

Keamanan Jaringan Wireless

Oleh :

Janner Simarmata
sijanner@yahoo.com
<http://simarmata.cogia.net>

*Dipublikasikan dan didedikasikan
untuk perkembangan pendidikan di Indonesia melalui*

MateriKuliah.Com

Lisensi Pemakaian Artikel:

*Seluruh artikel di **MateriKuliah.Com** dapat digunakan, dimodifikasi dan disebarakan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut Penulis. Hak Atas Kekayaan Intelektual setiap artikel di **MateriKuliah.Com** adalah milik Penulis masing-masing, dan mereka bersedia membagikan karya mereka semata-mata untuk perkembangan pendidikan di Indonesia. **MateriKuliah.Com** sangat berterima kasih untuk setiap artikel yang sudah Penulis kirimkan.*

1 Teknologi Wireless

Teknologi wireless, memungkinkan satu atau lebih peralatan untuk berkomunikasi tanpa koneksi fisik, yaitu tanpa membutuhkan jaringan atau peralatan kabel. Teknologi wireless menggunakan transmisi frekwensi radio sebagai alat untuk mengirimkan data, sedangkan teknologi kabel menggunakan kabel. Teknologi wireless berkisar dari sistem kompleks seperti *Wireless Local Area Network* (WLAN) dan telepon selular hingga peralatan sederhana seperti headphone wireless, microphone wireless dan peralatan lain yang tidak memproses atau menyimpan informasi. Disini juga termasuk peralatan infra merah

seperti remote control, keyboard dan mouse komputer wireless, dan headset stereo hi-fi wireless, semuanya membutuhkan garis pandang langsung antara transmitter dan receiver untuk membuat hubungan.

1.1 Jaringan Wireless

Jaringan Wireless berfungsi sebagai mekanisme pembawa antara peralatan atau antar peralatan dan jaringan kabel tradisional (*jaringan perusahaan dan internet*). Jaringan wireless banyak jenisnya tapi biasanya digolongkan ke dalam tiga kelompok berdasarkan jangkauannya: *Wireless Wide Area Network* (WWAN), WLAN, dan *Wireless Personal Area Network* (WPAN). WWAN meliputi teknologi dengan daerah jangkauan luas seperti selular 2G, *Cellular Digital Packet Data* (CDPD), *Global System for Mobile Communications* (GSM), dan Mobitex. WLAN, mewakili local area network wireless, termasuk diantaranya adalah 802.11, HiperLAN, dan beberapa lainnya. WPAN, mewakili teknologi personal area network wireless seperti Bluetooth dan infra merah. Semua teknologi ini disebut “**tetherless**” dimana mereka menerima dan mengirim informasi menggunakan gelombang electromagnet (EM). Teknologi wireless menggunakan panjang gelombang berkisar dari frekwensi radio (RF) hingga inframerah. Frekwensi pada RF mencakup bagian penting dari spectrum radiasi EM, yang berkisar dari 9 kilohertz (kHz), frekwensi terendah yang dialokasikan untuk komunikasi wireless, hingga ribuan *gigahertz* (GHz). Karena frekwensi bertambah diluar spectrum RF, energi EM bergerak ke IR dan kemudian ke spectrum yang tampak.

1.2 Kemunculan Teknologi Wireless

Mulanya, peralatan handheld mempunyai kegunaan yang terbatas karena ukurannya dan kebutuhan daya. Tapi, teknologi berkembang, dan peralatan handheld menjadi lebih kaya akan fitur dan mudah dibawa. Yang lebih penting, berbagai peralatan wireless dan teknologi yang mengikutinya sudah muncul. Telepon mobil, sebagai contoh, telah meningkat kegunaannya yang sekarang memungkinkannya berfungsi sebagai PDA selain telepon. Smart phone adalah gabungan teknologi telepon mobil dan PDA yang menyediakan layanan suara normal dan email, penulisan pesan teks, paging, akses web dan pengenalan suara. Generasi berikutnya dari telepon mobil, menggabungkan

kemampuan PDA, IR, Internet wireless, email dan global positioning system (GPS). Pembuat juga menggabungkan standar, dengan tujuan untuk menyediakan peralatan yang mampu mengirimkan banyak layanan. Perkembangan lain yang akan segera tersedia adalah sistem global untuk teknologi yang berdasar komunikasi bergerak (berdasar GSM) seperti *General Packet Radio Service* (GPRS), *Local Multipoint Distribution Service* (LMDS), *Enhanced Data GSM Environment* (EDGE), dan *Universal Mobile Telecommunications Service* (UMTS). Teknologi-teknologi ini akan menyediakan laju transmisi data yang tinggi dan kemampuan jaringan yang lebih besar. Tapi, masing-masing perkembangan baru akan menghadirkan resiko keamanannya sendiri, dan badan pemerintah harus memikirkan resiko ini untuk memastikan bahwa asset yang penting tetap terjaga.

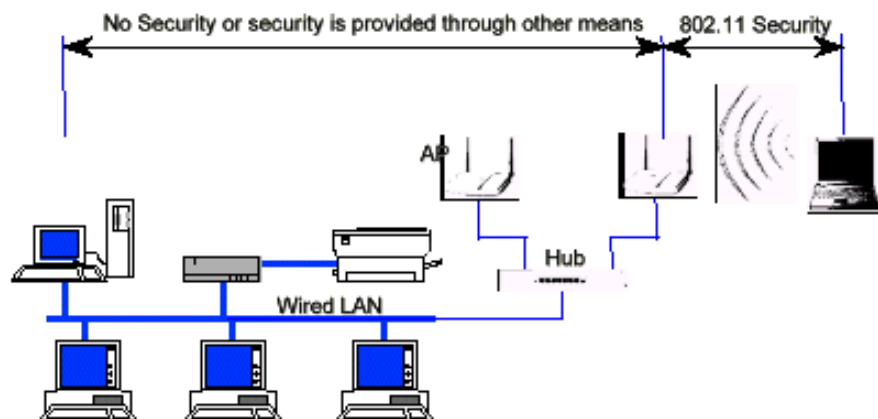
1.3 Ancaman Keamanan dan Penurunan Resiko Wireless

Ada sembilan kategori ancaman keamanan yang berkisar dari kesalahan dan penghilangan ancaman hingga privasi pribadi. Semuanya ini mewakili potensi ancaman dalam jaringan wireless juga. Tapi, perhatian utama pada komunikasi wireless adalah pencurian peralatan, hacker jahat, kode jahat, pencurian dan spionase industri dan asing. Pencurian bisa terjadi pada peralatan wireless karena mudah dibawa. Pengguna sistem yang berhak dan tidak berhak bisa melakukan penggelapan dan pencurian, pengguna yang berhak lebih mungkin untuk melakukan hal itu. Karena pengguna sistem bisa tahu resources apa yang dimiliki oleh suatu sistem dan kelemahan keamanan sistem, lebih mudah bagi mereka untuk melakukan penggelapan dan pencurian. Hacker jahat, kadang-kadang disebut cracker, adalah orang-orang yang masuk ke sistem tanpa hak, biasanya untuk kecurian pribadi atau untuk melakukan kejahatan. Hacker jahat biasanya orang-orang dari luar organisasi (*meskipun dalam organisasi dapat menjadi ancaman juga*). Hacker semacam ini bisa mendapat akses ke access point jaringan wireless dengan menguping pada komunikasi peralatan wireless. Kode jahat meliputi virus, worm, Kuda Trojan, logic bombs, atau software lain yang tidak diinginkan yang dirancang untuk merusak file atau melemahkan sistem. Pencurian pelayanan terjadi ketika pengguna tidak berhak mendapatkan akses ke jaringan dan memakai sumber daya jaringan. Spionase asing dan industri meliputi pengumpulan data rahasia perusahaan atau intelijen informasi

pemerintah yang dilakukan dengan menguping. Pada jaringan wireless, ancaman spionase dengan menguping dapat terjadi pada transmisi radio. Serangan yang dihasilkan dari ancaman ini, jika berhasil, menempatkan sistem perusahaan, dan datanya beresiko. Memastikan kerahasiaan, integritas, keaslian, dan ketersediaan adalah tujuan utama dari kebijakan keamanan semua pemerintah.

2 Keamanan WLAN 802.11

Spesifikasi IEEE 802.11 menunjukkan beberapa layanan yang menyediakan lingkungan operasi yang aman. Layanan keamanan disediakan sebagian besar oleh protocol *Wired Equivalent Privacy* (WEP) untuk melindungi link level data selama transmisi wireless antara klien dan access point. WEP tidak menyediakan keamanan end-to-end, tapi hanya untuk bagian wireless dari koneksi seperti ditunjukkan pada gambar 1.



Gambar 1. Keamanan WLAN 802.11 pada Jaringan yang umum

2.1 Fitur Keamanan WLAN 802.11

Tiga layanan keamanan dasar yang ditentukan oleh IEEE untuk lingkungan WLAN adalah sebagai berikut :

- Otentifikasi. Tujuan utama dari WEP adalah untuk menyediakan layanan keamanan untuk memastikan identitas lokasi klien yang berkomunikasi. Ini menyediakan kontrol bagi jaringan dengan menolak akses ke stasiun klien yang tidak dapat memberikan otentifikasi secara benar. Layanan ini menangani

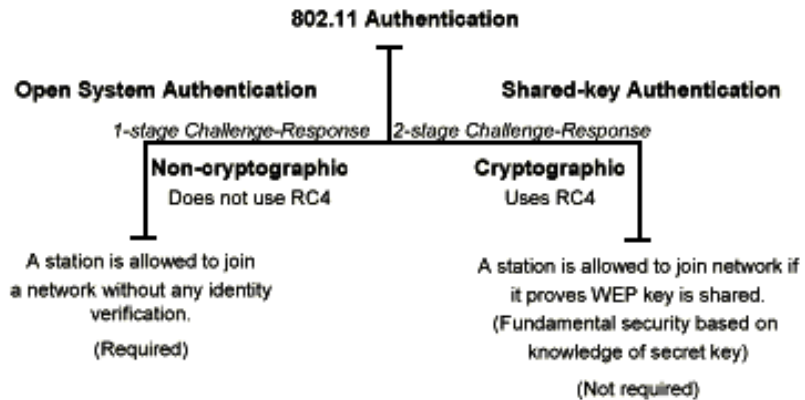
pertanyaan,”Apakah hanya orang-orang yang berhak yang diijinkan untuk mendapatkan akses ke jaringan saya ?”

- Kerahasiaan. Kerahasiaan, atau privasi, adalah tujuan kedua WEP. Ini dibuat untuk menyediakan “privasi yang diperoleh pada jaringan kabel.” Maksudnya adalah untuk mencegah bocornya informasi dengan cara menguping (*serangan pasif*). Layanan ini, secara umum, menangani pertanyaan,”Apakah hanya orang-orang yang berhak yang diijinkan melihat data saya ?”
- Integritas. Tujuan lain dari WEP adalah layanan keamanan yang dibuat untuk memastikan bahwa pesan tidak dirubah sewaktu pengiriman antara klien wireless dan access point dalam serangan aktif. Layanan ini menangani pertanyaan,”Apakah data yang datang ke atau keluar jaringan dapat dipercaya ? Apakah data ini telah dirusak ?”

Penting untuk dicatat bahwa standar tidak menangani layanan keamanan lain seperti audit, otorisasi, dan pengakuan.

2.1.1 Otentifikasi

Spesifikasi IEEE 802.11 menentukan dua cara untuk memvalidasi pengguna wireless yang mencoba untuk mendapatkan akses ke jaringan kabel: *otentifikasi open-system* dan *otentifikasi shared-key*. Otentifikasi shared-key didasarkan pada kriptografi, dan yang lainnya tidak. Teknik otentifikasi open-system bukan benar-benar otentifikasi; access point menerima stasion bergerak tanpa memverifikasi identitas stasion. Harus juga dicatat bahwa otentifikasi hanya satu arah yaitu hanya stasion bergerak yang di otentifikasi. Stasion bergerak harus percaya bahwa dia sedang berkomunikasi dengan AP nyata. Sistem klasifikasi (*taksonomi*) teknik ini untuk 802.11 digambarkan pada gambar 2.

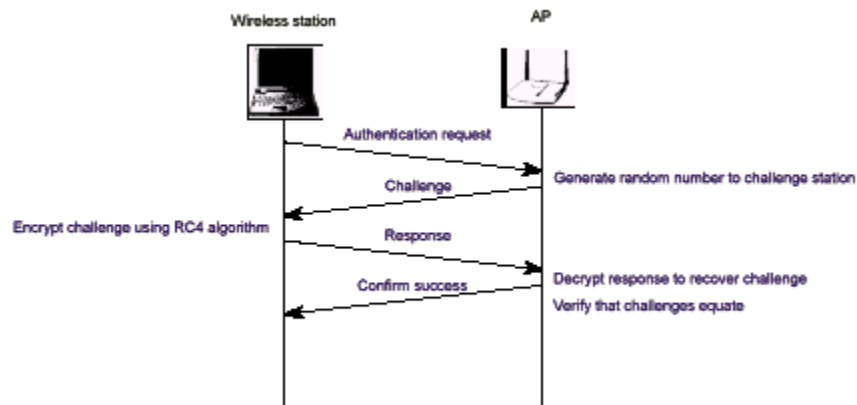


Gambar 2. Taksonomi Teknik Otentifikasi 802.11

Dengan otentifikasi open system, klien diotentifikasi jika dia merespon dengan alamat MAC selama keduanya bertukar pesan dengan access point. Selama pertukaran, klien tidak divalidasi tapi hanya merespon dengan kolom yang benar pada saat pertukaran pesan. Nyatanya, tanpa validasi kriptografis, otentifikasi open-system sangat rentan terhadap serangan dan mengundang akses yang tidak berhak. Otentifikasi open-system adalah satu-satunya bentuk otentifikasi yang dibutuhkan oleh spesifikasi 802.11.

Otentifikasi shared-key adalah teknik kriptografis untuk otentifikasi. Ini adalah skema “challenge-response” sederhana berdasarkan pada apakah klien mempunyai pengetahuan tentang rahasia shared. Pada skema ini, seperti digambarkan pada gambar 3, teguran acak dihasilkan oleh access point dan dikirimkan ke klien wireless. Klien, dengan menggunakan kunci kriptografis yang di shared dengan AP, mengenkrip teguran ini (atau disebut “nonce” dalam bahasa keamanan) dan mengembalikan hasilnya ke AP. AP mendekrip hasil yang dikirimkan oleh klien dan memungkinkan akses hanya jika nilai yang didekrip sama dengan teguran acak yang dikirimkan. Algoritma yang digunakan dalam perhitungan kriptografi dan untuk pembuatan teks teguran 128 bit adalah RC4 stream cipher yang dibuat oleh Ron Rivest dari MIT. Harus dicatat bahwa metoda otentifikasi yang dijelaskan diatas adalah teknik kriptografi yang belum sempurna, dan ini tidak menyediakan otentifikasi dua arah. Yaitu, klien tidak mengotentifikasi AP, dan karena itu tidak ada keyakinan bahwa klien sedang berkomunikasi dengan AP dan jaringan wireless yang sah. Juga penting dicatat bahwa skema challenge-response sepihak dan sederhana diketahui lemah. Mereka mengalami banyak serangan dari orang-orang

yang tidak berpengalaman. Spesifikasi IEEE 802.11 tidak memerlukan otentifikasi shared-key.



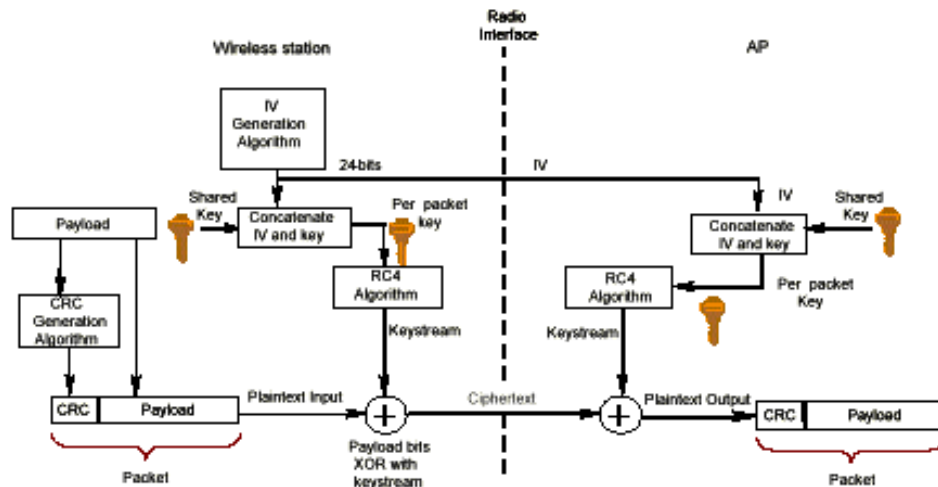
Gambar 3. Aliran Pesan Otentifikasi Shared-key

2.1.2 Privasi

Standar 802.11 mendukung privasi (*kerahasiaan*) melalui penggunaan teknik kriptografis untuk interface wireless. Teknik kriptografis WEP untuk kerahasiaan juga menggunakan algoritma RC4 symmetric-key, stream chipper untuk membuat urutan data semi acak. “Key stream” ini cukup dengan ditambah modulo 2 (*eksklusif OR*) ke data yang akan dikirimkan. Melalui teknik WEP, data dapat dilindungi dari pengungkapan selama pengiriman melalui hubungan wireless. WEP diterapkan ke semua data diatas lapisan WLAN 802.11 untuk melindungi lalu lintas seperti Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), dan Hyper Text Transfer Protocol (HTTP).

Seperti ditentukan pada standar 802.11, WEP mendukung hanya ukuran kunci kriptografis 40 bit untuk shared key. Tapi, banyak vendor menawarkan ekstensi WEP yang tidak standar yang mendukung panjang key dari 40 bit hingga 104 bit. Setidaknya satu vendor mendukung ukuran key 128 bit. Kunci WEP 104 bit, misalnya, dengan Initialization Vector (IV) 24 bit menjadi key RC4 128 bit. Secara umum, semuanya sama, kenaikan ukuran key meningkatkan keamanan dari teknik kriptografis. Tapi, selalu dimungkinkan bahwa kekurangan penerapan atau kekurangan rancangan menjadikan key yang panjang menurun keamanannya. Penelitian telah menunjukkan bahwa ukuran key

lebih besar dari 80 bit, membuat pemecahan kode menjadi hal yang tidak mungkin. Untuk key 80 bit, jumlah key yang mungkin-dengan ruang key lebih dari 10^{10} - melampaui daya perhitungan. Pada pelaksanaannya, sebagian besar penggunaan WLAN tergantung pada key 40 bit. Lebih lanjut, serangan baru-baru ini telah menunjukkan bahwa pendekatan WEP untuk privasi rentan terhadap serangan tertentu tanpa memandang ukuran key. Tapi, komunitas standar kriptografis dan vendor WLAN telah membuat WEP yang telah ditingkatkan, yang tersedia sebagai penerapan pra standar vendor tertentu. Privasi WEP digambarkan secara konsep pada gambar 4.



Gambar 4. Privasi WEP Menggunakan Algoritma RC4

2.1.3 Integritas

Spesifikasi IEEE 802.11 juga menguraikan alat untuk menyediakan integritas data pada pesan yang dikirimkan antara klien wireless dan access point. Layanan keamanan ini dirancang untuk menolak setiap pesan yang telah dirubah oleh musuh aktif “*ditengah*”. Teknik ini menggunakan pendekatan Cyclic Redundancy Check terenkripsi sederhana. Seperti digambarkan pada diagram diatas, CRC-32, atau urutan pengecekan frame, dihitung pada masing-masing payload sebelum transmisi. Paket yang dibungkus integritas kemudian dienkripsi menggunakan key stream RC4 untuk menyediakan ciphertext message. Pada bagian penerima, dekripsi dilakukan dan CRC dihitung ulang pada pesan yang diterima. CRC yang dihitung pada bagian penerima dibandingkan dengan

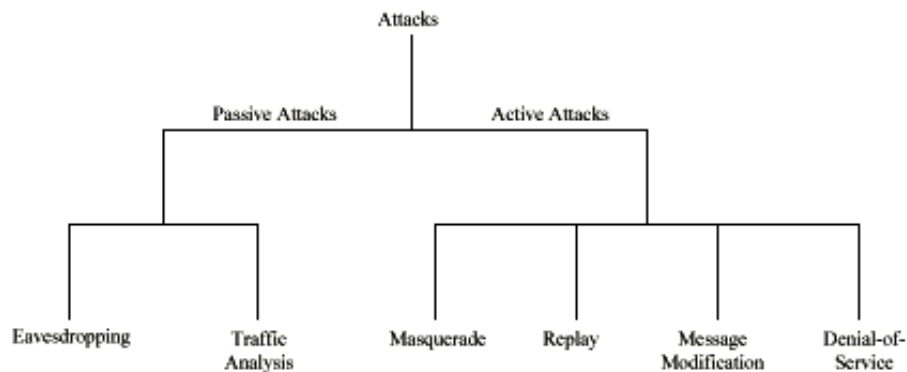
yang dihitung pada pesan asli. Jika CRC tidak sama, yaitu, “diterima dengan kesalahan”, ini akan mengindikasikan pelanggaran integritas dan paket akan dibuang. Seperti dengan layanan privasi, integritas 802.11 rentan terhadap serangan tertentu tanpa memandang ukuran kunci. Kekurangan mendasar dalam skema integritas WEP adalah CRC sederhana bukan mekanisme aman secara kriptografis seperti hash atau kode otentifikasi pesan. Sayangnya, spesifikasi IEEE 802.11 tidak menentukan alat apapun untuk manajemen key (*penanganan daur hidup dari key kriptografis dan materi terkait*). Oleh karena itu, pembuatan, pendistribusian, penyimpanan, loading, escrowing, pengarsipan, auditing, dan pemusnahan materi itu diserahkan pada WLAN yang dipakai. Manajemen key pada 802.11 diserahkan sebagai latihan bagi pengguna jaringan 802.11. Sebagai hasilnya, banyak kerentanan dapat dimasukkan ke lingkungan WLAN. Kerentanan ini termasuk kunci WEP yang tidak unik, tidak pernah berubah, default pabrik, atau kunci lemah (*semua nol, semua satu, berdasarkan pada password yang mudah ditebak, atau pola-pola lain yang mudah*). Sebagai tambahan, karena manajemen key bukan merupakan bagian dari spesifikasi 802.11 asli, karena distribusi key tidak terselesaikan, maka WLAN yang diamankan dengan WEP tidak terjaga dengan baik. Jika sebuah perusahaan mengetahui kebutuhan untuk sering merubah key dan membuatnya acak, maka ini merupakan tugas berat pada lingkungan WLAN yang besar. Sebagai contoh, kampus besar bisa mempunyai AP sebanyak 15.000. Pembuatan, pendistribusian, loading, dan pengaturan key untuk lingkungan seukuran ini merupakan tantangan yang cukup berat. Sudah disarankan bahwa satu-satunya cara untuk mendistribusikan key pada lingkungan dinamis yang besar adalah dengan mengumumkannya. Tapi, tenet kriptografi dasar adalah bahwa key kriptografis tetap rahasia. Karena itu kita mempunyai dikotomi. Dikotomi ini ada untuk setiap teknologi yang menolak untuk menangani masalah distribusi key.

2.2 Kebutuhan dan Ancaman Keamanan

Seperti dibicarakan diatas, industri WLAN 802.11 atau WiFi sedang berkembang dan sekarang sedang mendapatkan momentumnya. Semua indikasi ini menunjukkan bahwa pada tahun-tahun mendatang banyak organisasi akan menggunakan teknologi WLAN 802.11. Banyak organisasi, termasuk toko, rumah sakit, Bandar, dan perusahaan,

berencana untuk membelanjakan uangnya pada wireless. Tapi, meskipun sudah sangat berkembang dan sukses, semuanya masih tergantung pada WLAN 802.11. Sudah ada banyak laporan dan paper menggambarkan serangan pada jaringan wireless 802.11 yang menyebabkan organisasi mempunyai resiko keamanan.

Gambar 5 menyediakan taksonomi umum dari serangan keamanan untuk membantu organisasi dan pengguna mengerti beberapa serangan terhadap WLAN.



Gambar 5. Taksonomi dari Serangan Keamanan

Serangan keamanan jaringan biasanya dibagi menjadi serangan pasif dan aktif. Dua kelas ini dibagi lagi menjadi beberapa tipe serangan lain. Semua dibicarakan dibawah ini :

- Serangan Pasif. Sebuah serangan dimana pihak yang tidak berhak mendapatkan akses ke suatu asset dan tidak merubah isinya (*misalnya menguping*). Serangan pasif dapat berupa menguping atau analisis lalu lintas (kadang disebut analisis aliran lalu lintas).
 - Menguping. Penyerang memonitor transmisi isi pesan. Sebuah contoh dari ini adalah seseorang mendengarkan transmisi pada LAN antara dua workstation atau mencari frekwensi transmisi antara handset wireless dan base station.
 - Analisis lalu lintas. Penyerang, dengan cara yang lebih tak terlihat, mendapatkan intelijen dengan memonitor transmisi mengenai pola komunikasi. Banyak informasi yang dibawa pada aliran pesan antara pihak-pihak yang berkomunikasi.

- Serangan Aktif. Sebuah serangan dimana pihak yang tidak berhak membuat perubahan pada sebuah pesan, data stream, atau file. Dimungkinkan untuk mendeteksi tipe serangan tapi ini mungkin tidak bisa dicegah. Serangan aktif bisa dalam salah satu bentuk dari empat tipe yang ada: masquerading, replay, perubahan pesan, dan penolakan layanan (DoS).
 - Masquerading. Penyerang seolah-olah pengguna yang berhak dan karena itu mendapatkan privilege tertentu yang bukan haknya.
 - Replay. Penyerang memonitor transmisi (*serangan pasif*) dan mengirimkan lagi pesan sebagai pengguna yang sah.
 - Perubahan pesan. Penyerang merubah pesan yang sah dengan menghapus, menambah, merubah, atau merubah urutannya.
 - Penolakan layanan. Penyerang mencegah atau melarang pengguna atau manajemen fasilitas komunikasi.

Resiko yang berhubungan dengan 802.11 hasil dari satu atau lebih serangan-serangan ini. Konsekwensi dari serangan ini termasuk, tapi tidak terbatas pada, kehilangan informasi penting, biaya hokum dan recovery, citra ternoda, kehilangan layanan jaringan.

2.2.1 Kehilangan Kerahasiaan

Kerahasiaan adalah hak milik dimana informasinya tidak terbuka untuk orang-orang yang tidak berhak, entitas atau proses. Secara umum, ini adalah kebutuhan keamanan fundamental bagi sebagian besar organisasi. Dikarenakan sifat alami teknologi wireless yang membutuhkan radio dan pemancaran, maka kerahasiaan merupakan kebutuhan keamanan yang lebih sulit untuk dipenuhi dalam jaringan wireless. Penjahat tidak perlu masuk kedalam kabel jaringan untuk mengakses sumber daya jaringan. Lebih lagi, tidak dimungkinkan untuk mengontrol jarak dimana transmisi terjadi. Ini membuat penjagaan keamanan fisik tradisional kurang efektif. Penguping pasif pada komunikasi wireless 802.11 asli bisa menyebabkan resiko yang pada suatu organisasi. Penjahat bisa mendengarkan dan mendapatkan informasi sensitive termasuk informasi rahasia, password dan ID jaringan, dan data konfigurasi. Resiko ini ada karena sinyal 802.11 bisa menyebar keluar batas bangunan atau karena mungkin ada penyusup. Karena jangkauan pancaran 802.11 yang cukup jauh, penjahat dapat mendeteksi transmisi dari tempat parkir

atau jalan dekat gedung. Serangan semacam ini, yang dilakukan melalui penggunaan alat penganalisa jaringan wireless atau sniffer, biasanya mudah karena dua alasan: 1. fitur kerahasiaan teknologi WLAN tidak dimungkinkan, dan 2. karena banyak kerentanan pada keamanan teknologi 802.11, seperti yang dijelaskan diatas, menyebabkan penjahat dapat masuk ke sistem.

Penganalisa paket wireless, seperti AirSnort dan WEP crack, adalah alat yang tersedia di internet sekarang ini. AirSnort adalah salah satu dari alat pertama yang dibuat untuk mengotomatisasi proses analisa jaringan. Sayangnya, alat ini juga sering digunakan untuk membongkar jaringan wireless. AirSnort dapat mengambil keuntungan dari kekurangan pada algoritma penjadwalan key yang disediakan untuk penerapan RC4, yang membentuk bagian dari standar WEP asli. Untuk melakukan ini, AirSnort membutuhkan hanya sebuah komputer yang dijalankan dengan sistem operasi Linux dan kartu jaringan wireless. Software secara pasif memonitor transmisi data WLAN dan menghitung kunci enkripsi setelah setidaknya 100 MB paket jaringan telah dikumpulkan. Pada jaringan yang sangat sibuk, pengumpulan data sebanyak ini bisa hanya berlangsung selama tiga atau empat jam, jika volume lalu lintas rendah, bisa dibutuhkan waktu sehari-hari. Sebagai contoh, access point data yang sibuk yang mengirimkan 3000 byte pada 11 Mbps akan menghabiskan ruang IV 24 bit setelah sekitar 10 jam. Jika setelah sepuluh jam penyerang menemukan cipher text yang telah menggunakan key stream yang sama, baik integritas maupun kerahasiaan data bisa dengan mudah ditembus. Setelah paket jaringan telah diterima, key fundamental bisa ditebak dalam waktu kurang dari satu detik. Sekali pengguna jahat mengetahui key WEP, orang itu dapat membaca setiap paket yang bergerak di WLAN. Alat penyadapan semacam ini banyak tersedia, penggunaannya mudah, dan kemampuan untuk menghitung key membuaynya penting bagi administrator keamanan untuk menerapkan praktek wireless yang aman. AirSnort tidak dapat mengambil keuntungan dari algoritma penjadwalan key yang ditingkatkan dari RC4 pada penerapan pre standar.

Resiko lain untuk kehilangan kerahasiaan melalui menguping adalah memonitor pancaran. Penjahat dapat memonitor lalu lintas, menggunakan sebuah laptop dalam mode

asal pilih, ketika sebuah access point dihubungkan ke sebuah hub bukannya switch. Hub pada umumnya memancarkan semua lalu lintas jaringan ke semua peralatan yang terhubung, yang menyebabkan lalu lintas rentan terhadap penyadapan. Switches, di lain pihak, dapat di atur untuk menolak peralatan tertentu yang dihubungkan dari lalu lintas pancaran yang memotong dari peralatan khusus lainnya. Misalnya, jika sebuah access point wireless dihubungkan ke hub Ethernet, sebuah peralatan wireless yang memonitor lalu lintas pancaran dapat memotong data yang dikirimkan ke klien kabel maupun wireless. Karena itu, perusahaan harus mempertimbangkan menggunakan switches dari ada hub untuk koneksi ke access point wireless.

WLAN juga bisa kehilangan kerahasiaan karena serangan aktif. Software penyadapan seperti digambarkan diatas bisa mendapatkan nama dan password pengguna (*juga data lain yang bergerak di jaringan*) ketika data itu dikirimkan melalui koneksi wireless. Penjahat bisa melakukan masquerade sebagai pengguna sah dan mendapatkan akses ke jaringan kabel dari sebuah AP. Ketika sudah berada di jaringan, penyusup dapat menscan jaringan menggunakan peralatan yang banyak terdapat di pasaran. Penguping jahat kemudian menggunakan informasi nama pengguna, password, dan alamat IP untuk mendapatkan akses ke sumber daya jaringan dan data perusahaan yang sensitive. Akhirnya, AP jahat akan menimbulkan resiko keamanan. Pengguna jahat atau yang tidak bertanggungjawab dapat memasukkan AP jahat ke kamar mandi, meja ruang pertemuan, atau daerah tersembunyi lain dalam bangunan. AP jahat kemudian digunakan untuk memungkinkan orang-orang tidak berhak untuk mendapatkan akses ke jaringan. Selama lokasinya dekat dengan pengguna WLAN, dan diatur sehingga kehadirannya nampak seperti AP sah bagi klien wireless, maka AP jahat akan dapat meyakinkan klien wireless akan keabsahannya dan menyebabkannya mengirimkan lalu lintas melalui AP jahat itu. AP jahat dapat memotong lalu lintas wireless antara AP sah dan klien wireless. Ini hanya perlu diatur dengan sinyal yang lebih kuat dari pada AP yang sudah ada untuk memotong lalu lintas klien. Pengguna jahat dapat juga mendapatkan akses ke jaringan wireless melalui AP yang diatur untuk memungkinkan akses tanpa otorisasi. Juga penting untuk dicatat bahwa access point jahat tidak selalu perlu digunakan oleh pengguna jahat. Pada banyak kasus, AP jahat sering digunakan oleh pengguna yang ingin mendapatkan

keuntungan dari teknologi wireless tanpa persetujuan dari departemen IT. Sebagai tambahan, karena AP jahat sering digunakan tanpa sepengetahuan administrator keamanan, mereka sering digunakan tanpa konfigurasi keamanan yang sesuai.

2.2.2 Kehilangan Integritas

Masalah integritas data dalam jaringan wireless mirip dengan di jaringan kabel. Karena organisasi sering menerapkan komunikasi wireless dan kabel tanpa perlindungan kriptografis yang cukup terhadap data, maka integritas sukar untuk dicapai. Seorang hacker dapat membobol integritas data dengan menghapus atau merubah datai dalam sebuah email dari sebuah account pada sistem wireless. Ini dapat menjadi hal yang mengganggu bagi suatu organisasi jika email penting disebarkan ke banyak penerima email. Karena fitur keamanan yang ada pada standar 802.11 tidak menyediakan integritas pesan yang kuat, bentuk lain dari serangan aktif yang membobol integritas sistem sangat dimungkinkan. Seperti dibahas sebelumnya, mekanisme integritas berbasis WEP sebenarnya adalah CRC linear. Serangan dengan merubah pesan dimungkinkan ketika mekanisme pengecekan kriptografis seperti kode otentifikasi pesan dan hash tidak digunakan.

2.2.3 Kehilangan Ketersediaan Jaringan

Penyangkalan ketersediaan jaringan meliputi beberapa bentuk serangan DoS, seperti jamming. Jamming terjadi ketika pengguna jahat mengirimkan sinyal dari peralatan wireless supaya membanjiri sinyal wireless yang sah. Jamming juga bisa disebabkan oleh telepon wireless atau emisi oven microwave. Jamming menghasilkan kekacauan dalam komunikasi karena sinyal wireless sah tidak dapat berkomunikasi dalam jaringan. Pengguna tidak jahat dapat juga menyebabkan DoS. Seorang pengguna bisa secara tidak sengaja memonopoli sinyal jaringan dengan mendownload file yang besar, yang akan secara efektif menolak akses pengguna lain ke jaringan. Sebagai hasilnya, peraturan keamanan perusahaan seharusnya membatasi tipe dan jumlah data yang bisa didownload pengguna pada jaringan wireless.

2.2.4 Resiko Keamanan Lain

Dengan banyaknya peralatan wireless, lebih banyak pengguna mencari cara untuk berhubungan jarak jauh dengan jaringan organisasinya. Salah satu metoda semacam itu adalah penggunaan jaringan pihak ketiga yang tidak bisa dipercaya. Pusat konferensi biasanya menyediakan jaringan wireless bagi pengguna untuk berhubungan ke internet dan juga ke organisasinya saat konferensi berlangsung. Bandara, hotel, dan bahkan warung kopi mulai menggunakan jaringan wireless berbasis 802.11 yang dapat diakses umum untuk pelanggannya, bahkan menawarkan kemampuan VPN sebagai keamanan tambahan. Jaringan umum yang tidak dapat dipercaya ini menimbulkan risiko utama : 1. karena mereka umum, mereka dapat diakses oleh siapapun, bahkan pengguna jahat; 2. mereka berfungsi sebagai jembatan ke jaringan milik pengguna, oleh karena itu memungkinkan setiap orang pada jaringan umum untuk menyerang atau mendapatkan akses ke bridged network.; dan 3. mereka menggunakan antenna high gain untuk meningkatkan penerimaan dan meningkatkan daerah cakupan sehingga memungkinkan pengguna jahat untuk menguping pada sinyal mereka.

Dengan menghubungkan ke jaringan mereka sendiri melalui jaringan yang tidak dapat dipercaya, pengguna bisa membuat kerentanan pada jaringan dan sistem perusahaan mereka kecuali kalau organisasi mereka mengambil langkah untuk melindungi pengguna mereka dan mereka sendiri. Pengguna biasanya harus mengakses sumber daya yang dianggap oleh organisasi mereka sebagai public atau private. Perusahaan sebaiknya mempertimbangkan untuk melindungi sumber daya publiknya menggunakan protocol keamanan layer aplikasi seperti Transport Layer Security (TLS), the Internet Engineering Task Force membuat versi standar dari Secure Socket Layer (SSL). Tapi, pada sebagian besar perusahaan, ini tidak penting karena informasinya juga sudah diketahui publik. Untuk sumber daya privat, perusahaan seharusnya mempertimbangkan penggunaan VPN untuk mengamankan koneksi mereka karena ini akan membantu mencegah penguping dan akses yang tidak berhak ke sumber daya privat.

2.3 Pengurangan Resiko

Badan pemerintah dapat mengurangi resiko terhadap WLAN mereka dengan mengaplikasikan tindakan balasan untuk menangani ancaman dan kerawanan tertentu. Serangan balasan manajemen digabungkan dengan serangan balasan operasional dan teknis dapat secara efektif mengurangi resiko yang berhubungan dengan WLAN. Seharusnya sudah jelas bahwa tidak ada satu cara untuk menyelesaikan semua persoalan jika berhubungan dengan keamanan. Beberapa perusahaan mungkin dapat atau ingin mentolerir resiko lebih besar dari pada yang lain. Juga, keamanan membutuhkan biaya, baik dengan belanja peralatan keamanan, atau dengan pengeluaran biaya operasi. Beberapa perusahaan mau menerima resiko karena mengaplikasikan bermacam-macam serangan balasan melebihi kendala keuangan atau yang lainnya.

BIOGRAFI PENULIS



Janner Simarmata. Lahir di Aek Nabara, 07 Januari 1976. Tamat dari STM GKPS Pematang Siantar tahun 1995. Menyelesaikan program S1 pada jurusan Teknik Informatika di STMIK BANDUNG pada tahun 2000. Pernah mengajar di beberapa Perguruan Tinggi Swasta seperti: STMIK Mikroskil, STMIK Multimedia Prima, Unika Santo Thomas Sumatera Utara. Pada tahun 2004 melanjutkan studi pada program S2 (M.Kom) pada jurusan Ilmu Komputer Universitas Gadj Mada sampai sekarang.

Informasi lebih lanjut tentang penulis:

KEYWORD: *Janner Simarmata*

Email: *sijanner@yahoo.com*