Studi Serangan Terhadap Jaringan Nirkabel dengan Protokol Keamanan WEP

Glen Christian (13505098)
Teknik Informatika ITB, Bandung 40132, e-mail: if15098@students.if.itb.ac.id

Abstrak – Enkripsi WEP (Wired Equivalent Privacy) adalah salah satu metode pengamanan yang memungkinkan pengguna untuk melindungi data yang dikirim atau diterima dalam suatu koneksi nirkabel antara modem router pengguna dan komputer lainnya. Enkripsi yang dilakukan membuat data yang dipertukarkan tidak dapat dibaca jika ada seseorang yang melakukan *packet sniffing* pada jaringan tersebut, karena yang bersangkutan tidak mengetahui kunci enkripsi untuk melakukan ekstraksi informasi. Bagaimanapun juga, ketika *modem router* pengguna yang dituju menerima data tersebut, kunci enkripsi digunakan untuk membuat data yang telah dienkripsi tersebut dapat dibaca kembali. Pengguna lainnya yang melakukan suatu usaha untuk terhubung dengan jaringan terenkripsi harus memiliki kunci enkripsi untuk mendapat hak akses yang sama, serupa halnya dengan diperlukan kunci dengan bentuk yang spesifik untuk membuka pintu rumah seseorang. Pada umumnya, *modem router* memungkinkan kita untuk mengetahui kunci enkripsi WEP yang digunakannya. Pada beberapa kasus, kita akan diminta untuk melakukan input *pass phrase* yang secara otomatis akan membangkitkan kunci enkripsi, suatu kata yang terdiri dari huruf dan angka. Kunci tersebut akan digunakan ketika kita melakukan kustomisasi terhadap suatu *wireless adapter* untuk membuat koneksi terhadap suatu jaringan.

Kata Kunci: enkripsi, jaringan nirkabel, WEP.

1. PENDAHULUAN

Sebelum masuk ke pokok permasalahan yaitu serangan pada WEP, berikut akan dijelaskan bagaimanakah proses enkripsi yang dilakukan oleh WEP.

1.1 Bagaimana WEP bekerja

WEP menggunakkan algoritma RC4 untuk melakukan enkripsi paket berisi informasi sebelum dikirim dari access point atau wireless network card. Segera setelah access point menerima paket yang dikirim oleh network card milik pengguna, paket akan didekripsi.

Setiap byte akan dienkripsi dengan menggunakkan kunci yang berbeda. Hal ini member kepastian bahwa apabila seorang hacker mampu membobol kunci yang dimiliki suatu paket, maka informasi yang bisa diketahui hanya yang terdapat pada paket tersebut.

Cara melakukan enkripsi dengan algoritma RC4 cukup mudah untuk dimengerti. Operasi yang akan dilakukan adalah XOR terhadap plainteks dengan suatu keystream yang sangat panjang.

Hal-hal yang perlu diketahui seputar WEP:

1. Packet Key: dibangkitkan melalui kombinasi *pre-shared password*, *state array* dan *initialization vector* (IV).

2. Pre-shared Password: untuk setiap paket yang ditransmisikan digunakan pre-shared password yang sama.
3. State Array: sebuah bilangan yang diacak secara *random* kemudian dignunakan dalam RC4 untuk membentuk *key stream*.
4. Initialization Vector (IV): IV adalah bilangan dengan panjang 3 bytes dibangkitkan secara acak oleh komputer, ikut disimpan dalam cipherteks yang dikirim ke penerima. IV akan digunakan saat akan melakukan dekripsi.
5. Key Scheduling Algorithm: proses KSA yang melibatkan pembuatan *state array* yang akan digunakan sebagai input pada fase kedua yaitu PRGA.
6. Pseudo Random Generation Algorithm: array berisi state hasil proses KSA yang digunakan untuk membangkitkan key stream final. Setiap byte dari key stream dibangkitkan kemudian dilakukan operasi XOR dengan plainteks untuk membentuk cipherteks.

2. OVERVIEW TERHADAP SERANGAN WEP

Enkripsi pada WEP menggunakkan kunci rahasia, k, shared antara access point dan mobile node. Untuk melakukan komputasi sebuah frame WEP, data frame plainteks, M, dikonkatenasi dengan checksum miliknya yaitu c(M), untuk memproduksi M.c(M). Setelah itu, initialization vector (IV) dari tiap paket diletakkan sebelum kunci rahasia, k, untuk membuat kunci paket yaitu $IV \cdot k$. Setelah itu, algoritma stream cipher RC4 di-inisialisasi menggunakkan kunci paket tersebut, kemudian hasil output dari enkripsi tersebut dilakukan operasi XOR dengan checksum plainteks untuk membentuk cipherteks:

$$C = (M \cdot c(M)) \text{ XOR } RC4(IV \cdot k)$$

2.1 Serangan IV Fluhrer, Mantin dan Shamir

Algoritma stream cipher RC4 memiliki dua bagian, yang pertama adalah algoritma key scheduling dan yang kedua adalah output generator. Pada WEP, algoritma key scheduling menggunakkan kunci berukuran 64-bit (40-bit kunci rahasia dan 24-bit IV) atau kunci 128-bit (104-bit kunci rahasia dan 24-bit IV) untuk membentuk RC4 state array, S, yaitu merupakan permutasi dari {0,...,255}. Ouput generator menggunakkan state array S untuk membentuk psoudorandom sequence.

Serangan tersebut memanfaatkan hanya kata pertama dari keluaran pseudorandom sequence. Hasil keluaran byte pertama memiliki persamaan $S[S[1]+S[S[1]]$. Demikian, setelah tahap pertama yaitu pembentukan kunci, byte pertama bergantung hanya kepada tiga nilai dari state array yaitu ($S[1]$, $S[S[1]]$, $S[S[1]+S[S[1]])$. Serangan dilakukan berdasarkan kemampuan untuk mendapatkan informasi tentang kunci dengan cara melakukan observasi terhadap nilai-nilai tersebut.

Untuk melakukan serangan tersebut, dilakukan pencarian IV yang menempati algoritma pembentukan kunci menjadi sebuah state yang memberitahu informasi mengenai kunci. Menggunakkan terminology milik Fluhrer, cukup mudah untuk melakukan identifikasi apakah sebuah paket memiliki IV di dalamnya dan byte hasil keluaran tertentu. Setiap resolved packet memberikan informasi berisi hanya 1-byte kunci, sisa byte kunci harus ditebak sebelum paket lainnya memberikan informasi berisi byte kunci setelahnya.

3. IMPLEMENTASI

Pada saat serangan ini diimplementasikan, ada tiga tujuan utama yang ingin dicapai. Yang pertama dan terutama, ingin dilakukan pembuktian bahwa serangan tersebut dapat bekerja/dilakukan pada dunia nyata. Kedua, ingin dibuktikan bahwa serangan ini dapat dilakukan dengan biaya yang murah dan langkah yang mudah. Terakhir, ingin dilakukan pengembangan terhadap serangan RC4 dan serangan WEP.

3.1 Melakukan Packet Capturing

Dalam serangan ini, melakukan penangkapan paket yang terenkripsi WEP pada sebuah wireless network terbukti merupakan tahap serangan yang paling membutuhkan waktu. Untuk melakukan hal ini, hanya dibutuhkan sebuah Linksys wireless card seharga $100 berbasis chipset Intersil Prism II.

3.2 Mempersiapkan Serangan

Langkah terakhir yang dilakukan untuk melakukan serangan adalah menentukan nilai yang benar dari byte pertama tiap plainteks dari tiap paket, sehingga didapat byte pertama dari pseudorandom sequence dari byte pertama ciphertext. Untuk melakukan hal ini digunakan tcpdump dari lalu lintas data yang telah didekripsi, kemudian juga digunakan panjang paket untuk membedakan ARP dan IP traffic. Ternyata serangan belum berhasil, namun ditemukan bahwa encapsulation header pada versi 802.2 ditambahkan pada ARP dan IP traffic. Hal ini membuat serangan menjadi lebih mudah, semua paket IP dan ARP memiliki byte pertama dari plainteks yang sama (0xAA).

```
RecoverWEPKey()
    Key[0. . .KeySize] = 0
    for KeyByte = 0. . .KeySize
      Counts[0. . .255] = 0
      foreach packet !P
       if P.IV 2 {(KeyByte+3,0xFF,N) | N 2 0x00. .
       .0xFF}
          Counts[SimulateResolved(P,Key)]+ = 1
      Key[KeyByte] =
IndexOfMaximumElement(Counts)
    return Key
```

Dengan menggunakkan algoritma di atas, serangan akan berhasil pada waktu yang singkat (kira-kira satu atau dua hari).

Pertama-tama, dilakukan penangkapan paket dalam jumlah besar dari sebuah jaringan nirkabel. Pada saat pencarian IV dari paket yang telah ditangkap, ditemukan bahwa wireless card menggunakkan counter sederhana untuk melakukan komputasi IV, yaitu byte pertama di increment terlebih dahulu.

Algoritma di atas menunjukkan serangan dasar untuk mendapatkan kunci WEP.

4. PENGEMBANGAN SERANGAN

Beberapa modifikasi dapat dilakukan pada serangan ini untuk meningkatkan performansi serangan pencarian kunci WEP.

4.1 Memilih IV

Pada serangan dasar, hanya IV dengan bentuk tertentu yang menjadi pertimbangan. Bagaimanapun, ditemukan bahwa terdapat IV yang menghasilkan resolved state, dan pengetesan IV hanya dilakukan dengan input dari paper Fluhrer *et. al*. Terlebih, pencarian dapat dilakukan secara paralel.

4.2 Menebak Byte Kunci Awal

Berdasarkan serangan Fluhrer, Mantin dan Shamir yang bekerja berdasarkan ditemukannya byte kunci, menemukan byte kunci awal sangatlah penting. Terdapat dua pendekatan yang penting dalam menebak byte kunci awal. Yang pertama adalah IV dibangkitkan secara acak.

Pendekatan yang kedua berdasarkan key management pada WEP yang kurang baik. Karena kunci WEP harus diberikan input secara manual, diasumsikan bahwa daripada memberikan client string panjang dalam heksa, seorang pengguna akan memberikan input sebuah kata yang mudah diingat. Dapat disimpulkan bahwa seringkali kata yang mudah diingat oleh pengguna yang digunakan dalam pembentukan awal kunci (biasanya menggunakkan karakter ASCII).

Hal ini membuat pengurangan yang besar terhadap paket yang dibutuhkan untuk melakukan penebakan byte pertama dari kunci WEP.

```
RecoverWEPKeyImproved(CurrentKeyGuess,
KeyByte)
        Counts[0. . .255] = 0
        foreach packet !P
                if Resolved?(P.IV)
        Counts[SimulateResolved(P,CurrentKeyG
        uess)]+ =Weight(P,CurrentKeyGuess)
        Foreach
SelectMaximalIndexesWithBias(Counts)→ByteGu
ess
        CurrentKeyGuess[KeyByte] = ByteGuess
        if Equal?(KeyByte,KeyLength)
                if
CheckChecksums(CurrentKeyGuess)
                        return CurrentKeyGuess
                else
        Key=RecoverWEPKeyImproved(Current
KeyGuess,
        KeyByte+1)
                if notEqual?(Key,Failure)
                        return Key
        returnFailure
```

4.3 Beberapa Kasus Khusus

Pada beberapa kondisi dimana kasus tertentu memberikan indikasi yang lebih baik . Contohnya apabila didapat duplikasi pada tiga buah nilai pada posisi $S[1]$, $S[S[1]]$, dan $S[S[1]+S[S[1]]$, kemungkinan posisi tersebut dalam permutasi S tidak mengalami perubahan

5. FAKTOR PERFORMANSI

Banyak sekali variabel yang dapat mempengaruhi performansi serangan pencarian kunci pada WEP.

5.1 Pemilihan IV

Karena WEP standar tidak memiliki ketentuan bagaimana sebaiknya memilih IV, terdapat beberapa variasi dari pembangkitan IV yang digunakan pada wireless card versi 802.11. pada umumnya kebanyakan wireless card menggunakkan tiga metode yaitu: pembangkitan dengan counter, pembangkitan secara random, serta value-flipping. Serangan pada WEP tersebut hanya dapat dilakukan apabila digunakan metode pertama dan kedua. Value-flipping mencegah serangan ini dengan dasar mahalnya penggunaan ulang pseudorandom stream pada setiap paket.

Counter mode adalah metode yang paling mudah untuk diserang. Pada wireless card tersebut, dilakukan increment pada IV untuk setiap paket

yang dikirim (dimulai dari 0 atau angka random pada saat card tersebut dinyalakan).

Kesimpulannya, tidak ada cara yang benar-benar tepat untuk memilih IV sebelum dilakukan testing terlebih dahulu.

5.2 Key Selection

Manajemen pemilihan kunci pada WEP memberikan kontribusi pada kemudahan melakukan serangan pencarian kunci. Pada umumnya, kebanyakan jaringan menggunakkan single shared key antara basestation dan semua mobile nodes. Beberapa situs menggunakkan kata kunci yang mudah diingat oleh manusia untuk mempermudah distribusi kunci. Tidak ada cara yang umum untuk melakukan mapping password menjadi kunci WEP. Solusi sekarang yang digunakkan adalah melakukkan mapping nilai ASCII secara langsung ke dalam byte kunci. Lebih disarankan apabila digunakan fungsi hash untuk meningkatkan keamanan.

5.3 RC4

RC4 merupakan algoritma stream cipher yang dapat digunakan secara aman. Implementasi dari RC4 dalam SSL tidak dipengaruhi oleh serangan Fluhrer. Alasannya adalah karena kunci enkripsi pada SSL pre-processes didapat dengan melakukan hashing dengan algoritma MD5 dan SHA1.

RC4 sebenarnya masih dapat digunakan sebagai bagian solusi keamanan. Tetapi, harus ada pengembangan lebih lanjut pada algoritma tersebut sehingga tidak lagi ada kebocoran komponen kunci.

6. KESIMPULAN DAN SARAN

Karena adanya bentuk serangan diatas, jaringan versi 802.11 dengan protokol keamanan WEP harus diwaspadai sebagai jaringan yang sudah tidak aman lagi.

Jika kita menggunakkan sebuah jaringan nirkabel harus diperhatikan bahwa:

- Link layer tidak menyediakan layanan keamanan.
- Lebih baik menggunakkan layanan keamanan yang lebih tinggi seperti IPsec dan SSH, daripada menggunakkan WEP.
- Harus diasumsikan bahwa siapa saja dengan suatu jarak tertentu dapat melakukan komunikasi dengan jaringan sebagai pengguna yang sah.

7. Daftar Pustaka

[1] BORISOV, N., GOLDBERG, I., AND WAGNER, D. Intercepting mobile communications:
The insecurity of 802.11. *MOBICOM 2001* (2001).

[2] CAFARELLI, D. Personal communications, 2001.

[3] DIERKS, T., AND ALLEN, C. *The TLS Protocol, Version 1.0*. Internet
Engineering Task Force, Jan. 1999. RFC-2246, ftp://ftp.isi.edu/
in-notes/rfc2246.txt.
11

[4] FLUHRER, S., MANTIN, I., AND SHAMIR, A. Weaknesses in the key
scheduling algorithm of RC4. *Eighth Annual Workshop on Selected Areas
in Cryptography* (August 2001).
[5] HAMRICK, M. Personal communications, 2001.

[6] KENT, S., AND ATKINSON, R. Security architecture for the Internet protocol. Request for Comments 2401, Internet Engineering Task Force, November 1998.

[7] L. M. S. C. OF THE IEEE COMPUTER SOCIETY. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Standard 802.11, 1999 Edition* (1999).

[8] POSTEL, J., AND REYNOLDS, J. K. Standard for the transmission of IP datagrams over IEEE 802 networks. Request for Comments 1042, Internet Engineering Task Force, Feb. 1988.

[9] SCHNEIER, B. *Applied Cryptography - Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc., 1994.

[10] SHAMIR, A. Personal communications, 2001.

[11] YLONEN, T. SSH - secure login connections over the Internet. *USENIX Security Conference VI* (1996), 37–42.