Studi dan Analisis Serangan Terhadap E0 Cipher pada Protokol Komunikasi Bluetooth

Dian Syahfitra [1)]

1) Jurusan Teknik Informatika ITB, Jl Ganesha no 10 Bandung 40132,
email: if14021@students.if.itb.ac.id

Abstract *- Makalah ini memberikan sedikit studi tentang algoritma E0 pada komunikasi protocol Bluetooth. Algoritma E0 yang digunakan pada enkripsi Bluetooth dimaksudkan untuk menjaga keamanan dan efisiensi. Enkripsi dilakukan dengan untaian cipher E0 yang disinkronkan untuk setiap pesan yang akan dipertukarkan. Makalah ini juga memaparkan beberapa serangan pada algoritma E0 secara umum dan tidak mendetail. Pada perkembangannya E0 sudah dapat dikripanalisis dan rentan terhadap banyak serangan(attack). Makalah ini juga melakukan studi mengapa E0 rentan terhdap serangan-serangan tersebut.*

Kata Kunci *: Attack, Bluetooth, E0, Enkripsi*

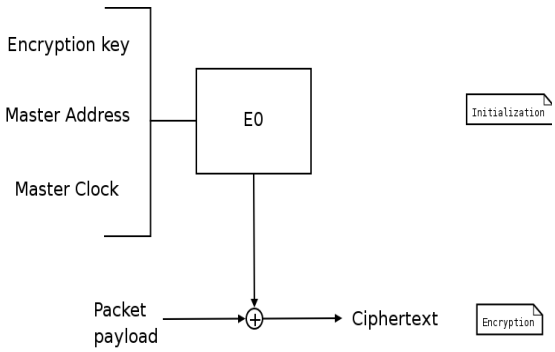
1. PENDAHULUAN

Bluetooth merupakan teknologi jaringan telekomunikasi nirkabel yang menyedikan standar dan protokol dalam petukaran data pada jarak 1-100 meter. Untuk menjaga keamanan data diperlukan enkripsi yang baik namun karena sifatnya mobile, enkripsi tersebut harus efisien dan menkonsumsi sedikit tenaga. E0(E nol) per merupakan metode yang dipilih untuk mengenkripsi pertukaran data dalam Bluetooth protokol. E0 termasuk salah satu jenis stream ciphers seperti layaknya A5 atau RC4.

Sebelum menuju ke algoritma E0 perlu diketahui tentang proses enkripsi pada Bluetooth sendiri. Proses enkripsi berjalan sebagai berikut; algoritma E0 memiliki 3 masukan yaitu :

1. Kunci enkripsi atau pada dunia nyata sering dikenal dengan nama PIN (*Personal Identification Number*) yang terdiri dari 1-16 karakter (8-128 bit). Kunci enkripsi kemudian akan di kombinasikan dengan EN_RAND untuk membentuk kunci tengah (K'_c)[2].
2. *Master Address*(BD_ADDR) yang nilainya sudah tertentu terdiri dari 48 bit yang dimiliki secara unik untuk setiap perangkat Bluetooth dan disebut dengan Bluetooth Device Address [6]
3. *Master Clock*, waktu pengiriman paket yang terdiri dari 26 bit [6].

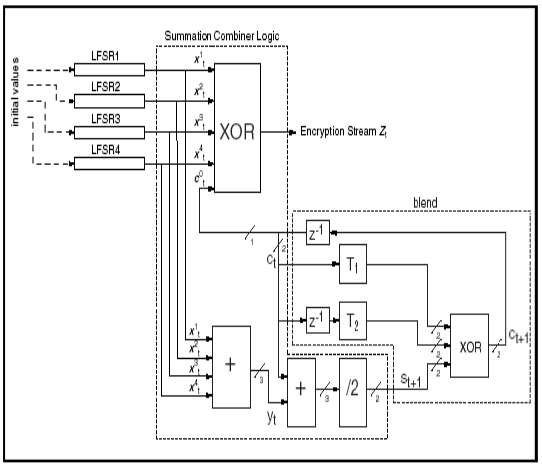
Masukan ini akan digunakan pada pembangkit kunci di algoritma E0. Hasil pembangkitan aliran kunci dari E0 akan digabung (XOR) dengan plaintext menjadi ciphertext dan sebaliknya .Sebagai ilustrasi dapat dilihat gambar 1 dibawah.



Gambar 1Skema Enkripsi Pada Bluetooth

Pembangkit aliran kunci (*Key Stream Generator*) dari inti E0 memiliki hanya 2 bagian utama yaitu combiner dan blender. Dalam *Bluetooth* spesifikasi algoritma enkripsi adalah sambungan sebagai deretan cipher menggunakan 4 LFSR(linier feedback shif register). Total panjang 128 bit, dimana untuk LFSR1 memiliki panjang 25 bit, LFSR2 memiliki panjang 31 bit, LFSR3 memiliki panjang 33 bit, LFSR4 memiliki panjang 39 bit. Pembangkit kunci dan autentikasi pada Bluetooth menggunakan algoritma SAFER+ 8-round[9].

Pembangkit kunci aliran diisi dengan nilai awal untuk LFSR(total 128 bits) dan 4 bits yang menspesifikasikan nilai c0 dan c-1. 132 bit nilai awal diturunkan dari empat input menggunakan pembangkit kunci aliran. Parameter input adalah kunci Kc, 128 bit angka acak RAND, 48 bit alamat BT, dan 26 *master clock* CLK 26-1. Saat kunci enkripsi sudah dibentuk lalu LFSR diisikan dengan nilai awalnya kemudian 200 bit cipher dibentuk dengan mengoperasikan generator. Dari bit ini 128 yang terakhir diumpan balikkan dalam generator sebagai angka awal dari keempat LFSR. Setelah itu ketika diberi *clock generator* menghasilkan deret enkripsi(atau dekripsi) yang di-XOR dengan data yang ditransmisikan (atau diterima). Untuk lebih detail dapat diliaht pada referensi [9].



Gambar 2 Algoritma E0

Algoritma E0 menggunakan 2 tingkat mekanisme pembentukan aliran kunci, tingkat pertama dari pembentukan aliran kunci digunakan untuk membentuk keadaan awal dan tingkat kedua dari pembentukan aliran kunci digunakan untuk mengenkripsi data[2]. Dua tingkat ini digunakan Scott R. Fluhrer1 and Stefan Lucks untuk menemukan sejumlah serangan.

2. PEMBAHASAN

Sejumlah serangan telah ditemukan pada algoritma E0 namun pada makalah ini hanya dibahas seebahagian kecil saja.

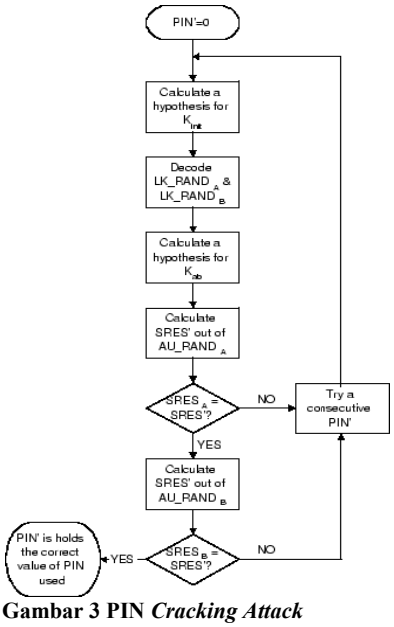
2.1 PIN Cracking Attack

Serangan ini dikemukan oleh Yaniv Shaked and Avishai Wool pada ACM *Conference Mobile Systems*[8]. Serangan sebagai berikut; Diasumsikan bahwa terjadi eavesdropped pada proses pertukaran RAND/proses pairing dan proses autentifikasi dan semua pesan di simpan seperti pada table 1.

Tabel 1Data Hasil *Eavesdropped*

No	Src	Des	Data	Len	Note
1	A	B	IN_RAND	128bit	Plain text
2	A	B	LK_RAND A	128bit	XORed with K_{init}
3	B	A	LK_RAND B	128bit	XORed with K_{init}
4	A	B	AU_RAND A	128bit	Plain text
5	B	A	SRES	32bit	Plain text
6	B	A	AU_RAND B	128bit	Plain text
7	A	B	SRES	32bit	Plain text

Penyerang dapat menggunakan algoritma *brute force attack* untuk menemukan PIN. Caranya dengan melakukan enumerasi PIN. Mengetahui IN_RAND dan BD_ADDR penyerang menggunakan E0 dan menebak PIN untuk mencari K_{init} . K_{init} hipotesis dapat digunakan untuk kunci inisialisasi untuk mendekode pesan 2 dan 3, pesan 2 dan 3 mengandung sejumlah informasi untuk mengkalkulasi kunci A dan B / K_{ab} . Hipotesis dari dapat dites kebenarannya menggunakan 4 pesan berikutnya (4-7). Serangan ini diulang sampai PIN dapat diperoleh. Serangan ini dapat berjalan baik untuk PIN dengan panjang maksimal 64bit, jika lebih panjang memungkinkan terjadinya kadidat PIN lebih dari 1. Untuk lebih jelas dapt dilihat pada gambar 3.



Gambar 3 PIN *Cracking Attack*

Pada uji coba yang dilakukan dengan computer Pentium IV 3 GHz, waktu yang diperlukan untuk memecahkan PIN sebagai berikut :

Tabel 2 Waktu Pencarian PIN *Base Algorithm*

Panjang(digit)	Waktu(detik)
4	1.15
5	11.37
6	113.53
7	1134.87

Pada perkemabangannya Yaniv Shaked and Avishai Wool membuat versi-versi perbaikan algoritma lebih baik dari algoritma dasar seperti manipulasi aljabar, PHT Lookup Table, ataupun As-Is yang dapat meningkatkan waktu komputasi hingga mencapai 0.063 detik untuk panjang PIN 4 digit.

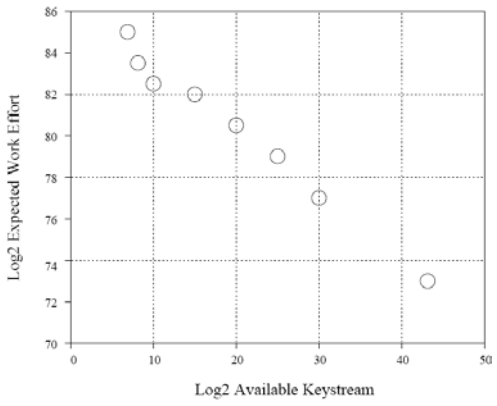
2.2 Attack Against Full E0

Serangan ini dikemukakan oleh Scott R. Fluhrer and Stefan Lucks. Serangan ini termasuk pada *Linear Consistency Attack* yang telah lebih dulu dikemukakan pada tahun 1989 oleh Zeng, Yang, and Rao[2]. Serangan ini didasarkan pada sejumlah keystream keluaran yang dapat merupakan suatu paket atau paket yang berbeda. Serangan ini berusaha untuk menerka 3 LSFR yang terkecil (1, 2, dan 3) dan FSM dari blander dan menggunakan bersama dengan keystream keluaran tersebut apaha output dari LFSR4 konsisten dengan asumsi. Serangan ini merupakan kombinasi dari sejumlha serangan yang sifatnya lebih khusus seperti *Base Attack*, *Attack on the Second Level* E0 *Keystream Generator*, *Attack on the First Level* E0 *Keystream Generator*, dan lainnya

Pada sejumlah keystream keluaran yang kita ketahui kita dapat memilih n tertentu. Kemudian dengan Serangan pada pembangkit kunci aliran tingkat 2 kita dapat menemukan LSFR1 dan blander FSM, lalu kita dapat menerka kunci K'c yang kemudian dapat dijadikan bahan untuk mencari kunci yang benar dengan mendekripsikan paket lain. Kompleksitas yang dibutuhkan untuk melakukan serangan ini dirumuskan dengan :

$$O(\min(F(n) + 2^{81};\ 2F(n=2) + 2^{51}))$$

Pada percobaan yang dilakukan oleh Scott R. Fluhrer and Stefan Lucks, penulis peroleh kesimpulan bahwa semakin banyak keystrem yang diketahui semakin kecil kompeksitas serangan ini.



2.3 Conditional Correlation Attack

Serangan ini dikemukakan oleh Yi Lu, Willi Meier, dan Serge Vaudenay. Sebelumya R. Anderson telah memulai ide tentang serangan terhubung terkondisi (Conditional Correlation Attack) dan pembangkit kunci tidak linear[4,5]. Kemudian notasi CCA diformulasikan oleh Lee dkk. Prinsip dasar dari CCA adalah keterhubungan linear dari input dikondisikan pada pola output dari fungsi tidak linear.

Dari percobaan yang dilakukan dengan computer Pentium 2.4 Ghz 2 GB RAM berhasil dipecahakn 30 kasus dalam waktu 19 jam dan semua nya benar.

Selain tiga serangan yang telah dituliskan, sebenarnya banyak serangan lain yang menimpa E0 seperti Serangan tebakan (*Guessing Attack*), Serangan aljabar, *A time-spaces trade of attack*, *Correlation Attack, Level Attack* dan sebagainya.

Dari sejumlah kripanalisis yang mencoba membuat serangan ke algoritma E0 dapat kita bagi menjadi 2 kelompok :

a. Kelompok petama adalah kelompok dengan serangan aliran kunci yang panjang, kelompok ini mempertimbangkan operasional Bluetooth pada kehidupan nyata. Mereka membutuhkan aliran kunci yang cukup panjang untuk melakukan serangan efektif. Kebanyakan bersifat korelasi atau korelasi cepat, yang mengeksploitasi keterhubungan keluaran LFSR dengan keluaran putaran[1,3]. Berikut sejumlah serangan yang termasuk kelompok ini.

Tabel 3 Kelompok *Long Keystream*

Attack	Data	PreComp	Compl x	Memor y
Fluhrer - Lucks	2^{43}	-	2^{73}	2^{51}
Fluhrer	$2^{12.4}$	2^{80}	2^{65}	2^{80}
Golic & al	2^{17}	2^{80}	2^{70}	2^{80}
Armknecht - Krause	2^{24}	-	2^{68}	2^{48}
Courtois	2^{24}	-	2^{49}	2^{37}
Lu & Vaudenay	$2^{39.6}$	-	2^{40}	2^{35}
Lu & al	$2^{28.4}$	2^{38}	2^{38}	2^{33}

b. Kelompok kedua adalah kelompok dengan serangan aliran kunci yang pendek. Umumnya panjang aliran kunci yang dibutuhkan hanya 128 bit. Walaupun kompleksitasnya masih tergolong tinggi, serangan kelompok ini dinilai lebih realistis[1,3]. Contoh prinsip serangan ini ; *Binary Decision Diagrams, Backtracking Methods* .

Attack	Keystr Len	Complx
Bleichenbacher	128	2^{100}
Krause	128	2^{81}
Levy - Wool	128	2^{86}

3. ANALISIS DAN PERBAIKAN

Kebutuhan terhadap keamanan komunikasi via Bluetooth memang masih rendah . Namun mungkin suatu saat akan berubah. Algoritma E0 dinilai sudah cukup baik karena memperhitungkan efisiensi dan performansi komunikasi. Sebagian besar keamanan Bluetooth yang perlu diperbaiki menurut penulis adalah bukan pada algoritmanya melainkan protokol keamanan komunikasi Bluetoothnya .

Berdasarkan pembahasan sebelumya, penulis menganalisis sejumlah hal mengapa terjadi banyak serangan ke algoritma E0:

a. Adanya keterhubungan yang cukup jelas antara LFSR untuk enkripsi dan LFSR untuk iterasi berikutnya merupkan hal yang sering diekploitasi pada serangan-serangan terhadap E0
b. Proses pairing antara dua device Bluetooth memungkinkan terjadinya eavesdropped dan MITM attack, dan pairing mempertukarkan data random yang cukup penting untuk enkripsi
c. E0 dirancang untuk data yang tingkat sekuritasnya tidak begitu tinggi dan harus memperhatikan dengan baik hal efisiensi
d. Pertukaran RAND pada protokol Bluetooth memberikan kemampuan untuk menganalisis data dan keystrem dengan lebih baik.
e. Kebiasaan pengguna menggunkan pin yang ukuranya pendek juga memudahkan serangan ke E0

Perbaikan yang penulis usulkan terhadap E0 juga enkripsi pada Bluetooth:

a. Algoritma di ubah dengan tidak memakai RAND yang dipertukarkan setiap saat melainkan fungsi random yang sudah di buat sendiri atau kunci dinamik yang selalu berubah ubah secara periodik sesuai iterasi. Pembangkitan kunci dinamik dapat diberikan dengan operan tertentu yang disisipkan pada ciphertext hasil. Solusi ini mengambil sebahagian dari AES yang merupakan kunci ekspansi[7].
b. Dengan tidak adanya pairing dan pertukaran RAND maka digantikan dengan protokol standar komunikasi dan handshaking biasa.
c. Perlunya menggunakan PIN yang cukup panjang untuk sulit di tebak

4. KESIMPULAN

Algoritma E0 merupakan stream cipher yang dirancang dengan tingkat keamanan yang tidak begitu tinggi. Sejumlah serangan terhadap algoritma E0 memungkinkan perbaikan algoritma, namun aspek efisiensi dan performansi masih peru diperhatikan. Aspek ini sulit untuk di coba karena harus mengimpplementasikan langsu ng pada perangkat keras.

DAFTAR REFERENSI

[1] Filiol E. 2006. *Zero-knowledge-like Proof of Cryptanalysis of Bluetooth Encryption (extended version).* Tel Aviv University. Israel.

[2] Fluhrer S. dan Lucks S.2001. *Analysis of the E0 Encryption System Selected Areas in Cryptography - SAC 2001*.Universitas Mannheim. Jerman

[3] Levy O. dan Wool A. 2005. *A Uniform Framework for Cryptanalysis of the Bluetooth E0 Cipher*. http://eprint.iacr.org/2005/107.pdf, Diakses pada 27 September 2007

[4] Lu, Yi., Meier W. dan Vaudenay S. 2005.*The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption*. Santa Barbara.

[5] Lu, Yi dan Serge Vaudenay. Cryptanalysis of Bluetooth Keystream Generator *Two-level E0*. http://lasecwww.epfl.ch, Diakses 27 September 2007

[6] Mavrogiannopoulos, Nikos. 16 Desember, 2005. On Bluetooth™security.

[7] Munir, Rinaldi. Agustus, 2006. *Kriptografi*. Bandung

[8] Shaked, Y and A. Wool. 2005 .*Cracking the Bluetooth PIN,. In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications,and Services (MobiSys)*. Settle. USA.

[9] Winata, Ali. 2002. *Sistem Keamanan Pada Bluetooth*. Institut Teknologi Bandung. Bandung