MODEL CHECKING TIMED AUTOMATA PADA PROSES AUTHENTIKASI SECURITY PROTOCOL PADA JARINGAN BERBASIS NIRKABEL

Muhammad Reza Mardiansyah[1], Bayu Erfianto[2], Tri Brotoharsono[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Protokol authentikasi EAP MD5 dan EAP TLS adalah protokol keamanan yang masih sering dijumpai pengunaannya saat ini. Protokol Keamanan tersebut menggunakan proses authentikasi pada jaringan nirkabel dengan menggunakan IEEE 802.1x sebagai media transmisinya. Terdapat 3 komponen yang berperan pada IEEE 802.1x yaitu suplican , authenticator dan authentication server. Ketiga komponen inilah yang akan dimodelkan dengan menggunakan timed automata untuk melihat kondisi yang terjadi jika dilakukan serangan dengan menggunakan man in the middle attack dan dilakukan penambahan aspek waktu pada protokol tersebut. Salah satu bentuk pengecekan terhadap model adalah dengan menggunakan timed automata. Timed Automata adalah finate automata klasik yang dapat memanipulasi waktu, berkembang terus menerus dan mensinkonisasikan dengan waktu mutlak[2]. Tugas akhir ini mengkhususkan diri pada proses memodelkan protokol authentikasi EAP MD5 dan EAP TLS dengan menggunakan Timed Automata dengan menambahkan kemungkinan retransmisi berdasarkan aspek waktu. Setelah model selesai maka berikutnya dilakukan pengecekan terhadap model berdasarkan aturan yang ada apakah dapat berjalan sesuai dengan aturan tersebut. Dari hasil verfikasi model tersebut dengan menggunakan alat UPPAAL maka dapat dilihat bahwasannya protokol authentikasi EAP MD5 dan EAP TLS dapat dimodelkan dengan menggunakan timed automata dan sesuai dengan aturan yang terdapat pada RFC protokol tersebut.

Kata Kunci : EAP MD5, EAP TLS, Timed Automata, UPPAAL

Abstract

Authentication protocols EAP MD5 and EAP TLS are security protocols that are still frequently encountered use today. This Security Protocol using the process of authentication on a wireless network using the IEEE 802.1x as the transmission medium. There are three components that use a role in the IEEE 802.1x are suplican, authenticator and authentication server. These three components will be modeled using timed automata to see the condition that occurs when an attack carried out by using the man in the middle attack and carried out additional aspects of the time in the protocol. One form of model checking is use timed automata. Timed automata are classic finate automata that can manipulate time, developing continuously and synchronously with the absolute time [2]. This final project focuses on the modeling process authentication protocols EAP MD5 and EAP TLS using Timed Automata with the added possibility of retransmission based on the aspect of time. Once completed, the next model to be checked against an existing model based on whether the rules can be run in accordance with these rules. From the results verify the model using UPPAAL tool, it can be seen authentication protocols EAP MD5 and EAP TLS can be modeled using timed automata, and in accordance with the rules contained in the RFC protocol.

Keywords : EAP MD5, EAP TLS, Timed Automata, UPPAAL

BAB I
Pendahuluan

1.1 Latar belakang

Perkembangan perangkat keras maupun perangkat lunak pada saat ini sangat berkembang dengan pesat begitu pula dengan perkembangan keamanan dari suatu jaringan komputer terutama yang berbasis nirkabel. Oleh karena itu diperlukan suatu kiat-kiat khusus untuk mengantisipasi seluruh perkembangan tersebut agar dapat menjadi nilai tambah bagi perkembangannya. Pentingnya untuk memodelkan suatu permasalahan menjadi bentuk yang lebih sederhana dan dapat bersifat handal menjadi dasar ketertarikan terhadap pemilihan judul tersebut.

Keamanan sering dipandang hanyalah merupakan masalah teknis yang melibatkan dapat atau tidaknya tertembusnya suatu sistem. Pada pandangan makro keamanan sendiri memiliki konsep yang lebih luas, yang berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya. Di dalam aplikasinya suatu pembentukan sistem yang aman akan mencoba melindungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain terhadap kita tetapi tidak memperdulikan aspek informasi waktu. Informasi waktu memungkinkan kita untuk mempelajari perbedaan dari skenario penyerangan[1]. Penambahan Informasi waktu sebagai syarat dari setiap transaksi dalam proses authentikasi menjadi ide dari pengerjaan tugas akhir ini.

Kondisi saat ini dalam menunjang aspek waktu di protocol keamanan sudah dilakukan namun sedikit berbeda dengan apa yang ingin diusulkan. Delzano et.al memperkenalkan prosedur *automatic* untuk memverifikasi protocol menggunakan *timestamps*[1]. Evans dan Scheneider memperkenalkan *framework* untuk waktu analysis[1]. Dan masih banyak lagi solusi-solusi yang ditawarkan pada saat ini.

Proses authentikasi pada jaringan nirkabel 802.1x memiliki 3 komponen yaitu supplicant yang terdapat pada *station*, autheticator yang merupakan *access point*, dan authetication server[3][7]. Terdapat 2 protocol yang digunakan dalam proses authentikasi tersebut yaitu EAP protocol yang menghubungkan supplicant dan autheticator dan Radius protocol yang menghubungkan autheticator dengan authetication server.

Metode formal adalah bahasa dan teknik berbasis matematika yang digunakan untuk menspesifikasi, mengimplementasi, dan memvalidasi serta memverifikasi baik perangkat lunak maupun perangkat keras[5]. Proses desain dimulai dari sebuah spesifikasi dari sistem yang akan dibuat. Sebuah spesifikasi dapat diterjemahkan menjadi beberapa implementasi. Setelah implementasi selesai maka tugas seorang desainer adalah menguji dan menjamin kebenaran dari implementasi. Proses pengujian dengan menggunakan simulasi dan sampel dari data disebut sebagai validasi.

Sementara itu proses verifikasi adalah membuktikan bahwa implementasi memang mengimplementasikan spesifikasi[5].

Tujuan dari formal verifikasi adalah membuktikan bahwa sebuah implementasi dapat mengimplementasikan apa yang dijabarkan pada spesifikasinya. Formal verifikasi dapat dilakukan dengan menggunakan *equivalent checker*, *model checker* dan *therem prover*. Dengan menggunakan model checker dibutuhkan suatu metode untuk teknik dari authentikasi *security* protocol yang mempertimbangkan isu waktu seperti timeout dan retransmisi. Metode yang berdasarkan dari model authentikasi security protocol menggunakan timed automata yang dipelajari dengan melihat perspektif dari teori bahasa formal.

1.2 Perumusan masalah

Dengan melihat pada latar belakang di atas, permasalahan yang akan dijabarkan dan diteliti adalah:

1. Bagaimana memodelkan proses authentikasi pada security protocol dengan menggunakan timed automata
2. Bagaimana hasil verifikasi yang dihasilkan dalam pengujian terhadap model timed automata tersebut

Adapun batasan masalah tugas akhir ini adalah sebagai berikut :

1. Hanya melakukan pemodelan pada proses authentikasi protocol EAP MD5 dan EAP TLS
2. Jaringan yang digunakan adalah jaringan nirkabel 802.1x untuk terhubung ke radius server
3. Menggunakan tools Uppaal 4.0.10 untuk memverifikasi model timed automata
4. Mengunakan nilai waktu RTT EAP berdasarkan retransmisi EAP pada IKEv2.
5. Proses transaksi yang melewati dari timeout yang mengakibatkan retransmisi diasumsikan terdapat intruder walaupun bisa berarti itu terjadi karena signal loss atau ada yang meninggalkan komunicasi.

1.3 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan Tugas Akhir ini adalah sebagai berikut:

1. Memodelkan proses authentikasi pada security protocol dengan menggunakan timed automata pada jaringan berbasis nirkabel.
2. Melakukan verifikasi proses authentikasi pada security protocol dengan model checking menggunakan timed automata pada jaringan berbasis nirkabel.

1.4 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam memecahkan masalah di atas adalah dengan menggunakan langkah-langkah berikut:

1. Identifikasi masalah

   Proses pertama kali yang dilakukan dalam penyelesaian tugas akhir ini adalah melakukan identifikasi permasalahan-permasalahan yang didapati dalam proses authentikasi pada protocol security saat ini dan dibandingan dengan solusi yang ada saat ini.

   Permasalahan yang dihadapi saat ini adalah belum digunakannya nilai waktu dalam pemodelan proses authentikasi dari suplican ke suatu radius server. Keuntungan yang dapat diperoleh dengan mempertimbangkan aspek waktu dalam proses pemodelan adalah kita dapat membedakan skenario dari penyerangan yang terjadi sehingga dengan mudah kita mempelajari dan memahami proses penyerangan yang dilakukan[1].

2. Literature Review

   a. Pencarian referensi dan sumber-sumber yang berhubungan dengan keamanan sistem, protocol authentikasi pada jaringan nirkabel dan timed automata.

   b. Mempelajari dan memahami model checking dengan menggunakan Uppaal 4.0.10

   c. Pencarian referensi dan sumber-sumber yang berhubungan model checking pada proses authentikasi security protocol menggunakan radius server

3. Methodological design

   Tahapan-tahapan yang dilakukan dalam methodological design adalah

   a. Menentukan model authentikasi

      Dalam proses pembangunan model authentikasi pada jaringan nirkabel digunakan 2 protocol yaitu EAP dan Radius. EAP yang digunakan EAP-MD5 dan EAP TLS yaitu protocol authentikasi antara supplicant dan autheticator. Memilih EAP-MD5 dan EAP TLS dikarenakan kedua protocol ini sering digunakan dalam proses authentikasi dijaringan nirkabel. Radius adalah protocol authentikasi antara autheticator dan authetication server.

   b. Membangun model authentikasi menggunakan time automata

      Setelah model authentikasi terbentuk maka berikutnya dilakukan proses penambahan timed automata dalam model authentikasi tersebut. Metode timed automata dipilih dikarena memiliki beberapa fitur. Pertama metode ini memerlukan desainer untuk memberikan rincian spesifikasi protocol yang tepat dan relatif untuk membantu agar tidak terjadi ambiguitas dari behavior protocol. Kedua nilai waktu seperti timeouts perlu diletakan pada setiap state, sementara retransmissions dapat dengan mudah ditetapkan sebagai transisi untuk protocol state lainnya

c. Menentukan scenario attack

Scenario attack yang digunakan adalah man in the middle (MITM) attack. MITM attack adalah keadaan dimana seorang pengguna network dapat berada diantara 2 user yang sedang berkomunikasi sedemikian rupa sehingga mampu menirukan kedua belah pihak dan akhirnya mendapatkan koneksi pada keduanya.

d. Memodelkan proses authentikasi di Uppaal

Tools yang digunakan untuk memodelkan proses authentikasi tersebut adalah Uppaal. Uppaal adalah tool untuk mensimulasikan, men-debug dan menverifikasi security protocol terhadap classical safety dan authentikasi di real-time scenario menggunakan reachability properties

e. Menentukan properti

Properti yang telah ditentukan nantinya akan digunakan untuk menguji model yang telah diskenariokan di Uppaal. Diharapkan properti skenario tersebut dapat mewakilkan dan skenario-skenario yang dapat ditemukan untuk menguji kehandalan dari model tersebut

f. Verifikasi

Verifikasi adalah proses akhir yang dilakukan untuk mengetahui kehandalan dari model tersebut dalam menghadapi serangan MITM.

4. Analisis

Proses menyeluruh terhadap pengerjaan dan hasil keluar dari tugas akhir ini.

5. Pembuatan laporan Tugas Akhir

BAB V
Penutup

5.1 Kesimpulan

Beberapa kesimpulan yang diperoleh dari tugas akhir ini adalah sebagai berikut:

1. Protokol Authentikasi EAP MD5 dan EAP TLS dapat dimodelkan dengan menggunakan Timed Automata dikarenakan dapat menangani proses authentikasi jika waktu proses authentikasi tersebut lebih kecil dari timeout.
2. Penambahan unsur waktu dalam proses authentikasi dapat meningkatkan kehandalan dari protokol tersebut dalam menghadapi serangan.
3. Pemodelan dengan menggunakan Timed Automata mampu menunjukkan proses dari authentikasi protokol tanpa mengurangi aturan baku dari proses protokol tersebut.
4. Seluruh kondisi retransmisi yang terdapat pada EAP MD5 ataupun EAP TLS dapat dimodelkan pada Timed Automata

5.2 Saran

Beberapa saran yang diusulkan pada tugas akhir ini adalah sebagai berikut:

1. Nilai waktu dari timeout harus dapat ditentukan bakunya dalam kondisi apaanpun sebagai acuan dari permodelan
2. Dengan menggunakan nilai probabilitas dapat dilihat nilai waktu yang tepat untuk proses authentikasi.
3. Pengecekan pesan yang diinputkan dapat menjadi pertimbangan bagi server dalam menetukan kodisi pada model timed automata

Referensi

[1] Alur, Rajeev dan Dill, David L. A Theory of Timed Automata. Stanford: Stanford University.

[2] Arifin , Zainal. 2008. Sistem Pengamanan Jaringan Wireless berbasis protokol 802.1x dan sertifikat. Yogyakarta : Andi Offset.

[3] Behrmann, Gerd, dkk.2004. A Tutorial on Uppaal. Denmark: Aalborg University.

[4] Corin, R , dkk. 2004. Timed Model Checking of Security Protocols. Netherlands: University of Twente.

[5] Fuad , Reza. Standar IEEE 802.1x Teori dan Implementasi. Semarang : Institut Teknologi Sepuluh November.

[6] http://en.wikipedia.org/wiki/Man-in-the-middle_attack diakses tanggal 25 Mei 2010 jam 20.25

[7] http://en.wikipedia.org/wiki/IEEE_802.1X diakses tanggal 25 Mei 2010 jam 20.25

[8] IEEE.2004. IEEE standar for local and metropolitan area networl Port-Based Network Access Control.

[9] Rahardjo, Budi. 2005. Pengantar Metode Formal. Bandung: Institut Teknologi Bandung.

[10] RFC 3748. 2004. Extensible Authetication Protocol (EAP).

[11] RFC 5216. 2008. The EAP-TLS Authetication Protocol.

[12] Setiawan, Agung W.2005. Remote Authentication Dial in User Service (RADIUS) untuk Authentikasi Pengguna Nirkabel LAN. Bandung:Institut Tekhnologi Bandung.

[13] Thomas , Tom . 2004. Network Security First-Step. Person Education : Andi Offset.