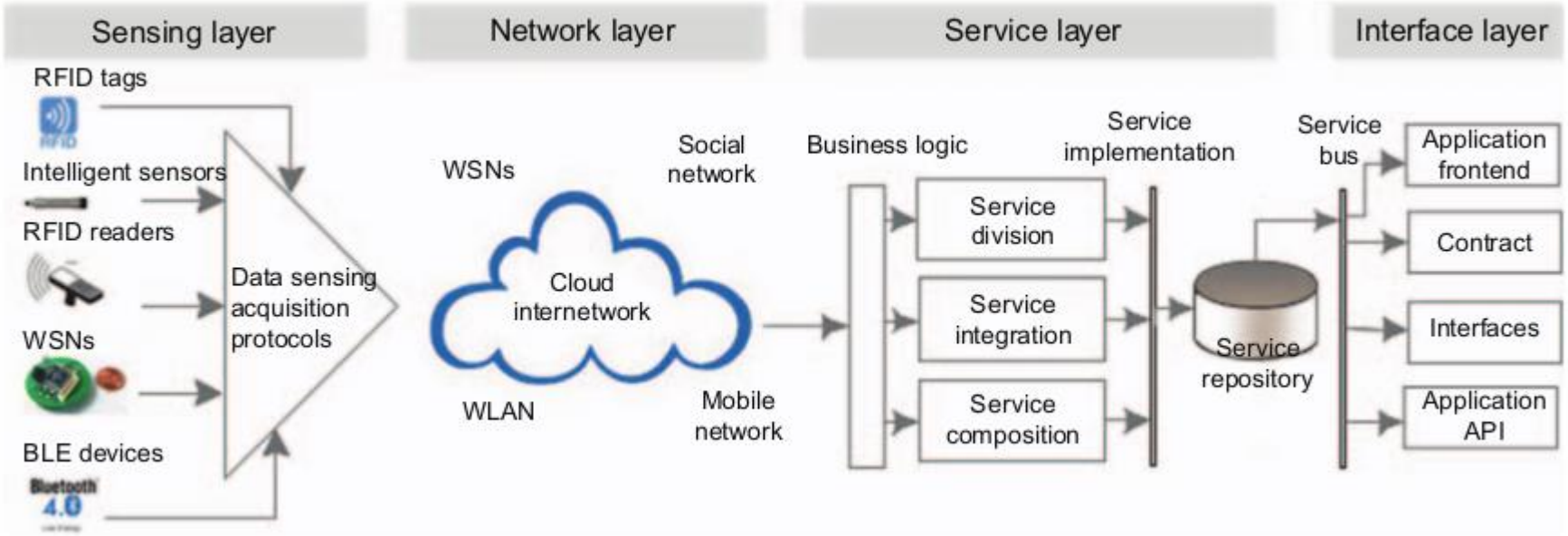
- Secure authentication provided to protect the potentially sensitive sensor data being shared over the IoT systems.
- Authentication commonly used :
  - one-way authentication
  - mutual authentication


ANY
QUESTIONS
?

Security Requirements in Internet of Things

IoT at least has four layer that has diffrent function

- Sensing layer is integrated with end components of IoT to sense and acquire the information of devices;
- Network layer is the infrastructure to support wireless or wired connections among things;
- Service layer is to provide and manage services required by users or applications;
- Application interfaces layer consists of interaction methods with users or applications.


Sensing layer
Network layer
Service layer
Interface layer
RFID tags
Intelligent sensors
RFID readers
WSNs
BLE devices
Data sensing acquisition protocols
WSNs
Social network
Cloud internetwork
WLAN
Mobile network
Business logic
Service implementation
Service division
Service integration
Service composition
Service repository
Service bus
Application frontend
Contract
Interfaces
Application API

Sensing Layer and End Node

Table 5.1 Security Threats and Vulnerabilities at IoT End-Node

Security Threats	Description
Unauthorized access	Due to physical capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker
Availability	The end-node stops to work since physically captured or attacked logically
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure
Denial of Services (DoS)	An attempt to make an IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Security Requirements in Internet of Things

Network Layer has requirements

- Privacy leakage;
- Communication security;
- Overconnected;
- MITM attack;
- Fake network message;
- Confidential compromise;
- Relay attack.

Security Requirements in Internet of Things

Network Layer has requirements

Table 5.3 Security Threats in Network Layer

Security Threats	Description
Data breach	Information release of secure information to an untrusted environment
DoS	An attempt to make an IoT end-node resource unavailable to its users
Public key and private key	The comprise of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path


ANY
QUESTIONS
?

Security Requirements in Internet of Things

Service Layer has requirements

- Authorization;
- Privacy leakage;
- Service abuses;
- Node identify masquerade;
- DoS attack;
- Replay attack;
- Service information sniffer and manipulation;
- Repudiation.

Service Layer has requirements

Table 5.5 The Security Threats in Service Layer

Security Threats	Description
Privacy threats	Privacy leakage or malicious location tracking
Services abuse	Unauthorized users access services or the authorized users access unsubscribed services
Identity masquerade	The IoT end-device, node, or gateway are masqueraded by attacker
Service information manipulation	The information in services is manipulated by the attacker
Repudiation	Denial of the operations have been done
DoS	An attempt to make an IoT end-node resource unavailable to its users
Replay attack	The attack resends the information to spoof the receiver
Routing attack	Attacks on a routing path

Security Requirements in Internet of Things

Application interface-layer has requirements

- Remote safe configuration;
- Integrity and confidentiality for transmission between layers;

Table 5.6 The Security Threats in Application–Interface Layer

Security Threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Misconfiguration at remote IoT end-node, end-device, or end-gateway
Security management	Log and keys leakage
Management system	Failure of management system


ANY
QUESTIONS
?

Fakultas Informatika
School of Computing
Telkom University

THANK YOU