Jurnal SimanteC
Vol 1, No 3 Desember 2010 ISSN 2088-2130

MEMBANGUN RADIUS SERVER UNTUK KEAMANAN WIFI KAMPUS

Agus Prihanto
Jurusan Teknik Elektro – Universitas Negeri Surabaya
email : cogierB201@yahoo.com

Banyak pihak yang masih mempertanyakan tentang keamanan wireless LAN. Apabila kita mengimplementasikan wireless LAN, maka kita juga harus memikirkan sistem keamanan apa yang akan diterapkan.

Untuk keamanan Wifi Kampus dapat digunakan free RADIUS server yang merupakan aplikasi open source. Hasil menunjukan dengan menggunakan RADIUS autentikasi user di jaringan WiFi Kampus dapat dikelola secara terpusat dan jika user tidak berhasil melakukan authentikasi ke server RADIUS, maka user tidak bisa memanfaatkan fasilitas jaringan kampus sekalipun hanya untuk intranet. Server RADIUS juga telah mendukung multiuser dan multiroaming, sehingga user bisa pindah-pindah ke Acces Point lainnya tanpa registrasi ulang.

Kata kunci : RADIUS, wifi kampus, keamanan

IMPLEMENTATION RADIUS SERVER FOR WIFI CAMPUS SECURITY

Many people are still worried about wireless LAN security. If we implement a wireless LAN, then we must consider what the security system are that will be applied.

For Campus Wifi security can be used free RADIUS server which is open source applications. The results showed of RADIUS that user authentication on the campus WiFi network can be centrally managed and if the user fail to authenticate on a RADIUS server, the user can not use the campus network facilities eventhough only for the intranet. Moreover, RADIUS server has multiuser support and multiroaming, so the user can be more mobility to another Access Point without re-registration.

Key words: RADIUS, wifi campus, security

1. PENDAHULUAN

1.1 Latar Belakang

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi *wireless*. Teknologi wireless juga diterapkan pada jaringan komputer, yang lebih dikenal dengan wireless LAN (WLAN). Kemudahan yang ditawarkan wireless LAN menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet. Hal ini dibarengi pula dengan harga sebuah Labtop yang telah dilengkapi teknologi Wifi sudah sangat terjangkau, sehingga ada kecenderungan orang untuk memilih labtop dari pada Desktop PC [2].

Beberapa tahun terakhir ini pengguna wireless LAN mengalami peningkatan yang pesat. Peningkatan pengguna ini juga dibarengi dengan peningkatan jumlah hotspot yang dipasang oleh ISP (*Internet Service Provider*) di tempat-tempat umum, seperti kafe, mal, bandara, dll. Teknologi Wireless LAN memang sangat cocok untuk membangun jaringan komputer secara temporal (*Ad-hoc*), yaitu infrastruktur yang mudah dibangun dan dibongkar sehingga sangat cocok untuk tempat-tempat umum, ruang rapat, seminar, kampus dan lainnya.

1.2 Permasalahan

Banyak pihak yang masih mempertanyakan tentang keamanan wireless LAN. Apabila kita meng-implementasikan wireless LAN, maka kita juga harus

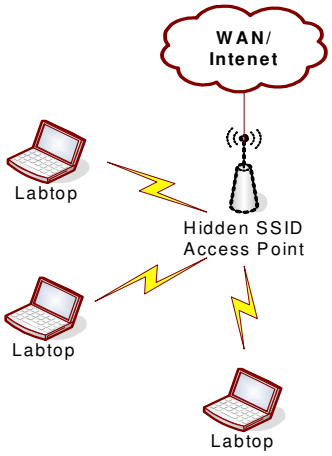
memikirkan sistem keamanan apa yang akan diterapkan. Banyak hotspot yang tidak menerapkan sistem keamanan yang memadai, sehingga memungkinkan pengguna yang tidak berhak (*ilegal*) dapat masuk ke jaringan komputer tersebut. Apabila hal ini sampai terjadi, maka pemilik hotspot tersebut secara langsung maupun tidak langsung akan dirugikan, penyusup itu dapat saja melakukan perbuatan yang tidak menyenangkan, seperti mengambil data, menyerang komputer-komputer yang ada di jaringan tersebut, kehilangan pendapatan (apabila pemilik hotspot adalah ISP), dll.

Memang tidak mudah untuk memanajemen user dalam jaringan hotspot. Semakin banyak user dan semakin luas jangkauan wilayah dari jaringan wirelless, maka diperlukan penerapan manajemen kemanan jaringan yang semakin bagus.

1.3 Alternatif Pemecahan

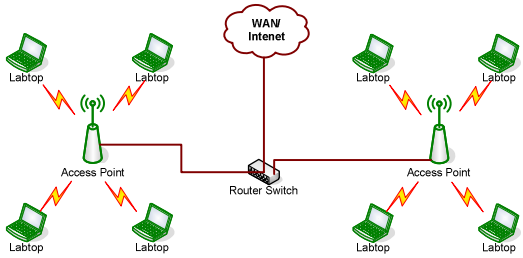
Banyak paper yang mencoba membahas mengenai bagaimana memanajemen user dan mengamankan jaringan hostpot. Diantara teknologi itu adalah :

- ***SSID (Service Set ID)*** dilakukan dengan menyembunyikan SSID namun kenyataannya cara ini tidak efektif sebab client akan tetap mengirimkan SSID dalam bentuk plain text (meskipun menggunakan enkripsi). Beberapa tools yang dapat digunakan untuk mendapatkan SSID yang di*hidden* antara lain, kismet (kisMAC), ssid_jack (airjack), aircrack, void11 dll [1].



Gambar 1. Bagan Hidden SSID Access Point

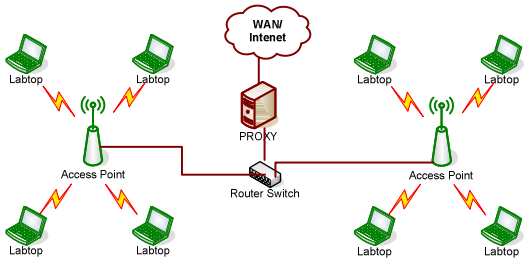
- ***WEP (Wired Equivalent Privacy)*** metode ini adalah system keamanan dan enkripsi pertama yang digunakan pada wireless, namun kelemahnnya karena enkripsi algoritma RC4 mempunyai kunci yang lemah yaitu kunci WEP bersifat statis. Beberapa bentuk serangan yang dilakukan misalnya FMS Attack (Fluhrer, Mantin, dan Shamir), atau dengan Traffict Injection. WEP juga menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna wireless LAN. Hal ini menyebabkan WEP tidak dapat diterapkan pada hotspot yang dipasang di tempat-tempat umum[1].



Gambar 2. Bagan Wifi Dengan MAC Filter

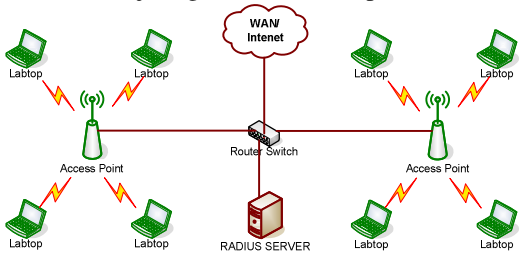
- ***MAC Filtering*** adalah sistem keamanan bawaan yang sudah melekat pada perangkat wireless Access Point maupun Router. Hal ini sebenarnya tidak banyak membantu mengamankan komunikasi wireless, karena MAC address sangat mudah di*spoofing* atau bahkan dirubah. Tools yang biasa digunakan network utilitis, regedit, smac, machange [1].
- ***DHCP***, server hanya meng-identifikasi MAC Address kemudian memberikan IP ke klien. Tidak ada proses autentikasi selama proses permintaan IP namun punya kelebihan yaitu effective cost penggunaan resource network[5].
- ***PPPoe and PPTP***, biasanya digunakan untuk proses autentikasi untuk jaringan ATM. Membutuhkan client resource seperti software client sehingga customer masih perlu intervensi[5].
- ***Proxy Server,*** teknologi sudah mendukung multi user dan *roaming* (perpindahan user) dalam jaringan, namun authentikasi yang diberikan hanya ketika user mau akses ke jaringan luar/internet. Sedangkan jika user hanya ingin membuat koneksi di jaringan lokal/intranet, maka authentikasi ini tidak akan muncul[5].

Jurnal SimanteC
Vol 1, No 3 Desember 2010 ISSN 2088-2130



Gambar 3. Bagan Wifi Dengan Proxy

- ***RADIUS (Remote Authentication Dial In User Service),*** teknologi sudah mendukung multi user dan *roaming* (perpindahan user) dalam jaringan. Authentikasi bersifat terpusat dan dilakukan diawal ketika seorang user mau menggunakan jaringan, baik untuk koneksi jaringan intranet maupun internet.

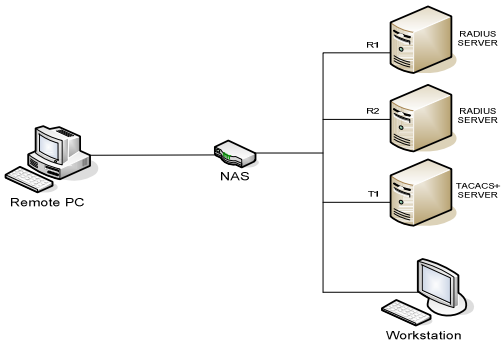


Gambar 4. Bagan Wifi Dengan RADIUS

2. PROTOKOL RADIUS

Remote Authentication Dial In User Service (RADIUS), adalah protokol yang dikembangkan untuk proses AAA (*authentication*, *authorization*, *and accounting*). Protocol AAA ini sendiri adalah sebuah model akses jaringan yang memisahkan tiga macam fungsi kontrol, yaitu Authentication, Authorization, dan Accounting, untuk diproses secara independen[2].

Pada dasarnya terdapat tiga komponen yang membentuk model ini yaitu *Remote User*, *Network Access Server* (NAS), dan *AAA server*. Proses yang terjadi dalam sistem ini adalah user meminta hak akses ke suatu jaringan (internet, atau *wireless LAN* misalnya) kepada *Network Access Server*. *Network Access Server* kemudian meng-identifikasi user tersebut melalui *AAA server*. Jika server AAA mengenali user tersebut, maka server AAA akan memberikan informasi kepada NAS bahwa user tersebut berhak menggunakan jaringan, dan layanan apa saja yang dapat diakses olehnya. Selanjutnya, dilakukan pencatatan atas beberapa informasi penting mengenai aktivitas user tersebut, seperti layanan apa saja yang digunakan, berapa besar data (dalam ukuran *bytes*) yang diakses oleh user, berapa lama user menggunakan jaringan, dan sebagainya.



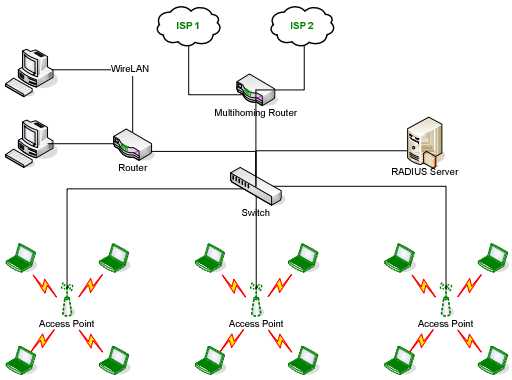
Gambar 5. Model AAA

System jaringan RADIUS menjalankan sistem administrasi pengguna yang terpusat, sistem ini akan mempermudah tugas administrator. Dapat kita bayangkan berapa banyak jumlah pelanggan yang dimiliki oleh sebuah ISP, dan ditambah lagi dengan penambahan pelanggan baru dan penghapusan pelanggan yang sudah tidak berlangganan lagi. Apabila tidak ada suatu sistem administrasi yang terpusat, maka akan merepotkan administrator dan tidak menutup kemungkinan ISP akan merugi atau pendapatan-nya berkurang. Dengan sistem ini pengguna dapat menggunakan *hotspot* di tempat yang berbeda-beda dengan melakukan autentikasi ke sebuah RADIUS server[6].

3. DESAIN JARINGAN WIFI KAMPUS

Berikut adalah stuktur umum jaringan Wifi Kampus yang dikembangkan :

Jurnal SimanteC
Vol 1, No 3 Desember 2010 ISSN 2088-2130



Gambar 6. Bagan Struktur Umum Wifi Kampus

Jaringan Wifi Kampus dengan RADIUS di atas dibagi menjadi 3 bagian yaitu :

1. ***Supplicant/Remote User***, terdiri dari User Labtop ataupun Desktop PC.
2. ***NAS***, terdiri dari Access Point/Hotspot ataupun Router sebagai Gateway dari koneksi user.
3. ***RADIUS Server***, yang melakukan proses AAA (Authentication, Authorization, Accounting) dan menyimpan data seluruh user secara terpusat.

Jaringan di atas juga mensupport 2 teknologi yaitu *WireLAN* (Kabel) dan *WirellessLAN* (Tanpa Kabel). Setiap User yang akan koneksi ke dalam jaringan Lokal Kampus maupun Internet diharuskan melakukan authentikasi terlebih dahulu melalui NAS (Access Point/Router Gateway) yang berwenang kemudian untuk diteruskan ke server RADIUS. Jika authentikasi berhasil dilakukan maka RADIUS server akan memberikan jawaban ke NAS dan NAS akan menerima atau menolak request user berdasarkan ke absahan authentikasi yang dilakukan user.

Untuk database user disimpan secara terpusat di Server RADIUS, sehingga jika ada user yang ingin pindah ke Access Point lain maka tidak diperlukan daftar ulang lagi. Hal ini akan memberikan kemudahan user untuk *roaming* (melakukan perpindahan) di antara Access Point/Hostpot.

4. IMPLEMENTASI

4.1 Alat dan Bahan

Dalam desain ini menggunakan *free* RADIUS server, Alasan utama kenapa memilih *free* RADIUS server adalah karena mahalnya harga RADIUS server komersial. Sebagai contoh : Interlink's Secure.XS harganya mulai dari $2375 untuk 250 pengguna, Funk Odyssey Server $2500, VOP Radius Small Business mulai dari $995 untuk 100 pengguna [4]. Harga RADIUS server komersial diatas kebanyakan tidak terjangkau bagi para pemilik *hotspot*, terutama bagi kalangan kampus.

Salah satu contoh RADIUS server yang non-komersial adalah FreeRADIUS server. FreeRADIUS server ini tidak kalah dengan RADIUS server yang komersial. Salah satu buktinya adalah freeRADIUS server sudah mendukung beberapa *Access Point* (AP)/ *Network Access Server* (NAS) dibawah ini [3]:

- 3Com/USR Hiper Arc Total Control
- 3Com/USR NetServer
- 3Com/USR TotalControl
- Ascend Max 4000 family
- Cisco Access Server family
- Cistron PortSlave
- Computone PowerRack
- Cyclades PathRAS
- Livingston PortMaster
- Multitech CommPlete Server
- Patton 2800 family

FreeRADIUS dapat berjalan di berbagai sistem operasi, misalnya Linux, FreeBSD, OpenBSD, OSF.

Untuk lebih detailnya, berikut adalah alat dan bahan yang diperlukan dalam membangun Wifi Kampus dengan RADIUS, yaitu :

- NOS Server (SUSE Linux 9.)
- Radius Server (Opensource:FreeRADIUS)
- Router Multihoming
- Access Point
- Gateway Router NAS
- Client (Desktop PC/Labtop, NOS:Wind/Linux)
- Hub Switch
- ISP (Penyedia Jaringan Internet)

4.2 Uji Coba

Untuk melengkapi tulisan ini, dilakukan suatu percobaan instalasi *free* RADIUS server pada satu buah komputer, sistem operasi yang digunakan adalah *SUSE Linux 9.0* dengan versi kernel 2.4.21. SUSE Linux 9.0 ternyata sudah mempunyai paket RADIUS server yang terdiri dari:

1. ***Big Sister***

   Paket ini merupakan Big Sister plug-in untuk pemonitoran sebuah RADIUS server.

2. ***FreeRADIUS***

   Paket ini merupakan RADIUS server.

3. ***freeradius-devel***

   Paket ini berisi file-file untuk pengembangan FreeRADIUS

4. ***pam_radius***

   Pam_radius adalah suatu modul PAM yang digunakan untuk autentikasi pengguna pada RADIUS server.

5. ***radiusclient***

   RADIUS client memberikan beberapa program untuk proses autentikasi melalui RADIUS server.

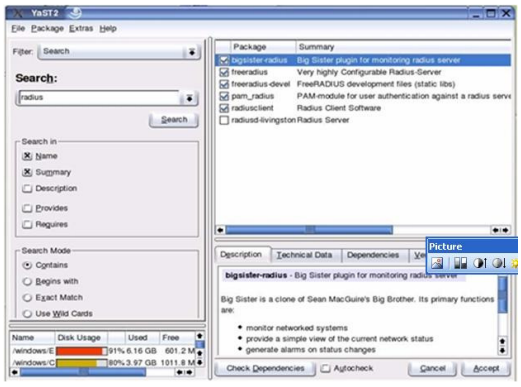
6. ***radiusd-livingston***

   Radiusd-livingston adalah RADIUS server dari Lucent Technologies

FreeRADIUS merupakan salah satu paket program yang terdapat di SUSE Linux 9.0, maka proses instalasinya relatif lebih mudah. Karena paket freeRADIUS bukan termasuk paket default yang otomatis terinstal apabila kita menginstal SUSE Linux 9.0, maka instalasinya harus dilakukan secara manual. Langkah-langkah proses instalasi paket freeRADIUS yang terdapat pada SUSE Linux 9.0 adalah sebagai berikut:

1. Kita dapat menggunakan program **YaST**. Ada dua cara untuk menjalankan program YaST, cara pertama : *Start Menu* → *System* → *YaST*, apabila kita login sebagai pengguna biasa (bukan super user), maka akan muncul window yang meminta password *root*. Sedangkan cara yang kedua adalah melalui *konsole* dan harus login sebagai *root*, kemudian ketik *yast*. Apabila window *YaST Control Center* sudah muncul, pada menu sebelah kiri pilih Software, kemudian pilih Install and Remove Software. Agar tidak terlalu binggung, kita dapat menggunakan fasilitas search untuk mencari paket RADIUS, pada menu filter pilih search, ketik radius pada kolom isian, tekan enter, maka akan muncul paket-paket RADIUS seperti yang telah disebutkan diatas.
2. Pilih paket yang ingin kita instal.
3. Tekan tombol accept apabila sudah selesai memilih paket yang akan diinstal.

Untuk lebih memperjelas proses instalasi *freeRADIUS* di SUSE Linux 9.0 diatas, lihat Gambar dibawah ini.



Gambar 7. YaST

Apabila kita telah memilih *freeRADIUS* sebagai RADIUS server, maka kita tidak boleh memilih *radiusd-livingston* sebagai RADIUS server dan begitu juga sebaliknya. Apabila kita memilih *freeRADIUS* dan *radiusd-livingston* bersama-sama, maka pada saat kita menekan tombol *accept* akan keluar window yang berisi peringatan bahwa ada konflik. Untuk menghindari konflik tersebut, maka kita harus memilih salah satu dari freeRADIUS dan radiusd-livingston yang akan digunakan sebagai RADIUS server.

5. SARAN DAN KESIMPULAN

5.1 Kesimpulan

- Server radius dapat digunakan untuk autentikasi user di jaringan WiFi Kampus secara terpusat.
- Jika User tidak berhasil melakukan authentikasi ke server RADIUS, maka user tidak bisa memanfaatkan fasilitas jaringan kampus sekalipun hanya untuk intranet.
- Server RADIUS WiFi kampus yang digunakan mendukung multiuser dan multiroaming, sehingga user bisa pindah-pindah ke Acces Point lainnya tanpa registrasi ulang.

5.2 Saran

- Untuk dapat mendeteksi posisi user, setiap NAS (Access Point, Router Gateway) dapat disetting menggunakan NAT (*Network Address Translation*). Dengan NAT, setiap user yang mencoba konek jaringan, maka server RADIUS akan mengenali MAC dan IP Address dari NAS yang gunakan oleh user (*mengikuti konsep NAT*). Dengan memetakan alamat NAS yang ada, maka dapat diketahui posisi seorang user pada saat itu.

DAFTAR PUSTAKA

[1] Josua M Sinambela, "Wireless Security (Hacking Wifi)", Seminar Open Source dan Hacking Wifi 2007di AMIKOM Yogyakarta

[2] Agung W. Setiawan, "Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN", FTI-ITB 2005

[3] Ventura, H., "Diameter: Next Generation's AAA Protocol", Tesis Master, Jurusan Teori Informasi, Lingkopings University, 2002.

[4] Phifer, Lisa. Using RADIUS for WLAN Authentication, Part II (December 10, 2003).

[5] Minhyung Kim, "High performance AAA architecture for massive IPv4 networks", Science Direct, 2006.

[6] http://en.wikipedia.org/wiki/RADIUS, 2010