SISTEM KEAMANAN DATA DENGAN METODE CRYPTOGRAPHY

Peniarsih, S.Kom, M.MSi

Abstract

For data protection is important enough there is no other way but to use a special program protection / encryption of data. When this has been a lot of outstanding special program data protection either freeware, shareware, and commercial is very good. In general, these programs not only provide a single method alone, but some kind so that we can choose who we think is the most secure. One method is public key encryption criptography. Cryptography is a science or art of secure messaging and performed by criptographer. Criptography Public Key cryptography is done by combining the two related keys called a key pair of public and private keys. Both keys are created at the same time and relate it mathematically.

Semetrik algorithm is a type of encryption algorithms are the most common. This algorithm is called symmetric because the same key used for encryption and decryption. Unlike the keys used in public key algorithms, symmetric key that is used on keys typically change often. When compared with the public key algorithms, symmetric key algorithms are very fast and therefore are more suitable when used to encrypt the data is very large. Modern cryptographic protocols that incorporate many current public key algorithm with a symmetric algorithm to obtain the advantages of each algorithm.

I. PENDAHULUAN

Kemajuan di bidang teknologi informasi telah memungkinkan institusi-institusi pendidikan atau lainnya melakukan interaksi dengan konsumen melalui jaringan komputer. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan, tetapi khusus dalam tulisan ini penulis akan membahas tentang enkripsi dan keamanan proteksi data dengan metode c*ryptography*.

Saat ini telah banyak beredar program khusus proteksi data baik freeware, shareware, maupun komersial yang sangat baik. Pada umumnya program tersebut tidak hanya menyediakan satu metoda saja, tetapi beberapa jenis sehingga kita dapat memilih yang menurut kita paling aman. Salah satu metode enkripsi adalah *criptography*. Sampai saat ini penulis memperhatikan telah banyak program proteksi data yang telah diterbitkan pada majalah Mikrodata ataupun Antivirus, tetapi jarang sekali yang cukup baik sehingga dapat dipercaya untuk melindungi data yang cukup penting.

Dari pengamatan penulis kekuatan dari metoda-metoda enkripsi adalah pada kunci (dari password yang kita masukkan) sehingga walaupun algoritma metoda tersebut telah tersebar luas orang tidak akan dapat membongkar data tanpa kunci yang tepat. Walaupun tentunya untuk menemukan metoda tersebut diperlukan teori matematika dan data statistika yang cukup rumit. Tetapi intinya disini ialah bagaimana kita mengimplementasikan metoda-metoda yang telah diakui keampuhannya tersebut didalam aplikasi kita sehingga dapat meningkatkan keamanan dari aplikasi yang kita buat.

II. TINJAUAN PUSTAKA

SISTEM KEAMANAN DATA

Keamanan merupakan komponen yang vital dalam komunikasi data elektronis. Masih banyak yang belum menyadari bahwa keamanan (security) merupakan sebuah komponen penting yang tidak murah. Teknologi kriptografi sangat berperan juga dalam proses komunikasi, yang digunakan untuk melakukan enkripsi (pengacakan) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan juga melakukan dekripsi (menyusun kembali) data yang telah teracak

tersebut. Berbagai sistem yang telah dikembangkan adalah seperti sistem private key dan public key. Penguasaan algoritma-algoritma populer digunakan untuk mengamankan data juga sangat penting. Contoh – contoh algoritma ini antara lain : DES, IDEA, RC5, RSA, dan ECC (*Elliptic Curve Cryptography*). Penelitian dalam bidang ini di perguruan tinggi merupakan suatu hal yang penting.

Bagi institusi-institusi atau pengguna lainnya, sarana komunikasi data elektronis memunculkan masalah baru, yaitu keamanan. Sistem autentikasi (bukti diri) konvensional dengan KTP, SIM, dsb. yang bersandar pada keunikan tanda tangan tidak berlaku untuk komunikasi elektronis. Pengewalan satpam tidak lagi bisa membantu keamanan kiriman dokumen. Komunikasi data elektronis memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi konvensional.

Dari sisi tindakan pihak yang bertanggung jawab, keamanan jaringan komputer terbagi dua level: 1. keamanan fisik peralatan mulai dari server, terminal/client router sampai dengan cabling; 2. keamanan sistem sekiranya ada penyelindup yang berhasil mendapatkan akses ke saluran fisik jaringan komputer. Sebagai contoh, dalam sistem mainframe-dumb-terminal di suatu gedung perkantoran, mulai dari komputer sentral sampai ke terminal secara fisik keamanan peralatan dikontrol penuh oleh otoritas sentral. Manakala sistem tersebut hendak diperpanjang sampai ke kantor-kantor cabang di luar gedung, maka sedikit banyak harus menggunakan komponen jaringan komputer yang tidak sepenuhnya dikuasai pemilik sistem seperti menyewa kabel leased-line atau menggunakan jasa komunikasi satelit.

Dari sisi pemakaian, sistem keamanan dipasang untuk mencegah: 1. pencurian, 2. kerusakan, 3 penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringan komputer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik namun kerusakan tetap bisa terjadi karena bug pada program aplikasi atau ada unsur kesengajaan yang mengarah ke penyalahgunaan sistem.

Di institusi pendidikan, selain kepentingan administratif sebagaimana di institusi-institusi lainnya, jaringan komputer Internet khususnya dapat digunakan untuk berinteraksi dengan konsumen (siswa). Pada umumnya, institusi pendidikan tidak menyelenggarakan pelayanan jasa yang ketat seperti penyelenggaraan bank atau asuransi. Namun demikian, dalam sistem terpadu, beberapa komponen bisa bersifat kritis seperti komunikasi data pembayaran SPP dan menyentuh rahasia pribadi seperti penggunaan email untuk konsultasi bimbingan dan penyuluhan. Untuk masalah pembayaan SPP, yang penting adalah akurasi data dan pada dasarnya daftar pembayar SPP tidak perlu disembunyikan karena pada akhirnya semua siswa membayar SPP. Untuk konsultasi psikologis sebaiknya memang hanya siswa dan pembibing saja yang bisa membaca teks komunikasi bahkan administrator jaringan pun harus dibuat tidak bisa membaca electronic-mail.

KRIPTOGRAFI

Pengertian Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata Crypto dan Graphia yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

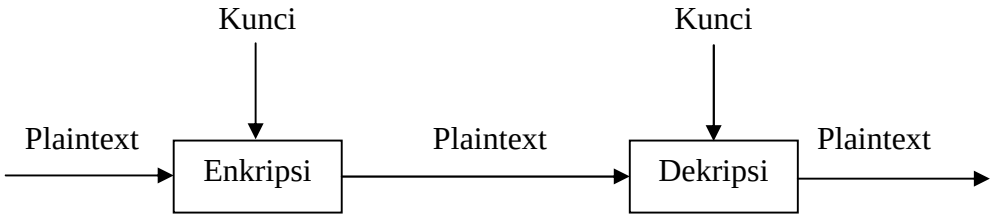
Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher

adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut *encryption* atau *encipherment*. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut *decryption* atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :



Gambar 1. Proses Enkripsi/Dekripsi Sederhana

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer*. Sedang, *cryptanalysis* adalah suatu ilmu dan seni membuka (breaking) ciphertext dan orang yang melakukannya disebut *cryptanalyst*.

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan.

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Dekripsi)

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila seseorang mengetahui algoritma yang kita gunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan.

Algoritma Kriptografi

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

a. Symmetric Algorithms

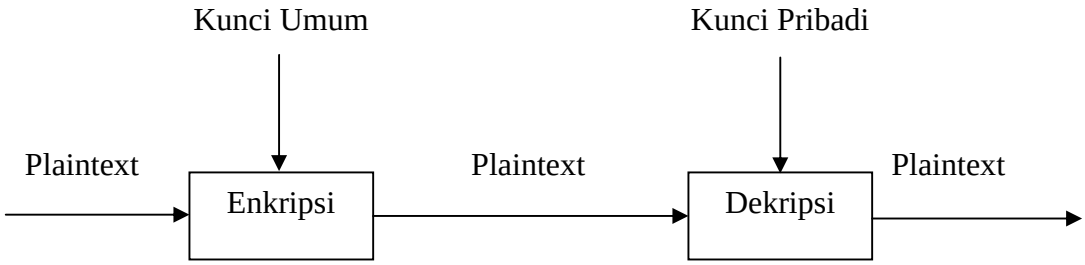
Algoritma kriptografi simeteris atau disebut juga algoritma kriptografi konvensioanl adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.

Algoritma kriptografi simeteris dibagi menajdi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Contoh algoritma kunci simetris yang terkenal adalah DES (*Data Encryption Standard*).

b. Asymmetric Algorithms

Algoritma kriptografi nirsimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (*public key algorithm*) karena kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya

diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA dan ECC.



Gambar 2. Proses Enkripsi/Dekripsi Public Key Cryptography

Algoritma RSA :

Key generation :

1. Hasilkan dua buah integer prima besar, p dan q
   Untuk memperoleh tingkat keamanan yang tinggi pilih p dan q
   yang berukuran besar, misalnya 1024 bit.
2. Hitung m = (p-1)*(q-1)
3. Hitung n = p*q
4. Pilih d yg relatively prime terhadap m
   e relatively prime thd m artinya faktor pembagi terbesar keduanya
   adalah 1, secara matematis disebut gcd(e,m) = 1. Untuk mencarinya
   dapat digunakan algoritma Euclid.
5. Cari d, sehingga e*d = 1 mod (m), atau d = (1+nm)/e
   Untuk bilangan besar, dapat digunakan algoritma extended Euclid.
6. Kunci publik : e, n
   Kunci private : d, n

Public key encryption

B mengenkripsi message M untuk A

Yg harus dilakukan B :
1. Ambil kunci publik A yg otentik (n, e)
2. Representasikan message sbg integer M dalam interval [0,n-1]
3. Hitung C = M ^ e (mod n)
4. Kirim C ke A

Untuk mendekripsi, A melakukan :
Gunakan kunci pribadi d untuk menghasilkan M = C^(d) (mod n)

Contoh Penerapan :

Misalkan :
Di sini saya pilih bilangan yg kecil agar memudahkan perhitungan, namun dalam aplikasi nyata pilih bilangan prima besar untuk meningkatkan keamanan.

p = 3
q = 11

n = 3 * 11 = 33
m = (3-1) * (11-1) = 20

e = 2 => gcd(e, 20) = 2
e = 3 => gcd(e, 20) = 1 (yes)

n = 0 => e = 1 / 3
n = 1 => e = 21 / 3 = 7 (yes)

Public key : (3, 33)
Private key : (7, 33)

Let's check the math using numbers
---

* Try encryption : message "2"

C = 2 ^ 3 (mod 33)
= 8
Try to decrypt : ciphertext "8"

M = 8 ^ 7 (mod 33)
= 2097152 (mod 33)
= 2

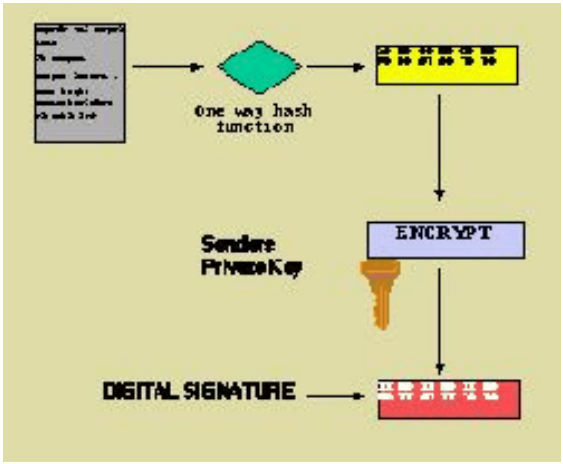
** Encrypt : message " " (ASCII=20)
C = 20 ^ 3 (mod 33)
= 8000 (mod 33)
= 14

Decrypt : ciphertext 32

M = 14 ^ 7 (mod 33)
= 105413504 (mod 33)
= 20

Tanda Tangan Digital

Penandatanganan digital terhadap suatu dokumen adalah sidik jari dari dokumen tersebut beserta *timestamp*-nya dienkripsi dengan menggunakan kunci privat pihak yang menandatangani. Tanda tangan digital memanfaatkan fungsi *hash* satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan.



Gambar 3. Tanda tangan digital

Sertifikat Digital

Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan *hash* dari suatu informasi rahasia yang ditandatangani oleh suatu pihak terpercaya. Sertifikat digital tersebut ditandatangani oleh sebuah pihak yang dipercaya yaitu *Certificate Authority* (CA).

Secure Socket Layer (SSL)

SSL dapat menjaga kerahasiaan (*confidentiality*) dari informasi yang dikirim karena menggunakan teknologi enkripsi yang maju dan dapat di-*update* jika ada teknologi baru yang lebih bagus. Dengan penggunaan sertifikat digital, SSL menyediakan otentikasi yang transparan antara *client* dengan *server*. SSL menggunakan algoritma RSA untuk membuat tanda tangan digital (*digital signature*) dan amplop digital (*digital envelope*). Selain itu, untuk melakukan enkripsi dan dekripsi data setelah koneksi dilakukan, SSL menggunakan RC4 sebagai algoritma standar untuk enkripsi kunci simetri.

Saat aplikasi menggunakan SSL, sebenarnya terjadi dua sesi, yakni sesi *handshake* dan sesi pertukaran informasi.

Biasanya, *browser-browser* seperti Netscape Navigator atau Microsoft Internet Explorer sudah menyertakan sertifikat digital dari CA utama yang terkenal, sehingga memudahkan pemeriksaan sertifikat digital pada koneksi SSL.Penyertaan serfikat digital CA utama pada *browser* akan menghindarkan *client* dari pemalsuan sertifikat CA utama.

Public Key Cryptography

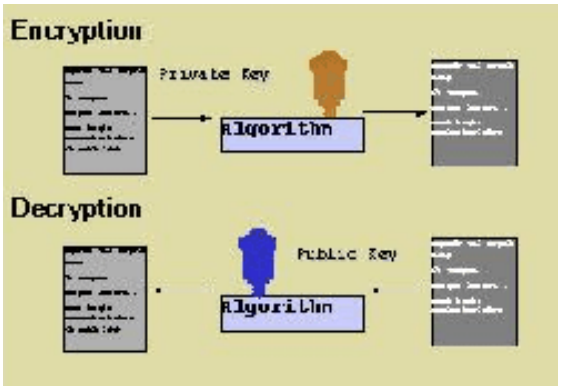
Public key cryptography (lawan dari *symmetric key cryptography*) bekerja berdasarkan fungsi satu arah. Fungsi yang dapat dengan mudah dikalkulasi akan tetapi sangat sulit untuk dibalik/*invers* atau *reverse* tanpa informasi yang mendetail. Salah satu contoh adalah faktorisasi; biasanya akan sulit untuk memfaktorkan bilangan yang besar, akan tetapi mudah untuk melakukan faktorisasi. Contohnya, akan sangat sulit untuk memfaktorkan 4399 daripada memverifikasi bahwa 53 x 83 = 4399. *Public key cryptography* menggunakan sifat-sifat asimetrik ini untuk membuat fungsi satu arah, sebuah fungsi dimana semua orang dapat melakukan satu operasi (enkripsi atau verifikasi sign) akan tetapi sangat sulit untuk menginvers operasi (dekripsi atau membuat sign) tanpa informasi yang selengkap-lengkapnya.

Public key cryptography dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang berhubungan yang kita sebut sebagai pasangan kunci publik dan kunci privat. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan berhubungan secara matematis. Secara matematis, kunci privat dibutuhkan untuk melakukan operasi invers terhadap kunci public dan kunci publik dibutuhkan untuk melakukan operasi invers

terhadap operasi yang dilakukan oleh kunci privat.

Jika kunci publik didistribusikan secara luas, dan kunci privat disimpan di tempat yang tersembunyi maka akan diperoleh fungsi dari banyak ke satu. Semua orang dapat menggunakan kunci publik untuk melakukan operasi kriptografi akan tetapi hanya orang yang memegang kunci privat yang dapat melakukan invers terhadap data yang telah terenkripsi tersebut. Selain itu dapat juga diperoleh fungsi dari satu ke banyak, yaitu pada saat orang yang memegang kunci privat melakukan operasi enkripsi maka semua orang yang memiliki kunci publik dapat melakukan invers terhadap data hasil enkripsi tersebut.

Algoritma *Public Key Cryptography*
Sistem kriptografi asimetris menggunakan dua buah key, yaitu public key dan private key.
Salah satu key akan diberi tahu kepada publik.



Gambar 4. Kriptografi asimetris

Matematika merupakan perangkat bantu analisis dalam masalah sekuriti. Sebagai contoh berikut ini adalah penulisan protokol SSL yang memungkinkan pertukaran session key antara Web server dan client. Pada versi SSL protokol tersebut dilaksanakan dengan cara berikut ini:

- Pada pesan pertama mengirimkan session key ke server dengan menggunakan publik key .
- Kemudian akan menghasilkan ``tantangan'' (challenge)
- akan melakukan ``sign'' dan akan mengirimkan kembali ke dengan sertifikat

Versi SSL di atas tidak memiliki otentikasi client seperti yang diharapkan. Sehingga dapat menimbulkan suatu ``attaclk''. Perbaikan dari masalah ini dilakukan dengan mengubah tahapan ke tiga menjadi :
Dalam bahasan ini tidak dibahas lebih dalam lagi mengenai pemanfaatan matematika dalam sekuriti, karena sudah merupakan suatu syarat mutlak yang lazim diketahui.
Dalam mendisain sekuriti dapat dipakai 5 tahapan dasar berikut ini :

1. Pada aplikasi yang bersangkutan, apakah mekanisme proteksi difokuskan, apakah pada data, operasi, atau pengguna
2. Pada layer manakahdari sistem komputer mekanisme sekuriti akan ditempatkan ?
3. Mana yang lebih diinginkan kesederhanaan dan jaminan tinggi atau pada sistem yang memiliki feature yang kaya.
4. Apakah tugas untuk mendefinisikan dan mengerapkan security harus diberikan pada badan terpusat atau diberikan pada masing-masing individu pada suatu sistem ?
5. Bagaimana dapat melindungi dari penyerang yang ingin meperoleh akses pada sistem yang dilindungi mekanisme proteksi ?

Asimetrik kriptografi digunakan dalam public key kriptografi. Ada 2 key, private dan public key. Private key disimpan sendiri, dan publik key didistribusikan. Bila publik key digunakan untuk menenkripsi maka hanya private key yang dapat mendekripsi. Begitu juga sebaliknya.

Key yang digunakan pada sistem kriptografi memegang peran yang sangat penting.

- Pseudo random number
- Panjangnya key, semakin panjang semakin aman. Tetapi perlu diingat bahwa membandingkan dua buah sistem kriptografi yang berbeda dengan berdasarkan panjang keynya saja tidaklah cukup.
- Private key harus disimpan secara aman baik dalam file (dengan PIN atau passphrase) atau dengan smart card.
  Untuk menyusun strategi sekuriti yang baik perlu difiikrikan pertimbangan dasar berikuti ini :
- Kemungkinan dipenuhinya (ekonomis dan pertimbangan waktu)
- Apakah sistem tetap dapat difungsikan

- Kesesuaian kultur
- Hukum setempat yang berlaku

Matematika merupakan perangkat bantu analisis dan sintesis dalam masalah sekuriti. Sebagai contoh berikut ini adalah penulisan protokol SSL yang memungkinkan pertukaran session key antara Web server dan client.

III. SPESIFIKASI RANCANGAN SISTEM

3.1. Keuntungan *Public Key Cryptography*

Pada algoritma public key ini, semua orang dapat mengenkripsi data dengan memakai public key penerima yang telah diketahui secara umum. Akan tetapi data yang telah terenkripsi tersebut hanya dapat didekripsi dengan menggunakan private key yang hanya diketahui oleh penerima.

3.2. Pemilihan Sistem dan Algoritma

Pendekatan multidimensi dalam desain dan implementasi sekuriti saat ini sudah tak dapat ditawar lagi. Sebaliknya pendekatan tradisonal mulai ditinggalkan. Pendekatan multidimensi mencakup keseluruhan sumber daya, policy, dan mekanisme sekuriti yang komprehensif. Kunci dalam pelaksanaan sistem sekuriti model ini harus melibatkan keseluruhan staf dari semua jajaran dan area yang ada dalam organisasi tersebut. Tanpa pemahaman yang cukup dan kerjasama dari semua pihak maka mekanisme sekuriti tersebut tidak dapat dilaksanakan dengan baik.

Untuk mendapatkan pertahanan yang kuat diperlukan sistem pertahanan bertingkat yang melibatkan policy dan teknologi. Secara konseptual pertahanan dapat dibagi menjadi tiga tingkat :

- **Perimeter**
  Pertahanan yang terletak paling luar adalah perimeter dimana terdapat mekanisme firewall, mekanisme akses kontrol, proses autentikasi user yang memadai, VPN (virtual private network), enkripsi, antivirus, network screening software, real time audit, intrusion detection system, dan lain-lain. Pada tingkat pertahanan ini terdapat alarm yang akan menyala apabila terjadi serangan terhadap sistem
- **Servers**
  Server merupakan entry-point dari setiap layanan. Hampir semua layanan, data, dan pengolahan informasi dilakukan di dalam server. Server memerlukan penanganan sekuriti yang komprehensif dan mekanisme administrasi yang tepat. Diantaranya adalah melakukan pemeriksaan, update patch, dan audit log yang berkala
- **Desktops**
  Desktop merupakan tempat akses pengguna ke dalam sistem. Pengalaman telah menunjukkan bahwa kelemahan sekuriti terbesar ada pada tingkat desktop karena pengguna dengan tingkat pemahaman sekuriti yang rendah dapat membuat lobang sekuriti seperti menjalankan email bervirus, mendownload file bervirus, meninggalkan sesi kerja di desktop, dan lain-lain.

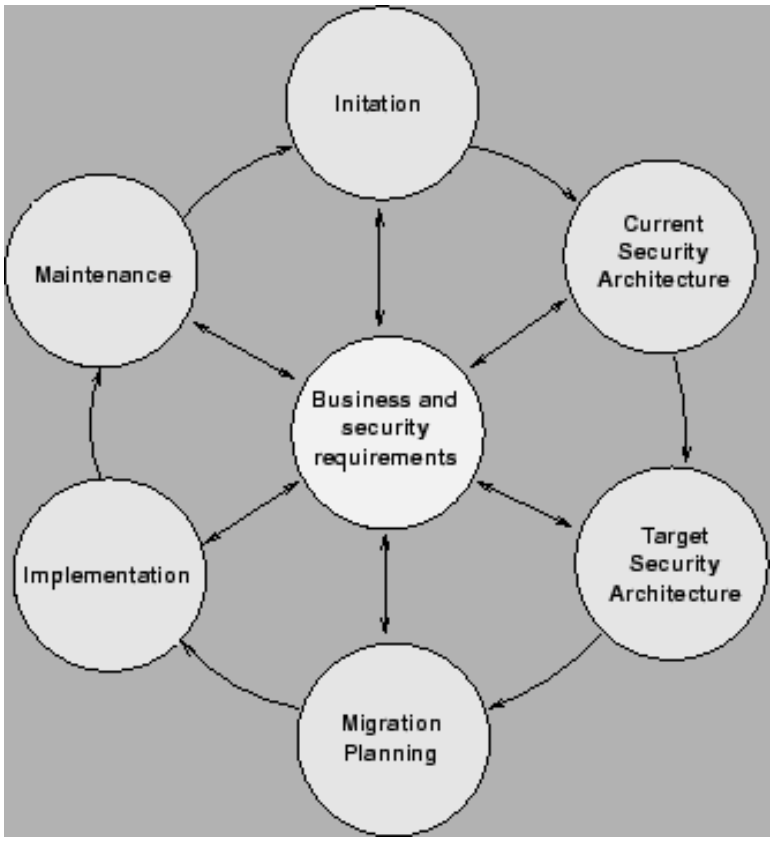
3.3. Sekuritas

3.3.1. Tahapan Desain Sekuriti

Sekuriti adalah proses tahap demi tahap, teknis, bisnis, dan manajemen. Oleh karena itu diperlukan langkah-langkah yang tepat sebagai strategi implementasi sekuriti secara menyeluruh dan komprehensif.

- **Inisialisasi**
  Objektif dari tahap ini adalah mendefinisikan kebutuhan yang relevan dan dapat diaplikasikan dalam evolusi arsitektur sekuriti. Dalam tahap ini perlu adanya edukasi dan penyebaran informasi yang memadai untuk mempersiapkan seluruh jajaran staf dan manajemen.
- **Mendefinisikan system sekuriti awal**
  Objektif dari tahap ini adalah mendefinisikan status system sekuriti awal, mendokumentasi, melakukan analisa resiko, dan mencanangkan perubahan yang relevan dari hasil analisa resiko.
- **Mendefinisikan arsitektur sekuriti yang diharapkan**
  Objektif dari tahap ini adalah mendefinisikan arsitektur sekuriti baru berdasarkan hasil analisa resiko dan prediksi terhadap kemungkinan terburuk. Dalam tahap ini dibentuk juga model dari sub-arsitektur lainnya yang hendak dibangun dan mempengaruhi sistem sekuriti secara keseluruhan.

- **Merencanakan pengemba-ngan dan perubahan**
  Melakukan perubahan dalam suatu organisasi bukan merupakan hal yang mudah, termasuk dalam merubah sistem sekuriti yang sedang berjalan, karena secara langsung maupun tidak langsung akan mempengaruhi proses-proses lain yang sedang berjalan. Objektif dari tahap ini adalah membuat rencana pengembangan yang komprehensif dengan memperhatikan semua aspek dan mempunyai kekuatan legal yang kuat. Rencana tersebut diharapkan dapat secara fleksibel mengadopsi feedback yang mungkin muncul pada masa pengembangan.
- **Implementasi**
  Objektif dari tahap ini adalah mengeksekusi rencana pengembangan tersebut. Termasuk dalam proses ini adalah memasukkan arsitektur sekuriti ke dalam pengambilan keputusan di tingkat manajerial dan melakukan adjustment akibat dari feedback.
- **Maintenance**
  Sekuriti adalah hal yang sangat dinamik dan ditambah pula dengan perubahan-perubahan teknologi yang cepat. Hal ini memerlukan proses pemeliharaan (maintenance) untuk beradaptasi kepada semua perubahan-perubahan yang terjadi sehingga dapat mengantisipasi terjadinya kelemahan pada sekuriti.



Gambar 5. Pendekatan implementasi sekuriti

Tindakan responsif

Jika alarm tanda bahaya berbunyi, sederetan tindakan responsif harus dilakukan segera mungkin. Dalam kegiatan ini termasuk pemanfaatan teknik forensik digital. Mekanisme ini dapat meresponse dan mengembalikan sistem pada state dimana security incidents belum terjadi. Tindakan responsif meliputi :

- Prosedur standar dalam menghadapi security incidents.
- Mekanisme respon yang cepat ketika terjadi incidents
- Disaster Recovery Plan (DRP), termasuk juga dilakukannya proses auditing.
- Prosedur untuk melakukan forensik dan audit terhadap bukti security

incidents. Untuk informasi sensitif (misal log file, password file dan sebagainya), diterapkan mekanisme *two-person rule* yaitu harus minimum 2 orang yang terpisah dan berkualifikasi dapat melakukan perubahan.

- ❖ Prosedur hukum jika security incidents menimbulkan adanya konflik/dispute
- ❖ Penjejakan paket ke arah jaringan di atas (upstream).

3.3.2. Prinsip disain teknologi

Prinsip utama dalam mendisain sistem sekuriti telah dipublikasikan oleh Jerome Saltzer dan MD. Schroeder sejak tahun 1975. Prinsip ini hingga kini tetap dapat berlaku, yaitu :

- **Hak terendah mungkin (least priviledge)**.
  Setiap pengguna atau proses, harus hanya memiliki hak yang memang benar-benar dibutuhkan. Hal ini akan mencegah kerusakan yang dapat ditimbulkan oleh penyerang. Hak akses harus secara eksplisit diminta, ketimbang secara default diberikan.

- **Mekanisme yang ekonomis**.
  Disain sistem harus kecil, dan sederhana sehingga dapat diverifikasi dan diimplementasi dengan benar. Untuk itu perlu dipertimbangkan juga bagaimana cara verifikasi terhadap sistem pembangun yang digunakan. Pada beberapa standard sekuriti untuk aplikasi perbankan , keberadaan source code menjadi syarat dalam verifikasi.

- **Perantaraan yang lengkap**.
  Setiap akses harus diuji untuk otorisasi yang tepat

- **Disain terbuka**.
  Sekuriti harus didisain dengan asumsi yang tak bergantung pada pengabaian dari penyerang. Desain sistem harus bersifat terbuka, artinya jika memiliki *source code* maka kode tersebut harus dibuka, sehingga meminimalkan kemungkinan adanya *backdoor* (celah keamanan) dalam sistem.

- **Pemisahan hak akses (previledge)**
  Bila mungkin, akses ke resource sistem harus bergantung pada lebih dari satu persyaratan yang harus dipenuhi. Model sekuriti yang memisahkan tingkat pengguna akan lebih baik.

- **Mekanisme kesamaan terendah**
  User harus terpisahkan satu dengan yang lainnya pada sistem.

- **Penerimaan psikologi**.
  Pengendalian sekuriti harus mudah digunakan oleh pemakai sehingga mereka akan menggunakan dan tidak mengabaikannya. Sudah saatnya disainer memikirkan perilaku pengguna.

3.3.3. Strategi dalam implementasi

Untuk menerapkan sekuriti, berbagai pihak pada dasarnya menggunakan pendekatan berikut ini :

- **Tanpa sekuriti**. Banyak orang tidak melakukan apa-apa yang berkaitan dengan sekuriti, dengan kata lain hanya menerapkan sekuriti minimal (out of the box, by default) yang disediakan oleh vendor. Jelas hal ini kuranglah baik.

- ***"Security through obscurity"*** (security dengan cara penyembunyian) Pada pendekatan ini sistem diasumsikan akan lebih aman bila tak ada orang yang tahu mengenai sistem itu, misal keberadaannya, isinya, dan sebagainya. Sayangnya hal tersebut kurang berarti di Internet, sekali suatu situs terkoneksi ke Internet dengan cepat keberadaanya segera diketahui. Ada juga yang berkeyakinan bahwa dengan menggunakan sistem yan tak diketahui oleh umum maka dia akan memperoleh sistem yang lebih aman.

- **Host security.** Pada pendekatan ini, maka tiap host pada sistem akan dibuat secure. Permasalahan dari pendekatan ini adalah kompleksitas. Saat ini relatif pada suatu organisasi besar memiliki sistem ang heterogen. Sehingga proses menjadikan tiap host menjadi secure sangatlah kompleks. Pendekatan ini cocok untuk kantor yang memiliki jumlah host yang sedikit.

- **Network security**. Ketika sistem bertambah besar, maka menjaga keamanan dengan memeriksa host demi host yang ada di sistem menjadi tidak praktis. Dengan pendekatan sekuriti jaringan, maka usaha dikonsentrasikan dengan mengontrol akses ke jaringan pada sistem.

Tetapi dengan bertambah besar dan terdistribusinya sistem komputer yang dimiliki suatu organisasi maka pendekatan tersebut tidaklah mencukupi. Sehingga perlu digunakan pendekatan sistem sekuriti yang berlapis. Yang perlu diingat, adalah kenyataan bahwa tak ada satu model pun yang dapat memenuhi semua kebutuhan dari sekuriti sistem yang kita inginkan. Sehingga kombinasi dari berbagi pendekatan perlu dilakukan.

3.3.4. Disain sistem dari sisi user

Orang/pengguna merupakan sisi terlemah dari sekuriti. Mereka tak memahami komputer, mereka percaya apa yang disebutkan komputer. Mereka tak memahami resiko. Mereka tak mengetahui ancaman yang ada. Orang menginginkan sistem yang aman tetapi mereka tak mau melihat bagaimana kerja sistem tersebut. Pengguna tak memiliki ide, apakah situs yang dimasukinya situs yang bisa dipercaya atau tidak.

Di samping itu, akibat pengabaian para pendisain sistem terhadap perilaku user dalam berinteraksi terhadap sistem, maka timbul kesalahan misalnya adanya pengetatan yang tak perlu, yang malah mengakibatkan user mengabaikan pengetatan itu. Atau penyesuaian kecil yang seharusnya bisa dilakukan untuk menambah keamanan, tetapi tak dilakukan. Sebagai contoh *layout page* tidak pernah mempertimbangkan sisi sekuriti, ataupun belum ada desain layout yang meningkatkan kewaspadaan pengguna akan keamanan. Disan halaman Web lebih ditekankan pada sisi estetika belaka. Untuk itu sebaiknya dalam disain sistem, user diasumsikan sebagai pihak yang memiliki kewaspadaan terendah, yang mudah melakukan kesalahan. Artinya pihak perancanglah yang mencoba menutupi, atau memaksa si user menjadi waspada.
Beberapa langkah yang perlu dilakukan oleh penyedia layanan dalam merancang sistem yang berkaitan dengan sisi pengguna adalah :

- **Sekuriti perlu menjadi pertimbangan yang penting dari disain sistem** . Memberikan umpan balik pada mekanisme sekuriti akan meningkatkan pemahaman user terhadap mekanisme sekuriti ini.

- **Menginformasikan user tentang ancaman potensial pada sistem** . Kepedulian akan ancaman ini akan mengurangi ketakpedulian pengguna terhadap ditail langkah transaksi yang dilakukan. Memang para pengguna Internet di Indonesia kebanyakan memiliki kendala dalam hal **bahasa** . Sehingga mereka sering melewati dan tak membaca pesan yang tampil di layar. Hal ini menuntut Semakin perlunya menu dan keterangan berbahasa Indonesia pada.

- **Kepedulian user perlu selalu dipelihara**
  Secara rutin penyedia layanan harus memberikan jawaban terhadap pertanyaaan masalah sekuriti, baik yang secara langsung maupun tidak

- **Berikan user panduan tentang sekuriti sistem** , **termasuk langkah-langkah yang sensitif.**
  Sebaiknya ketika user baru memulai menggunakan suatu layanan, mereka telah di-"paksa" untuk membaca petunjuk ini terlebih dahulu.

IV. PENUTUP

Kesimpulan dan Saran

A. Kesimpulan

1. Pendekatan multidimensi dalam desain dan implementasi sekuriti mencakup keseluruhan sumber daya, policy, dan mekanisme sekuriti yang komprehensif.
2. Public Key Criptography dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang berhubungan yang disebut sebagai pasangan kunci public dan kunci privat.
3. Protokol kriptografi modern pada saat ini banyak yang menggabungkan algoritma kunci publik dengan algoritma simetrik untuk memperoleh keunggulan-

keunggulan pada masing-masing algoritma.

B. Saran

1. Dalam mendisain sekuriti hendaknya mengikuti tahapan-tahapan dasar yang benar.
2. Dalam mendisain sekuriti hendaknya dilakukan pemilihan algoritma yang sesuai.
3. Gunakan kunci / password yang baik dan benar agar tidak dapat dideteksi oleh orang yang tidak bertangung jawab.
4. Biasakan menggunakan kata kunci yang bercampur dengan character dan numeric karena akan sangat sulit melacaknya.

DAFTAR PUSTAKA

1. http://www.tedi-h.com/papers/p kripto.html, Tedi Hariyanto, "Pengenalan Kriptografi", edisi Juni 1999.
2. http://www.budi.insan.co.id/courses/el695
3. http://www.criptography.com
4. http://www.infokomputer.com/arsip/internet/0698/cakra/cakrawa1.shtml Budi Sukmawan, "Keamanan Data dan Metode Enkripsi", edisi Jan. 1998.
5. http://www.ilmukomputer.com/populer/afs/afs-security.pdf, Phil Zimmerman,"Sekilas Tentang Enkripsi",NeoTek, April 2002.
6. Budi Raharjo, " Keamanan system informasi Berbasis Internet " PT Insan Infonesia – Bandung & PT INDOCISC – Jakarta, 2002
7. http://www.tedi-h.com/papers/p kripto.html
8. http://www.budi.insan.co.id/courses/el695
9. http://www.criptography.com