ANALISIS DAN PERBANDINGAN KEAMANAN JARINGAN PADA MEKANISME AUTENTIKASI MENGGUNAKAN KERBEROS DAN HTTP OVER SSL

Fajar Andrianto[1], Fazmah Arief Yulianto[2], Niken Dwi Wahyu Cahyani[3]

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

Abstrak

Perkembangan teknologi yang semakin maju mengakibatkan tingkat kebutuhan terhadap keamanan informasi menjadi penting. Seiring berkembangnya informasi munculah permasalahan baru mengenai keamanan jaringan, contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut sniffing, selain ancaman pengendusan juga terdapat ancaman lainnya seperti MITM attack (man in the middle) yang memungkinkan attacker berada di tengah komunikasi bebas mendengarkan atau mengubah percakapan antara dua pihak.

Kerberos merupakan suatu protocol autentikasi jaringan yang dirancang untuk memberikan autentikasi yang kuat, Kerberos memungkinkan client dan server untuk saling mengotentikasi sebelum melakukan koneksi [8]. Sedangkan HTTP over SSL atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin [9].

Melalui tugas akhir ini dilakukan analisis dan perbandingan keamanan jaringan pada mekanisme autentikasi menggunakan kerberos dan HTTP over SSL. Masing-masing mekanisme autentikasi diuji menggunakan serangan sniffing dan MITM attack. Sehingga kita dapat mengetahui bagaimana perbandingan keamanan autentikasi dalam hal ini adalah ancaman serangan dari penggunaan kerberos dan HTTP over SSL sebagai protokol autentikasi.

Dari hasil pengujian yang dilakukan didapatkan bahwa kerberos dan HTTP over SSL relative masih rentan terhadap serangan menggunakan tools tertentu, baik kerberos maupun HTTP over SSL masih terdapat celah keamanan yang masih mungkin dimanfaatkan oleh para attacker.

Kata Kunci : kerberos, HTTP over SSL, sniffing, MITM attack

Abstract

The increasing development of advanced technologies has made security of information very essential. New problems on network security emerge as the growth of information itself. One of those threats is sniffing which tracks down user activities on networks. The other one is “man in the middle” (MITM) which illegally permit attacker to intercept in the middle of communication so they can freely listen or change the conversation between two parties.

Kerberos is a network authentication protocol designed to provide strong authentication. Kerberos allows the client and server to authenticate each other before making a connection [8]. Whilst, HTTP over SSL, which is usually implemented with HTTPS, is an HTTP protocol that uses Secure Socket Layer (SSL) as a sub-layer under the HTTP so it can be much more secure [9].

Through this thesis, an analysis and comparison of network security is performed on the authentication mechanism using Kerberos and HTTP over SSL. Each authentication mechanism was tested using MITM attacks and sniffing attacks. Thus the comparison of security authentication is able to note, in this case is the threat of attacks, from the usage of Kerberos and HTTP over SSL as the authentication protocol.

The test results showed that the Kerberos and HTTP over SSL is relatively vulnerable to attacks using certain tools. Both Kerberos and HTTP over SSL still has security holes that may be exploited by attackers.

Keywords : kerberos, HTTP over SSL, sniffing, MITM attack

1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan teknologi yang semakin maju mengakibatkan tingkat kebutuhan terhadap keamanan informasi menjadi penting. Seiring berkembangnya informasi munculah permasalahan baru mengenai keamanan jaringan itu sendiri. Contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut *sniffing*, serangan ini memungkinkan informasi penting seperti password dari suatu account bisa diketahui oleh hecker, selain ancaman pengendusan juga terdapat ancaman lainnya seperti *MITM* attack (man in the middle) yang memungkinkan attacker berada di tengah komunikasi bebas mendengarkan dan mengubah percakapan antara dua pihak dan masih banyak lagi serangan yang ada. Mulailah berkembang anggapan bahwa internet merupakan tempat yang tidak aman. Banyak protokol yang menggunakan internet tidak memberikan sistem autentikasi yang aman pada sistem informasinya. Beberapa system menggunakan firewall untuk mengatasi masalah keamanan jaringan. Tetapi sayangnya, firewall mengasumsikan bahwa ancaman bahaya berasal dari luar, padahal seringkali pada kenyataannya tidaklah demikian. Ancaman bahaya justru sering datang dari dalam.

Karena hal-hal tersebut di atas, maka diperlukan suatu protokol yang dapat diandalkan dalam autentikasi. Terdapat berbagai macam protokol yang bisa digunakan, tetapi tidak semuanya bisa menahan serangan dari penyusup. Dalam Tugas Akhir ini dibahas dua mekanisme autentikasi menggunakan protokol autentikasi *kerberos* dan penggunaan *HTTP over SSL*, baik kerberos maupun *HTTP over SSL* keduanya memiliki kelebihan masing-masing dalam autentikasi dan dari segi keamanan jaringan. Kerberos sudah banyak diterapkan dalam sebuah system yang membutuhkan mekanisme autentikasi efektif dan aman dalam pemenuhan banyak layanan di jaringan. *HTTP over SSL* menyediakan autentikasi yang membutuhkan tingkat keamanan yang tinggi seperti yang telah banyak diterapkan di aplikasi web yang membutuhkan transaksi aman dalam operasionalnya. Antara Kerberos dan *HTTP over SSL* bisa digunakan dalam autentikasi client dan server. Dari hal tersebut dibandingkan penggunaan autentikasi yang komplek dan yang sederhana apakah memiliki pengaruh yang signifikan dalam masalah keamanan di jaringan.

Kerberos merupakan suatu protocol autentikasi jaringan yang dirancang untuk memberikan autentikasi yang kuat, *Kerberos* memungkinkan client dan server untuk saling mengotentikasi sebelum melakukan koneksi [8]**.** Sedangkan *HTTP over SSL* atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin [9]. Kedua autentikasi tersebut memiliki kelebihan dan kekurangan masing-masing. Dari analisis segi mekanisme kedua sistem autentikasi tersebut, dapat diduga bahwa kerberos bisa diandalkan untuk menjamin keamanan autentikasi di banding menggunakan *HTTP over SSL*

karena dilihat dari mekanisme kerberos yang menggunakan suatu tiket granting dalam prosesnya.

Pada Tugas Akhir ini di implementasikan dan dibandingkan metode mana yang bisa diandalkan dalam proses autentikasi dari segi ketahanan terhadap serangan dari luar seperti sniffing dan MITM attack dengan kata lain dari segi keamanannya.

1.2 Perumusan Masalah

Rumusan masalah yang ada pada Tugas Akhir ini yaitu sebagai berikut :

- Bagaimana ketahanan terhadap serangan pada protokol *kerberos* dan *HTTP over SSL*.
- Bagaimana hasil perbandingan terhadap serangan pada *kerberos* dan *HTTP over SSL*.

Adapun batasan masalah dari Tugas Akhir ini adalah :

- OS yang digunakan dalam pengujian adalah windows server 2003, windows XP karena OS tersebut telah memenuhi resaurce yang dibutuhkan dalam tahap pengujian.
- Hal yang dianalisis adalah dari segi keamanan autentikasi terhadap serangan sniffing
- Skenario uji serangan yang dipakai menggunakan serangan *MITM* attack (man in the middle), Password Attacks karena serangan tersebut berhubungan dengan mekanisme autentikasi.

1.3 Tujuan

Adapun tujuan yang ada pada Tugas Akhir ini adalah sebagai berikut :

- Menganalisis mekanisme autentikasi dari penggunaan *kerberos* dan *HTTP over SSL* sebagai protokol autentikasi.
- Menganalisis perbandingan keamanan autentikasi dalam hal ini adalah ancaman serangan dari penggunaan *kerberos* dan *HTTP over SSL* sebagai protokol autentikasi.

1.4 Metodologi Penyelesaian Masalah

Metodologi yang akan digunakan dalam menyelesaikan Tugas Akhir ini adalah sebagai berikut :

- Identifikasi
  Kerberos merupakan suatu protocol autentikasi jaringan. Kerberos dirancang untuk memberikan autentikasi yang kuat. Kerberos memungkinkan *client* dan *server* untuk saling mengotentikasi sebelum melakukan koneksi [8]. Beberapa situs menggunakan firewall untuk

mengatasi masalah keamanan jaringan mereka. Tetapi, firewall mengasumsikan bahwa ancaman bahaya berasal dari luar, padahal seringkali pada kenyataannya tidaklah demikian. Ancaman bahaya justru sering datang dari dalam. Kerberos merupakan protokol autentikasi yang bisa diandalkan, kerberos dirancang untuk memberikan autentikasi yang kuat untuk aplikasi client/server dengan menggunakan *secret-key cryptography* [19].

HTTP over SSL atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin. Dengan HTTPS kita dapat melakukan proteksi data yaitu hanya penerima saja yang dapat membaca data, Kenyamanan (data privacy), memungkinkan identifikasi server ataupun client, otentikasi server dan klien, dan integritas data[9]. SSL adalah protokol yang memiliki tingkat keamanan sangat tinggi [13]. Perkembangan Internet yang cukup pesat membawa pengaruh yang cukup besar bagi pihak-pihak yang memanfaatkan internet untuk melakukan berbagai hal misalnya tukar-menukar data, transaksi online, promosi dan lain-lain. Dengan adanya kejahatan-kejahatan internet ini para pengguna semakin tidak aman dan menjadi intaian para penjahat setiap kali mereka berinternet. SSL menyediakan metode enkripsi yang digunakan untuk mengamankan data dengan mengubah data asli kedalam bentuk unicode dengan aturan tertentu.

- Literatur

  Mempelajari literatur-literatur yang berkaitan dengan konsep Autentikasi, kerberos, HTTP over SSL ,sniffing MITM attack (man in the middle), Password Attacks, hacking kemudian melakukan kajian terhadap materi-materi tersebut.

- Desain Penelitian

  Model autentikasi yang diterapkan adalah menggunakan *kerberos* dan *HTTP over SSL*, dimana untuk setiap protokol autentikasi akan dibuat prototype autentikasinya dengan menggunakan satu platform OS yang sama pada saat tahap pengujian.

  Setelah dibuat prototype dari kedua model autentikasi dilakukan serangan untuk kedua model tersebut. Jenis serangan yang dilakukan adalah *sniffing* dengan *MITM attack* dan Password *attacks*. Pemilihan serangan dilakukan untuk menganalisis paket data yang bisa dimanfaatkan untuk masuk dalam sistem. *MITM attack* dan Password *attacks* merupakan serangan yang dilakukan oleh para hacker dalam menyusup sebuah sistem.

  a. *MITM* attack (man in the middle) yang memungkinkan attacker berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Man-In-The-Middle Attack adalah sebuah aksi sniffing yang memanfaatkan kelemahan switch dan kesalahan penangannan ARP chache dan TCP/IP [10]. Awalnya adalah menempatkan komputer hacker ditengah dua komputer yang sedang berhubungan sehingga paket data harus melalui komputer hacker dulu agar paket data itu bisa

dilihat atau diintip oleh hacker. Aplikasi yang digunakan adalah Ettercap, ARPSpoof.

b. Password attacks
Menggunakan teknik brute force dimana serangan dilakukan oleh sebuah aplikasi untuk menyusup pada sistem.

Tujuan dari dilakukan serangan adalah :

a. untuk mengetahui apakah terdapat celah pada sistem keamanan menggunakan kedua protokol tersebut.
b. untuk mengetahui tingkat ketahanan keamanan dari penerapan kedua protokol tersebut terhadap serangan yang dilakukan

- Pengujian

Pengujian yang dilakukan adalah dari segi autentikasi menggunakan kedua model yang ada kemudian dilakukan serangan untuk tiap model sesuai dengan skenario serangan.
Metrik pengujian secara kuantitatif dilakukan dengan banyaknya serangan yang berhasil, kemudian pengujian secara kualitatif dimana informasi apa saja yang didapatkan dari proses sniffing untuk tiap protokol yang diuji. Setelah dilakukan pengujian lakukan analisis sesuai tujuan dari dilakukannya serangan.
Hasil yang diharapkan tercapai adalah :

a. Mengetahui bagaimana ketahanan terhadap serangan pada protokol *kerberos*.
b. Mengetahui bagaimana ketahanan terhadap serangan pada *HTTP over SSL*.

- Analisis

Menganalisis hasil dari pengujian diatas dengan menggunakan sampel pengujian sesuai pada tahap pengujian dengan batasan jumlah serangan attack yang telah ditentukan, kemudian di buat kesimpulan yang ada sesuai dengan tujuan tugas akhir ini.

- Pembuatan Laporan

Mendokumentasikan tahap-tahap yang telah dilakukan pada bagian metodologi ini mulai dari studi literatur sampai analisis hasil testing yang berisi kesimpulan sebagai bahan literatur penelitian.

5. Penutup

5.1 Kesimpulan

Berdasarkan hasil pengujian MITM attack, sniffing dan password attack pada kerberos dan http over SSL maka dapat ditarik kesimpulan sebagai berikut :

1. Kerberos dan http over ssl dalam autentikasi user masih memiliki celah keamanan yang bisa dimanfaatkan oleh attacker guna mendapatkan informasi yang bisa digunakan untuk masuk dalam system. Kedua proses autentikasi menggunakan kerberos dan http over ssl masih bisa diserang menggunakan MITM attack. Pada kerberos celah keamanan yang bisa dimanfaatkan adalah pada saat mekanisme awal user meminta TGT pada AS, pada proses tersebut paket data yang berhasil di sniffing bisa di sniffing menggunakan kerbsniff dan bisa dicrack menggunakan aplikasi kerbcrack. Pada http over ssl celah keamanan yang bisa dimanfaatkan adalah pada saat server mengimkan certifikat yang akan digunakan si client, pada proses tersebut attacker bisa memanipulasi certifikat yang dikirimkan dari server ke client dengan memanfaatkan kelengahan user dalam memvalidasi certifikat yang akan digunakan.

2. Kerberos menyediakan konsep autentikasi yang cukup efektif apabila dilihat dari parameter pengenalan identitas antara client dan server, karena antara client dan server saling mengautentikasi satu sama lain. Sehingga tingkat kepercayaan antara client dan server bisa lebih valid.

3. HTTP over ssl menyediakan konsep autentikasi sederhana dengan pembungkusan informasi dengan ssl yang aman apabila di lihat dari parameter pengendusan informasi paket data melalui jaringan, karena paket data yang ada di jaringan belum bisa di crack untuk mendapatkan informasi yang bisa diguakan untuk menyusup ke system.

4. Kedua mekanisme autentikasi baik kerberos maupun http over ssl memiliki kelebihan dan kekurangan masing-masing, dimana keduanya relative masih rentan terhadap serangan tertentu. Kerberos dari segi mekanisme autentikasi memiliki system yang lebih dibanding menggunakan http over ssl tetapi dari segi pengenkripsian data penggunaan http over ssl lebih bisa diandalkan.

5.2 Saran

1. Menambahkan mekanisme keamanan terhadap kerberos maupun http over ssl dalam penerapannya.

2. Mengintegrasikan kedua mekanisme jika memungkinkan dalam pengimplementasian.

3. Dari segi keamanan jaringan perlu adanya pemahaman terhadap serangan-serangan yang biasa terjadi pada kerberos dan http over ssl.

Daftar pustaka

[1] Anang. *Mengamankan Sistem dengan Kerberos*. 2009, http://www.bestlib.co.cc/2009/07/mengamankan-sistem-dengan kerberos.html.

[2] Anonim. *Kerberos*. 2009, http://lecturer.eepisits.edu/~isbat/materikuliah/security%20lab/kerberos.pdf.

[3] B.C Neuman, T.Ts'o. *Kerberos: An Authentication Service for Computer Networks*. IEEE Communications, 1994.

[4] Brenton, Chris and Cameron Hunt. *Network Security 2nd edition*. SYBEX Inc., 2003.

[5] Chown, P. *Advanced Encryption Standard (AES)*.2002 http://www.ietf.org/rfc/rfc3268.txt

[6] Dedi Dwianto. *Hacking With Basic Command*. 2009, http://lirva32.org/ammar/idsecconf2008/theday-cmdline/theday-commandlinehacking.pdf.

[7] Derek, Konigsberg. *Kerberos The Network Authentication Protocol*, Linux Enthusiasts and Professionals.

[8] Fabrice, KAH. *Understanding Kerberos v5 Authentication Protocol*. 2003.

[9] Ferdian P,Agung kaharesa. *Protocol HTTP dan handshaking client-server untuk berkomunikasi via HTTPS*. 2009, http://te.ugm.ac.id/~risanuri/v01/wpcontent/uploads/2009/06/http%20dan%20handshake%20via%20https%20_32582,32649.pdf.

[10] Forum stikompoltek. *Man in The Middle Attack 1*.2009, http://forum.stikompoltek.ac.id/index.php?sid=6ae03d212741388e52d81c5e10710856.

[11] Graham Cole .Kerberos Security in Windows.

[12] Indonesia .net developer community. *Configuring Kerberos*. 2008, http://netindonesia.net/blogs/si_hendrik/archive/2008/06/03/configuring-kerberos-todo-checklist.aspx.

[13] La Ode Abdul Jumar. *SSH (secure shell) dan SSL (secure socket layer)*.2003, http://www.polibatam.ac.id/~webmaster/print.php?sid=73.

[14] McClure, Stuart and Saumil Shah. *Web Hacking serangan dan pertahananya*. Andi.2003.

[15] Menezes, Alfred J. *Handbook of Applied Cryptography*. CRC Press, 1996.

[16] Munir, Rinaldi. *Kriptografi*. Informatika, 2006.

[17] Putri Cristianti. *Keamanan Sistem Informasi Karberos pada Autentikasi*. 2009, http://putriechristianti.blog.upi.edu/2009/10/19/keamanan-sistem-informasi-kerberos-pada-authentication/ 2003.

[18] Schneier, Bruce. *Aplied Cryptography 2nd*. John Willey & Sons, 1996.

[19] Stallings Williams. *Network And Internetwork Security Principles And Practice*. The Institute of Electrical and Electronics Engineers, Inc., New York. 1995

[20] Stallings Williams. *Cryptography and Network Security*. The Institute of Electrical and Electronics Engineers, Inc., New York. 1996

[21] S'to. *Seni Teknik Hacking 1:Uncensored*. Jasakom. 2004

[22] Surya L, Suhardi. *Mengukur Efektifitas Keamanan Informasi dengan Metrik Keamanan Teknologi Informasi. 2009,* http://www.batan.go.id/sjk/eII2006/Page04/P04h.pdf
[23] Sysneta. *Autentication Methods*. 2008, http://www.sysneta.com/authentication-methods.
[24] Wijaya Hendra ,Ir . *Windows Server 2003 : pedoman persiapan pengambilan sertifikat MCSE ujian nimor 70-290.* Elex Media Komputindo. 2004
[25] Wikipedia. *karberos.*2009, http://id.wikipedia.org/wiki/karberos.
[26] Wikström, Edvard. *Secure Communication: Is it possible with SSL and or SSH?*. 2008, http://www.ida.liu.se/~TDDC03/oldprojects/2004/final-projects/prj022.pdf.
[27] Wildan, Fakhri, Achmad Rony Fauzan, dan Imam Ahmadi. *Penerapan Kriptografi pada Sistem Otentikasi Terpusat Kerberos v5*. 2006 http://www.informatika.org/~rinaldi/Kriptografi/2005-2006/Makalah/Makalah2005-06.pdf.