Pemanfaatan Protokol 802.11 Dilihat dari Sisi Kelemahan dan Keamanan

Eriek Orlando

STMIK Jakarta STI&K, Jl. BRI Radio Dalam, Kebayoran Baru, Jakarta Selatan
E-mail : eriek@jak-stik.ac.id

Abstrak

Pengaksesan suatu jaringan harus melibatkan beberapa komputer yang telah dihubungan ke perangkat NIC ke wired network dengan kabel, namun pada WLAN kabel tidak ada melainkan dipancarkan ke semua arah dan setiap komputer dengan wireless NIC dapat terhubung ke wireless LAN. Semua perangkat wireless dapat terhubung ke suatu wireless LAN melalui Access Point, baik menjadi anggota atau bukan anggota dari network tersebut. Dengan demikian tidak ada gunanya network tersebut dilindungi dengan NAT Firewall sebab siapa saja bisa langsung masuk ke balik NAT firewall. Selain kelemahan tidak adanya perlindungan fisik yang inheren pada koneksi wireless, kelemahan lain adalah terletak pada layer 2 management frame 802.11 serta kelemahan inheren protocol 802.11b itu sendiri.

Kata Kunci : *LAN, WLAN, NIC, NAT, Firewall*

Pendahuluan

Dalam perkembangan perangkat telekomunikasi tentunya kita sering mendengar kata wireless, yaitu penghubung dua perangkat yang tidak menggunakan media kabel. Teknologi wireless merupakan teknologi nirkabel, dalam melakukan hubungan telekomunikasi tidak lagi menggunakan media atau sarana kabel tetapi dengan menggunakan gelombang elektromagnetik sebagai pengganti kabel.

Perkembangan teknologi wireless tumbuh dan berkembang dengan pesat, dimana setiap saat kita selalu membutuhkan sarana telekomunikasi. Hal ini terbukti dengan semakin banyaknya pemakaian telepon selular, selain itu berkembang pula teknologi wireless yang digunakan untuk akses internet.

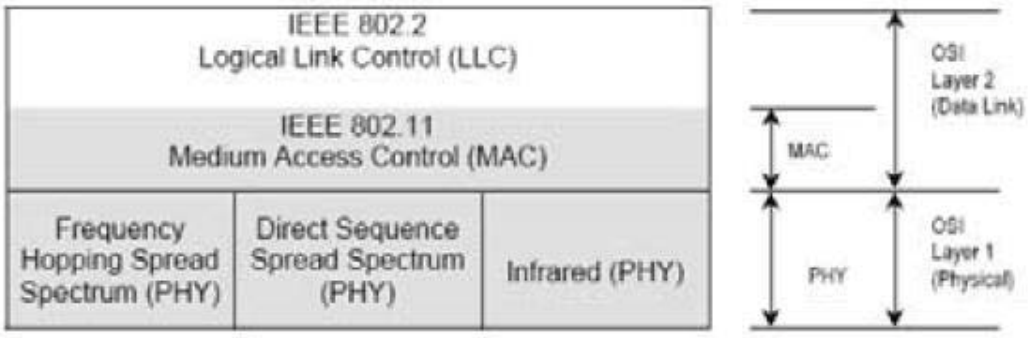
Jaringan komputer saat ini sangat dibutuhkan untuk menghubungkan berbagai instansi pemerintahan, kampus, dan bahkan untuk bisnis dimana banyak sekali perusahaan yang memerlukan informasi dan data-data dari kantor-kantor lainnya dan dari rekan kerja, afiliasi bisnis, dan konsumen.Sering kali terjadi permasalahan pada jaringan komputer antara lain data yang dikirimkan lambat, rusak dan bahkan tidak sampai ke tujuan. Komunikasi sering mengalami timeout, hingga masalah keamanan.

Tinjauan Pustaka

Arsitektur Jaringan IEEE 802.11

Standar IEEE 802.11 mendefinisikan Medium Access Control (MAC) dan Physical (PHY) untuk jaringan nirkabel. Standar tersebut menjelaskan jaringan local dimana peralatan yang terhubung dapat saling berkomunikasi selama berada dalam jarak yang dekat satu sama lain. Standar ini hampir sama dengan IEEE 802.3 yang mendefinisikan Ethernet, tapi ada beberapa bagian yang khusus untuk transmisi data secara nirkabel.[5]

Pada Standar 802.11 mendefinisikan tiga tipe dari physical layer seperti pada gambar diatas Frequency Hopping Spread, Spectrum (FHSS), Direct Sequence Spread Spectrum (DHSS) dan infra merah. Infra merah jarang sekali dipakai karena jangkauannya yang sangat dekat. Tidak semua dari keluarga 802.11 menggunakan Physical Layer yang sama dan mendapatkan kecepatan transmisi data yang sama.



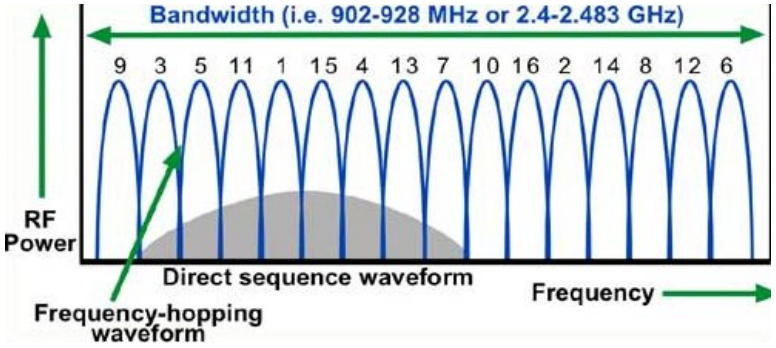
Gambar 1. Arsitektur Jaringan IEEE 802.11

- FHSS

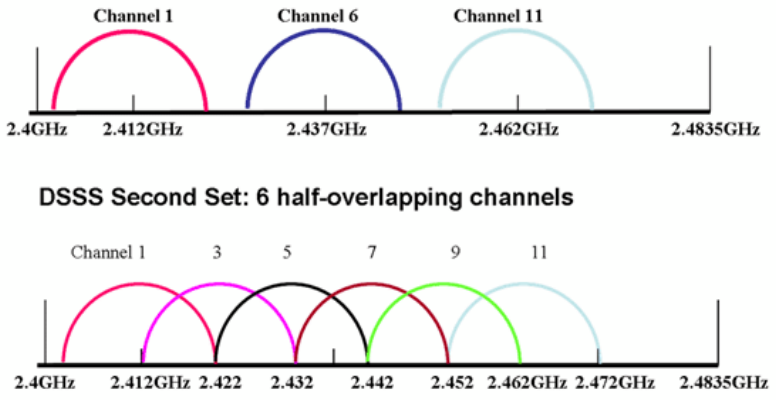
Frequency Hopping Spread Spectrum merupakan teknik spread spectrum yang menggunakan teknik lompatan frekuensi yang berubah-ubah pada sinyal carrier untuk membawa suatu data informasi. Lihat gambar 2.

- DSSS

DSSS merupakan suatu metode untuk mengirimkan data dimana sistem pengirim dan penerima keduanya berada pada set frekuensi yang lebarnya adalah 22 MHz. Lihat gambar 3.



Gambar 2. Frequency Hopping Spread Spectrum

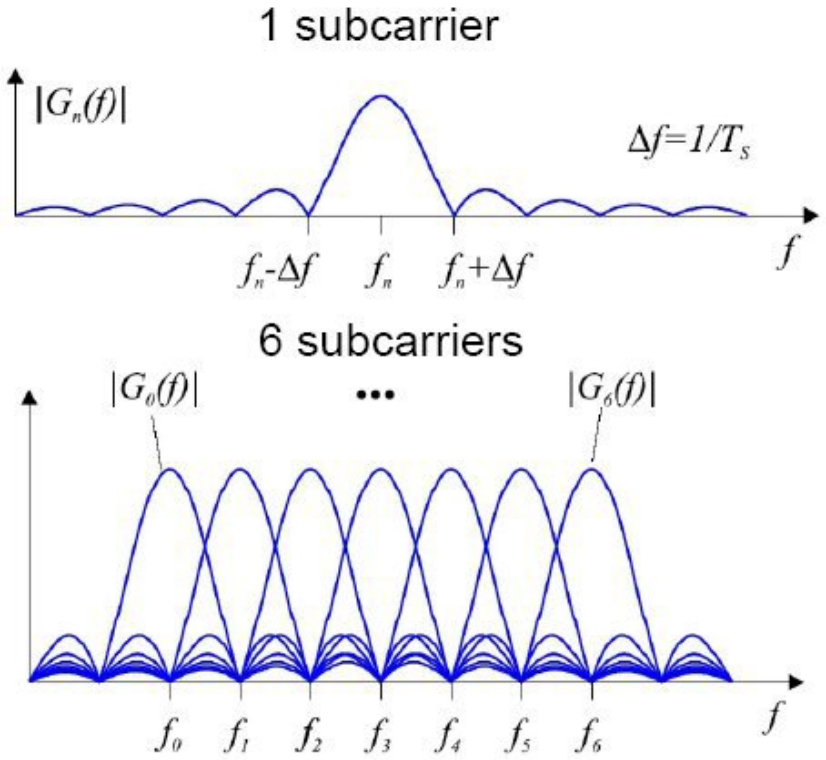


Gambar 3. Direct Sequence Spread Spectrum

- OFDM

Merupakan sebuah sistem modulasi

digital di mana sebuah sinyal dibagi menjadi beberapa kanal dengan pita frekuensi yang sempit dan saling berdekatan, dengan setiap kanal menggunakan frekuensi yang berbeda.



Gambar 4. Orthogonal Frequency Division Multiplexing

Modulation Technique	DHSSS	FHSSS	ODFDM
Narrowband Interference	Less resistance (22 Mhz wide contiguous bands)	More resistance (79 Mhz wide contiguous bands)	Much less (multicarrier modulation)
Interference susceptibility	Medium	High	Low
Collocation	Less	More	Uses several parallel sub-carriers
Compatibility	None	802.11b (WiFi Alliance)	802.11a, 802.11g
Implementation Cost	Comparatively Less	Comparatively more	High
Data Rate & Throughput	2Mbps for 802.11	5 – 6 Mbps	25 Mbps

Gambar 5 Perbedaan DHSS, FHSS, ODFM

Basic Service Set (BSS) BSS dapat dikatakan sebagai area

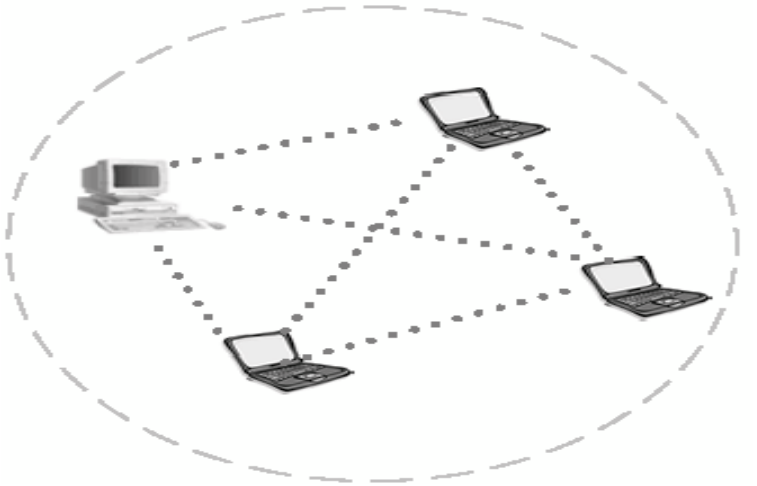
komunikasi yang mengijinkan anggota untuk bertukar informasi. Ada dua tipe BSS yang sesuai dengan dua metode transmisi yang didukung oleh WLAN.[4]

1. Jaringan Point-to-Point (Jaringan Ad-hoc)

Sebuah grup dengan dua atau lebih station nirkabel yang saling berkomunikasi tanpa harus menggunakan access point. Jaringan ini akan terbentuk apabila antara terminal laptop, atau desktop PC) yang telah dilengkapi wireless LAN card saling terhubung tanpa access point. Setiap station dapat berkomunikasi tanpa harus menggunakan fasilitas access point. Konfigurasi ini disebut juga IBSS (Independent Basic Service Set).

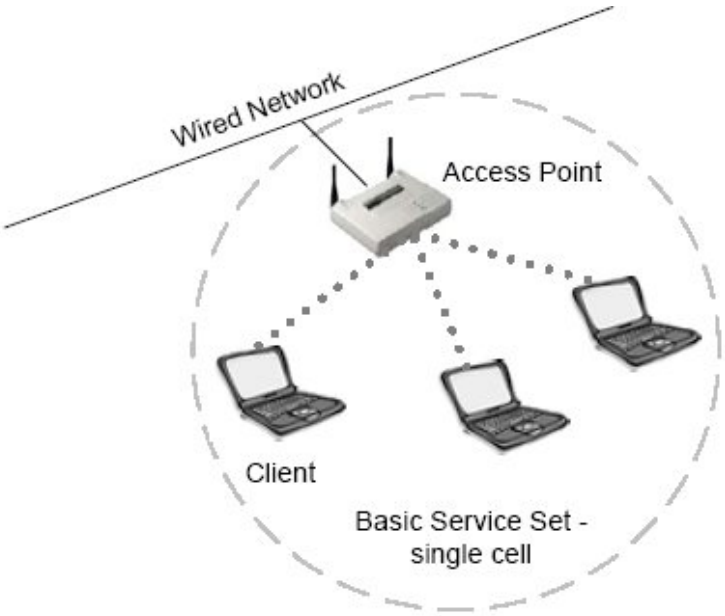
2. Jaringan Infrastruktur

Tipe kedua struktur jaringan yang didukung WLAN IEEE 802.11 adalah setiap station membutuhkan access point untuk saling berkomunikasi. Tipe struktur jaringan ini menggunakan access point sebagai relay antar station nirkabel atau antar station nirkabel dengan infrastruktur berkabel atau disebut dengan Infrastructure Basic Service Set



Gambar 6. Jaringan Point-to-Point (Jaringan Ad Hoc)

.

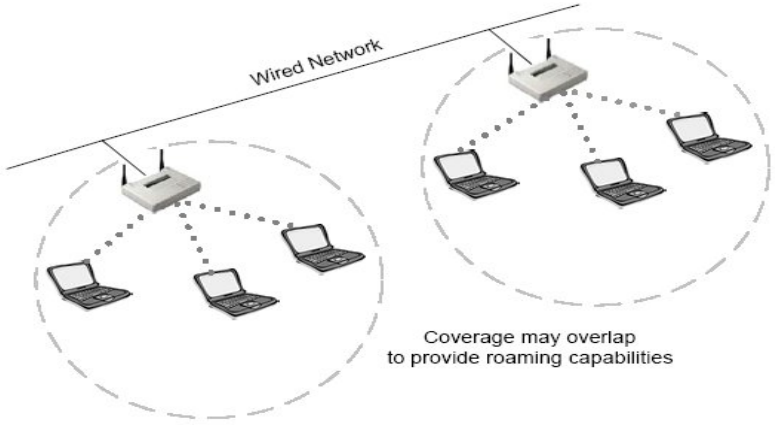


Gambar 7. Infrastructure Basic Service Set

Dikarenakan access point menyebabkan station nirkabel berkomunikasi dengan access point yang menyampaikan atau meneruskan setiap frame, yang memungkinkan cakupan area konfigurasi ini empat kali lebih luas dari IBSS. Hasil ini didapat dari fakta bahwa access point dapat menambah jarak cakupan menjadi dua kali lebih luas didalam infrastruktur BSS. Dari rumus luas area PIr^2 dimana r adalah radius, maka dengan menambah dua kali radius menyebabkan area cakupan meningkat empat kali.

ESS (Extended Service Set)

Dikarenakan sifat sinyal yang menyebar melalui udara, infrastruktur BSS mempunyai jarak cakupan yang terbatas. Untuk menambah area cakupan membutuhkan instalasi satu atau lebih tambahan access point. Access point yang lain membentuk satu infrastruktur BSS yang baru. Koneksi antara dua atau lebih access point teradi dengan menggunakan DS (Distribution System). Fungsi DS adalah untuk koneksi antar access point dan station pada masing-masing infrastruktur BSS. Sebagai tambahan DS memperbolehkan frame-frame mengikuti station bergerak ketika station tersebut bergerak dari satu BSS ke BSS yang lain. Koneksi antara dua atau lebih infrastruktur BSS menghasilkan ESS.



Gambar 8. Extended Service Set (ESS)

Access point berkomunikasi satu dengan yang lain melalui DS yang biasanya adalah wired LAN. Seperti pada Gambar 8, tiap BSS memiliki daerah cakupannya sendiri. BSS dapat secara sebagian atau keseluruhannya overlap dengan BSS lainnya tanpa terjadi masalah. Standar IEEE 802.11 memungkinkan BSS dapat melakukan overlap terhadap BSS lain tanpa masalah dikarenakan penggunaan kanal frekuensi yang berbeda. Untuk memastikan station berkomunikasi dengan access point yang benar dan berfungsi sebagai hub antar BSS, digunakan pengenal atau pengidentifikasi yang disebut SSID (Station Set ID) yang berfungsi untuk mengidentifikasi setiap access point.

Metode Penelitian

Referensi yang penulis dapatkan untuk membantu membuat penulisan penelitian ini adalah sebagai berikut :

1. Sumber acuan umum, berupa buku teks dan ensiklopedia.
2. Sumber acuan khusus, berupa: jurnal, bulletin penelitian dan sumber acuan lain yang memuat hasil-hasil penelitian yang relevan dengan judul penelitan yang penulis lakukan.

Hasil dan Pembahasan

Proteksi Wireless LAN Sangat Kurang

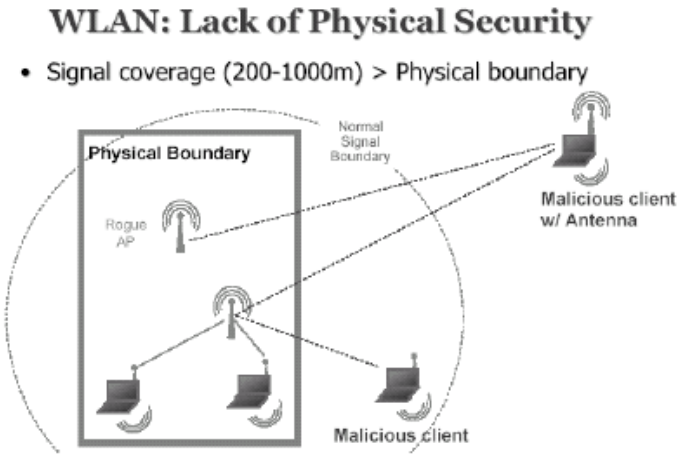
Hasil war driving yang dilakukan oleh PISA di Hongkong pada bulan Juli 2002 menunjukkan hampir 77% dari 187 access point yang ditemukan tidak mengaktifkan WEP encryption. Hasil war driving secara global juga menunjukkan kecenderungan yang sama. 72% dari sekitar 25.000 access point yang ditemukan tidak mengaktifkan enkripsi. Semua ini rawan terhadap sniffer seperti misalnya Ethereal.

Lebih jauh lagi, 51% dari 187 access point menggunakan default SSID, diketahuinya MAC address dan SSID membuat setiap orang dapat terhubung. Apabila hasil survei war driving hanya untuk kepentingan statistik dan tidak mencari informasi lebih jauh terhadap access

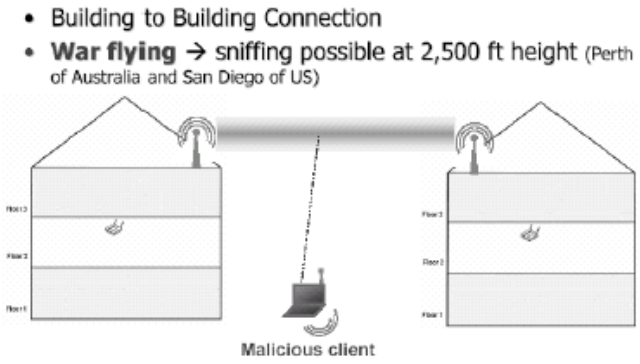
point tertentu, maka pada war chalking akan dicari karakteristik lebih jauh terhadap access point tertentu. Pada war chalking access point yang termonitor ditandai dengan istilah chalking apakah merupakan open node, closed node, ataupun wep node. War chalking dengan demikian dapat digunakan untuk masuk ke network selain untuk mengkoneksi internet.

Perlindungan Fisik Tidak Ada

Sinyal wireless LAN normalnya dapat ditangkap pada kisaran sekitar 200 meter dari access point, tetapi client yang menggunakan antena eksternal dapat menangkap sinyal sampai sejauh 1000 meter. Apabila anda menempatkan access point dekat pintu atau jendela, dapat dipastikan para tetangga dapat ikut menikmati akses Internet atau melakukan sniffing terhadap traffic network.



Gambar 9. Wireless LAN kurang perlindungan



Gambar 10. Wireless LAN Antar Gedung

Apabila infrastruktur wireless LAN itu melibatkan koneksi wireless antar gedung tinggi, maka client yang tidak diinginkan dapat melakukan sniffing dari bawah sejauh sampai 2.500 kaki atau sekitar 762 meter. Jadi walaupun sinyal wireless LAN para ISP yang dipasangkan di puncak-puncak gedung tinggi dapat di-sniffing dari bawah atau dikenal sebagai war flying.

Tidak adanya perlindungan fisik ini pula yang membawa masalah bukan saja akses ilegal terhadap suatu access point, melainkan juga munculnya access point-access point liar dengan berbagai tujuan. Risiko-risiko security di antaranya:

- Pada network kantor misalnya, bisa saja seorang karyawan tanpa izin memasang access point-nya sendiri demi keleluasaan pekerjaannya. Hal ini bisa menjadi bahaya bagi network perusahaan itu secara keseluruhan.
- Seseorang bisa mengaktifkan access point-nya sendiri di tempat umum dan tampil seolah-olah sebagai access point resmi dan menangkap network traffic pada akses WLAN untuk umum.

- Untuk melakukan sniffing suatu komputer tidak harus terhubung dengan access point. Dengan demikian untuk pemakai perorangan hampir tidak mungkin mengetahui apakah network traffic-nya sedang disniffing.
- Bukan itu saja suatu laptop yang tidak terhubung ke wireless network tetapi WNIC-nya tetap terpasang dapat terkena serangan client-to-client. Ini dikarenakan sifat WNIC yang dapat mengaktifkan ad-hoc peer-to-peer network tanpa adanya access point. Koneksi ini dikenal sebagai Independent Basic Service Set. Jadi walaupun suatu perusahaan tidak memasang wireless LAN tetapi network-nya dapat diserang lewat salah satu komputer yang terhubung padanya dan kebetulan pada komputer itu tanpa disadari masih terpasang WNIC.
- Tidak adanya perlindungan fisik pula yang membuat wireless network mudah terganggu oleh peralatan rumah tangga biasa seperti microwave oven, cordless phone, serta peralatan-peralatan yang menggunakan teknologi Bluetooth. Ini dikarenakan banyak peralatan yang menggunakan frekuensi 2,4GHz seperti halnya wireless network (peralatan dengan protokol 802.11b).

Untuk mengatasi kelemahan tidak adanya perlindungan fisik ini, beberapa tindakan dapat dilakukan untuk meminimumkan risiko di antaranya:

- Jangan menempatkan access point dekat pintu atau jendela
- Kurangi daya broadcast access point
- Matikan access point bila tidak sedang dipakai
- Untuk perusahaan: jangan biarkan adanya rogue access point dan kalau menggunakan building antena, gunakan directional radiation dan atur sudut pancarannya.

Default Configuration

Banyak wireless LAN yang terpasang dengan default configuration yang lemah dan rawan terhadap penyusup:

- WEP encryption tidak diaktifkan : WEP encryption berlaku umum untuk semua client dan dapat di-crack, tetapi paling tidak anda akan terlindung dari casual hacker.
- SSID default dan dibroadcast : Access Point mempunyai default SSID, seperti Linksys, Cisco, SMC dan semua di-broadcast.
- Akses admin mudah dilakukan : Admin name dan password default harus dihindari karena access point dapat diakses lewat web, telnet, ataupun SNMP tanpa difilter sama sekali. Bila access point ini mempunyai feature SNMP, maka jangan gunakan default community string atau matikan sama sekali fungsi SNMP.
- Tidak ada access control terhadap client : Walaupun memang access point mempunyai fasilitas untuk memfilter komputer dengan MAC address, mana saja yang boleh mengakses suatu access point, dalam kenyataannya ini hanya dapat dilakukan dalam sisitem skala kecil.

Jenis Serangan di Internet

Terdapat berbagai serangan di internet, antara lain : [1]

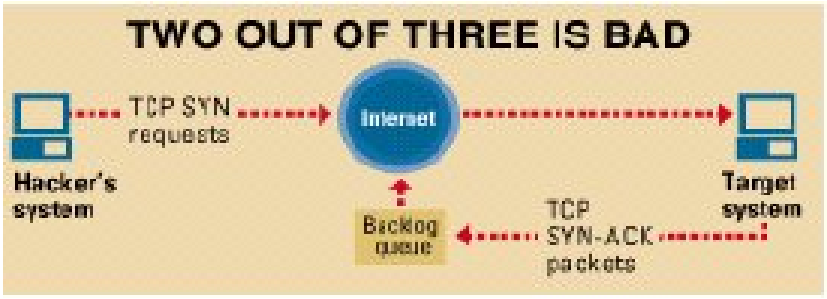
- Ping of Death

Ping of Death menggunakan program utility ping yang ada di sistem operasi komputer. Biasanya ping digunakan untuk mengecek berapa waktu yang dibutuhkan untuk mengirimkan sejumlah data tertentu dari satu komputer ke komputer lain. Panjang maksimum data yang dapat dikirim menurut spesifikasi protokol IP adalah 65,536 byte.

Pada Ping of Death data yang dikirim melebihi maksimum paket yang di ijinkan menurut spesifikasi protokol IP. Konsekuensinya, pada sistem yang tidak siap akan menyebabkan sistem tersebut crash atau putus, hang atau reboot pada saat sistem tersebut menerima paket yang demikian panjang. Serangan ini sudah tidak baru lagi, semua vendor sistem operasi telah memperbaiki sistemnya untuk menangani kiriman paket yang oversize.

- Teardrop

Teardrop adalah teknik yang dikembangkan dengan cara mengeksplotasi proses disassembly-reassembly paket data. Dalam jaringan Internet seringkali data harus di potong kecil-kecil untuk menjamin reliabilitas dan proses multiple akses jaringan. Potongan paket data ini kadang harus dipotong ulang menjadi lebih kecil lagi pada saat disalurkan melalui saluran Wide Area Network agar pada saat melalui saluran Wide Area Network yang tidak reliable proses.

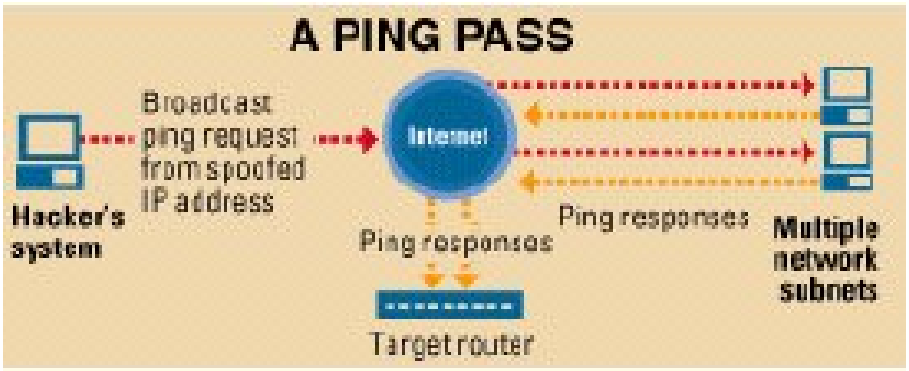


Gambar 12. TCP SYN ACK

- Smurf Attack

Smurf Attack jauh lebih membahayakan. Smurf Attack adalah serangan secara paksa pada fitur spesifikasi IP yang dikenal sebagai direct broadcast addressing. Seorang Smurf hacker biasanya membanjiri router kita dengan paket permintaan echo Internet Control Message Protocol yang kita kenal sebagai aplikasi ping. Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan anda maka router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terjadi trafik ICMP echo respons dan permintaan dalam jumlah yang sangat besar. Lebih sial lagi jika hacker ini memilih untuk men-spoof alamat IP sumber permintaan ICMP tersebut, akibatnya ICMP trafik tidak hanya akan memacetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di-spoof, jaringan ini di kenal sebagai jaringan korban.

Untuk menjaga agar jaringan kita tidak menjadi perantara bagi serangan Smurf ini, maka broadcast addressing harus dimatikan dirouter kecuali jika kita sangat membutuhkannya untuk keperluan multicast, yang saat ini belum 100% di definisikan. Alternatif lain dengan cara memfilter permohonan ICMP echo pada firewall. Untuk menghindari agar jaringan kita tidak menjadi korban Smurf Attack, ada baiknya kita mempunyai upstream firewall yang di setting untuk memfilter ICMP echo atau membatasi trafik echo agar presentasinya kecil dibandingkan trafik jaringan secara keseluruhan.



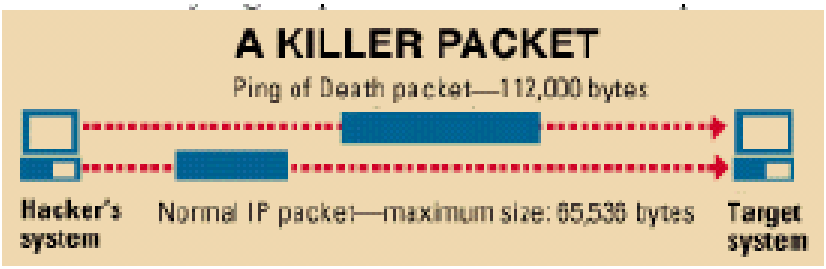
Gambar 13. Proses Broadcast Ping

Kelemahan Inheren Protokol 802.11b

Wireless LAN masih berkembang dan sampai sekarang masih terdapat celah yang besar antara kebutuhan security dengan apa yang terdapat pada protokol 802.11b. Beberapa penggunaan protokol 802.11b mempunyai banyak kelemahan:[3][6]

- Otentikasi yang lemah

Pada protokol 802.11b tidak terdapat user authentication dan SSID dibroadcast dan dengan mudah dapat diketahui dengan



Gambar 11. Ping of Death

Pengiriman data menjadi lebih reliable, pada proses pemotongan data paket yang normal setiap potongan diberikan informasi offset data yang kira-kira berbunyi "potongan paket ini merupakan potongan 600 byte dari total 800 byte paket yang dikirim". Program teardrop akan memanipulasi offset potongan data sehingga akhirnya terjadi overlapping antara paket yang diterima dibagian penerima setelah potongan potongan paket ini direassembly. Seringkali overlapping ini menimbulkan sistem yang crash, hang dan reboot pada komputer yang berlawanan.

- SYN Attack

  Kelemahan dari spesifikasi TCP/IP sangat terbuka terhadap serangan paket SYN. Paket SYN dikirimkan pada saat memulai handshake antara aplikasi sebelum transaksi atau pengiriman data dilakukan. Pada kondisi normal aplikasi client akan mengirimkan paket TCP SYN untuk mensinkronisasi paket pada aplikasi diserver. Server akan mengirimkan respond berupa knowledgement paket TCP SYN ACK. Setelah paket TCP SYN ACK di terima dengan baik oleh client, maka client akan mengirimkan paket ACK sebagai tanda transaksi pengiriman atau penerimaan data akan di mulai. Dalam serangan SYN flood client akan membanjiri server dengan banyak paket TCP SYN. Setiap paket TCP SYN yang dikirim akan menyebabkan server menjawab dengan paket TCP SYN ACK. Server akan terus mencatat untuk menunggu responds TCP ACK dari client yang mengirimkan paket TCP SYN.

  Tempat antrian backlog ini tentunya terbatas dan biasanya kecil dimemori. Pada saat antrian backlog ini penuh, sistem tidak akan merespond paket TCP SYN lain yang masuk dalam bahasa sederhananya sistem akan diam atau hang. Sialnya paket TCP SYN ACK yang masuk antrian backlog hanya akan dibuang dari backlog pada saat terjadi time out dari timer TCP yang menandakan tidak ada responds dari client pengirim. Biasanya internal timer TCP ini di set cukup lama, kunci SYN attack adalah dengan membanjiri server dengan paket TCP SYN menggunakan alamat IP sumber yang salah. Akibatnya karena alamat IP sumber tersebut tidak ada, jelas tidak akan ada TCP ACK yang akan dikirim sebagai responds dari responds paket TCP SYN ACK.

  Dengan cara ini server akan tampak diam dan tidak memproses responds dalam waktu yang lama. Berbagai vendor komputer sekarang telah menambahkan pertahanan untuk SYN attack dan juga programmer firewall menjamin bahwa firewall mereka tidak mengirimkan packet dengan alamat IP sumber yang salah.

- Land Attack

  Pada Land Attack gabungan sederhana dari SYN attack hacker membanjiri jaringan dengan paket TCP SYN dengan alamat IP sumber dari sistem yang di serang. Biarpun dengan perbaikan SYN attack diatas, Land attack ternyata menimbulkan masalah pada beberapa sistem.

  Serangan jenis ini relatif baru, beberapa vendor sistem operasi telah menyediakan perbaikannya. Cara lain untuk mempertahankan jaringan dari serangan Land attack ini adalah dengan memfilter pada software firewall anda dari semua paket yang masuk dari alamat IP yang diketahui tidak baik. Paket yang dikirim dari internal sistem anda biasanya tidak baik, oleh karena itu ada baiknya di filter alamat 10.0.0.0-10.255.255.255, 127.0.0.0-127.255.255.255, 172.16.0.0-172.31.255.255, dan 192.168.0.0-192.168.255.255.

menjalankan Network Stumbler. MAC address selain dapat dimonitor juga dapat dipalsukan, tidak adanya mutual authentication yang memungkinkan munculnya access point palsu.

- WEP bersifat statik
  WEP dirancang hanya untuk melindungi network traffic dari pengintaian yang dapat dengan mudah melihat network traffic dengan sniffer seperti Ethereal. Tetapi walaupun telah diproteksi dengan WEP, apabila sniffer berhasil mengumpulkan data sampai sekitar 4 juta frame (pada network yang sibuk hanya memerlukan waktu 5 jam untuk mendapatkan 4 juta frame), maka software seperti WEP Crack atau AirSnort dapat mengcrack enkripsi 128 bit ini.
- Message integrity yang lemah
  Paket data 802.11b hanya ditujukan untuk menangani error detection dengan menggunakan CRC32 linear checksum yang rawan terhadap bit-flipping attack (berakibat pada pengubahan pesan yang terkirim). Juga tidak terdapat pengecekan terhadap message sequence maupun timestamp, yang membuat wireless LAN rawan terhadap replay attack (berakibat pada indentity spoofing).

Peningkatan Security pada Protokol 802.11

Dengan begitu banyaknya kelemahan pada wireless LAN yang menggunakan protokol 802.11b, kini peningkatan security sedang dilakukan dengan pengembangan protokol 802.11i yang diharapkan selesai pada akhir 2003. Selain itu sebagai subset dari 802.11b,WPA (Wi-Fi Protected Access) diusulkan oleh Wi-Fi Alliance yang akan menyediakan authentication framework TKIP yang akan memperkuat integritas WEP dengan adanya Message Integrity Code (MIC) untuk mencegah pemalsuan paket data, IV sequencing yang baru untuk mencegah replay attack serta WEP re-keying yang berubah setiap 10.000 paket.

Semua perbaikan yang mengubah total hampir keseluruhan konsep security pada protokol 802.11 ternyata belum mengatasi keseluruhan masalah security pada wireless LAN. Salah satu masalah ini terletak pada layer 2 management frame. Menurut spesifikasi standard 802.11 :[2]

- Management frame tidak diotentikasi.
  Management frame terdiri dari association terhubung ke access point, disassociation terputus dari acces point, serta beacon broadcasting MAC address, SSD, dan time stamp secara periodik oleh access point. Konsekuensinya tidak ada cara untuk membedakan access point yang sesungguhnya dari acces point palsu, serta penyerang dapat melakukan deasosiasi terhadap klien sehingga terputus hubungannya dari access point.
- Management frame dikirim sebagai clear text.
  Hal ini mengakibatkan mudahnya melakukan sniffing. Kelemahan-kelemahan ini dimanfaatkan untuk mengembangkan hacking tools terhadap wireless LAN, seperti AirJack yang dikembangkan Abaddon dan diperkenalkan dalam BlackHat Briefings 2002. AirJack adalah tool untuk melakukan disassociation DoS attack terhadap WNIC card tipe Prism dan Hermes selain fungsi-fungsi lain yang tidak kalah bagusnya.
- WLAN-Jack: DoS terhadap WLAN
  Dapat dijalankan secara broadcasted atau directed. Pada directed mode korban akan mengira kerusakan ada pada WNIC-nya.
- ESSID-Jack: Mendapatkan SSID yang disembunyikan
  Mengirimkan de-authentication frame ke broadcast address dan listen ke client probe request serta access point probe response.
- Monkey-Jack: Man-in-the-Middle Attack
  Men-deauthenticate korban dari access point sebenarnya dengan mengirimkan deauthenticate frame menggunakan MAC address dari access point. Korban akan men-scan access point kembali. Korban terasosiasi ke access point palsu pada mesin penyerang. Akibatnya penyerang berhasil menyusup di antara client dengan server.
- Kracker-Jack: Menyerang VPN yang Lemah
  Berbagai tool untuk wireless hacking yang tersedia untuk sistem operasi Windows bersifat sangat hardware specific sehingga anda harus memperhatikan WNIC apa yang sesuai untuk dipakai untuk tool tertentu. AiroPeek NX, suatu wireless auditing tool misalnya dapat berfungsi dengan WNIC ORiNOCO, tetapi tidak dengan WNIC Avaya yang dikatakan identik merupakan pecahan dari Lucent.

Penutup

Kesimpulan dan Saran

Untuk pemakaian pribadi security yang ada sekarang terutama WEP encryption sudah memadai untuk mengatasi serangan casual hacker. Adapun untuk perusahaan perlu dipertimbangkan penempatan access point pada DMZ Demiliterized zone, sedangkan internal network harus berada di tempat yang aman. Juga perlu dipertimbangkan metode keamanan dari pihak ketiga baik yang generik seperti firewall, VPN, Remote Authentication Dial-In User Service (RADIUS), maupun yang merupakan pengayaan terhadap WEP encryption seperti TKIP Temporal Key Integrity Protocol, AES

Advanced Encryption Standard dan SSL Secure Socket Layer serta implementasi IDS Intrusion Detection System. Windows XP, misalnya selain wireless friendly, juga sudah lebih secure dari versi-versi Windows sebelumnya dengan sudah terintegrasinya AES.

DAFTAR PUSTAKA

[1]. Budi Rahardjo, *Keamanan Sistem Informasi berbasis Internet*, 2010

[2]. Microsoft Corporation," *Microsoft Galvanizes Industry Effort for Secure Wireless andWired LAN*", Anchim, Calif, March 26, 2011

[3]. Rob Flickenger, " *Getting Started with Lucent's 802.11b Wireless LAN Card "*, March 11, 2009

[4]. L. Goldberg, "Wireless LANs: Mobile Computing's Second Wave," Electronic Design, 26 June 2007.

[5]. K. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September / October 2006.

[6]. Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman, Foryanto, "A Short Tutorial on Wireless LANs and IEEE 802.11" , 2009