

## 802.11 dan Keamanannya

Menurut Ohrtman dan Roeder (2003) tidak seperti sistem dengan kabel yang secara fisik dapat diamankan, jaringan *wireless* tidak terkungkung hanya di dalam gedung saja. Jaringan ini masih dapat terambil sejauh 1000 kaki di luar lingkungannya dengan sebuah laptop dan antena penguat. Hal ini membuat WLAN tidak kebal terhadap intersepsi.

Dengan mengetahui hal tersebut, komite 802.11 telah menambahkan lini pertama pertahanan yang disebut *Wireless Equivalency protocol* (WEP). WEP adalah protokol enkripsi yang menyediakan level keamanan seperti pada kabel. Saat ini, beberapa kelemahan telah ditemukan dalam protokol WEP. Mengacu kepada *Wi-Fi Alliance*, organisasi yang lebih kecil harus setidaknya mengaktifkan WEP, menggunakan *passwords* untuk melindungi pemakaian sumberdaya bersama, mengubah nama jaringan *default* (SSID), menggunakan penyaringan alamat MAC, menggunakan *session keys*, dan menggunakan sistem *virtual private network* (VPN). Mereka juga menyarankan agar perusahaan yang lebih besar berpikir untuk menggunakan metode keamanan tambahan.

### Keamanan 802.11 Dasar dan Permasalahannya yang Diketahui

Ketika pertama kali IEEE 802.11b diperkenalkan, keamanannya tergantung pada dua mekanisme keamanan dasar: SSID dan WEP. Beberapa pabrik menambahkan penyaringan alamat MAC ke dalam produknya.

#### Service Set ID (SSID)

SSID adalah sebuah *string* yang digunakan untuk menentukan domain *roaming* diantara banyak *access point* (AP). SSID dapat menjadi sebuah *password* dasar untuk masuk ke dalam jaringan. Namun, klaim ini dengan mudah dapat ditentang karena AP menyiarkan SSIDnya beberapa kali dalam satu detik dan peralatan analisis seperti Airmagnet, NetStumbler, atau Wildpackets Airopeek dapat digunakan untuk membacanya. Pengamanan dengan SSID patut dipertimbangkan, mengubah SSID secara periodik atau dengan tidak menyiarkan SSID dapat menjadi pertahanan lapis pertama.

#### Wired Equivalent Protocol (WEP)

Standar IEEE 802.11b juga menyediakan sebuah metode autentikasi dan enkripsi yang disebut WEP untuk mengatasi masalah keamanan. Enkripsi WEP berdasarkan atas RC4 dengan level enkripsi 64-bit atau 128-bit yang lebih tinggi. Untuk mencegah akses yang tidak diizinkan, WEP juga menyediakan protokol autentikasi.

Dua bentuk autentikasi yang diberikan 802.11b: *open system* dan *shared key*. Dengan *open system*, pengguna melewati proses autentikasi. Cara ini sering ditemukan di akses jaringan umum seperti bandara. Cara ini umum digunakan jika proses autentikasi sudah dilayani oleh metode lain seperti *login* menggunakan halaman *web*. Dengan *shared key*, proses autentikasi dilakukan dengan mencocokkan dua buah kunci yang sama yang dimiliki oleh AP dan *client*. Cara ini terlihat lebih aman, namun dengan waktu yang cukup, jarak yang cukup dekat, dan *tools* yang diunduh dari internet, seorang *hacker* dapat dengan mudah mengetahui kuncinya. Cara ini juga akan menjadi rumit jika melibatkan jaringan yang besar karena membutuhkan waktu yang banyak untuk mengubah kunci secara periodik ke seluruh perangkat.

### Penyaringan Alamat MAC

Setiap peralatan jaringan memiliki alamat MAC yang unik, berbeda satu dengan yang lainnya. Dengan mendaftarkan alamat yang diperbolehkan atau yang tidak diperbolehkan masuk ke dalam jaringan pada AP, maka jaringan memiliki prosedur untuk melakukan proses autentikasi. Dengan peralatan tertentu, *sniffer* dengan mudah mengetahui alamat-alamat MAC yang beroperasi dalam jaringan, dengan *driver* Linux yang ada di internet untuk banyak kartu WLAN, seorang *hacker* dapat mengganti alamat MAC kartu jaringannya untuk menyamar menjadi peralatan yang telah terautentikasi.

### Tipe-tipe Ancaman Keamanan

#### Resiko Keamanan

Keamanan dapat didefinisikan sebagai menjaga orang-orang melakukan sesuatu yang kita tidak inginkan untuk dilakukannya, atas, atau dari data, komputer, atau peralatan lainnya. Informasi yang tersimpan, akurasi dan nilai informasi, akses atas layanan di dalam atau keluar, dan privasi organisasi adalah yang menanggung resiko. Resiko keamanan datang dari *hacker*, penyusup kriminal, saingan usaha, orang luar, kontraktor atau pegawai yang tidak puas.

#### Model Keamanan WLAN

Empat penggolongan serangan utama yang disebabkan oleh penyusuk ke dalam jaringan: intersepsi (*interception*), pabrikasi (*fabrication*), modifikasi (*modification*), dan interupsi (*interruption*). Penggolongan yang kelima dari serangan adalah penyangkalan informasi (*repudiation*) adalah serangan atas akuntabilitas informasi. Tabel 4. Menjelaskan kelima penggolongan serangan tersebut.

**Tabel 4.** Lima Penggolongan Serangan

Attack	On	Solved By
Interception	Confidentiality and privacy	Encryption/decryption
Fabrication	Authenticity	Authentication
Modification Replay Reaction	Integrity	Attacks on Integrity can be solved by digital signatures on every message.
Interruption	Availability	No effective solutions exist for interruption / Denial of Service attacks on availability.
Repudiation	Nonrepudiation	Non-repudication currently still suffers of cases of identity theft.

Sumber: Ohrtman dan Roeder (2003)

### Intersepsi

Intersepsi adalah serangan pasif atas kerahasiaan informasi dimana entitas penyusup dapat membaca informasi yang dikirimkan oleh sumber ke tujuannya. *Sniffing* adalah salah satu contoh serangan intersepsi.

***Eavesdropping dan Sniffing*** *Eavesdropping* adalah secara pasif mengumpulkan informasi dari jaringan. Sama seperti mendengarkan pembicaraan, informasi dapat didengarkan dalam jaringan. Dengan tambahan peralatan yang telah ada saat ini, *eavesdropper* (pelaku *eavesdropping*) tidak hanya terbatas mengumpulkan paket untuk dianalisis, tetapi ia dapat secara aktual melihat sesi interaktif seperti halaman web yang dilihat pengguna yang valid. *Eavesdropper* juga dapat menangkap pertukaran autentikasi yang lemah, seperti *login* situs *web*, menduplikasinya dan kemudian meningkatkan kemampuan akses.

### Pabrikasi

Pabrikasi adalah serangan aktif atas autentikasi di mana penyusup berpura-pura menjadi entitas sumber. Paket-paket tiruan (*spoofed*) dan e-mail palsu adalah contoh dari serangan pabrikasi. Contoh pabrikasi yaitu *man-in-the-middle attacks*, *spoofing*, *insertion attacks*, dan *brute-force password attacks*.

**Man-in-the-Middle Attacks** Untuk dapat melakukan serangan ini, dua *host* harus diyakinkan jika komputer di tengah (*in-the-middle*) adalah *host* yang lainnya. Versi klasik dari serangan ini terjadi ketika penyerang mengintersepsi paket dari jaringan, memodifikasinya, dan memasukkannya kembali ke dalam jaringan.

**Spoofing** *Spoofing* adalah berpura-pura menjadi seseorang atau sesuatu yang sebenarnya bukan diri kita, seperti menggunakan *password* dan *user ID* seseorang.

**Insertion Attacks** Tindakan mengatur perangkat untuk menambahkan akses ke sebuah jaringan atau memasukkan perangkat yang tidak terotorisasi ke dalam jaringan untuk menambahkan akses dinamai *insertion attack*. AP yang tidak terotorisasi dapat ditempatkan ke dalam jaringan sehingga pengguna akan terhubung dengannya daripada ke peralatan yang semestinya. Jika AP ini ditempatkan di bawah *firewall* perusahaan maka ancaman akan semakin serius.

**Brute-Force Password Attacks** Juga dikenal sebagai *password cracking* (pemecah kata kunci) atau *dictionary attack*, serangan jenis ini memanfaatkan sebuah kamus (*dictionary*) dan membuat percobaan yang berulang untuk menguji *password* untuk mendapatkan akses ke jaringan.

#### **Modifikasi (*Modification*)**

Modifikasi adalah sebuah serangan aktif atas integritas dimana entitas penyusup mengubah informasi yang dikirimkan oleh entitas pengirim ke entitas penerima.

**Kehilangan Perangkat (*Lost of Equipment*)** Kehilangan perangkat telah menjadi hal yang menyita perhatian otoritas keamanan. Peralatan yang diambil alih dapat digunakan untuk mengakses jaringan sebagai pengguna yang telah terotorisasi. Ancaman semacam ini juga berlaku untuk jaringan dengan kabel.

**Infeksi oleh Virus** Infeksi virus juga hal lain yang kerap menimpa jaringan dengan kabel ataupun *wireless*. Virus dapat menginfeksi peralatan dengan perangkat *wireless* dan menyebar lebih luas melalui jaringan kabel ataupun tanpa kabel.

## **Replay**

*Replay* adalah serangan aktif atas integritas dimana penyusup mengirimkan kembali informasi yang telah dikirim dari entitas sumber ke entitas tujuan. Metode keamanan 802.11 dasar tidak memiliki perlindungan terhadap *replay*.

**Traffict Redirection** Sebuah stasiun penyerang dapat meracuni (*poison*) tabel *Address Resolution Protocol* (ARP) dalam *switch* dalam jaringan kabel melalui AP, menyebabkan paket untuk jaringan dengan kabel diarahkan ulang ke stasiun penyerang. Dengan demikian, penyerang kemudian dapat melakukan *man-in-the-middle attack*.

**Invasi dan Pencurian Sumberdaya** Sekali penyerang mendapatkan pengetahuan tentang bagaimana admittasi kontrol WLAN, ia juga akan mendapatkan akses penuh terhadap jaringan. Hal tersebut terjadi misalnya ketikan alamat MAC dan alamat IP pengguna valid diketahui, ia akan menunggu pengguna tersebut berhenti menggunakan jaringan dan kemudian menggantikannya dan berpura-pura menjadi seorang pengguna yang terotorisasi, dengan demikian ia mampu memanfaatkan jaringan dengan sama.

## **Reaksi (Reaction)**

Reaksi adalah serangan aktif dimana paket dikirimkan oleh seorang penyusup ke tujuan. Penyusup kemudian memonitor reaksi . Informasi tambahan kemudian diperoleh dari sisi saluran baru tersebut.

## **Interupsi (Interruption)**

Interupsi adalah serangan aktif atas ketersediaan informasi dimana seorang penyusup menghalangi informasi yang dikirimkan dari entitas asal ke entitas tujuan. Contoh serangan jenis ini adalah *denial of service* (DoS) dan *network flooding*.

**Denial of Service (DoS)** Serangan DoS tidak membuat *hacker* dapat mengakses jaringan, tetapi secara mendasar membuat sistem komputer tidak dapat diakses dengan memberikan beban berlebih (*overloading*) kepada server atau jaringan dengan lalu lintas yang tak berguna sehingga pengguna yang terlegitimasi tidak dapat mengaksesnya lagi.

**Rogue Networks dan Station Redirection** Sebuah AP yang nakal (*rogue*) dimiliki oleh penyusup yang menerima koneksi dari stasiun yang kemudian melakukan intersepsi trafik dan mungkin juga melakukan *man-in-the-middle attack* sebelum mengizinkan lalu lintas informasi mengalir ke jaringan yang sebenarnya.

### **Repudiation**

*Repudiation* adalah serangan aktif atas pengakuan (*nonrepudiation*) oleh sumber ataupun tujuan informasi dimana entitas sumber menyangkal telah mengirimkan pesan atau entitas tujuan menyangkal menerima sebuah pesan. Keamanan 802.11 dasar tidak memiliki pengakuan.

### **Kebijakan Keamanan – Sebuah Rentang Opsi**

Setiap bisnis memiliki kebutuhan pengamanan yang unik, tabel 2. menunjukkan level pengamanan yang bervariasi, konfigurasi, apa yang diamankan oleh konfigurasi dan aplikasi apa yang mungkin digunakan dalam konfigurasi.

**Tabel 2.** Rentang Opsi Pengamanan untuk Jaringan *Wireless*

	<b>Security Level</b>	<b>Configuration</b>	<b>What Is Secured?</b>	<b>Applications</b>
0	No security	Network out of the box and no configuration (no WEP)	Nothing	There is no legitimate unsecured application. Nevertheless, many users operate their equipment in this mode out of the box.
1	Public access	User authentication and must supply VPN through the Internet back to the enterprise	Network access	Hot spots, libraries, coffee shops, hotels, airports, and so on with portability
2	Limited security	40- or 128-bit WEP, MAC <i>access control list</i> (ACL),	Some network	Home and SOHO with portability

		and no broadcast	access and data privacy	
3	Basic security	<i>Wi-Fi Protected Access (WPA)</i> (later 802.11i)	Network access and data privacy	Home, SOHO, and small enterprise with portability
4	Advanced security	802.1x/EAP-X and RADIUS	Network access and data privacy	Enterprise with portability
5	End-to-end security	VPNs such as the <i>Point-to-Point Tunneling Protocol (PPTP)</i> , <i>PPTPv2</i> , <i>Layer 2 Tunneling Protocol (L2TP)</i> , Kerberos, and <i>IP Security (IPSec)</i>	Network access and data privacy	Special applications, business travelers, telecommuting, business to business, and enterprise with outside users

Sumber: Ohrtman dan Roeder (2003)

### Pengamanan 802.11 dengan WPA

Wi-Fi Protected Access (WPA) diterapkan untuk menggantikan WEP dengan kemampuan yang lebih tinggi. WPA menggunakan *Temporal Key Integrity Protocol (TKIP)*, sebuah enkripsi yang lebih kuat daripada yang digunakan dalam WEP. TKIP menggunakan *key hashing (KeyMix)* dan pemeriksaan integritas pesan nonlinear (MIC). TKIP juga menggunakan protokol *rapid-keying (ReKey)* yang mengubah kunci enkripsi setiap sekitar 10.000 paket. Namun, TKIP tidak menghilangkan cacat fundamental dalam keamanan *wireless*. Jika penyusup menyerang TKIP, iya tidak hanya akan merusak kerahasiaan informasi, namun juga penguasaan kendali akses dan autentikasi.

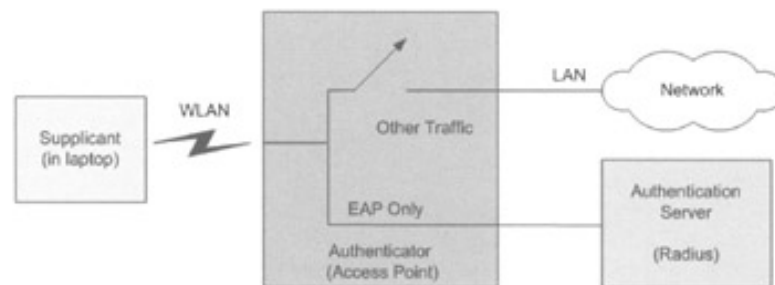
WPA dapat berjalan dengan dua cara yang berbeda, tergantung tipe jaringan. Di rumah dan kantor kecil (SOHO) yang tidak memiliki server autentikasi (*authentication server / AS*), WPA akan bekerja pada mode *preshared key* atau kunci yang dibagikan. Pengguna secara sederhana memasukkan kunci jaringan untuk mengaksesnya. Dalam mode *managed*, WPA akan bekerja dengan AS dan membutuhkan dukungan dari 802.1x dan EAP (*Extensible Authentication Protocol*). 802.1x dan EAP mengizinkan *adapter* jaringan klien melakukan negosiasi melalui AP dengan AS sebagai *backend*

menggunakan transaksi yang terenkripsi dengan aman untuk mempertukarkan kunci sesi (*session key*). WPA2 atau WPA generasi kedua telah mendukung algoritma enkripsi yang disebut *Advanced Encryption Standard* (AES) yang menggantikan algoritma enkripsi berbasis RC4 dalam 802.11i.

### Pengamanan Tingkat Lanjut dengan 802.1x dan EAP

802.1x menyediakan sebuah *framework* autentikasi untuk WLAN, mengizinkan pengguna diotentikasi oleh otoritas pusat. Algoritma yang saat ini digunakan untuk menentukan pengguna autentik terbuka dan dapat menggunakan lebih dari satu algoritma. Contohnya adalah solusi dengan sertifikat (seperti *EAP-Transport Layer Security* [EAP-TLS]), berdasarkan *password* (seperti *EAP-One Time Password* [OTP-OTP] dan *EAP-Message Digest 5* [EAP-MD5]), berdasarkan kartu cerdas (*smart-card*) (seperti *EAP-Subscriber Identification Module* [EAP-SIM]), dan hibrid (seperti *EAP-Tunneled TLS Authentication Protocol* [EAP-TTLS]) yang menggunakan algoritma sertifikat dan *password*. Beberapa perusahaan juga menawarkan algoritma solusi EAP milik sendiri seperti Cisco's *Lightweight EAP* (LEAP). 802.1x menggunakan EAP, sebuah protokol yang telah ada (RFC2284) yang bekerja pada Ethernet, Token Ring, atau WLAN untuk pertukaran pesan selama proses autentikasi.

**802.1x Network Port Authentication** Autentikasi 802.1x untuk WLAN memiliki 3 komponen utama: *supplicant* (umumnya perangkat lunak klien), *authenticator* (biasanya AP), dan AS (biasanya sebuah *server* RADIUS, meskipun RADIUS tidak secara spesifik diperlukan oleh 802.1x). *Authenticator* menghubungkan jaringan LAN diilustrasikan dalam gambar 2..



**Gambar 2.** Autentikasi dalam 802.1x

**Extensible Authentication Protocol (EAP)** EAP didesain atas pemikiran akan fleksibilitas dan telah digunakan sebagai dasar dari banyak tipe autentikasi jaringan. 802.1x adalah berdasarkan atas EAP. Ini berarti bahwa *switch* dan AP yang mendukung 802.1x dapat mendukung berbagai metode autentikasi,

termasuk berdasarkan sertifikat, *smart card*, *token card*, *one-time password*, dan lainnya. IEEE 802.1x dapat terintegrasi dengan baik terhadap standar terbuka untuk *authentication*, *authorization*, dan *accounting* (AAA) (termasuk RADIUS dan *Lightweight Directory Access Protocol* [LDAP]) jadi ini juga dapat diterapkan pada infrastruktur yang ada untuk mengatur *dial-up network* dan VPN. Server RADIUS yang mendukung EAP dapat digunakan untuk mengatur akses jaringan berbasis IEEE 802.1x.

#### Virtual Private Network (VPN)

Sebuah VPN mengizinkan kelompok yang spesifik dari pengguna untuk mengakses jaringan *private* (pribadi) secara aman melalui internet atau jaringan lainnya. VPN memanfaatkan *tunneling* (terowongan), enkripsi, autentikasi dan kendali akses atas jaringan publik.

#### Pustaka:

Ohrman F dan Roeder R, 2003, *Wi-Fi Handbook: Building 802.11b Wireless Networks*, McGraw-Hill