Hacking Wifi

Josua M Sinambela
Unit Sistem & Teknologi Informasi
Teknik Elektro UGM
josh at gadjahmada edu
http://josh.staff.ugm.ac.id

Pembahasan

- Wifi Today
- Standard Keamanan Wireless (Wifi)
- No ESSID ?
- MAC Filtering ?
- Cracking WEP & WPA
- Hotspot / Captive Portal
- Miss configuration jaringan Wifi
- Rogue AP
- Denial of Service
- Kesimpulan

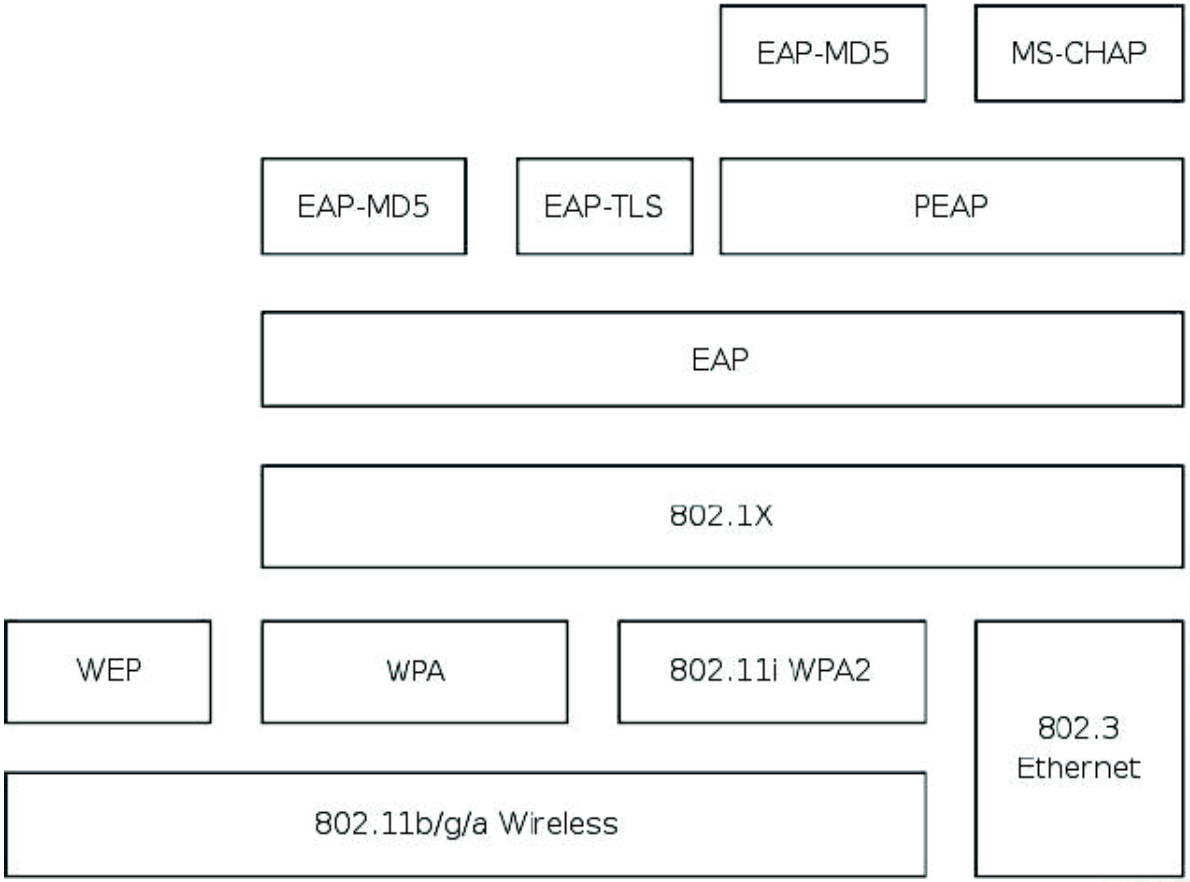
Wifi Today

- Jaringan di Kampus & Perkantoran (b/g)
- Antar ISP (a/b/g)
- Warnet-ISP (b/g)
- Hotspot di Hotel-hotel, RT/RW-net, Swalayan, Supermarket, CoffeeShop (b/g)
- Aparat Pemerintahan, Kepolisian dan Militer (a/b/g)

Standard Keamanan Wireless (Wifi)

- WEP
  - Algoritma RC4 yang lemah
  - CRC32 untuk integritas
  - Kunci bersifat statik
  - Umumnya AP/Card/Driver support WEP
- WPA (solusi sementara pengganti WEP)
  - PSK : Algoritma RC4 + Temporal Key (TKIP)
  - RADIUS : RC4 + Temporal Key (TKIP) + 802.1X + better ICV (MIC)
  - Umumnya AP/Card sudah mendukung, butuh upgrade applikasi, driver atau firmware
- WPA2 (RSN 802.11i)
  - Algoritma enkripsi AES dan TKIP
  - Butuh hardware baru (hardware keluaran 2003-kini)

802.blabla


EAP-MD5
MS-CHAP
EAP-MD5
EAP-TLS
PEAP
EAP
802.1X
WEP
WPA
802.11i WPA2
802.3
Ethernet
802.11b/g/a Wireless

No ESSID ?

- Menyembunyikan ESSID (hidden SSID)
  - Tidak menyertakan ESSID pada beacon
  - Saat deauth, SSID pasti akan di broadcast
- ESSID yang disembunyikan dapat dengan mudah dicloaked (dibuka)
- Tools Linux: aircrack, airjack & kismet
- Tools windows : airmagnet, airsnort
- Demo

MAC Filtering ?

- Fasilitas MAC Filtering umumnya sudah disediakanVendor Access Point/Router
- Useless, karena MAC address sangat mudah diganti atau ditiru (spoof).
- Tidak ada istilah konflik MAC address pada Wifi
- Demo

Cracking WEP & WPA

- Cracking WEP
  - Mengumpulkan IV yang lemah sebanyak mungkin (FMS attack : Key Scheduling Algorithm). Sangat bergantung pada jumlah IV lemah yang ditemukan.
  - Mengumpulkan IV yang unique (chopping attack)
  - Mempercepat proses pengumpulan IV dengan menggunakan trafik Injection.

Cracking WEP & WPA

- Cracking WPA (PSK)
  - WPA dapat diserang dengan menggunakan dictionary atau bruteforce attack.
  - Menggunakan kamus kata
  - Dapat dilakukan secara offline
- Tools : Aircrack, WEPlab, Airsnort

Hotspot / Captive Portal

- Hotspot umumnya dibangun dengan Captive Portal
- Otentikasi berdasar user/password
- Identifikasi setelah mendapat otentikasi, menggunakan MAC dan IP Address
  - MAC dan IP dapat di spoof
- Trafik masih Plain Text
  - Komunikasi setelah otentikasi dapat disadap
- Demo

Miss configuration jaringan Wifi

- Vendor umumnya menyediakan default konfigurasi
  - User/password
  - IP address
  - SNMP enable, private & public access
  - No Encryption
- Teknisi/Admin just plug n play
- Kesalahan konfigurasi pada design Hotspot/Captive portal
- Kesalahan setting firewall

Rogue AP

- AP yang terpasang secara ilegal pada area tertentu
- Digunakan oleh Hacker untuk menjebak targetnya.
  - Menggunakan ESSID yang sama dengan AP real.
  - Mendapatkan user/password pada hotspot
  - Membelokkan komunikasi data yang terjadi, sehingga memungkinkan dilakukan serangan MITM (Man In the Middle)
- Umumnya menggunakan Host AP (AP yang dibangun menggunakan Kartu Wireless Client)

Denial of Services

- Wireless sangat rentan dengan DoS
- Interference & Jamming
- Deauth broadcast
- Tools : void11, airjack, aircrack

Kesimpulan

- Ganti setting default AP
  - SSID, IP Address, Remote Manageable, User/Password
- Gunakan kombinasi beberapa fitur keamanan wireless (tidak menggunakan satu fitur saja
  - MAC Filtering, Disable ESSID,
  - Enkripsi minimum menggunakan WPA(PSK).
- Batasi Transmit Power pada AP
- The best solution today : WPA2/RSN 802.11i dengan mutualisme otentikasi
- Koneksi wireless tidak reliable !!

Pustaka

- S. Fluhrer1, I. Mantin2, & A. ShamirAug, 2001 http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf
- http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Robert Moskowitz December 1, 2003 http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding.pdf
- George OuJune 2, 2005 http://blogs.zdnet.com/Ou/?p=67
- Cedric Blancher June, 2005 http://sid.rstack.org/pres/0506_Recon_WirelessInjection.pdf
- Jouni Malinen, Host AP driver for Intersil **Prism2/2.5/3**, hostapd, and WPA Supplicant http://hostap.epitest.fi/
- http://www.aircrack-ng.org/
- http://www.kismetwireless.net/
- http://www.wlsec.net/void11/
- http://airsnort.shmoo.com/
- http://sourceforge.net/projects/cowpatty
- http://www.blackalchemy.to/project/fakeap/