Pengamanan ganda pada penggunaan akun AI3

Rizkiana Novitasari -- 13507122
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If17122@students.if.itb.ac.id

***Abstract*—penggunaan akses internet di ITB memanfaatkan akun AI3 untuk bisa mengakses jaringan di luar ITB(semua web yang berekstensi *.itb.ac.id adalah web jeringan dalam ITB) dan juga user yang ingin mengakses web dalam ITB dari jaringan di luar ITB. Kasus yang sedang marak beredar di kalangan user AI3 adalah pengguna ganda untuk satu akun AI3, hal ini biasa terjadi apabila ada kegiatan saling pinjam akun untuk mengakses jaringan di luar ITB. Penyebaran *username* dan *password* AI3 ini mengakibatkan kesulitan bagi user akun yang sebenarnya untuk mengakses internet. Makalah ini akan membahas bagaimana algoritma RSA bisa membantu untuk meningkatkan pengamanan pada penggunaan akun AI3.**

***Index Terms*— AI3, RSA, internet, ITB.**

I. INTRODUCTION

Asian Internet Interconnection Initiative

Akun *proxy* internet AI3 merupakan gerbang bagi masing-masing civitas ITB untuk dapat mengakses internet dari dalam kampus ITB serta akses *Virtual* Privat *Network*(VPN) dari mana saja. Dengan akun ini, civitas dapat secara bebas menggunakan internet untuk mengakses informasi dari seluruh dunia melalui akses internet. Bagi mahasiswa, internet saat ini merupakan kebutuhan yang sangat penting. Hampir keseluruhan bah-bahan materi belajar serta bahan tugas tersedia di sana.

Sejarah AI3

AI3 (*Asian Internet Interconnection Initiative*) *Project* merupakan program kerjasama internasional yang diinisialisasi dengan partner pertamanya adalah ITB sejak tahun 1996. Kerjasama ini bertujuan untuk mengembangkan internet di lingkup internasional berupa pengembangan infrastruktur dan penyediaan layanan teknologi informasi di belahan dunia. Pada saat itu, internet merupakan kebutuhan mendesak yang harus segera dipenuhi supaya tercipta lingkungan yang kondusif untuk praktisi dan peneliti dalam pengembangan teknologi praktis di wilayah Asia Pasifik.

AI3 project pertama kali diluncurkan oleh WIDE Project dan JSAT berupa *network* testbed berbasis satelit di Asia Tenggara (Salah satunya adalah *transreceiver satellite* yang terpasang di gedung PAU-ITB pada tahun 1996). Dengan infrastruktur tersebut, seluruh tim AI3 project, dan ITB khususnya dapat menikmati akses jaringan internet internasional, serta dapat menyelenggarakan rangkaian penelitian berbasis jaringan internet dengan memanfaatkan testbed tersebut. AI3 Project dalam hal ini, berupaya untuk memberikan sumbangsih, mempromosikan, serta memotivasi terselenggaranya upaya-upaya untuk meningkatkan infrastruktur informasi internasional seperti internet, AII, dan APII.

Partner AI3 Project di Asia setelah ITB, terus berkembang meliputi :

- AI3 Partners
  - WIDE Japan
- AI3 Ku-band
  - NAIST Nara Institute of Science and Technology Japan
  - ITB Institute of Technologi Bandung Indonesia
  - AIT Asian Institute of Technology Thailand
- AI3 C-band
  - SFC Keio University Japan
  - Temasek Poly Temasek Polytechnic Singapore
  - USM Universiti Sains Malaysia Malaysia
  - ASTI Advanced Science and Technology Institute Philippine
  - IOIT Institute of Information Technology Vietnam

Kerja sama tersebut saat ini saat ini masih terjalin erat. Pertemuan-pertemuan secara online dan offline diselenggarakan setiap 6 bulan untuk melihat perkembangan dan kemajuan yang berhasil dicapai. Tahun 2006 merupakan tonggak 10 tahun kerja sama tersebut dibangun. Hingga saat ini infrastruktur teknologi informasi sudah terbangun dengan baik. Peranan AI3 pun meningkat yaitu dengan terus berupaya untuk meningkatkan kerjasamanya menuju jenjang yang lebih tinggi dalam bentuk layanan konten berupa *School on Internet* (SOI).

SOI Asia (*School on the Internet Asia*) Project berawal

pada tahun 2001. Saat ini project tersebut memperingati 5 tahun bergabungnya dengan AI3 project. Project ini mulai direncanakan pada tahun 2001 dan setup pertama SOI Asia *network* berhasil dilakukan di *National University of Laos* in LAO P.D.R pada tanggal 5 Januari 2002.

Dengan momen memperingati 10 tahun AI3 dan 5 tahun SOI, ITB sebagai universitas unggulan Indonesia, dihadapkan pada tantangan untuk dapat menjadi model universitas yang mampu mengoptimalkan sumber daya teknologi informasi yang dimilikinya untuk mempercepat perkembangan kemajuan teknologi di Indonesia.

Akun untuk penggunaan AI3

ITB *Network Account* merupakan satu-satunya *account* yang bisa digunakan untuk mengakses layanan-layanan yang ada pada jaringan kampus ITB. Layanan-layanan itu seperti :

- Email @students.itb.ac.id (khusus untuk mahasiswa)
- Hotspot ITB, akses wireless *network*.
- Internet *Proxy*
- Virtual Privat *Network*
- Web user directory My.itb.ac.id

Layanan-layanan diatas akan terus bertambah dan dikembangkan, namun authentikasinya akan tetap menggunakan *Account* INA.

Account INA diperuntukkan bagi semua civitas ITB dan diharapkan dapat mendukung aktivitas akademik maupun non-akademik dikampus ITB. Jika pengguna sudah mempunyai *account* INA, maka secara otomatis pengguna dapat menggunakan layanan-layanan diatas. Kecuali layanan tertentu, seperti Internet *Proxy*, yang membutuhkan registrasi tambahan. Untuk mengetahui informasi lebih lanjut, silakan lihat policy/aturan dari setiap layanan tersebut.

Layanan INA

Nicadm

Mirip seperti layanan terdahulu, namun kali ini INA membuat beberapa layanan tambahan di luar layanan inti. Layanan terdiri dari dua jenis, yaitu standard dan plus. Yang membedakannya hanya jenis *service*.

Apa yang berubah dari layanan yang ada sekarang ? Pertama, INA akan memblok semua port keluar masuk, kecuali layanan di bawah. Kedua, aplikasi email akan keluar masuk lewat *Mail Exchanger server*. Ini terjadi secara otomatis, jadi tidak perlu merubah *setting* MTA yang ada. Ketiga, untuk melakukan *browsing*, pengguna masih perlu memasukkan *proxy* server dalam *setting browser*, hanya ip adressnya saja yang berbeda. Lebih detail pengguna bisa lihat pada bagian guidance. Keempat, pengguna perlu registrasi ulang untuk bisa menikmati layanan di bawah. Userid yang lama tidak dipakai lagi. Jadi buat pengguna yang sudah membayar untuk bulan terakhir, tidak perlu membayar apa-apa lagi, hanya registrasi ulang dengan menunjukkan bukti kuitansi.

Untuk pengguna yang mempunyai aplikasi khusus yang tidak bisa bekerja karena portnya terkena blok, maka pengguna bisa komplain ke 1[at]itb.ac.id. Jika memang aplikasi tersebut untuk kepentingan riset dan akademis, kami bisa membukanya kembali khusus untuk ip address pengguna.

Layanan Standar

Dengan layanan standard ini, pengguna sudah dapat mengeksporasi internet tanpa batas waktu dengan 4 macam layanan, yaitu HTTP, SMTP, Webmail dan beberapa layanan umum lainnya. Pada saat registrasi, pengguna akan mendapatkan 1 buah ITB ID yang berfungsi sebagai tanda pengenal yang diperlukan untuk dapat membuka layanan HTTP dan Webmail. Dan ITB ID ini juga nantinya akan membuat pengguna berhak menggunakan helpdesk.

Layanan HTTP

Layanan ini memberikan akses HTTP kepada pengguna dengan menggunakan sebuah ITB ID. Penyedia jasa tidak menyediakan fasilitas akses komputer, melainkan hanya bandwith dan *proxy* server.

Layanan SMTP

Layanan ini dimaksudkan untuk pengguna yang mempunyai sebuah mailbox yang tersedia pada masing-masing departemen dan unit ITB lainnya. Penyedia jasa dalam layanan ini memberikan fasilitas bandwith dan MailExchanger server tanpa mailbox.

Layanan Webmail

Dengan layanan ini pengguna dapat menggunakan fasiltas mail berikut mailbox dengan quota 10 MB yang dapat diakses melalui HTTP dan POP3. Pengguna membutuhkan ITB ID untuk dapat menggunakan layanan ini.

Layanan lainnya

Secara umum, semua port keluar dan masuk ditutup. Ini untuk pertimbangan keamanan dan efisiensi. Namun di luar itu, ada beberapa port yang akan dibiarkan terbuka, yaitu port untuk layanan :

- pop (in/out)
- imap (in/out)
- ssh (in/out)
- http (in)
- ftp (in)

- telnet (in/out)
- IRC (out)
- DNS (out)
- ICQ (in/out)
- ntp (in/out)

Registrasi

Untuk dapat mendaftarkan diri, biasanya tiap-tiap departemen mempunyai tempat pendaftaran sendiri yang diatus oleh masing-masing penanggung jawab dan admin lokal. Bila hal ini tidak dapat/sulit dijangkau maka anda dapat mendaftarkan lansung di sekertariat INA di gedung PAU lantai 4.

Biaya

* Layanan standard (per bulan)
  - Mahasiswa Rp 10.000,-
  - Dosen Rp 15.000,-
  - Karyawan Rp 5.000,-

* Layanan Shell (per semester)
  Rp 50.000,-

Akses Internet User Guest

Layanan ini ditujukan bagi unit kerja di ITB yang sedang kedatangan tamu. Unit kerja diperbolehkan memberikan akses internet bagi tamu yang sedang berkunjung ke ITB.

Syarat administrasi untuk dapat menikmati layanan ini adalah surat permohonan akses user guest yang ditandatangani oleh Kepala Bagian Sistem Informasi dari unit kerja tempat tamu berada. Dalam surat tersebut harus dituliskan informasi mengenai :

1. Jumlah user guest yang akan dipesan.
2. Tanggal awal dan tanggal akhir penggunaan user guest.
3. Nama penganggung jawab user guest.
4. Alamat email penanggung jawab sebagai tempat pengiriman user dan *password* user guest.

Biaya administrasi yang harus dibayar adalah :

- Untuk pemakaian <= 3 hari, biayanya adalah Rp. 10.000,00 per hari per user.
- Untuk pemakaian > 3 hari, biayanya adalah Rp. 5.000,00 per hari per user.

Surat tersebut harus disampaikan ke Gedung Sekretariat AI3 ITB, Gedung PAU Lt. 4.

Account user guest akan aktif pada tanggal yang diinginkan dan *password* akan dikirimkan ke alamat email penanggung jawab user tersebut.

Manajemen Account

Berikut merupakan beberapa fasilitas yang bisa dimanfaatkan seorang pemilik akun sebagai bentuk kendali terhadap akun yang ia miliki.

- Pengubahan Password
- Pengubahan Reset Password
- Pengecekan User
- Pengecekan Password
- Pengecekan Status Akses Internet
- Reset Password
- Reset oleh Admin
- Pemblokiran Account
- Voucher Internet
- Registrasi Voip

Penggunaan akun AI3 sekarang

1. User membeli voucher pada bagian terkait.
2. Setiap user melakukan registrasi untuk mendapatkan akun. Ketika registrasi berhasil, setiap user akan memiliki *username* yang bersifat unik dan *password* berupa kata atau kalimat yang dipilih oleh pengguna.
3. Setiap kali pengguna akan melakukan akses ke jaringan di luar ITB, pengguna akan memasukkan *username* dan *password* dari akun yang ia miliki ke tempat yang telah disediakan *browser*.
4. User bisa sewaktu-waktu mengubah *username* atau *password* yang ia miliki.
5. User bisa sewaktu-waktu memblokir suatu akun dengan validasi *username* dan *password* sebelumnya.

Algoritma RSA

Di kriptografi, RSA(yang merupakan singkatan dari Rivest, Shamir, dan Adleman yang pertama kali mendeskripsikan RSA secara publik) merupakan algoritma untuk kriptografi kunci publik. RSA merupakan algoritma pertama yang dikenal cocok untuk tanda-tangan dan juga enkripsi, dan merupakan yang pertama dari kemajuan besar pertama di kriptografi kunci publik. RSA secara luas digunakan dalam *protocol electronic commerce*, dan diyakini aman karena diberikan kunci yang cukup panjang dan penggunaan implementasi *up-to-date*.

Operasi RSA

Algoritma RSA melibatkan tiga step : *key generation*, enkripsi, dan dekripsi.

Key generation

RSA melibatkan kunci publik dan kunci privat. Kunci publik bisa diketahui oleh semua orang dan digunakan untuk mengenkripsi pesanl pesan dienkripse dengan kunci publik dan hanya bisa didekripsi menggunakan kunci privat. Kunci untuk algoritma RSA di-*generate* dengan cara berikut :

1. Pilih dua angka prima berbeda ***p*** dan ***q***
   - Untuk tujuan keamanan, *integer* p dan ***q*** harus dipilih seragam secara acak dan harus memiliki panjang bit yang sama. *Integer* prima bisa ditemukan secara efisien menggunakan primality test.
2. Hitung ***n*** = ***pq***
   - ***n*** digunakan sebagai modulus kedua kunci publik dan kunci privat.
3. Hitung ***φ(pq) = (p − 1)(q − 1).***
4. Pilih sebuah *integer* ***e*** sehingga ***1 < e < φ(pq),*** dan ***e*** dan ***φ(pq)*** tidak mempunyai pembagi selain 1 (***e*** adalah FPB ***φ(pq)***).
   - ***e*** merupakan eksponen kunci publik.
   - ***e*** memiliki panjang bit pendek dan hasil Hamming weight kecil untuk enkripsi yang lebih efisien. Nilai e yang kecil telah menunjukkan lebih aman dibeberapa *setting*.
5. Tentukan d (menggunakan aritmatika modular)

$$de \equiv 1 \pmod{\varphi(pq)}$$

   - ***d*** merupakan eksponen kunci privat.
   - ***ed-1*** bisa dibagi oleh ***(p-1)(q-1)***

kunci publik terdiri dari modulus ***n*** dan eksponen publik (atau enkripsi) ***e***. kunci privat terdiri dari eksponen privat(atau dekripsi) ***d*** yang harus dijaga kerahasiaannya.

Enkripsi

A mengirimkan kunci publik ke B dan menjaga kunci privatnya. B mengirim pesan M ke A.

B mengubah M ke *integer* 0<m<n dengan menggunakan protocol reversible dikenal dengan skema padding. B kemudian menghitung ciphertext c yang didapat dari :

$$c = m^e \bmod n$$

B akan mengirimkan c ke A.

Dekripsi

A bisa memulihkan m dari C dengan mneggunakan kunci privatnya ,***d***, dengan perhitungan :

$$m = c^d \bmod n.$$

Dengan diberikan m, A bisa mendapatkan pesan asli M dengan membalikkan skema padding.

Keamanan Algoritma RSA

Hal-hal yang mengancam keamanan dari sistem enkripsi dan dekripsi yang dimiliki oleh RSA pada dasarnya di akibatkan oleh dua problem matematika :

- faktorisasi bilangan berjumlah banyak
- pencarian modulo akar e^n dari sebuah bilangan komposist n yang faktornya tidak diketahui.

Akibat hal-hal diatas, banyak ancaman yang mungkin menyerang RSA. Sistem yang digunakan algoritma untuk melakukan proses enkripsi dan dekripsi mempunyai kemungkinan-kemungkinan kelemahan yang bisa diserang oleh para penyadap (atau dalam kasus pemanfaatan algoritma RSA ini, peminjam akun). Beberapa kelemahan RSA yang beresiko membobol keamanan :

- nilai ***n*** terlalu kecil sehingga mudah difaktorisasi
- jumlah nilai eksponen e^n yang terlalu kecil
- ukuran kunci yang terlalu kecil sehingga sandi dapat dijebol dengan brute force attack
- nilai ***d*** terlalu kecil
- penggunaan nilai modulus yang familiar hal ini memudahkan para hacker untuk menjebol sandi yang ada.

II. PENDEFINISIAN MASALAH

Kekurangan dari sistem pengamanan akun AI3 yang ada sekarang adalah hanya ada satu lapis pengamanan dibagian pengguna. Hal ini mengakibatkan apabila *username* dan *password* akun tersebut berhasil di bobol oleh orang lain maka seluruh aspek keamanan dari akun tersebut akan terancam. Berikut merupakan salah satu masalah yang dihadapi berhubungan dengan kekurangan tersebut.

1. Peminjaman akun
   Kasus ini sering terjadi di kalangan mahasiswa, khususnya. Hal ini terjadi karena akun peminjam telah habis masa berlakunya. Hal ini biasanya terjadi dengan kesepakatan diantara peminjam dan pemilik dari akun itu sendiri.

2. Pengaksesan akun diluar izin pemilik
   Pengaksesan ini biasanya terjadi karena perluasan kasus yang pertama. Berawal dari peminjaman biasa dan dilanjutkan dengan peminjaman terus-terusan karena *username* dan *password* akun AI3 tidak diganti pemilik dan peminjam tidak meminta izin lagi untuk meminjam akun tersebut. Peminjam biasanya mengakses internet dengan menggunakan akun AI3 kapanpun tanpa meminta izin lagi terlebih dahulu. Hal ini mengakibatkan pemilik sah akun AI3 tidak bisa mengakses internet dan tidak bisa mengetahui siapa yang tengah menggunakan akun miliknya.

3. Pengubahan *password* bukan oleh pemilik
   Kasus ini merupakan perluasan dari kedua kasus di atas. Hal ini biasanya dilakukan oleh peminjam yang keterlaluan. Peminjam yang telah meminjam akun AI3 seseorang dan dengan semena-mena mengganti *password* akun tersebut sehingga pemilik sah tidak bisa mengakses akun tersebut lagi.

Kenapa hal tersebut bisa menjadi masalah? Akun AI3 tidak hanya bisa dimanfaatkan untuk mengakses internet di luar ITB dan juga sebaliknya tetapi juga bisa sebagai akun email dengan ekstensi *@students.itb.ac.id. Dengan kasus yang telah dijelaskan sebelumnya, dikhawatirkan terjadi kasus lebih lanjut yang melibatkan penggunaan akun email ini dengan semena-mena. Seperti pengiriman email yang mengatasnamakan pemilik akun padahal dikirim oleh orang lain.

III. SOLUSI YANG DITAWARKAN

Penjelasan program

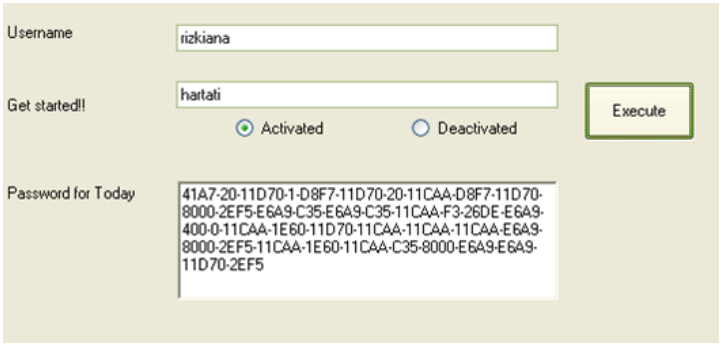
Algoritma RSA bisa dimanfaatkan untuk meningkatkan keamanan dari penggunaan AI3.
Cara kerja :

1. **Pembuatan akun AI3**
   Pembuatan ini biasanya dengan masuk ke alamat http://students.itb.ac.id/zimbra/dan mendaftarkan diri dan mengisi form yang telah disediakan. Pengaktifan akun ini sendiri biasa dilakukan dengan memasukan kode dari voucher yang dibeli di bagian terkait.

2. **Kepemilikian kunci publik dan kunci privat**
   Dengan melakukan pembuatan akun AI3, pemilik akun akan memiliki kunci publik dan admin akan memiliki kunci privat yang merupakan pasangan kunci tersebut. Kunci-kunci ini akan diketahui hanya oleh admin. User tidak akan mengetahui kuncinya karena kunci ini akan ada disistem yang akan mengenali kunci di setiap user dari *username* yang dimiliki karena *username* bersifat unik. Kunci ini akan berguna untuk membangkitkan *password* setiap akan melakukan akses internet.

3. **Aktivasi akun di setiap akses awal internet**
   Pengguna akan melakukan aktivasi akun setiap akan akses internet. Aktivasi ini dilakukan dengan memasukkan kata apapun yang disukai oleh user. Aktivasi ini akan membangkitkan *password*.

4. ***Generate password* dinamis disetiap akses internet**
   Hasil aktivasi akun di setiap akses awal internet akan membangkitkan *password* yang akan digunakan untuk akses internet.

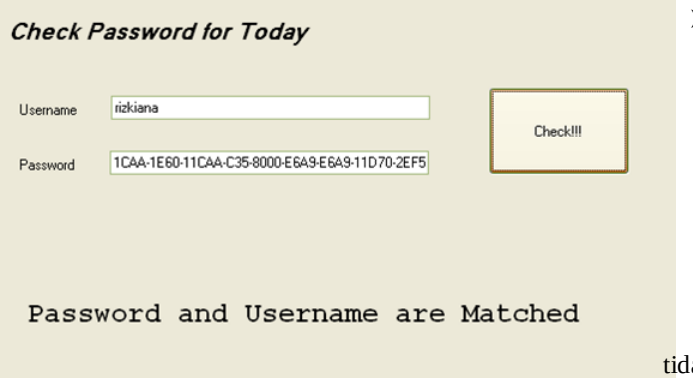


5. **Deaktivasi akun di akhir akses internet**
   Deaktivasi ini dilakukan di akhir akses internet sehingga semua akses yang menggunakan *username* terkait akan di tutup. Deaktivasi ini dilakukan dengan memasukkan kata yang telah digunakan user untuk melakukan aktivasi di awal.

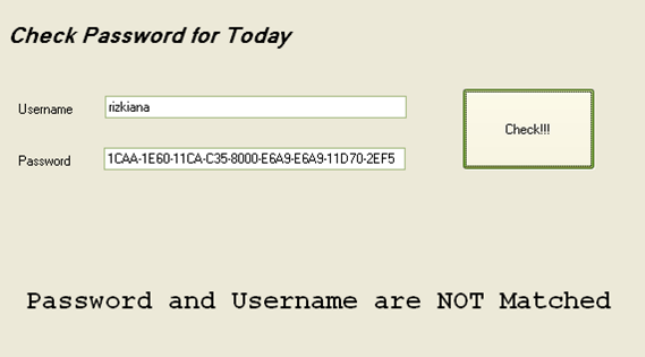
Fitur-fitur lain yang membantu

Pemeriksaan kecocokan *password* dan *username*

1. Contoh *password* dan *username* yang cocok



2. Contoh *password* dan *username* yang tidak cocok



Kelebihan Program

1. **Kendali utama aktif tidaknya akun berada di pemiliknya.**

Ketika seseorang melakukan pembuatan akun dia akan memiliki sebuah *password* pilihannya untuk *username* tersebut. *Password* tersebut akan digunakan untuk mengaktivasi dan mendeaktivasi penggunaan akun untuk user tersebut. Kelebihan dari adanya kendali utama ini adalah pemilik akun tetap bisa meminjamkan akun yang dia miliki namun tetap memiliki kendali terhadap akun tersebut dan dia tidak perlu membocorakn *password* utama, cukup *password* dinamis yang akan digenerate ketika melakukan aktivasi akun untuk hari tersebut.

2. ***Password* lebih dinamis.**

Password yang digunakan untuk melewati *proxy* adalah *password* dinamis yang dihasilkan dari proses aktivasi akun. Untuk menentukan *password* ini benar atau salah, admin hanya perlu melakukan validasi dengan algoritma RSA berdasarkan *password* utama yang ia pegang (sebagai message yang dienkripsi) dan dengan pasangan kunci publik dan kunci privat yang dimilik *username* dari akun tersebut.

Kekurangan Program dan Penanganan sementara

1. ***Password* terlalu panjang**

- Penganganan sementara
  Password bisa di copy-paste dari program yang ada sehingga pengguna tidak perlu mengingat *password* tersebut. Apabila *password* tersebut akan dipinjamkan bisa diberitahukan melalui messenger atau email dalam kampus.

IV. KESIMPULAN

Penggunaan sistem pengamanan AI3 sekarang dirasa tidak aman karena telah banyak keluhan dan masalah yang diakibatkan oleh lemahnya sistem pengamanan tersebut. Kekurangan dari sistem pengamanan akun AI3 yang ada sekarang adalah hanya ada satu lapis pengamanan dibagian pengguna. Hal ini mengakibatkan apabila *username* dan *password* akun tersebut berhasil di bobol oleh orang lain maka seluruh aspek keamanan dari akun tersebut akan terancam. Berikut merupakan salah satu masalah yang dihadapi berhubungan dengan kekurangan tersebut.

1. Peminjaman akun
2. Pengaksesan akun diluar izin pemilik
3. Pengubahan *password* bukan oleh pemilik

Dengan kata lain, sekali *username* dan *password* diketahui oleh orang lain, besar kemungkinan pengguna asli tidak bisa mengakses akun tersebut lagi. Karena sekali seseorang mengetahui *username* dan *password* akun AI3 dia menjadi berwenang untuk melakukan apapun terhadap akun tersebut, termasuk di dalamnya menghapus, mengganti *username*, mengganti *password*, memblokir akun, dan bahkan mengirimkan email dengan menggunakan *username* pemilik sah.

Algoritma RSA sebagai salah satu algoritma kunci publik bisa membantu permasalahan keamanan ini. Aplikasi yang diajukan memanfaatkan penggunaan algoritma RSA. Permasalahan keamanan yang ada bisa ditanggulangi dengan aplikasi tersebut. Apilkasi ini memiliki dua jenis *password*. Satu *password* untuk melakukan aktivasi akun dan satu *password* untuk melakukan akses internet. Dengan adanya pengamanan yang ganda seperti ini, apabila user ingin berbagi akses dia bisa memberikan *username* dan *password* untuk akses internet tapi tetap menyimpan *username* dan *password* untuk aktivasi akun. Apabila peminjam melakukan peminjaman tanpa diketahui pemilik asli, pemilik asli bisa mengdeaktivasi akun yang dia miliki, mengganti *password* utama, dan mendapatkan *password* untuk akses internet yang baru.

Dengan demikian, pengamanan ganda yang diaplikasikan bisa membuat user berbagi akses dengan orang lain dan tetap memegang kendali utama dari penggunaan akun itu sendiri.

REFERENCES

[1] http://en.wikipedia.org/wiki/RSA diakses tanggal 13 mei 2010, pukul 19.00

[2] http://nic-ng.itb.ac.id/cake/index.php diakses tanggal 13 mei 2010, pukul 19.00

[3] http://www.itb.ac.id/directory/2 diakses tanggal 13 mei 2010, pukul 19.00

[4] http://www.comlabs.itb.ac.id/?p=94 diakses tanggal 13 mei 2010, pukul 19.00

[5] Andy Wicaksono, Prasetyo. "Enkripsi Menggunakan Algoritma RSA",2009, halaman 3-4.

PERNYATAAN

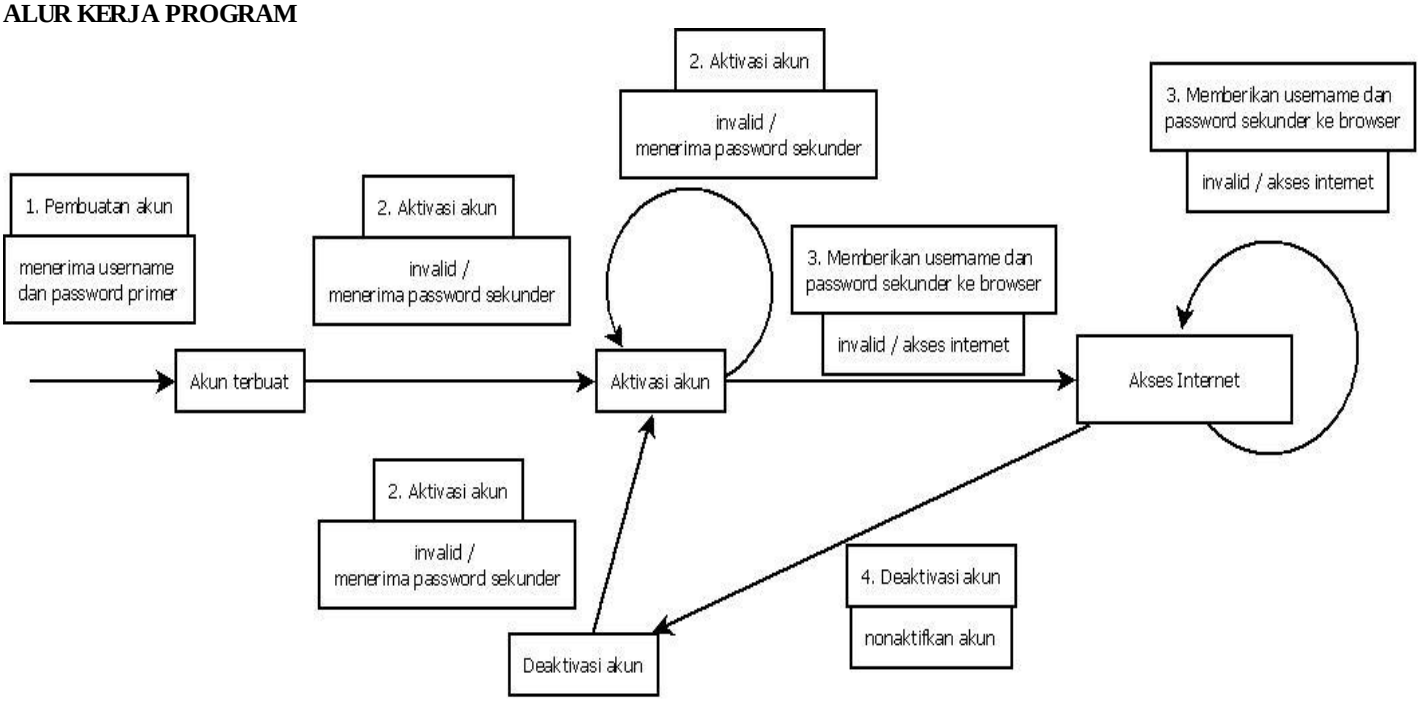
Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Mei 2010

Rizkiana Novitasari

LAMPIRAN

ALUR KERJA PROGRAM



Penjelasan alur kerja

1. Pembuatan akun

Pada pembuatan akun, akan terbentuk *username* dan *password* primer bagi user. Selain itu juga akan terbentuk pasangan kunci publik dan kunci privat antara *username* yang bersangkutan dengan admin. Data-data tersebut akan disimpan di admin dan tidak ada orang lain yang mengetahui. User tidak mengetahui kunci-kunci ini akan tetapi kunci ini bisa diakses user untuk *generate password* sekunder.

2. Aktivasi akun

Pada aktivasi akun, user akan meminta akses internet dengan mengaktifkan akunnya dengan memasukan *username* dan *password* primer, validasi dilakukan di pihak admin dengan memeriksa basis data user. Permintaan akses ini masih secara umum dalam artian user masih harus memberikan *password* sekunder ketika *browser* meminta. *Password* sekinder ini didapatkan ketika aktivasi akun berhasil dan menghasilkan *password* sekunder.

3. Memberikan *username* dan *password* sekunder ke *browser*

User akan memberikan *username* dan *password* sekunder ketika *browser* memintanya. Validasi dari kebenaran

4. Deaktivasi akun