Wireless Security

Keamanan Siber

Always The First

Materi

- Pengenalan Jaringan Wireless
- Jenis Jaringan Wireless
- Wireless Security
- Ancaman pada Jaringan Wireless
- Teknik Pengamanan Jaringan Wireless
- Pengujian Keamanan Wireless

Jaringan Wireless

- Jaringan Wireless adalah jenis jaringan komunikasi yang menghubungkan perangkat elektronik tanpa menggunakan kabel fisik.
- Jaringan Wireless berkomunikasi dan berbagi data melalui gelombang elektromagnetik, seperti gelombang radio, mikro gelombang, atau inframerah.

Jenis Jaringan Wireless

- Wi-Fi (Wireless Fidelity)
- Bluetooth
- Cellular Network
- Satellite Communication
- NFC (Near Field Communication)

Wi-Fi (Wireless Fidelity)

- Jaringan Wi-Fi adalah salah satu jenis jaringan nirkabel yang paling umum. Wi-Fi memungkinkan perangkat untuk terhubung ke jaringan internet dan berkomunikasi satu sama lain melalui hotspot yang diaktifkan oleh perangkat seperti router Wi-Fi.

Bluetooth

- Bluetooth adalah teknologi nirkabel yang digunakan untuk menghubungkan perangkat dalam jarak yang pendek, seperti headset nirkabel, speaker, atau perangkat input seperti keyboard dan mouse.

Cellular Network

- Jaringan seluler adalah jaringan nirkabel yang lebih besar dan kompleks, yang memungkinkan perangkat seluler seperti smartphone dan tablet untuk berkomunikasi melalui jaringan seluler seperti 4G dan 5G.

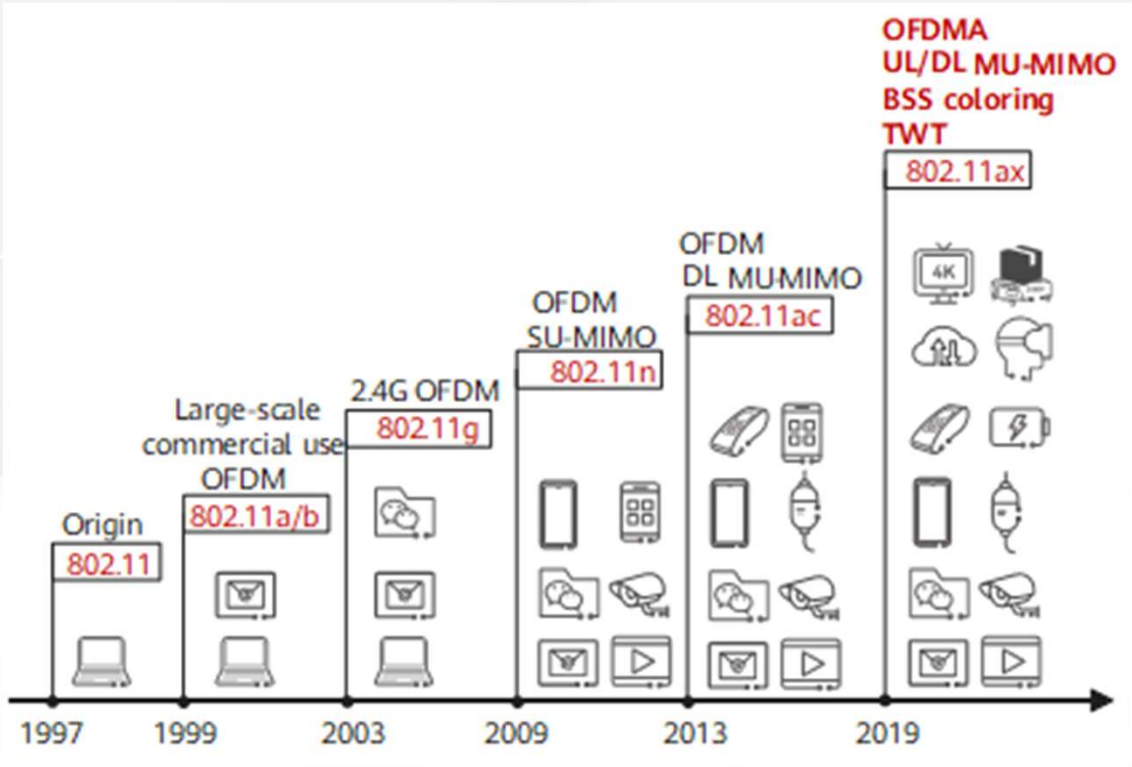
Satellite Communication

- Komunikasi satelit menggunakan satelit untuk mentransmisikan sinyal nirkabel ke dan dari berbagai lokasi di seluruh dunia.
  - Umumnya digunakan untuk komunikasi di daerah yang sulit dijangkau oleh infrastruktur kabel atau seluler.

NFC (Near Field Communication)

- NFC adalah teknologi nirkabel yang memungkinkan pertukaran data antara perangkat dalam jarak sangat pendek, biasanya beberapa sentimeter.
  - NFC sering digunakan untuk pembayaran nirkabel dan berbagi informasi antara perangkat.

Evolusi Standar IEEE 802.11



	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz
Max # SU Streams	1	1	1	1	4	8	8
Max # MU Streams	NA	NA	NA	NA	NA	4 (DL only)	8 (UL & DL)
Modulation	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Max Constellation / Code Rate	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Max # OFDM tones	NA	NA	64	64	128	512	2048
Subcarrier Spacing	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

- DSSS (Direct Sequence Spread Spectrum)
- FHSS (Frequency Hopping Spread)
- CCK (Complementary code keying)
- OFDM (Orthogonal Frequency Division Multiplexing)
- OFDMA (Orthogonal Frequency Division Multiple Access)

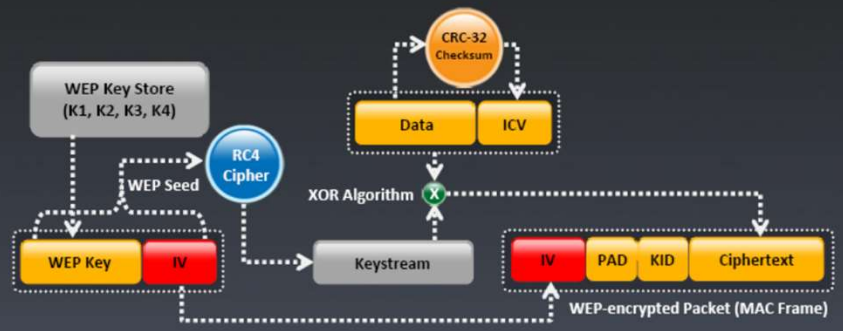
Wireless Security

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access 2)
- WPA3 (Wi-Fi Protected Access 3)

WEP (Wired Equivalent Privacy)

- WEP adalah protokol keamanan pertama yang digunakan dalam jaringan nirkabel.
- Namun, WEP memiliki serangkaian masalah keamanan yang serius dan relatif mudah dipecahkan.
  - WEP menggunakan enkripsi RC4 yang sudah usang dan memiliki masalah serius dalam menghasilkan kunci enkripsi yang kuat.
  - Akibatnya, penyerang yang memiliki pengetahuan teknis yang cukup dapat dengan relatif mudah membobol enkripsi WEP dan mengakses data yang dikirimkan melalui jaringan.

How WEP Works?

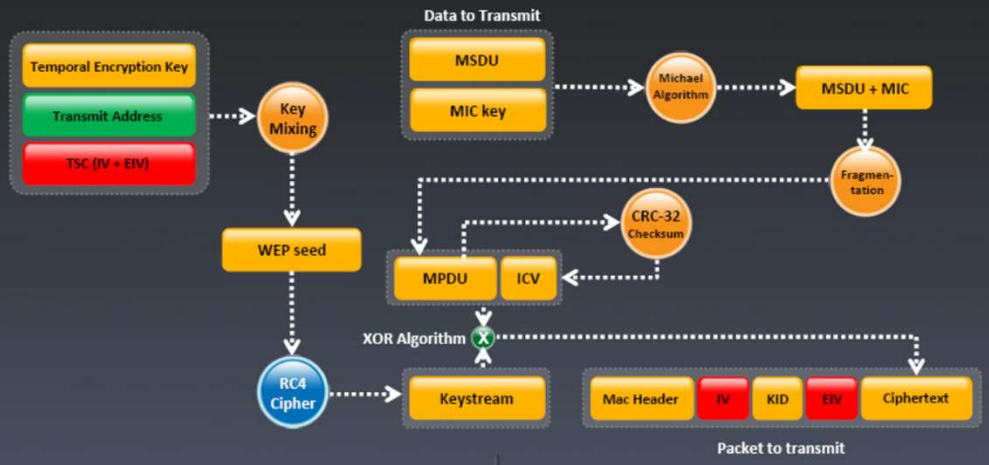


1. A 32-bit Integrity Check Value (ICV) is calculated for the frame data
2. The ICV is appended to the end of the frame data
3. A 24-bit Initialization Vector (IV) is generated and appended to the WEP encryption key
4. The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream
5. The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data
6. The IV is added to the encrypted data and ICV to generate a MAC frame

WPA (Wi-Fi Protected Access)

- WPA adalah perbaikan dari WEP.
- WPA memperkenalkan protokol TKIP (Temporal Key Integrity Protocol) yang lebih aman dan dinamis.
- WPA menghasilkan kunci enkripsi yang berubah secara otomatis dan lebih sulit untuk dipecahkan.
  - Selain itu, WPA juga memperkenalkan mekanisme message integrity check (MIC) untuk mendeteksi manipulasi data.
  - WPA disertai dengan mode "WPA-Personal" (atau WPA-PSK) yang menggunakan kata sandi pre-shared key (PSK) sebagai metode autentikasi.

How WPA Works?



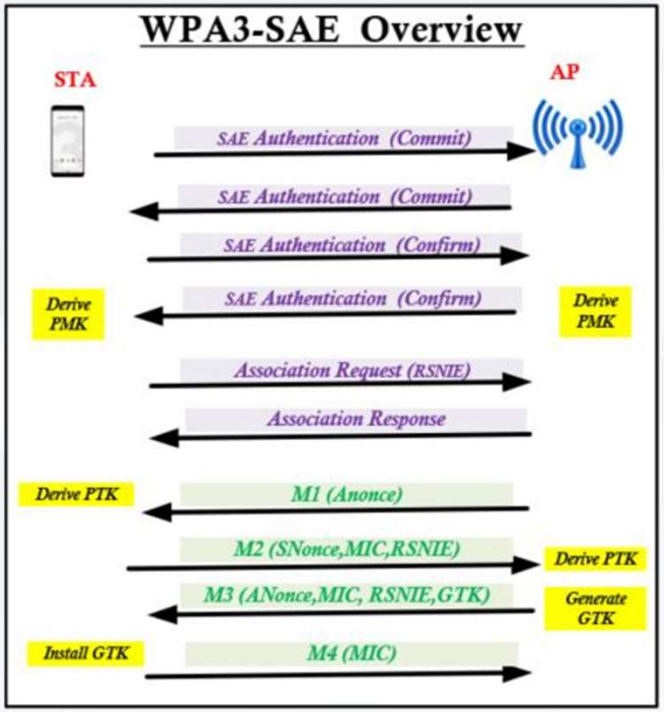
1. Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to **RC4 algorithm** to generate a **Keystream**
2. MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using **Michael algorithm**
3. The combination of MSDU and MIC is fragmented to generate **MAC Protocol Data Unit (MPDU)**
4. A **32-bit Integrity Check Value (ICV)** is calculated for the MPDU
5. The combination of MPDU and ICV is bitwise **XORed with Keystream** to produce the encrypted data
6. The **IV** is added to the encrypted data to generate **MAC frame**

WPA2 (Wi-Fi Protected Access 2)

- WPA2 adalah pengembangan lebih lanjut dari WPA dan dianggap sebagai standar keamanan nirkabel yang paling kuat hingga saat ini.
- WPA2 menggunakan enkripsi AES (Advanced Encryption Standard) yang lebih aman dan efisien.
- Ada dua mode autentikasi dalam WPA2:
  - "WPA2-Personal" (atau WPA2-PSK) menggunakan kata sandi pre-shared key (PSK), dan
  - "WPA2-Enterprise" yang melibatkan server autentikasi (biasanya menggunakan RADIUS) untuk mengelola akun pengguna.

WPA3 (Wi-Fi Protected Access 3)

- WPA3 (Wi-Fi Protected Access 3) adalah generasi terbaru dari protokol keamanan nirkabel untuk jaringan Wi-Fi.
- Diperkenalkan sebagai pengganti WPA2, WPA3 dirancang untuk memberikan lapisan keamanan yang lebih kuat dan lebih tahan terhadap berbagai serangan yang mungkin terjadi pada jaringan nirkabel.



Proteksi terhadap Serangan Brute-Force

- WPA3 menghadirkan perlindungan terhadap serangan pencobaan kata sandi yang berulang-ulang (brute-force) dengan mengimplementasikan mekanisme Simultaneous Authentication of Equals (SAE).
- SAE memastikan bahwa proses autentikasi antara perangkat dan titik akses adalah proses yang aman dan efisien.

Enkripsi Individual Data Streams

- WPA3 menggunakan enkripsi yang berbeda untuk setiap perangkat yang terhubung, sehingga melindungi setiap jalur data secara individu.
- WPA3 memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan WPA2, yang menggunakan enkripsi yang sama untuk semua perangkat.

Peningkatan Keamanan Saat Menggunakan Koneksi Terbuka

- WPA3 memperkenalkan mode "Enhanced Open" yang memberikan lapisan keamanan tambahan saat perangkat terhubung ke jaringan terbuka (tanpa memerlukan kata sandi).

Proteksi terhadap Penyerangan Dictionary

- WPA3 mempersulit serangan dengan kata sandi yang didasarkan pada kamus (dictionary-based) dengan memperkenalkan password-based key derivation (PBKDF2) yang lebih kuat.

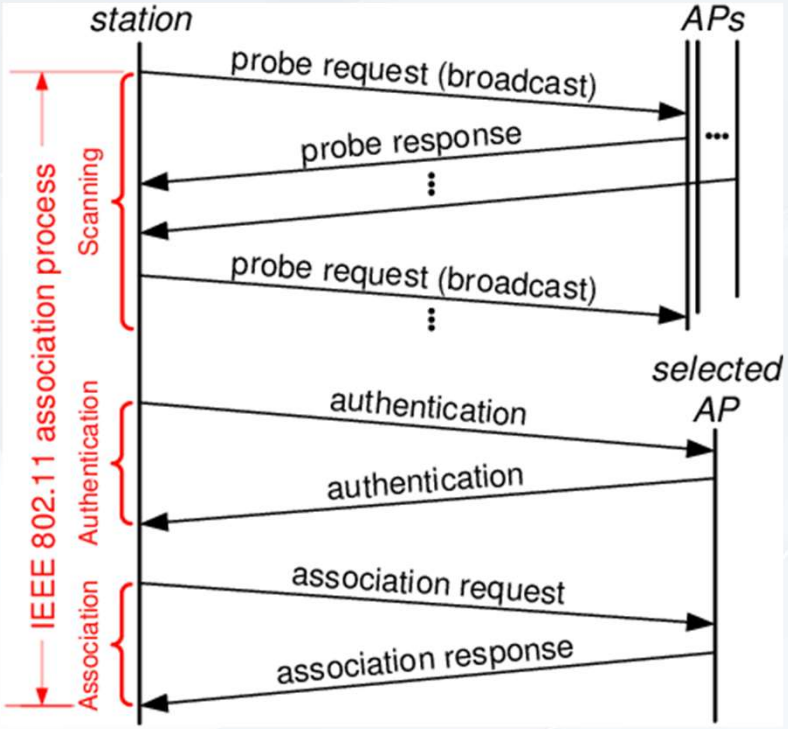
Privasi di Jaringan Terbuka

- Dalam jaringan Wi-Fi yang terbuka, WPA3 memastikan bahwa data yang dikirimkan antara perangkat dan titik akses tetap terenkripsi, melindungi privasi pengguna dari mata-mata yang tidak sah.

Akses Pribadi ke Hotspot Umum

- WPA3 memungkinkan perangkat-perangkat individu untuk memiliki kunci enkripsi unik saat terhubung ke hotspot umum, sehingga melindungi data dari perangkat lain yang terhubung ke jaringan yang sama.

Cara Wireless terhubung ke Access Point

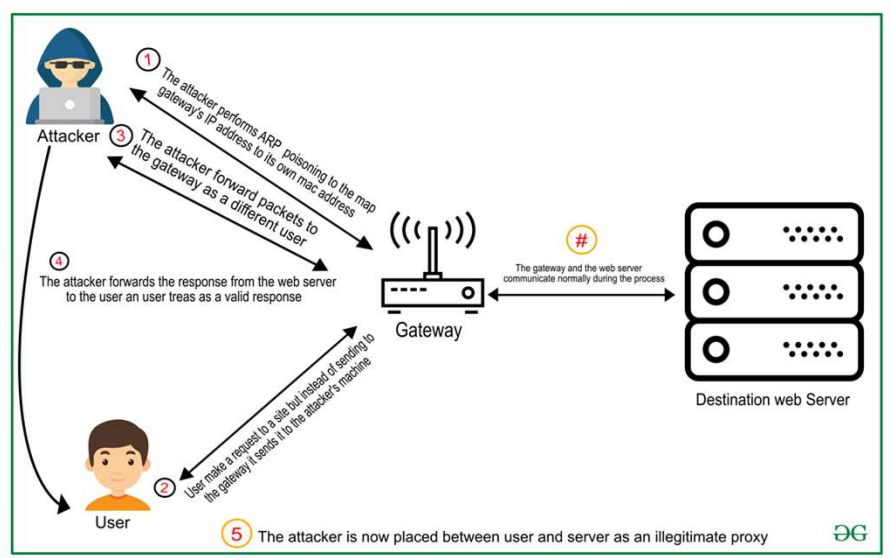


Ancaman pada Jaringan Wireless

- Serangan Man-in-the-Middle (MitM)
- Pencurian Identitas (Identity Theft)
- Serangan DoS (Denial of Service)
- Serangan Deauthentication atau Disassociation
- Pengintaian (Eavesdropping)
- Cracking WEP/WPA Keys
- Serangan Rogue Access Point / Evil Twin
- Serangan Jamming
- Cracking Handshake WPA/WPA2

Serangan Man-in-the-Middle (MitM)

- Penyerang memposisikan dirinya di antara dua pihak yang berkomunikasi dan memantau atau bahkan memanipulasi komunikasi di antara mereka.
  - Ini dapat menyebabkan pencurian data sensitif atau bahkan perusakan informasi.

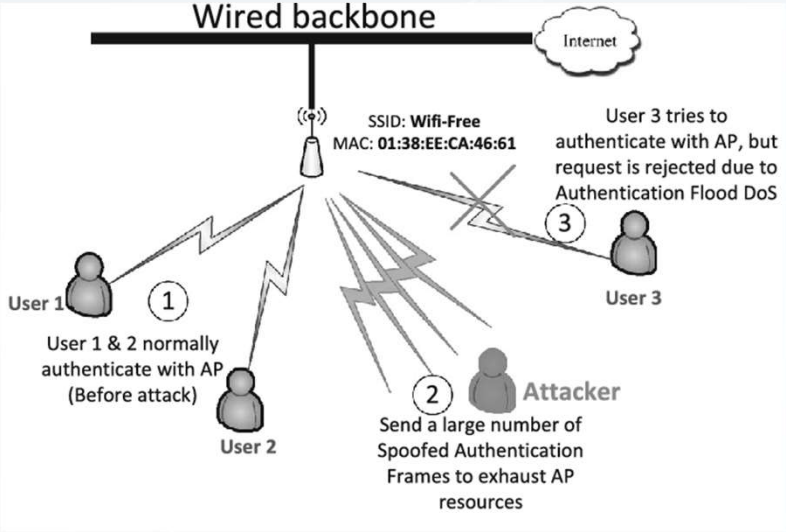


Pencurian Identitas (Identity Theft)

- Penyerang dapat mencuri kredensial atau informasi identitas pribadi dari perangkat yang terhubung ke jaringan nirkabel.
- Hal ini bisa dilakukan dengan menggunakan teknik seperti phishing atau serangan MitM.

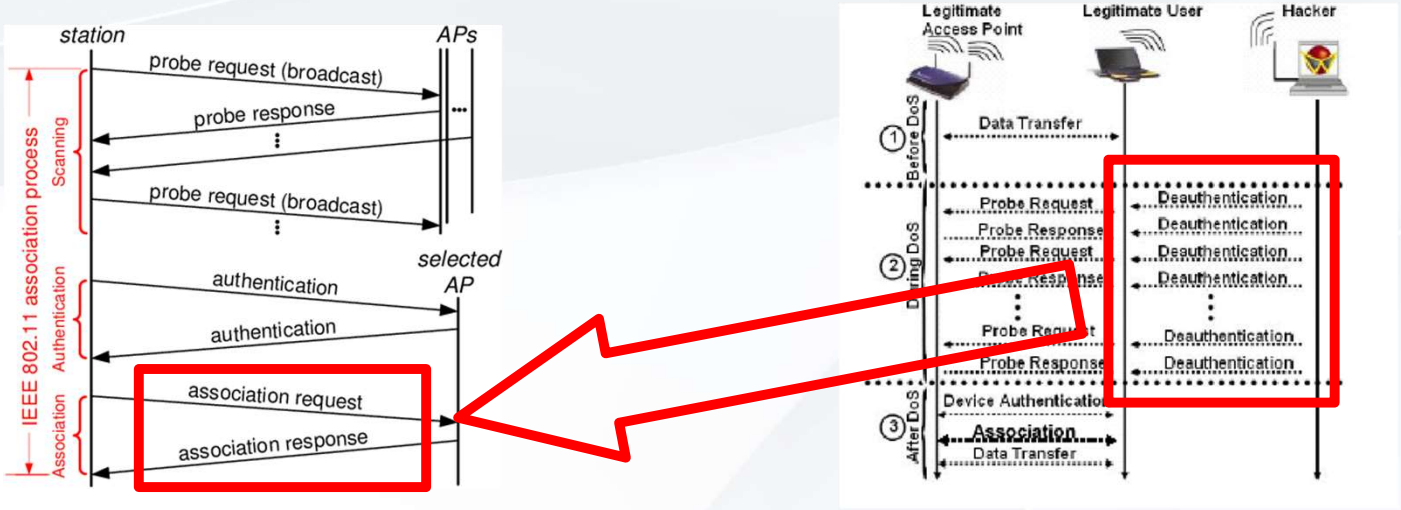
Serangan DoS (Denial of Service)

- Dalam serangan DoS, penyerang berusaha untuk membuat sumber daya jaringan menjadi tidak tersedia bagi pengguna yang sah.
  - Serangan DoS dapat mengakibatkan gangguan layanan atau bahkan penurunan produktivitas.



Serangan Deauthentication atau Disassociation

- Penyerang dapat menggunakan serangan ini untuk memutuskan koneksi perangkat yang terhubung ke jaringan, memaksa mereka untuk terputus dari jaringan secara tiba-tiba.

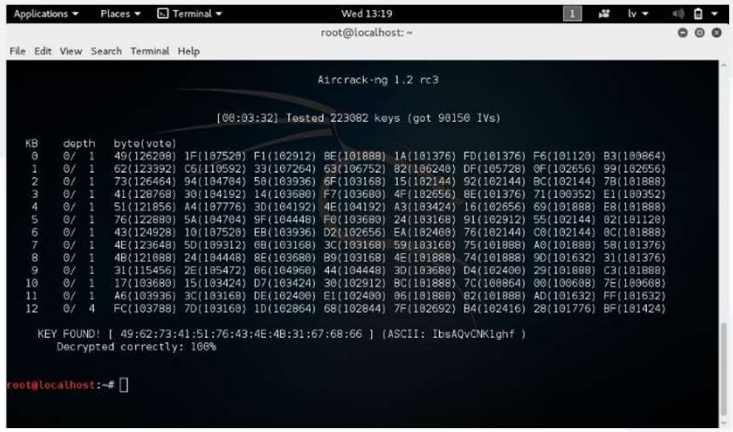


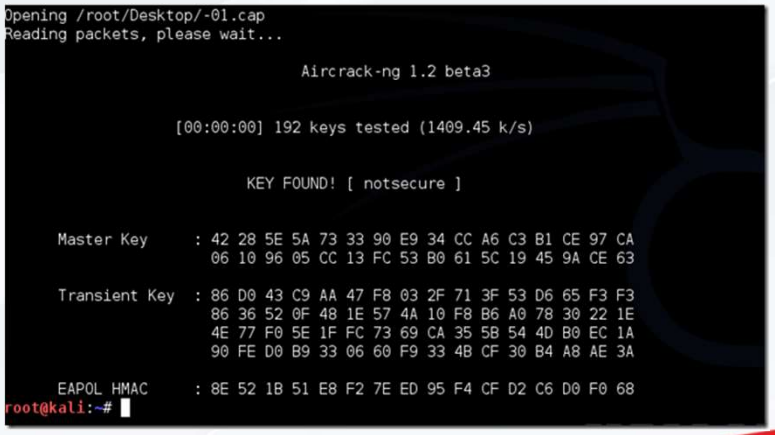
Pengintaian (Eavesdropping)

- Penyerang dapat memonitor lalu lintas nirkabel untuk mencuri informasi sensitif yang dikirimkan melalui jaringan, seperti kata sandi atau data pribadi.

Cracking WEP/WPA Keys

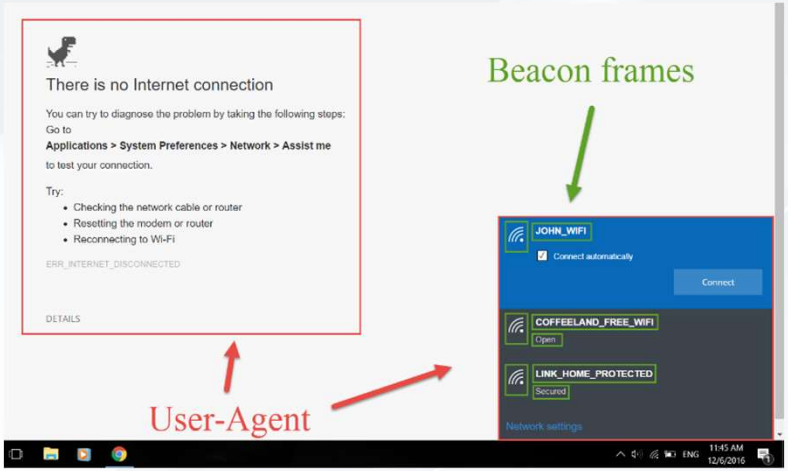
- Keamanan jaringan Wi-Fi sering dijamin oleh enkripsi menggunakan protokol seperti WEP (Wired Equivalent Privacy) atau WPA/WPA2 (Wi-Fi Protected Access).
  - Namun, penyerang yang canggih dapat mencoba menguraikan atau menebak kata sandi enkripsi ini untuk mendapatkan akses ke jaringan.





Serangan Rogue Access Point

- Penyerang dapat membuat rogue access point, yaitu titik akses palsu yang terlihat seperti jaringan sah.
  - Pengguna yang tidak curiga dapat terhubung ke titik akses palsu ini dan memberikan akses ke penyerang.



Serangan Jamming

- Penyerang dapat menggunakan perangkat untuk menghasilkan gangguan dalam frekuensi yang sama dengan jaringan Wi-Fi, mengakibatkan gangguan atau bahkan pemutusan koneksi.
  - Pada dasarnya ini adalah proses deauth dalam jumlah besar dan mempengaruhi seluruh client yang mengakses Access Point target.

Cracking Handshake WPA/WPA2

- Penyerang dapat mencoba menyerang handshake yang terjadi saat perangkat terhubung ke jaringan Wi-Fi yang dilindungi oleh WPA/WPA2.
  - Hal ini memungkinkan attacker untuk mencoba menguraikan kata sandi jaringan.
  - Berbeda dengan cracking WEP, pada Wireless yang menerapkan WPA/WPA2, yang dicari adalah handshake pertama kali saat konek ke AP.

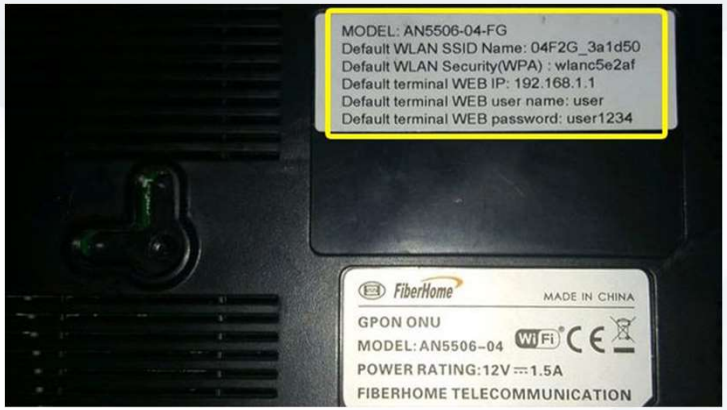
```
Reading packets, please wait...
                           Aircrack-ng 1.2 rc4

     [00:00:22] 127848/9894689 keys tested (5937.54 k/s)

     Time left: 27 minutes, 25 seconds                          1.29%

                    Current passphrase: 024384581


     Master Key     : 61 67 9B EA 83 66 11 CA DF B6 6E 4F 64 95 1B F8
                      8A 9C CD E3 21 91 C8 2E 74 65 FA A9 EC 8C B2 3C

     Transient Key  : 3B 52 B7 E2 56 DA 26 55 8B D9 11 AB 40 27 A8 9D
                      95 04 4A 3D 79 6D 2B A5 BF A6 A0 F8 0A 51 6E 3E
                      04 CF 2E F9 A2 09 67 2C 0C A0 18 62 A9 A1 58 59
                      8C E7 F7 60 D1 FC 98 7A 5D 5F 2A 75 27 06 71 12

     EAPOL HMAC     : 70 7F 00 8D D8 55 73 40 D9 E4 D1 7A 81 F5 31 6E
```

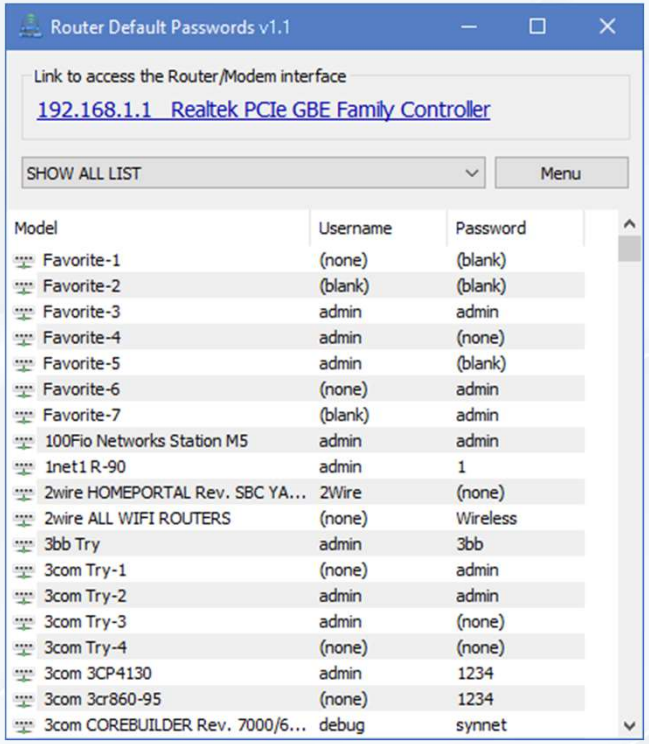
```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: WPA/WPA2
Hash.Target......: Handshake.hccapx
Time.Started.....: Mon Jul 09 17:24:43 2018 (4 mins, 44 secs)
Time.Estimated...: Mon Jul 09 17:29:27 2018 (0 secs)
Guess.Base.......: File (eightdigit.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#3.....:   352.8 kH/s (3.69ms) @ Accel:64 Loops:16 Thr:1024 Vec:1
Recovered........: 1/4 (25.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 100000000/100000000 (100.00%)
Rejected.........: 0/100000000 (0.00%)
Restore.Point....: 100000000/100000000 (100.00%)
Candidates.#3....: 99614720 -> 99999999
HWMon.Dev.#3.....: Temp: 65c Fan: 47% Util: 42% Core:1974MHz Mem:4513MHz Bus:16

Started: Mon Jul 09 17:24:41 2018
Stopped: Mon Jul 09 17:29:28 2018
```

```
[+] Bourgeois Pig Guest  (57db) WPA Handshake capture: Discovered new client: F0:D5:BF:BD:D5:2B

[+] Bourgeois Pig Guest  (58db) WPA Handshake capture: Discovered new client: 6C:8D:C1:A8:E4:E9

[+] Bourgeois Pig Guest  (59db) WPA Handshake capture: Listening. (clients:2, deauth:14s, timeout:8m1s)


[+] successfully captured handshake
[+] saving copy of handshake to hs/handshake_BourgeoisPigGuest_DE-F2-86-EC-CA-A0_2018-12-24T01-40-28.cap saved

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for de:f2:86:ec:ca:a0
[!]    pyrit: .cap file does not contain a valid handshake
[+] cowpatty: .cap file contains a valid handshake for (Bourgeois Pig Guest )
[+] aircrack: .cap file contains a valid handshake for DE:F2:86:EC:CA:A0

[+] Cracking WPA Handshake: Using aircrack-ng via passwords.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 2234.0kps (current key: christmasham)

[+] Cracked WPA Handshake PSK: christmasham

[+]   Access Point Name: Bourgeois Pig Guest
[+]  Access Point BSSID: DE:F2:86:EC:CA:A0
[+]         Encryption: WPA
[+]      Handshake File: hs/handshake_BourgeoisPigGuest_DE-F2-86-EC-CA-A0_2018-12-24T01-40-28.cap
[+]      PSK (password): christmasham
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
```

Best Practice Securing Wi-Fi

- Ganti Default Username dan Password:
  - Saat mengatur router Wi-Fi, gantilah username dan password bawaan (default) dengan yang kuat dan sulit ditebak.
  - Hal ini akan mengurangi risiko akses yang tidak sah.



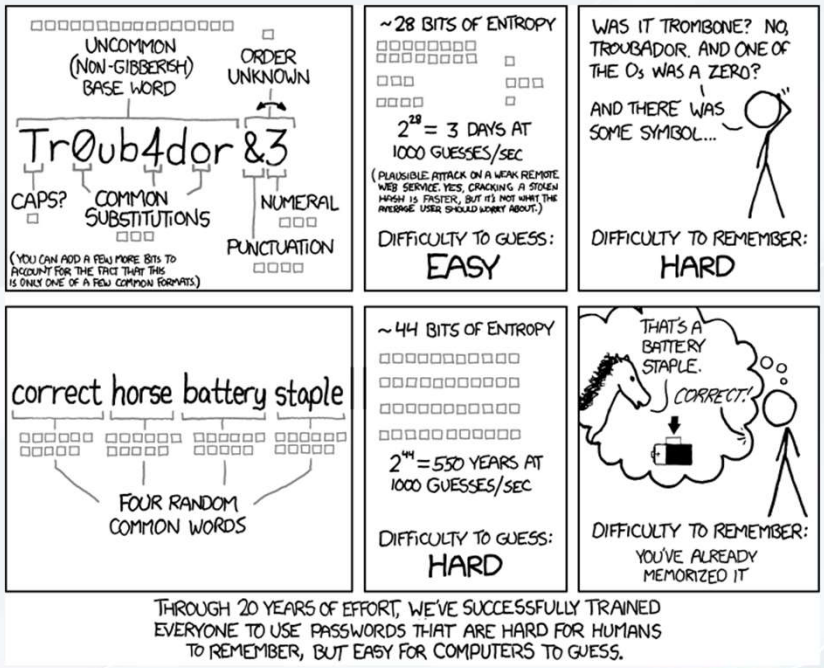


Best Practice Securing Wi-Fi (2)

- Aktifkan Enkripsi WPA3 atau WPA2:
  - Gunakan enkripsi yang kuat seperti WPA3 atau WPA2 untuk melindungi data yang dikirimkan antara perangkat dan router.
  - Pastikan menggunakan kata sandi yang kuat untuk enkripsi.

Best Practice Securing Wi-Fi (3)

- Pilih Kata Sandi yang Kuat:
  - Buat kata sandi yang panjang, kompleks, dan unik.
  - Campurkan huruf besar, huruf kecil, angka, dan karakter khusus. Jangan gunakan informasi pribadi atau kata yang mudah ditebak.

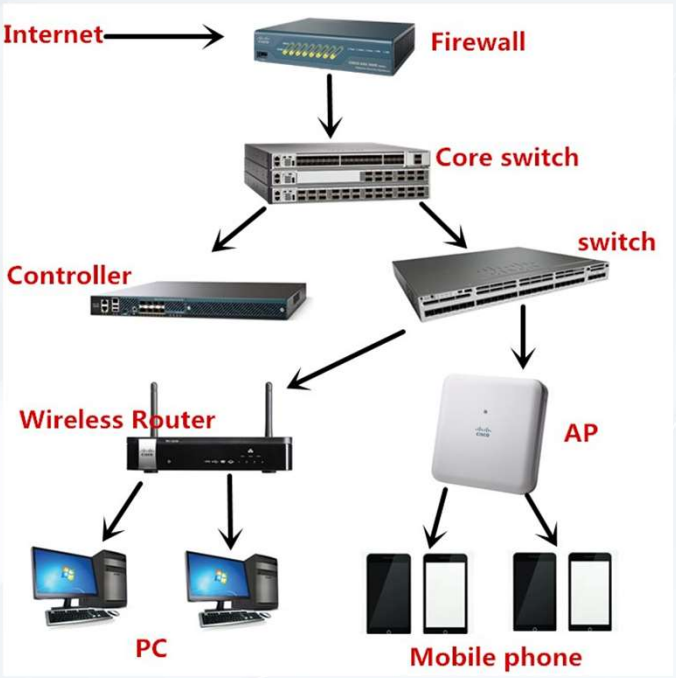


Best Practice Securing Wi-Fi (4)

- Matikan SSID Broadcast:
  - Matikan penyiaran nama jaringan (SSID) agar jaringan tidak terlihat oleh orang asing.
  - Pengguna yang sah masih dapat menghubungkan perangkat dengan memasukkan nama jaringan secara manual.

Best Practice Securing Wi-Fi (5)

- Aktifkan Firewall:
  - Aktifkan firewall di router untuk menghalangi akses yang tidak sah ke jaringan.



Best Practice Securing Wi-Fi (6)

- Batasi Jangkauan Sinyal:
  - Konfigurasikan router agar sinyalnya hanya mencakup area yang diperlukan dan tidak mencapai luar ruangan.
  - Ini akan mengurangi risiko akses yang tidak sah dari luar.

Best Practice Securing Wi-Fi (7)

- Aktifkan Network Encryption:
  - Gunakan teknologi seperti WPA3 atau WPA2 untuk mengenkripsi lalu lintas data di jaringan.
  - akan melindungi data yang dikirimkan antara perangkat dan router dari mata-mata yang tidak sah.

Best Practice Securing Wi-Fi (8)

- Aktifkan MAC Filtering:
  - Matikan opsi untuk mengizinkan hanya perangkat-perangkat dengan alamat MAC yang telah ditambahkan ke daftar izin untuk terhubung ke jaringan.

Best Practice Securing Wi-Fi (9)

- Perbarui Firmware:
  - Pastikan perangkat router yang digunakan menjalankan versi firmware terbaru dengan pembaruan keamanan terbaru.

Best Practice Securing Wi-Fi (10)

- Jangan Bagikan Kata Sandi:
  - Hindari membagikan kata sandi jaringan Wi-Fi kepada orang yang tidak perlu tahu.
  - Jika perlu memberikan akses, pertimbangkan pengaturan tamu yang terisolasi.

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

INSTITUT TEKNOLOGI DAN PENDIDIKAN MAHADEWA · BALI ·

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First

Best Practice Securing Wi-Fi (11)

- Gunakan Jaringan Tamu:
  - Banyak router modern mendukung jaringan tamu yang terisolasi dari jaringan utama.
  - Hal ini memungkinkan pengunjung terhubung tanpa mengakses perangkat di jaringan.