

# Koneksi Nirkabel yang Aman\*

Jim Geovedi

`jim.geovedi@bellua.com`

Merupakan rahasia umum jika WEP (*Wired Equivalent Privacy*) tidak lagi mampu diandalkan untuk menyediakan koneksi nirkabel (wireless) yang aman dari ulah orang usil atau ingin mengambil keuntungan atas apa yang kita miliki—dikenal dengan jargon *hackers*. Tidak lama setelah proses pengembangan WEP, kerapuhan dalam aspek kriptografi muncul.

Berbagai macam penelitian mengenai WEP telah dilakukan dan diperoleh kesimpulan bahwa walaupun sebuah jaringan wireless terlindungi oleh WEP, pihak ketiga (*hackers*) masih dapat membobol masuk. Seorang hacker yang memiliki perlengkapan wireless seadanya dan peralatan software yang digunakan untuk mengumpulkan dan menganalisis cukup data, dapat mengetahui kunci enkripsi yang digunakan.

Dengan semakin banyaknya *access point* terpasang di hotel, bandar udara, dan pusat-pusat keramaian, maka dibutuhkan sebuah pengembangan metode keamanan yang mampu membuat para pengguna wireless merasa nyaman. Agar mereka dapat merasa tenang untuk mengirimkan rencana kerja perusahaan tahun mendatang, tanpa takut bahwa rencana kerja tersebut dapat disadap atau disabotase oleh kompetitor.

Beberapa bulan lalu, saya dan rekan melakukan *wardriving* (*scanning*

---

\*Diterbitkan di harian Kompas, Kamis 24 Juni, 2004

terhadap *access point*) di Jakarta dan Bandung. Dari hasil wardriving tersebut, sebagian besar *access point* yang teridentifikasi tidak mengaktifkan WEP. Dan, banyak dari para pemilik maupun pengguna jaringan wireless ini yang mengeluh.

Yang menjadi keluhan adalah dengan diaktifkannya modus enkripsi WEP maka kecepatan koneksi menjadi berkurang secara drastis, ada yang mengatakan penurunan *throughput* dengan menggunakan WEP bisa sebanyak 50 persen. Sehingga banyak di antara mereka yang memilih untuk tidak menggunakan perlindungan enkripsi WEP. Ironisnya, ada sebuah bank berlokasi di Jakarta yang menggunakan akses wireless tanpa menggunakan enkripsi WEP dan melakukan transaksinya dengan *plaintext*.

Secara pribadi, saya tidak melihat kelemahan enkripsi menjadi alasan untuk tidak mengimplementasikan teknologi WEP, tapi karena tidak adanya konsistensi dalam administrasi WEP di antara produk-produk WLAN (*Wireless LAN*) yang digunakan. Ini juga termasuk produk-produk yang memiliki label sertifikasi. Beberapa produk membutuhkan kode-kode heksadesimal, beberapa yang lain menerima alphanumeric (gabungan alfabet dan angka) sebagai passphrase.

Menyikapi kelemahan yang dimiliki oleh WEP, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai WPA (*WiFi Protected Access*). Teknik WPA adalah model kompatibel dengan spesifikasi standar draf **IEEE 802.11i**. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau corporate, dan tersedia untuk publik secepat mungkin.

Adanya WPA yang "menggantikan" WPE, apakah benar perasaan "tenang" tersebut didapatkan? Ada banyak tanggapan pro dan kontra mengenai hal tersebut. Ada yang mengatakan, WPA mempunyai mekanisme enkripsi yang lebih kuat. Namun, ada yang pesimistis karena alur komunikasi yang digunakan adalah tidak aman, di mana teknik man-

in-the-middle bisa digunakan untuk mengakali proses pengiriman data.

Agar tujuan WPA tercapai, setidaknya dua pengembangan sekuriti utama dilakukan. Teknik WPA dibentuk untuk menyediakan pengembangan enkripsi data yang menjadi titik lemah WEP, serta menyediakan user authentication yang tampaknya hilang pada pengembangan konsep WEP.

Teknik WPA didesain menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik, dengan menggunakan TKIP (*Temporal Key Integrity Protocol*) yang mampu secara dinamis berubah setelah 10.000 paket data ditransmisikan. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali.

*Background process* secara otomatis dilakukan tanpa diketahui oleh pengguna. Dengan melakukan regenerasi kunci enkripsi kurang lebih setiap lima menit, jaringan WiFi yang menggunakan WPA telah memperlambat kerja hackers yang mencoba melakukan cracking kunci terdahulu.

Walaupun menggunakan standar enkripsi 64 dan 128 bit, seperti yang dimiliki teknologi WEP, TKIP membuat WPA menjadi lebih efektif sebagai sebuah mekanisme enkripsi. Namun, masalah penurunan throughput seperti yang dikeluhkan oleh para pengguna jaringan wireless seperti tidak menemui jawaban dari dokumen standar yang dicari.

Sebab, masalah yang berhubungan dengan throughput sangatlah bergantung pada hardware yang dimiliki, secara lebih spesifik adalah chipset yang digunakan. Anggapan saat ini, jika penurunan throughput terjadi pada implementasi WEP, maka tingkat penurunan tersebut akan jauh lebih besar jika WPA dan TKIP diimplementasikan walaupun beberapa produk mengklaim bahwa penurunan throughput telah diatasi, tentunya dengan penggunaan chipset yang lebih besar kemampuan dan kapasitasnya.

Proses otentifikasi WPA menggunakan 802.1x dan EAP (*Extensible Authentication Protocol*). Secara bersamaan, implementasi tersebut akan menyediakan kerangka kerja yang kokoh pada proses otentifikasi pengguna. Kerangka-kerja tersebut akan melakukan utilisasi sebuah server otentifikasi terpusat, seperti RADIUS, untuk melakukan otentifikasi pengguna sebelum bergabung ke jaringan wireless. Juga diberlakukan mutual authentication, sehingga pengguna jaringan wireless tidak secara sengaja bergabung ke jaringan lain yang mungkin akan mencuri identitas jaringannya.

Mekanisme enkripsi AES (*Advanced Encryption Standard*) tampaknya akan diadopsi WPA dengan mekanisme otentifikasi pengguna. Namun, AES sepertinya belum perlu karena TKIP diprediksikan mampu menyediakan sebuah kerangka enkripsi yang sangat tangguh walaupun belum diketahui untuk berapa lama ketangguhannya dapat bertahan.

Bagi para pengguna teknologi wireless, pertanyaannya bukanlah dititikberatkan pada pemahaman bahwa WPA adalah lebih baik dari WEP, namun lebih kepada improvisasi tepat guna yang mampu menyelesaikan masalah keamanan wireless saat ini. Di kemudian hari, kita akan beranggapan pengguna adalah raja. Apa yang dibutuhkan para pengguna teknologi wireless adalah kemudahan menggunakan teknologi itu.

Untuk dapat menggunakan "kelebihan" yang dimiliki WPA, pengguna harus memiliki hardware dan software yang kompatibel dengan standar tersebut. Dari sisi hardware, hal tersebut berarti wireless access points dan wireless NIC (*Network Interface Card*) yang digunakan harus mengenali standar WPA. Sayangnya, sebagian produsen hardware tidak akan mendukung WPA melalui firmware upgrade, sehingga pengguna seperti dipaksa membeli wireless hardware baru untuk menggunakan WPA.

Dari sisi software, belum ada sistem operasi Windows yang mendukung WPA secara default. Komputer yang menggunakan sistem operasi Windows dengan hardware kompatibel dengan standar WPA dapat mengimplementasikannya setelah menginstal WPA client. WPA

client baru dapat bekerja pada sistem operasi Windows Server 2003 dan Windows XP. Bagi para pengguna sistem operasi lainnya belum ditemukan informasi mengenai kemungkinan mengimplementasikan WPA.

Melakukan migrasi hardware dan implementasi WPA dapat dibayangkan sebagai sebuah pekerjaan yang sangat besar. Untungnya, hal tersebut bukanlah sesuatu yang harus dilakukan pada saat yang bersamaan. Wireless Access Points dapat mendukung WPA dan WEP secara bersamaan. Hal ini memungkinkan migrasi perlahan ke implementasi WPA.

Pada jaringan wireless yang membutuhkan tingkat sekuriti tingkat tinggi, variasi sistem tambahan propietari dibuat untuk menjadi standar transmisi WiFi. Pada perkembangannya, beberapa produsen WiFi telah mengembangkan teknologi enkripsi untuk mengakomodasi kebutuhan pengamanan jaringan wireless.