SIMULASI SISTEM KEAMANAN JARINGAN WiMAX

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat untuk Menyelesaikan Program Strata I
Pada Jurusan Teknik Elektro Fakultas Teknik Universitas Andalas

OLEH :

BERLIAN PUTRA
NIM. 05 175 092

PEMBIMBING I:

DR. Eng. RAHMADI KURNIA
NIP. 19690820 199703 1002

PEMBIMBING II:

HASDI PUTRA, ST
NIP. 19830727 200812 1003

JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS ANDALAS
PADANG

2010

ABSTRAK

Standar 802.16 dikembangkan oleh Institute of Electrical and Electronics Engineers (IEEE), memberikan perspektif baru dalam mengakses data dengan kecepatan tinggi tanpa tergantung pada jaringan kabel atau modem. Tahun 2002 terbentuk forum Worldwide Interoperability for Microwave Access (WiMAX) yang mengacu pada standar 802.16 dan bertugas menginterkoneksikan berbagai standar teknis yang bersifat global menjadi satu kesatuan. Kecepatan koneksi atau kemajuan teknologi yang baru bukan hanya aspek yang penting yang harus dievaluasi, tetapi keduanya merupakan fakta transmisi wireless yang tidak aman untuk berkomunikasi. Aspek keamanan merupakan hal yang sangat penting untuk teknologi broadband dalam mengakses data.

Dalam tugas akhir ini dibahas tentang simulasi sistem keamanan jaringan WiMAX, fitur-fitur yang ada pada sistem keamanan WiMAX berdasarkan pada spesifikasi standar 802.16. Teknologi WiMAX merupakan solusi untuk kota atau daerah pedesaan yang belum berkembang dalam penyediaan akses data. Enkripsi data yang digunakan berupa Digital Encryption Standart (DES), dan Advance Encryption Standart (AES). Proses Authorization pada setiap Subscriber Station (SS) yang sangat baik dengan sertifikat X.509 yang unik, handal dan dapat dipercaya ketangguhannya. Serta proses pertukaran Traffic Encryption Key (TEK) yang sangat rahasia menjadi unggulan dalam sistem keamanannya.

Tugas akhir ini menitikberatkan pada pembuatan simulasi WiMAX menggunakan perangkat lunak. Untuk mencapai tujuan tersebut, dilakukan perancangan mekanisme keamanan jaringannya. Di dalam simulasi ini ditampilkan sebuah base station dan dua buah subscriber station yang melakukan komunikasi data. Kemudian dilakukan proses pengujian keamanan jaringan WiMAX. WiMAX dapat melaksanakan sistem keamanan jaringan dengan baik. Akan tetapi terdapat beberapa kelemahan diantaranya adalah ketiadaan pengesahan timbal balik, manajemen pesan tidak dienkripsi, eavesdropping, Man-In-The-Midle.

Kata Kunci *: IEEE 802.16 (WiMAX), Subscriber Station (SS), Base Station (BS), DES, AES, Authorization, dan TEK.*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem keamanan pada suatu jaringan menjadi salah satu hal penting dalam sebuah sistem informasi. Keamanan jaringan biasanya tidak terlalu diperhatikan oleh pemilik sistem informasi ataupun pengelolanya. Keamanan jaringan biasanya menjadi prioritas terakhir untuk diperhatikan, bahkan sekalipun terjadi penurunan kemampuan kerja komputer. Jika hal tersebut terjadi, pemilik pada umumnya akan mengurangi aspek keamanan atau bahkan aspek keamanan akan ditiadakan untuk tujuan mengurangi beban kerja komputer. Sebagai konsekuensi peniadaan sistem keamanan maka kemungkinan informasi penting dan rahasia dapat diketahui oleh pihak lain. Hal buruk lain yang dapat terjadi misalnya informasi penting tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeruk keuntungan sendiri bahkan dapat merusak kinerja pemilik informasi. Kejahatan seperti itu biasanya dilakukan langsung terhadap sistem keamanan yang bersifat fisik, sistem keamanan yang berhubungan dengan personal, keamanan data, dan media serta teknik komunikasi dan keamanan operasi.

Sistem komunikasi nirkabel generasi keempat atau sering disingkat 4G adalah hasil pengembangan generasi ketiga (3G). Sistem ini disebut dengan nama sistem akses nirkabel berkecepatan tinggi atau broadband wireless access (BWA) yang berbasis WiMAX. Tujuan jaringan komunikasi 4G yakni untuk menyediakan seperangkat standar tertentu yang dapat memenuhi kebutuhan aplikasi – aplikasi nirkabel cukup luas variasinya serta untuk menyediakan akses

secara global. Sistem komunikasi nirkabel membutuhkan implementasi sistem keamanan yang sesuai dengan ciri dan arsitektur masing-masing.

Sistem WiMAX dirancang dengan suatu tampilan menuju sebuah keadaan keamanan tingkat tinggi, yang mana didukung oleh teknik *encryption* dan skema *authentication* [*Mobile Broadcasting with WiMAX*:19]. Ini merupakan hal yang penting dari sebuah sistem keamanan jaringan. Pentingnya dari standard IEEE 802.16 WiMAX adalah pertumbuhan dan akan bersaing dengan teknologi seperti UMTS. Meskipun demikian, penerimaan dan penggunaan dari teknologi dan penyedia juga bergantung pada keamanan. Fitur dasar keamanan WiMAX itu sendiri adalah berdasarkan dari arsitektur keamanan WiMAX, beberapa kelemahan dari jaringannya, potensi serangan seperti penyadapan [*WiMAX Security Architecture – Analysis and Assessment*:1:September/2007].

Seorang penyerang bisa memperoleh pesan TEK dan mengulang pesannya untuk keuntungan informasi dibutuhkan pada membuka dekripsi data. Untuk mengatasinya, digunakanlah teknik *encryption* yang kuat. Sebelumnya digunakan metode *authentication*, agar informasi yang dikirimkan sesuai dengan *subscribe station* yang ditujukan [*WiMAX Security Architecture – Analysis and Assessment*:1:September/2007]. Berdasarkan penelitian yang telah dilakukan sebelumnya, maka penulis akan membuat **Simulasi Sistem Keamanan Jaringan WiMAX**.

1.2 Perumusan Masalah

Sistem keamanan jaringan merupakan suatu metode yang digunakan untuk mengatasi masalah keamanan jaringan pada saat pengiriman data, agar data yang

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dalam tugas akhir ini, dapat disimpulkanm beberapa hal sebagai berikut :

1. Sistem kemananan jaringan WiMAX menggunakan tiga mekanisme yaitu *authorization*, pertukaran TEK, dan *data encryption*. Dengan mekanisme tersebut WiMAX dapat melaksanakan keamanan data SS dengan baik.
2. Algoritma enkripsi yang digunakan pada sistem keamanan jaringan WiMAX adalah *Triple* DES dan AES mode CTR. SS (B) dapat membuka enkripsi data yang dikirimkan SS (A) sama dengan data aslinya setelah memperoleh izin dari BS,
3. Pada proses pengujian, algoritma *brute force* tidak dapat membuka enkripsi data SS (A), hal ini membuktikan bahwa tingkat kemanan dari WiMAX sangatlah baik. Algoritma *brute force* merupakan algortima yang umum digunakan dalam menyerang keamanan jaringan GSM.
4. Pada proses pengujian menggunakan metode *dictionary attack*, *dictionary attack* tidak dapat membuka enkripsi data. Hal ini dikarenakan dari 1000 kombinasi kunci yang digunakan tidak sesuai dengan kunci pada enkripsi data.

DAFTAR PUSTAKA

[1] Advanced Encryption Standardriz. http://r12k4.files.wordpress.com/2008/01/advanced-encryption-standardriz.doc (diakses 19 Agustus 2009 : 22.17 WIB).

[2] Ahson Syed, and Ilyas Mohammad. 2008. "WiMAX Standards and Security".Taylor & Francis Group; London.

[3] Ahson Syed, and Ilyas Mohammad. 2008. "WiMAX Technologies, Performance Analysis, and QoS".Taylor & Francis Group; London.

[4] Algoritma *Brute Force*. http://mufidnilmada.staff.gunadarma.ac.id/Downloads/files/9707/Algoritma+Brute+Force+Bagian+1.ppt (diakses 21 Desember 2009 : 10.13 WIB).

[5] Algoritma DES. http://images.rahmanmillenium.multiply.com/attachment/0/R0KgwwoKCjwAAEkqLcc1/Mengenal%20Algoritma%20DES.PDF (diakses 09 Januari 2010 : 13.37 WIB).

[6] Bagus Eko Prasetyo Indra. 2006. "Simulasi Jaringan Wireless GSM Berbasis Perangkat Lunak". Jurusan Teknik Telekomunikasi – Politeknik Elektronika Negeri Surabaya; Surabaya.

[7] Divisi Litbang LPKBM Madcoms. 2005. "Panduan Pemrograman dan Referensi Kamus Visual Basic 6.0". ANDI; Yogyakarta.

[8] Eren Evren. 2007. "WiMAX Security Architecture – Analysis and Assessment". University of Applied Sciences Dortmund; Germany.

[9] Erickson Jon. 2003. "Hacking – The Art of Exploitation". No Starch Press; San Francisco.