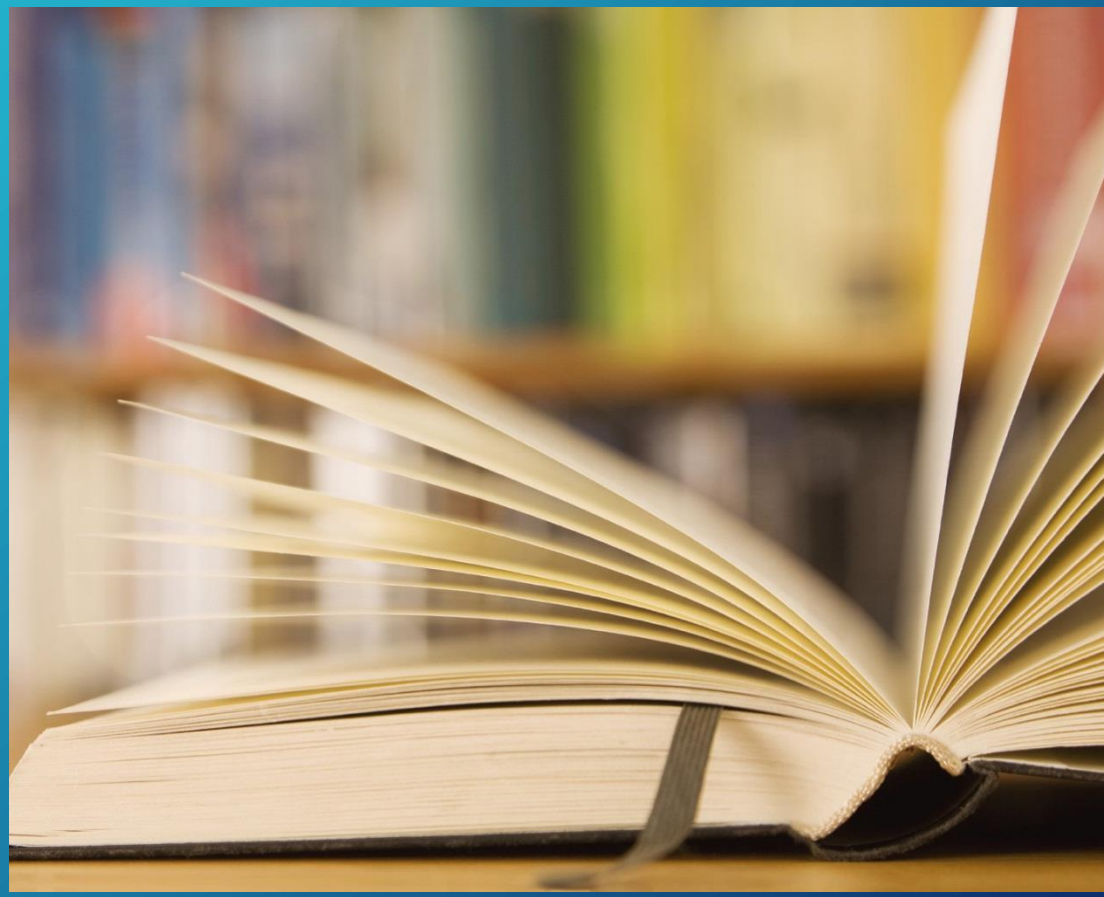
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

# WIRELESS SECURITY



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

# Agenda

- Wireless Network
- Wireless vs Wired Network
- Wireless Fidelity
- Wifi Components
- WEP
- WPA
- WPA2
- Ancaman Wireless Network
- Mengamankan Wireless Network

# Wireless Network

**Wireless Network (Jaringan Nirkabel)** adalah jaringan yang menggunakan koneksi nirkabel antar node

Wireless Network memiliki keunggulan dimana operator telekomunikasi atau organisasi bisa menghemat biaya dalam instalasi dan menyederhanakan proses instalasi dan konfigurasi jaringan

Beberapa contoh Wireless Network:

- Wireless Fidelity (Wi-Fi)
- Bluetooth
- Infrared
- Cellular Network

Namun demikian, tipikal wireless network memiliki resikonya tersendiri dari kacamata security dibanding wired network.

Dalam kuliah ini scope pembahasan Wireless Network adalah Wi-Fi

# Wireless vs Wired Network

| Aspek | Wireless Network | Wired Network |
|---|---|---|
| User Mobility | Terbatas dalam jangkauan sinyal antenna | Terbatas jangkauan kabel dan switch/router |
| Office Reconfigurations | Simple | Rumit dan membutuhkan biaya lebih tinggi |
| Reliability | Tergantung jarak dan kuat sinyal | Lebih stabil |
| Potensi Interferensi RF | Sangat concern | Bukan isu |
| Keamanan | Lebih rentan | Lebih aman dibanding wireless |
| Kecepatan | Lebih lambat | Lebih cepat |
| Biaya Instalasi | Cenderung murah | Lebih mahal |
| Expandability | Fleksibel | Butuh instalasi kabel baru |

# Wireless Fidelity

Wi-Fi dibuat oleh Wireless Ethernet Compatibility Alliance yang kemudian menjadi Wi-Fi Alliance.

Wi-Fi adalah teknologi wireless LAN yang menggunakan standar 802.11 untuk berkomunikasi. Wi-Fi menggunakan gelombang radio untuk berkomunikasi antara device klien dengan access point yang terhubung dengan router, LAN lain hingga ke WAN atau internet

Protocol yang paling umum digunakan adalah:

- 802.11a → Freq 5 dan 3,7 GHz; BW 20 MHz
- 802.11b → Freq 2,4 GHz; BW 22 MHz
- 802.11g → Freq 2,4 GHz; BW 20 MHz
- 802.11n → Freq 5 GHz – BW 20 MHz dan Freq 2.4 GHz – BW 40 MHz

# WiFi Components

Access Points

- Perangkat keras yang menghubungkan jaringan ISP dengan dengan perangkat klien

Wireless Repeater

- Penguat dari Access Point untuk menjangkau klien yang lebih jauh

Wireless Router

- Router yang memiliki kemampuan seperti Access Point juga

Antenna

- Sebagai penerima dan pemancar gelombang radio yang ditransmisikan oleh access point

# WEP (Wired Equivaclent Privacy) Encryption

- WEP adalah protocol keamanan yang didefinisikan untuk standar 802.11b
- Protokol ini adalah protocol keamanan nirkabel yang pertama sehingga sudah diketahui celah keamanannya sehingga paling mudah diserang dan diretas
- WEP masih menjadi protocol yang paling banyak digunakan karena WEP adalah protocol keamanan default jaringan. Alasan lain adalah perangkat lama tersebut belum mendukung sistem keamanan WPA yang lebih baru

# WPA (Wifi Protected Access) Encryption

- WEP adalah protocol keamanan yang didefinisikan untuk standar 802.11i
- Protokol ini adalah pengganti WEP dengan mengadopsi enkripsi TKIP (Temporal Key Integrity Protocol) yang kemudian digantikan oleh AES (Advanced Encryption Standard). Namun masih adanya fitur WEP yang tersedia menjadikannya masih belum aman

# WPA 2(Wifi Protected Access II) Encryption

- WEP adalah protocol keamanan yang didefinisikan untuk standar 802.11i
- Protokol ini adalah penerus WPA dengan mengadopsi enkripsi AES-CCMP (Advanced Encryption Standard-Counter Cipher Mode with Block Chaining Message Authentication Code Protocol).
- WPA2 Personal
  - Menggunakan set-up password PSK (Pre-shared Key) untuk otentikasi
- WPA2 Enterprise
  - Menggunakan EAP dan RADIUS untuk otentikasi terpusat menginat penggunaannya yang massif digunakan dalam skala besar

# WEP vs WPA vs WPA 2

| Enkripsi | Algoritma Enkripsi | Initialization Vector Size | Encryption Key Length | Integrity Check Mechanism |
|---|---|---|---|---|
| WEP | RC4 | 24-bits | 40/104-bit | CRC-32 |
| WPA | RC4, TKIP | 48-bits | 128-bit | Michael algorithm dan CRC-32 |
| WPA2 | AES-CCMP | 48-bit | 128-bit | CBC-MAC |

# Ancaman Wireless Network

- Rogue Access Point Attack → Serangan berupa instalasi perangkat Wifi Ilegal dengan SSID yang sama dengan AP Resmi, sehingga attacker bisa ngambil alih koneksi korban
- Adhoc Connection Attack → Klien Wifi berkomunikasi secara langsung secara adhoc tanpa membutuhkan AP
- AP MAC Spoofing → Hacker berpura-pura sebagai klien Wifi dengan melakukan spoofing MAC Address klien, terhubung dengan klien dan melihat trafik korban
- DOS Attack → Wireless DoS yang menyibukkan jaringan wireless
- Jamming Signal Attack → Attacker mengaburkan sinyal dengan memberikan interferensi dengan sinyal eksisting

# Mengamankan Wireless Network

- Creating an Inventory of Wireless Devices
  - Dokumentasikan semua klien yang sering terhubung dengan AP berdasarkan model, enkripsi, firmware, wireless channel, dll
  - Ini membantu admin untuk menganalisa mana perangkat wireless yang terpercaya
- Disable SSID Broadcasting
  - Matikan SSID Broadcasting, sehingga hanya yang mengetahui SSIDnya saja yang bisa tersambung dengan AP
  - Ini meminimalisir kemungkinan serangan Wireless DoS
- Gunakan enkripsi wireless yang lebih kuat → WPA
- Implementasikan MAC Address Filtering
  - Mencatat MAC klien dan memblokir klien lain kecuali di allow oleh admin
- Deteksi Rogue AP
  - Lakukan wireless scanning
  - Cari AP yang tidak tercatat inventory

# Mengamankan Wireless Network

- Konfigurasi security pada Wireless Router
  - Ubah default password pada wireless router
  - Gunakan password yang kompleks dan kuat
  - Ubah password secara berkala
  - Gunakan https sebagai interface konfigurasi admin
  - Disable remote router access
  - Enable logging pada router