

PERTEMUAN 6

INTERNET OF THINGS



Internet of Things



WHY IS IOT SECURITY SO IMPORTANT?

- Penelitian terbaru menunjukkan bahwa 90% konsumen kurang percaya pada keamanan di perangkat IoT.
- Sebuah survei tahun 2019 yang dilakukan di Australia, Kanada, Prancis, Jepang, Inggris, dan AS mengungkapkan bahwa 63% konsumen takut menggunakan perangkat yang terkoneksi.
- Pada tahun 2026, kita akan memiliki lebih dari 26 miliar perangkat yang terhubung di dunia.
- Permasalahan yang muncul terkait dengan kondisi tersebut
 1. Bagaimana Anda menjaga miliaran perangkat tetap aman?
 2. Bagaimana dengan jaringan yang mereka jalankan?
 3. Bagaimana Anda memastikan data dari semua perangkat itu tidak disusupi?

FACTORS IMPACTING IOT SECURITY

1. **Pengambilan keputusan berbasis data selalu membutuhkan data yang dapat diandalkan.** Keputusan penting terkait bisnis, keselamatan, dan kesehatan semakin didasarkan pada data. Untuk membuat keputusan yang tepat, data harus akurat dan aman.
2. **Perangkat yang berbeda memerlukan solusi yang berbeda.** Perangkat datang dalam berbagai bentuk dan bentuk. Beberapa perangkat memiliki kemampuan yang dibatasi dengan kemampuan yang sangat terbatas dan untuk perangkat tersebut metode keamanan tradisional tidak mungkin digunakan.
3. **Keamanan ekosistem edge to edge.** Di IoT, kesuksesan bergantung pada ekosistem kolaboratif penyedia jaringan produsen perangkat, penyedia platform, pengembang aplikasi, dan pengguna akhir. Memastikan keamanan ekosistem end-to-end sangat penting.

How to handle IoT security challenges



Determine what to include in your vulnerability and penetration testing efforts.



Understand which tools to use.



Look for both standard vulnerabilities (i.e., missing patches) and deeper ones (i.e., lack of encryption).



Choose how to document findings.

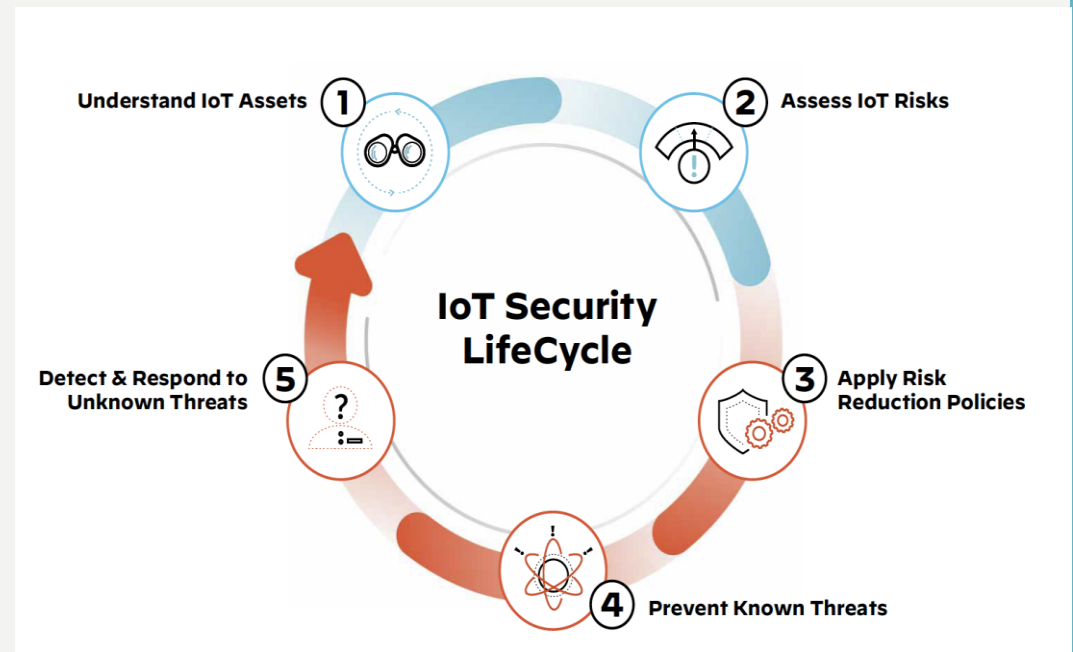
PROTECTING IOT SOLUTIONS ALONG LONG LIFECYCLES

Menurut Forbes, 4,1 miliar catatan terekspos oleh pelanggaran data pada paruh pertama tahun 2019 saja. Konsekuensi dari serangan siber dapat menghancurkan perusahaan dan menyebabkan hilangnya reputasi, pelanggan, dan pendapatan.



PROTECTING IOT SOLUTIONS ALONG LONG LIFECYCLES







- Solusi keamanan siber canggih:
 1. Melindungi aset IoT yang terhubung dari kloning dan akses berbahaya
 2. Menyediakan dan menyimpan dengan aman ID digital dan kunci enkripsi yang beragam dalam wadah keamanan perangkat keras yang canggih
 3. Memastikan otentikasi timbal balik yang aman antar mitra
 4. Memastikan kerahasiaan dan integritas data melalui mekanisme berbasis enkripsi
 5. Mendukung manajemen kredensial yang aman dan berskala besar untuk siklus hidup perangkat yang terhubung





SECURING THE IOT

UNDERSTANDING IOT RISKS

		IoT Characteristics	Potential Security Weakness & Targets
Web & Mobile Application		<ul style="list-style-type: none"> Closed/open platforms Variable policies High data volume handling 	<ul style="list-style-type: none"> Code Lack of penetration testing Weak User/Third Party Authentication
Cloud		<ul style="list-style-type: none"> Public/private/hybrid cloud deployment 	<ul style="list-style-type: none"> Code Policy management
Communications		<ul style="list-style-type: none"> 2G, 3G, LTE, 5G DSL, Fibre, LPWAN Wi-Fi Bluetooth MQTT, IP, ZigBee, Mesh RF, Wi-Fi ect 	<ul style="list-style-type: none"> Insecure communications
Gateways / Smart Edge Devices		<ul style="list-style-type: none"> Variable communications protocols Time-Sensitive data analysis 	<ul style="list-style-type: none"> Policy management Denial-of-service No / insecure updates Poor hardware design
IoT Sensors / Actuators		<ul style="list-style-type: none"> Limited power Low bandwidth Constrained capabilities 	<ul style="list-style-type: none"> Design faults Software / firmware implementation faults Inability to update
Data Types		<ul style="list-style-type: none"> Sensitive data: video, audio, location, personal information Technical data: environmental measurement, uptime reports 	<ul style="list-style-type: none"> Users Policy management Data storage

Source: Juniper Research

THE OBJECTIVES OF SECURITY

- Tujuan utama keamanan pada IoT adalah untuk mengurangi resiko pada bisnis (sistem)
- Secara umum, faktor keamanan pada IoT harus dapat melindungi 3 pilar, yaitu :
 - Confidentially
 - Integrity
 - Availability

Confidentiality

Unauthorised access to devices, applications and data is prevented

Integrity

Data stored, received or transmitted by devices and application is not altered

Availability

Device communications and management interfaces are not disrupted; nominal service is available

IoT Security – System of Layers



DEVICE

1. Device Identification & Authentication

- Elemen inti pada sistem IoT yang memastikan bahwa pengguna dan perangkat sesuai dengan apa yang sudah di konfigurasi di awal pembuatan sistem.

2. Firmware/Code Authentication

- Firmware atau kode aplikasi yang berjalan pada perangkat berpotensi dimanipulasi oleh penjahat dunia maya. Oleh karena itu, kita harus memastikan bahwa firmware dan source code asli terlindungi dari serangan

3. Communication/Data Encryption

- Penting untuk mengenkripsi data selama perjalanan lengkapnya melalui ekosistem IoT: baik saat diam maupun selama transmisi data, terutama jika ini dilakukan secara nirkabel.

GATEWAYS, NETWORKS & CONNECTIONS

- Alat dan sistem IoT yang terdapat pada layer ini memungkinkan untuk membagi data antar jaringan, alat lain, dan aplikasi lain menggunakan sebuah jembatan yang menghubungkan antar jaringan bahkan antara konsumen dan sumber data.
- Komunikasi jarak jauh, gateways, dan perangkat jaringan lain (smart edge device) dapat digunakan sebagai pusat pertukaran dan enkripsi data ketika terjadi transaksi data.
- Tidak semua enkripsi data dapat dilakukan oleh sensor IT. Akan tetapi, perangkat pada layer ini dapat memverifikasi user atau perangkat lain menggunakan pesan terverifikasi ataupun routing.

CLOUD APPLICATIONS & USERS

- Lapisan IoT ini menawarkan sumber daya komputasi cloud yang berguna untuk komputasi berat. Sejumlah besar data dapat dianalisis secara retrospektif, digunakan untuk meningkatkan kinerja perangkat dan sistem di lapisan lain dan memberikan informasi ke user.
- Oleh karena itu penting bahwa aplikasi harus diverifikasi dengan cara yang sama dengan device layer. Selain itu, pengguna platform, sistem, dan aplikasi harus diverifikasi keasliannya untuk mencegah manipulasi data atau penyalahgunaan sistem.
- Enkripsi data harus dilihat sebagai standar di lapisan ini.



STRATEGIES FOR SUCCESSFUL IOT SECURITY DEPLOYMENT

Protecting Confidentiality

Security Tool	Function	Protects Against	Position in IoT Layers	Notes
Cryptographic Authentication	Secure mutual authentication between authorised parties	Unauthorised access to data and services	All	
TEE (Trusted Execution Environment)	Isolates cryptographic functions from software applications	Access to sensitive code	Devices	Depending on business risk, can be used with/without a SE
SE (Secure Element)	Isolates cryptographic functions via dedicated hardware	Theft of device ID, application access	Devices, Gateways	On-device hardware security and lifecycle management enabler
HSM (Hardware Security Module)	Secure key management and crypto-processing	Theft of device ID	Cloud & Applications	Cloud/server enabler for lifecycle management
Lifecycle Management Platform	Regular renewal of credentials, firmware and policies	Theft of device ID, unauthorised device access	All	Platform to provision, decommission and update devices
Data Encryption	Ensures data is only readable to authorised parties	Theft of data (eavesdropper)	All	
User & Developer Education	Promotes cybersecurity best practices	Device/system/ application access	All	

Protecting Integrity

Security Tool	Function	Protects Against	Position in IoT Layers
Secure Boot	Ensures device boots only using valid software	Firmware/operating system tampering	Devices
MAC (Message Authentication Code)	Proves origin and integrity of a message	Data alteration/tampering	All
Data Encryption	Complicate tampering attempts	Message details access	All
Digital Certificates & Signatures	Provides proof of message origin	Execution of unauthorised code and fake data injection	Mainly devices

Protecting Availability

Security Tool	Function	Protects Against	Position in IoT Layers	Notes
Firewall	Validates or blocks inbound and outbound connections according to ruleset	DDoS, potentially malicious traffic from external sources.	Gateways, Networks & Connections	DDoS protection is limited
IPS (Intrusion Prevention System)	Attempts to prevent malicious attackers from accessing or disrupting a network	DDoS, malware and malicious network activity	Gateways, Networks & Connections	Actively blocks suspicious traffic
IDS (Intrusion Detection System)	Attempts to detect unusual activity associated with malicious entities	Malware and malicious network activity	Gateways, Networks & Connections	Events flagged, not prevented
DDoS Prevention Service	Establishes hardened infrastructure to enable continuity in the event of a DDoS attack	High volume DDoS	Gateways, Networks & Connections	Third party provided service

What Level Security do I need ?

Threat	Threat Class	Impact	Mitigation Measures	Probability of Threat Occurrence	Threat Severity	Mitigation	Risk Score
What will happen to the network if the device, or group of devices is inadvertently taken offline?	Availability	What is the impact of the threat? How far does it reach? Will it impact customer trust, compliance adherence, income or revenues?	Are there elements across the ecosystem that will reduce the probability of a threat occurrence?	(a)	(b)	(m)	$[(a) - (m)] \times (b)$
Are component suppliers trustworthy and are associated software components updateable?	Confidentiality			(a)	(b)	(m)	$[(a) - (m)] \times (b)$
Can devices be securely authenticated on the network?	Confidentiality			(a)	(b)	(m)	$[(a) - (m)] \times (b)$
Can data on the device be encrypted at rest?	Integrity			(a)	(b)	(m)	$[(a) - (m)] \times (b)$
What will happen to the service if the device, or group of devices, reports false data?	Integrity			(a)	(b)	(m)	$[(a) - (m)] \times (b)$
What will happen if data stored on the device is stolen or mishandled?	Integrity			(a)	(b)	(m)	$[(a) - (m)] \times (b)$



EXAMINING THE COST OF IOT SECURITY

DIY or IoT Security Specialist? Cost Consideration Model



IoT Security Implementation - A Comparison

IoT Specialist Approach

Delivered as a package, with shared infrastructure



Objective Security Risk Assessment
Accounting for customer industry & ecosystem



Market-Specific Solution
Scalable, end-to-end security architecture, protecting from the edge up to the cloud



Faster Time-to-Market
Via industry bestpractice knowledge and shared encryption infrastructure

DIY Approach

Self-sourced, requiring expert in-house knowledge



Gain In-House Expertise
By hiring & training security experts



Secure the Supply chain
Through generation & provision of unique digital IDs. Design & deploy appropriate security containers & ID management for devices & users



Deploy Cryptography Infrastructure
Either as an in-house effort, or find 'as-a-service' HSM/PKI provider for security lifecycle management



Conformity with Industry Standards
In-depth knowledge of regulatory requirements and protocols



Scalable Architecture
Regular updates via remote security lifecycle management, to ensure business continuity



Slower Time-to-Market
By replicating specialist approach & avoiding risks associated with poor implementation

Poor Implementation Risks



Business Disruption



Brand Damage



Data theft



Regulatory Fines



Ransomware



Loss of Revenue





THANK YOU

SUMBER

- <https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security>
- <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security/key-principles>
- <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses>
- <https://www.ericsson.com/en/internet-of-things/iot-security>

Modul 6

A. Tujuan

Mahasiswa mampu memahami arsitektur sistem IoT :

- Implementasi keamanan pada arsitektur IoT

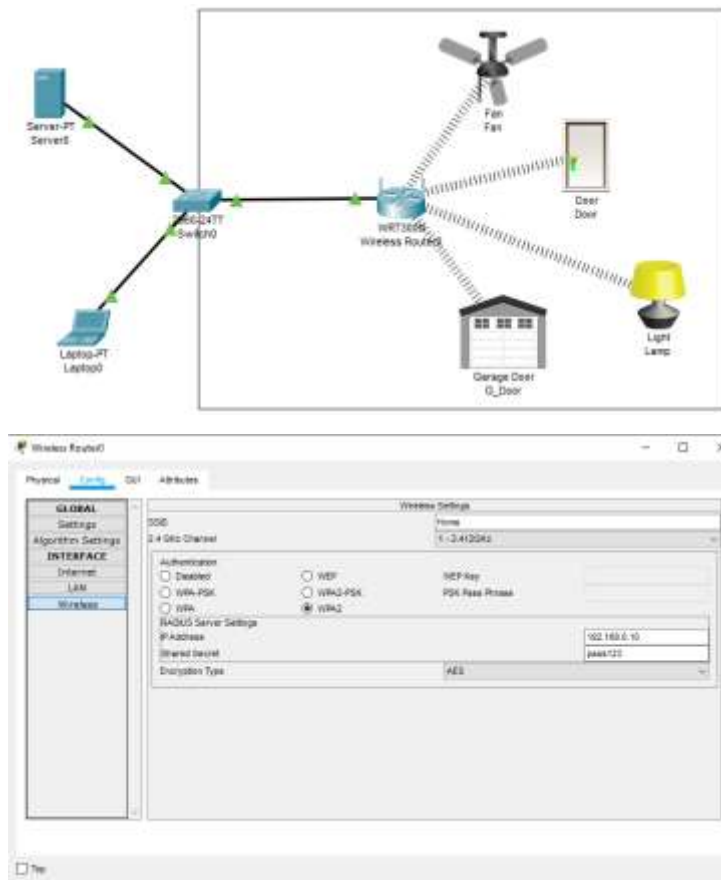
B. Kuis

Petunjuk: **Kerjakan soal berikut !**

1. IoT menerapkan konsep security by design untuk mengimplementasikan keamanan pada sebuah jaringan atau sistem yang digunakan. Jelaskan apa yang dimaksud dengan *security by design* !
2. Implementasi keamanan pada IoT harus dapat melindungi beberapa faktor. Jelaskan apa saja yang harus dilindungi pada sebuah sistem IoT !

C. Simulasi

1. Menambahkan keamanan pada jaringan wireless IoT menggunakan WPA2 dan AES



Rangkaian simulasi IoT diatas menunjukkan bahwa tiap device terkoneksi dengan wireless router. Setting protokol keamanan wifi menggunakan WPA2 enterprise, dengan tipe enkripsi AES. Untuk konfigurasi lebih lanjut lihat di video SPADA.

D. TUGAS INDIVIDU

1. Membuat simulasi rangkaian IoT menggunakan wireless router. Tambahkan protokol keamanan dan tipe enkripsi dalam membuat registration server. Protokol dan algoritma enkripsi yang dipakai boleh berbeda dengan contoh yang ada (contoh : WPA2 Enterprise, AES)

2. Device yang digunakan adalah hasil dari tugas pertemuan sebelumnya (membuat registration server). Tambahkan wireless router agar device dapat terkoneksi pada jaringan wifi.

3. Pengumpulan Tugas.

- Tugas yang diupload di akun github masing-masing adalah :
 - a. Hasil pengerjaan kuis pada poin B
 - b. Penjelasan simulasi IoT dan screenshot arsitektur IoT
 - c. File tugas 6 packet tracer (tugas6.pkt)
- Semua tugas diupload ke akun github masing-masing. Kemudian link github dikumpulkan di SPADA. Format penamaan file word SKD_namakelas_nim_nama
- **Untuk kelas TI D pengumpulan paling lambat tanggal 3 Oktober 2021 jam 23.59**
- **Untuk kelas TI E pengumpulan paling lambat tanggal 5 Oktober 2021 jam 23.59**
- Contoh : <https://github.com/fadilrahman46/IoT>