KAJIAN FUNGSI PROYOKOL RADIUS UNTUK AUTENTIKASI DI JARINGAN OWLAN

Dinny Astuti[1], -[2]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak
tidak tersedia

Kata Kunci :

Abstract
not available

Keywords :

BAB I
PENDAHULUAN

I.1 Latar Belakang Masalah

Internet service provider (ISP) menawarkan akses *dial-up* dan penyediaan jaringan perusahaan untuk mendukung para *telecommuter* menghadapi beberapa tantangan yang sulit. Seiring dengan meningkatnya pelanggan *dial-up* yang bersifat residential dan penyediaan *modem*(atau ISDN port),sehingga memungkinkan bisnis bisa dijalankan dimana saja. Untuk memenuhi permintaan ini, ISP (dial provider) mengembangkan suatu *network access server* yang padat *port* dengan jumlah yang banyak dan kompleks untuk menangani ribuan koneksi *dial-up* individual.

Sementara itu, perangkat kantor utama yang berukuran kecil, seperti komputer laptop dan telepon seluler, digunakan untuk memaksimalkan waktu untuk menciptakan daya kerja yang berkesinambungan tidak terbatas jarak dan waktu. Perangkat-perangkat berjalan ini membutuhkan akses yang aman dan handal untuk mengakses *e-mail* dan *web* dari mana saja di seluruh penjuru dunia. Tetapi para *provider dial-up* harus menawarkan lebih dari sekedar penyediaan port modem di sisi lain dari panggilan telepon. Mereka juga harus menyediakan perlindungan melawan serangan pencurian layanan oleh ketidaktelitian individual dengan *excess free time*; mereka harus memeriksa level otorisasi akses pelanggan; dan untuk biaya *recovery*, billing, dan kepentingan perencanaan sumber daya, mereka membutuhkan penghitung waktu koneksi ke jaringan. Kemudian, untuk menyediakan daerah cakupan maksimum berdasarkan pelanggan mobile dan pertumbuhan roaming, mereka harus memilih untuk menyatukan sumber daya NAS mereka sementara menahan kendali melalui akses pelanggan mereka, penggunaan, dan informasi *billing*. Semua layanan ini mensyaratkan kordinasi antara system administrasi yang bermacam-macam yang didukung oleh antar provider dial-up.

Untuk memenuhi semua tantangan diatas dalam suatu aturan yang sederhana dan berskala,semua itu ada pada *Authentication, Authorization,* dan *Accounting* (AAA). Pada intinya, AAA merupakan suatu gambaran kerja untuk

mengkordinasikan disiplin individual dengan teknologi jaringan yang jamak dan *platform* yang berbeda. Praktisnya, suatu server AAA dengan database dari profile pengguna dan data konfigurasi berhubungan dengan *client* AAA yang berada pada komponen jaringan, seperti NAS dan *router*, untuk menyediakan penyebaran layanan AAA. Layanan yang disediakan oleh *framework* AAA ini adalah :

Authentikasi, berkaitan dengan validasi awal identitas pengguna akhir untuk mengijinkan akses ke jaringan. Server AAA membandingkan data authentikasi yang diberikan oleh user dengan data authentikasi user yang tersimpan pada database,jika cocok maka user tersebut dijamin bisa mengakses jaringan, jika tidak cocok maka authentikasinya gagal dan user tidak bisa mengakses jaringan.

Authorisasi, menjelaskan tentang hak dan layanan apa yang user dapatkan ketika mengakses jaringan. Hal ini mungkin saja menyertakan suatu IP *address*, menyerukan suatu filter untuk mencari aplikasi atau protokol mana yang mendukung, dan lain sebagainya

Akunting, menyediakan metodologi untuk mengumpulkan informasi tentang pemakaian sumber daya pelanggan,dimana kemudian diproses untuk kepentingan *billing, auditing*, dan perencanaan kapasitas.

Protocol AAA yang paling dikenal dan banyak digunakan adalah RADIUS (*Remote Authentication Dial-in User Service*). Protocol ini dikembangkan pada pertengahan 1990-an oleh Livingston enterprise untuk menyediakan layanan authentikasi dan akunting bagi perangkat NAS. Attribute fungsionalnya diantaranya Operasi yang berdasarkan *client-server*, dalam hal kemanan jaringan RADIUS menggunakan *shared secret key* dan adanya enkripsi message untuk mencegah para hacker membaca paket data, authentikasi yang fleksibel dimana RADIUS ini mendukung berbagai mekanisme authentikasi termasuk PAP dan CHAP. Adanya pasangan attribute/value, pesan RADIUS membawa informasi AAA dikodekan dalam field type-length-value yang disebut dengan attribute. Attribute fungsional diatas mengandung beberapa kelemahan yang akan kita analisa nanti, yang berakibat menurunnya performansi suatu jaringan akses dikarenakan proses authentikasinya.

Tugas akhir ini membahas dan menganalisa secara teoritis tingkat keamanan komunikasi data yang dapat diberikan oleh protocol RADIUS dalam suatu jaringan akses.

I.2 Tujuan Penulisan

Adapun tujuan dari penelitian ini adalah :

menganalisa secara deskriptif mengenai system keamanan dari kinerja protokol RADIUS dalam membawa data authentikasi meliputi analisa kelemahan,dan modifikasi dari protocol tersebut melalui analisa scenario pengiriman paket-paket RADIUS dalam suatu proses authentikasi.

I.3 Pembatasan Masalah

Dalam pembahasan tugas akhir ini,penelitian dibatasi dalam ruang lingkup :

1. analisa deskriptif yang meliputi logika operasi protocol RADIUS dalam membawa data authentikasinya saja, untuk RADIUS akunting tidak akan dibahas.
2. parameter yang akan dianalisa meliputi client-server packet exchange sequence , operasi MD5, mekanisme shared secret protocol RADIUS.

I.4 Metodologi Penelitian

Metodologi yang ditempuh dalam tugas akhir ini :

1. Studi Literatur, yaitu mempelajari literatur-literatur yang berhubungan dengan masalah tersebut diatas, meliputi : identifikasi masalah dan pendalaman materi tentang konsep RADIUS, prosedur otentikasi
2. Analisis teoritis
3. Menganalisa Pemanfaatan protocol RADIUS untuk membawa otentikasi dalam suatu contoh kasus
4. Kesimpulan hasil analisa

I.5 Sistematika Penulisan

Penulisan Tugas Akhir ini dibagi dalam 5 bagian utama :

BAB I : Pendahuluan

Menguraikan mengenai latar belakang, tujuan dan manfaat penelitian, perumusan masalah, sistematika penulisan.

BAB II : Dasar Teori

Membahas tentang konsep dasar protocol AAA,khususnya RADIUS diantaranya tipe node, format message,type-type message dan attribute dari paket RADIUS

BAB III : Mekanisme protocol RADIUS

Membahas operasi dari protocol RADIUS meliputi cara kerja, operasi MD5, mekanisme shared secret

BAB IV : Kajian fungsi protocol RADIUS dalam membawa authentikasi

Analisa operasi protokol RADIUS yang diberikan dalam 2 contoh kasus yaitu Telnet user ke spesifik host dan user framed yang diauthentikasi dengan PPP CHAP

BAB V : Kesimpulan dan saran

Kesimpulan dari hasil analisis serta evaluasi saran pengembangan lebih lanjut.

BAB V
KESIMPULAN DAN SARAN

V.1 Kesimpulan

1. Paket access-requestnya tidak dilindungi sama sekali sehingga penyerang bisa dengan mudah mendapat request authenticator ataupun response authenticator dari paket yang bisa ditangkap penyerang di jaringan, Sehingga memungkinkan system menggunakan request authenticator yang berulang.
2. Attribute user-password pada paket-paket yang dikirimkan bisa dengan mudah didapat sehingga nilai MD5 antara Shared Secret dan Request Authenticator pun bisa dicari, tetapi waktu yang diperlukan untuk memecahkan kode shared secretnya sangatlah lama walaupun sudah diketahui nilai request authenticatornya.
3. Untuk penggunaan 16 karakter ASCII sebagai input dari shared secretnya diperlukan waktu sebanyak 22092081055991055991059768953998 5.34799 tahun untuk bisa memecahkan kode shared secret dari suatu implementasi client-server RADIUS.

V.2 Saran

1. Perlu dianalisa lebih lanjut mengenai penggunaan mekanisme authentikasi yang berbeda-beda untuk melihat unjuk kerja fleksibilitas dari protocol RADIUS.
2. Sebaiknya dilakukan analisa terhadap protocol authentikasi lain agar dapat dilihat perbandingan unjuk kerja keamanan antar protocol-protokol tersebut untuk implementasi di jaringan OWLAN.
3. Pendekatan analisa yang dilakukan pada bab IV lebih cenderung pada pendekatan teoritis karena adanya keterbatasan dalam implementasi

teknologi tersebut, maka disarankan pada analisa selanjutnya dapat digunakan metode analisis yang lebih bersifat eksperimental, sehingga unjuk kerja protocol dapat diukur dengan lebih sempurna.

DAFTAR PUSTAKA

Bruce, Morrison ,"*The RADIUS protocol and Application*", Pegasus network, 2000

C. Rigney. Et al, *"Remote Authentication Dial-In User Service (RADIUS)*", IETF, RFC 2865, june 2000

C. Finseth, " *An Access Control Protocol, sometime called TACACs*", IETF, RFC 1492, July 1993

C. Metz, "*AAA Protocol: Authentication, Authorization, Accounting for the internet*," , cisco system, 2003

Davies. Joseph, " *RADIUS protocol security and best practices* ", Microsoft Corporation, jan 2003

H. Krawczyk, M. bellare, R. canneti," *HMAC-MD5 : Keyed-MD5 for message authentication*", IETF.org, march 1996

H. Krawczyk, M. bellare, R. cannet, " *HMAC : Keyed hashing for message authentication*", IETF, RFC xxxx, august 1996

Laurila, juha-ala, " *Wireless LAN access network architecture for mobile operator*", white paper IEEE comm. Magazine, nov 2001

Mike. Klein, " *Using AAA technology in wireless LAN and mobile IP application*", RSA conference, feb 2002

Paul. Condor, etc ,"*IEEE 802.1x RADIUS usage guidelines*", IETF, RFC 2026, april 2001

R. Rivest, " *the MD5 message digest algorithm*", IETF, RFC 1321, april 1992