

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 ketidaktepatan 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 koordinasi 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 autentikasi yang diberikan oleh user dengan data autentikasi user yang tersimpan pada database, jika cocok maka user tersebut dijamin bisa mengakses jaringan, jika tidak cocok maka autentikasinya 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 autentikasi dan akunting bagi perangkat NAS. Attribute fungsionalnya diantaranya Operasi yang berdasarkan *client-server*, dalam hal keamanan jaringan RADIUS menggunakan *shared secret key* dan adanya enkripsi message untuk mencegah para hacker membaca paket data, autentikasi yang fleksibel dimana RADIUS ini mendukung berbagai mekanisme autentikasi 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 autentikasinya.

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

1.2 Tujuan Penulisan

Adapun tujuan dari penelitian ini adalah :

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

1.3 Pembatasan Masalah

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

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

1.4 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 protokol 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 autentikasi
Analisa operasi protokol RADIUS yang diberikan dalam 2 contoh kasus yaitu Telnet user ke spesifik host dan user framed yang di autentikasi dengan PPP CHAP
- BAB V : Kesimpulan dan saran
Kesimpulan dari hasil analisis serta evaluasi saran pengembangan lebih lanjut.