Studi Mengenai Wi-Fi Protected Access dan Analisa Serangan Terhadapnya

Samuel Simon – NIM: 13506032
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganeca 10, Bandung
E-mail: if16032@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang studi mengenai *Wi-Fi Protected Access* (WPA) dan menganalisa berbagai kemungkinan serangan terhadapnya. WPA merupakan sebuah metode pengamanan jaringan nirkabel yang mengenkripsi data dengan berbasiskan algoritma RC4 dan menggunakan vektor inisialisasi sepanjang 48 bit. Selain itu, WPA mengimplemetasikan protokol yang mampu mengubah kunci setiap beberapa menit serta dilengkapi dengan algoritma *checksum* CRC yang dikembangkan khusus untuk menghindari berbagai serangan yang mungkin terjadi.

Namun, di balik berbagai kelebihan yang dimilikinya, masih terdapat berbagai ancaman serangan terhadap WPA. Jenis ancaman serangan yang akan dibahas secara khusus dalam makalah ini adalah serangan terhadap *Temporal Key Integrity Protocol (TKIP)*, protokol yang dibuat khusus dan telah mendapatkan sertifikasi untuk digunakan pada WPA. Serangan ini muncul akibat penggunaan algoritma hashing, *Message Integrity Check* (MIC) yang dikembangkan dari algoritma enkripsi yang tidak terlalu baik. Di bagian akhir, akan dijelaskan pula teknik-teknik yang dapat digunakan untuk menangkal serangan ini.

Kata kunci: *Wi-Fi Protected Access, RC4, Temporal Key Integrity Protocol, WPA attack.*

1. Pendahuluan

Perkembangan jaringan komputer menciptakan berbagai cara pengaksesan jaringan, termasuk pengaksesan dengan cara nirkabel atau biasa disebut Wi-Fi (*Wireless Fidelity*). Mobilitas dan kemudahan pengaksesan membuat akses nirkabel berkembang drastis dan jumlah penggunanya pun semakin meningkat. Namun, dengan semakin umumnya penggunaa jaringan nirkabel, berbagai jenis serangan dan pencurian data dalam jaringan ini juga turut meningkat. Hal ini memicu dikembangkannya metode enkripsi khusus untuk jaringan nirkabel, dikarenakan jaringan ini lebih rentan terhadap serangan. Generasi pertama metode enkripsi untuk jaringan nirkabel adalah *Wired Equivalent Privacy* (WEP), sebuah metode enkripsi data yang memanfaatkan algoritma RC4.

Setelah berhasil diimplementasi selama beberapa tahun, pengguna jaringan nirkabel menyadari bahwa WEP merupakan metode enkripsi yang sangat mudah diserang karena memiliki banyak kelemahan. Untuk mengatasi masalah tersebut, dikembangkan sebuah teknik pengamanan baru yang dinamakan *Wi-Fi Protected Access (WPA)*. WPA memberikan banyak perubahan dibandingkan WEP. Meskipun masih tetap berbasiskan algoritma RC4, WPA menggunakan vektor inisialisasi sepanjang 48 bit yang membuatnya sulit untuk diserang. Selain itu, WPA mengimplementasikan sebuah protokol baru yang mampu mengubah kunci setiap beberapa menit. Untuk memperkuat teknik pengamanan ini, algoritma checksum CRC yang dinamakan *Message Integrity Check (MIC)* juga dikembangkan untuk menghindari berbagai serangan seperti yang menimpa WEP.

Dengan berbagai perbaikan tersebut, WPA menjadi standar baru menggantikan WEP dalam pengamanan data jaringan nirkabel. Namun ternyata teknik ini masih rentan terhadap beberapa serangan lain. Hal ini disebabkan oleh penggunaan algoritma RC4 yang menjadi dasar pengembangan teknik ini.

2. Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) adalah protokol yang dikembangkan oleh Wi-Fi Alliance sebagai respon dari banyaknya kelemahan yang ditemukan pada sistem sebelumnya, *Wired Equivalent Privacy (WEP)*. Protokol baru ini mengimplementasikan banyak hal baru dari standar IEEE 802.11i dan telah disiapkan untuk menjadi pengganti WEP ketika 802.11i masih dalam tahap persiapan. Hal paling signifikan dari pengembangan WPA adalah penambahan *Temporal Key Integrity Protocol (TKIP)*. TKIP menerapkan tiga kemampuan baru untuk mengatasi celah-celah keamanan yang ada dalam jaringan yang diproteksi dengan WEP. Pertama-tama, TKIP mengimplementasikan fungsi penggabungan kunci yag mengkombinasikan kunci rahasia utama dan vektor inisialisasi sebelum meneruskannya ke dalam proses inisialisasi RC4. Kemudian, WPA mengimplementasikan pencacah

untuk menghindari percobaan serangan berkali-kali. Paket yang diterimaketika pencacah telah melewati angka batas maksimal akan ditolak oleh access point. Kemampuan ketiga yang ditambahkan adalah pengimplementasian pengecekan integritas pesan sepanjang 64 bit yang dikenal dengan nama MIC. Selain itu, TKIP memastikan setiap paket data dikirimkan dengan kunci enkripsi yadng unik. Penggabungan kunci yang dilakukan di awal proses menambah kompleksitas angka sehingga menyulitkan setiap usaha serangan yang dilayangkan.

2.1 Ancaman Keamanan Terhadap WPA

Meskipun dilengkapi dengan berbagai kemampuan baru yang dikembangkan untuk menghilangkan kelemahan-kelemahan keamanan yang terdapat pada WEP, WPA ternyata masih memiliki banyak celah keamanan lain. Dua hal yang paling menonjol adalah serangan terhadap kunci WPA yang pendek dan serangan terhadap TKIP.

Kunci WPA yang pendek dapat diserang dengan mudah tanpa harus menyerang protokol WPA itu sendiri. Jika kunci WPA terdiri dari 20 karakter atau kurang dan kunci tersebut merupakan kata yang ada dalam kamus, maka serangan dapat dengan mudah dilakukan. Serangan dilakukan dengan mencegat paket-paket dari pertukaran kunci yang terjadi, kemudian pelaku serangan dapat mengekstraksi kunci enkripsi dan mendapatkan akses ke dalam jaringan.

Pertukaran kunci selalu terjadi di awal setiap koneksi antara *access point* dan klien. Oleh sebab itu, pelaku serangan dapat mendapatkan akses dalam waktu beberapa menit saja. Selain itu, tingkat keamanan yang hanya 2,5 bit per karakter menjadikan tingkat keamanan yang sangat rendah bagi kunci ini.

Serangan terhadap TKIP dilakukan dengan cara mencegat paket-paket data pendek yang dikirimkan kedua pihak (*access point* atau klien) seperti paket-paket permintaan maupun respon ARP. Setelah itu, dari data yang didapat, pelaku serangan dapat mendapatkan informasi-informasi yang diperlukan untuk melakuka serangan.

3. TKIP Attack

WPA menerapkan dua modus yang dapat digunakan untuk memastikan keamanan data yang dikirimkannya selama transmisi data, TKIP dan (AES)-CCMP. TKIP merupakan sebuah protokol yang mengimplementasian fungsi penggabunga kunci dengan vektor inisialisasi di setiap paketnya. Selain itu, TKIP dilengkapi dengan pengecekan integritas pesan yang dikenal dengan MIC atau MICHAEL. Sebuah kemampuan untuk mencegah serangan-serangan sederhana juga ditambahkan dengan sebuah pencacah yang mendeteksi serangan-serangan tersebut. Pencacah ini akan memastikan setiap data yang dikirim dapat diterima sesuai dengan urutan data sehingga tidak dimungkinkan terjadinya serangan.

Namun, serangan terhadap TKIP dapat dilakukan dengan mengambil potongan-potongan data yang dikirimkan. Serangan dilancarkan dengan mengambil paket-paket data kecil yang ditransmisikan oleh *access point*. Paket-paket ini biasanya merupakan paket yang sangat mudah dikenali berdasarkan ukurannya yang kecil dan sangat mencolok perbedaannya dibandingkan dengan paket-paket data lain, seperti paket-paket data permintaan dan respon ARP.

Paket-paket tersebut dikirimkan secara *broadcast* dalam satu jaringan sehingga memungkinkan untuk mengambil paket data tersebut. Dalam paket-paket tersebut, terdapat alamat perangkat pengirim dan penerima paket data yang tidak dilindungi oleh WEP maupun TKIP.

Dengan menggunakan serangan ini, data-data yang ada dapat didekripsi dengan kecepatan hingga satu byte dalam waktu satu menit. Selain itu, jika fungsi QoS diaktifkan, maka setiap serangan terhadap 1 paket akan menyebabkan terinjeksinya 15 paket yang terenkripsi lain.

3.1 Aplikasi Serangan Terhadap WPA

Untuk melakukan serangan, dapat digunakan perangkat lunak bantuan yang biasa dipakai untuk memonitor jaringan nirkabel, seperti aircrack-ng, kismet, atau WireShark. Piranti lunak tersebut diatur dalam mode monitor agar dapat menangkap data-data yang dikirimkan secara *broadcast*. Setelah mengamati paket-paket data yag ditrasmisikan, pelaku serangan dapat melihat jenis algoritma yang dipake dalam transmisi tersebut. Hal ini dapat terlihat tipe enkripsi yang ada dari informasi paket data yang ditangkap. Bentuk informasi paket data tersebut kurang lebih sebagai berikut:

SSID : **Bubba**
Server : localhost:2501
BSSID : **00:40:15:E4:C3:25**
Manuf : Unknown
Max Rate: 11.0
BSS Time: 1f6b97f6463
First : Wed Nov 8 17:33:30 2006
Latest : Wed Nov 8 17:34:41 2006
Clients : 1
Type : Access Point (infrastructure)
Channel : **3**

Privacy : Yes
Encrypt : **WPA**
Decryptd: No
Beacon : 25600 (26.214400 sec)
Packets : 135
Data : 1
LLC : 133
Crypt : 1
Weak : 0
Dupe IV : 0
Data : 0B
Signal :
Power : -47 (best -45)
Noise : 0 (best 0)
IP Type : TCP (4 octets)
IP Range: 192.168.1.2

Dari data tersebut dapat diketahui bahwa enkripsi dilakukan dengan menggunakan WPA. Setelah mengetahuinya, serangan dilanjutka dengan mengambil catatan dari arus lalu lintas data yang terjadi. Data yang diambil cukup berupa vektor inisialisasi saja. Setelah itu, potongan-potongan data yang telah dicatat tersebut digabung menjadi satu.

Setelah mendapatkan data-data tersebut, serangan dapat dilakukan dengan memanfaatkan celah pada vektor inisialisasi. Celah ini memungkinkan pengambilan informasi dari satu byte pertama rangkaian kunci tersebut, sehingga saat satu byte tersebut telah diperoleh, maka kunci yang lainnya dapat diperoleh dengan mudah.

Karena standard yang digunakan adalah paket data sesuai dengan aturan 802.11, maka susunan paket data tersebut dapat diketahui dengan pasti dan byte pertama pun dapat diperolah dengan melakukan operasi XOR byte pertama dari paket data terenkripsi dan 0xAA.

Vektor inisialisasi terdiri dari 24 bit (3 byte) dan adalah kasus ini, sebuah vektor inisialisasi yang lemah berada dalam bentuk A+3, N-1, X dimana:

- A adalah byte dari kunci yang ingin diperoleh
- N adalah parameter modulus yang digunaka pada algoritma RC4 (256)
- X adalah nilai acark dari 0 hingga 255

Algoritma pengamanan ini membutuhkan penyerangan beberapa kali secara sekuensial terhadap byte-byte dalam paket kunci. Sebuah larik K dapat digunaka untuk membantu menyelesaikan masalah ini.

- K[0], K[1], K[2] menampung nilai vektor inisialisasi
- K[3], K[4], ... K[panjang kunci WPA] menampung kunci WPA
- K[panjang kunci+1], K[panjang kunci+2], K[panjang kunci+3] juga menampung vektor inisialisasi
- K[panjang kunci+3+1], K[panjang kunci+3+2], .. K[2*panjang kunci+3+1] kembali berisi kunci WPA.

Serangan dilakukan dengan mengkalkulasi byte pertama dari paket data tersebut, kemudian melakukan hal perhitungan berulang sesuai dengan jumlah pengulangan, yaitu tiga kali. Jika pengulangan kurang dari 3, maka tahap ini gagal. Jika berhasil, kurangi hasil modulus byte pertama da 256 degan K[A+3]

Proses tersebut dilakukan sebanyak 60 vektor inisialisasi dan menggunakan variabel x dan hasil yang diperoleh memiliki tingkat keberhasilan 50%.

Untuk menghindari CRC, dapat digunakan operasi linear dengan XOR, dalam arti: CRC(x ^ y) = CRC(*x*) ^ CRC(*y*). Mengingat algoritma RC4 juga menggunakan XOR untuk mengenkripsi data, pelaku serangan dapat mengubah CRCnya pula.

Dengan menggunakan CRC linear, dengan diberikan data terenkripsi C, serangan dapat dilakukan untuk mendapatkan data C^1 dengan memberikan CRC yang tepat. Data baru yang akan dibangun akan menjadi C^1 = C ^ *d*, dimana *d* adalah delta paket yang dipilih. Aplikasi tersebut dapat memakai asumsi:

- || adalah operator penggabungan: AB||CD = ABCD
- IV adalah vektor inisialisasi
- K adalah kata kunci yang digunakan
- M adalah data asli yang tidak terenkripsi
- M^1 adalah data yang diperoleh setelah mendekripsi C^1
- RC4(K) kunci acak yang dibangkitkan oleh algoritma RC4 yang diberi masukan K

Pembuktian untuk mendapatkan data dengan membangun hasil dari data terenkripsi adalah sebagai berikut:

- C = RC4(IV || K) ^ (M || CRC(M))
- C^1 = C ^ (d || CRC(d))
  1. = RC4(IV || K) ^ (M || CRC(M)) ^ (d || CRC(d))
  2. = RC4(IV || K) ^ ((M ^ d) || (CRC(M) ^ CRC(d))
  3. = RC4(IV || K) ^ ((M ^ d) || CRC(M ^ d))
  4. = RC4(IV || k) ^ (M^1 || CRC(M^1))

Oleh sebab itu, hanya diperlukan proses XOR terhadap paket yang ditangkap dan *d* paket untuk memperoleh paket baru dengan CRC yang benar.

Proses-proses tersebut dilanjutkan dengan menginjeksi paket-paket data ke dalam jaringan dan mengirimkanya ke klien. Proses penyerangan terhadap protokol TKIP membutuhkan waktu untuk mendapatkan keseluruhan kunci. Hal ini disebabkan teknik penyerangan hanya menghasilkan kunci sepanjang 1 byte setiap kali serangan berhasil dilakukan.

Berdasarkan percobaan yang telah dilakukan, untuk mendekripsi kunci-kunci dalam jaringan yang menggunakan WPA, diperlukan waktu sekitar 900 detik (12-15 menit). Hal ini disebabkan tujuan dari serangan ini adalah mendekripsi semua byte yang ada dalam paket ARP. Paket ARP itu sendiri terdiri dari alamat IP pengirim dan penerima.

4. Penanganan Celah Keamanan

Untuk menangani berbagai masalah keamanan, terutama yang disebabkan oleh faktor TKIP, terdapat beberapa pencegahan yang dapat dilakukan untuk meminimalisir ancaman yang dihadapi, antara lain:

- Jika vektor inisialisasi yang diterima oleh klien memiliki nilai yang salah, transmisi dapat dinyatakan mengalami kegagalan dan paket dapat diabaikan. Jika nilai yang diperoleh benar, namun terdapat kegagalan pada verifikasi MIC, maka dapat diasumsikan terjadi penyerangan. Saat hal ini terjadi, maka *access point* dapat diperingatkan dengan sebuah *MIC falure report frame*. Jika terjadi lebih dari dua kesalahan verifikasi dalam waktu kurang dari 60 detik, maka semua proses komunikasi dimatikan dan akan diulang kembali 60 detik kemudian.

- Ketika paket berhasil diterima dengan benar, TSC dapat diubah. Jika sebuah paket memiliki nilai yang lebih kecil dibanding dengan TSC, maka paket tersebut dapat diabaikan.

Meskipun cara-cara tersebut telah dilakukan, masih terdapat kemungkinan melakukan serangan. Penyerangan dapat dilakukan pada jalur QoS yang biasanya memiliki lalu lintas data yang tidak terlalu padat dengan nilai TSC yang masih rendah pula. Bila pemilihan nilai vektor inisialisasi salah, maka paket akan diabaikan, namun bila pemilihan nilai benar, maka sebuah *MIC failure report time* akan dikirimkan oleh klien, tetapi nilai TSC tidak bertambah.

Penyerang harus menunggu paling tidak 60 detik setelah setiap percobaan penyerangan yang dilakukannya untuk mencegah terputusnya koneksi yang mengakibatkan usaha penyerangan gagal. Dalam waktu lebih dari 12 menit, penyerang dapat mendekripsi paling tidak 12 byte data asli (MIC da ICV). Untuk menentukan byte-byte lain yang belum diketahui (alamat pasti pengirim dan penerima), penyerang dapat memilih suatu nilai secara acak dan memverifikasikannya pada ICV yang telah didekripsi.

Setelah MIC dan seluruh data asli telah diketahui, penyerang dapat dengan mudah membalik proses algoritma MICHAEL dan mendapatkan kunci MIC yang digunakan untuk melindungi pesan yang dikirim dari *access point* kepada klien. Algoritma MICHAEL tidak didesain sebagai sebuah fungsi satu arah sehingga proses membalik algoritma ini sama efisien dengan menghitung algoritma ini secara normal.

Pada tahap ini, penyerang telah mendapatkan kunci MIC dan mengetahui setiap aliran data komunikasi dari *access point* ke klien. Penyerang dapat dengan mudah mengirimkan paket kepada klien lain dengan memanfaatkan setiap jalur QoS dan nilai TSC masih tetap lebih rendah dibanding nilai yang diperoleh dari paket yang ditangkap.

Dalam berbagai jaringan nirkabel pada umumnya, lalu lintas data hanya berlangsung di jalur 0 sehingga penyerang dapat memanfaatkan ketujuh jalur lain untuk mengirimkan ke klien. Setelah serangan tersebut berhasil dilaksanakan, penyerang dapat memperoleh kunci-kunci lain dalam waktu 4-5 menit. Hal ini disebabkan penyerang harus mendekripsi 4 byte ICV.

Byte yang menyimpan alamat IP dapat ditebak dan MIC dapat dikalkulasi dengan menggunakan kunci MIC yang telah diperoleh sebelumnya, kemudian dapat diverifikasi dengan ICV.

Langkah lebih jauh yang dapat ditempuh oleh penyerang adalah dengan pengiriman pesan yang dapat memicu bekerjanya *Intrusion Detection System (IDS)* yang bekerja pada lapisan IP sehingga dapat membawa gangguan yang cukup signifikan pada sistem.

Hal lain yang dapat terjadi adalah, jalur lalu lintas data diubah dengan memberikan respon ARP palsu. Penyerang juga dapat membangun jalur dua arah ke klien yang lain, jika klien terhubung ke internet dan menggunakan *firewall* untuk semua koneksi yang masuk, namun masih membuka koneksi yang menuju luar. Respon dari klien memang tidak dapat dibaca langsung, namun dapat diteruskan ke jaringan internet.

Meskipun jaringan yang digunakan tidak mendukung IEEE 802.11e dengan kemampuan QoS, serangan seperti ini masih mungkin terjadi. Pada kasus ini, penyerang harus mencegah klien menerima paket data yang dimaksudkan penyerang untuk diserang. Penyerang juga harus memutuskan koneksi klien dari akses poin untuk sementara waktu saat serangan sedang dilaksanakan sehinggan nilai TSC tidak meningkat.

Setelah penyerang berhasil mengeksekusi serangannya, ia dapat mengirimka sebuah paket data ke klien. Namun, cara serangan seperti ini sangat tidak mungkin dilakukan.

Jika peyerang berencana untuk mendapatkan kunci yang masih berlaku untuk jalur QoS dan kunci MIC untuk jalur kedua arah, maka penyerang tersebut harus dapat menggunakan kunci-kunci yang telah berhasil diperolehnya untuk mendapatkan kunci-kunci tambahan lainnya dan penyerang juga dapat mengirimkan paket-paket tanpa batasan.

Untuk menghindari kasus-kasus khusus tersebut, maka cara-cara yang dapat dilakukan adalah:

1. TKIP Key Rotation
   Dengan menggunakan infrastruktur yang mendukung, kunci TKIP dapat diubah setiap beberapa waktu. Kunci-kunci lain pun dapat diubah secara periodik oleh sistem. Dengan mengubah kunci-kunci yang digunakan dapat membatasi serangan yang dilakukan karena jumlah byte yang berhasil didekripsi dapat dikurangi. Selain itu, jika QoS tidak diperlukan maka sebaiknya fungsi ini dimatikan.

   Selain itu, hal lain yang dapat dilakukan adalah menghilangkan fungsi pengiriman *MIC failure report frame* pada klien. Sedangkan solusi terbaik yang dapat dilakukan adalah dengan menghindari penggunaan TKIP dan beralih menggunakan CCMP sebagai metode pengamanan.

2. Monitoring and Logging
   Beberapa infrastruktur memiliki kemampuan mengamati lalu lintas data yang dikirimkan. Dengan demikian, sistem akan memberi peringatan bila ada klien yang menunjukkan kemungkinan terkena serangan TKIP.

   Selain itu sistem akan membuat catatan tentang hal ini sehingga mempermudah pemantauan.

3. Wireless Intrusion Prevention
   Solusi lain adalah dengan penggunaan sistem pengecek intrusi/gangguan keamanan. Dengan adanya sistem ini, maka berbagai jenis serangan yang ditujukan ke sistem akan dapat terpantau dan sistem akan segera mengambil keputusan berdasarkan ancaman tersebut.

   Selain itu, sistem juga dapat mengamati gangguan keamanan lain yang terjadi pada sistem. Untuk setiap gangguan yang muncul, sistem akan memberikan peringatan kepada pengelola jaringan secara langsung. Hal lain yang dapat dilakukan oleh sistem ini adalah pencatatan informasi penyerang dalam sistem sehingga penyerang dapat dibuat tidak bisa mengakses sistem.

5. Kesimpulan

WEP telah diketahui sebagai sebuah sistem yang tidak aman sejak tahun 2001, oleh sebab itu dikembangkan WPA yang dimaksudkan untuk menghilangkan berbagai ancaman keamanan data seperti yang terjadi pada WEP.

WPA mengusung berbagai kemampuan baru yang belum ada sebelumnya, seperti TKIP. Namun, protokol tersebut tidak banyak berbeda dengan WEP sehingga masih banyak serangan yang mengancam teknologi ini. Bahkan, dalam ujicoba yang telah dilakukan, jaringan yang dilindungi dengan WPA dan menggunakan kata kunci yang kuatpun tidak 100% aman dan masih dapat diserang.

Meskipun serangan ini bukan merupakan jenis serangan yang dapat memperoleh keseluruhan kunci, namun serangan ini juga harus diwaspadai. Oleh sebab itu, sudah cukup banyak industri manufaktur yang mengembangkan berbagai piranti lunak dalam perangkat mereka untuk mengenali serangan-serangan yang ada sehingga dapat menangkalnya dengan lebih baik.

Untuk pengamanan yang lebih baik, penggunaan TKIP sebaiknya diubah menjadi CCMP atau mengganti WPA dengan metode yang lebih baik seperti WPA2.

6. Referensi

- A. Klein. Attacks on the RC4 stream cipher. Designs, Codes and Cryptography, hal. 269-286. 2008.

- Edney, Jon; Arbaugh, William A. 2003. Real 802.11 Security: Wi-Fi Protected

Access and 802.11i. Addison Wesley Professional.

- Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, WISA, volume 4867 of Lecture Notes in Computer Science, hal. 188-202. Springer. 2007.

- Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Selected Areas in Cryptography 2007, Lecture Notes in Computer Science. Springer. 2007.

- "Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP". Wi-Fi Alliance. 2002-10-31. http://wi-fi.org/pressroom_overview.php?newsid=55.

- "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements" (pdf). IEEE Standards. 2004-07-23. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.