Artikel oleh TIM PANDU **Kategori : Security**

Navigasi

Ke halaman utama
Ke daftar artikel

Public Key Infrastructure dan Open Source

Avinanta Tarigan, SKom[1] - I Made Wiryana, SSi, SKom, MSc[2]

Ringkasan:

Sekuriti sering dipandang hanyalah merupakan masalah teknis yang melibatkan bisa atau tidak tertembusnya suatu sistem, Pada pandangan makro sekuriti sendiri memiliki konsep yang lebih luas,yang berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnnya. Open Source menyediakan keamanan tidak melalui ketertutupan mekanisme tetapi melalui keterbukaan mekanisme pengujian. Di samping itu memungkinkan dikembangkannya produk sekuriti yang tak menimbulkan ketergantungan pada negara lain.

Tulisan ini dipaparkan pada seminar **Secure Your Future**, di Kampus Trisakti, 19 Oktober 2000.

Daftar Isi

1 Konsep security

Security is a process not a product .....

Internet awalnya dikembangkan untuk menghubungkan antar pihak yang saling dipercaya dengan tujuan saling bertukar menukar informasi. Walau merupakan proyek Departemen Pertahanan Amerika, Internet digunakan dan dikembangkan untuk tujuan kolaborasi dunia akademi yang serba terbuka. Sehingga pada awal perkembangannya masalah privacy bukanlah merupakan hal yang besar. Bahkan pada era awal Internet, sering dengan sengaja orang memberikan informasi pribadinya kepada rekan kerjanya di benua lain. Saat itu pengguna sering memberikan informasi mengenai dirinya melalui file `.plan` ataupun `.project`. Juga melalui informasi yang didapat dari jasa `finger` yang dapat melaporkan apakah seseorang sudah membaca email atau sudah login ke mesinnya. Semuanya hanya bertujuan rekan kerjanya dapat mengetahui dengan mudah mengenai dirinya.

Perkembangan internet begitu pesat dan kini telah menjadi suatu jaringan raksasa yang saling menghubungkan berbagai jaringan. Pemanfaatannya di bidang bisnis menjadikan terjadinya pergeseran model. Dari bentukan komunitas pengguna internet yang cenderung berupa suatu *Gemainschaft* dengan norma internal dan tradisi yang diatur berdasarkan status dan didorong oleh kecintaan, kewajiban serta kesamaan pemahaman dan tujuan, sekarang telah bergeser dan cenderung menjadi suatu *Gesselschaft* yang terdiri dari individu (organisasi) yang memiliki interest masing-masing yang saling berkompetisi untuk kepentingan material sehingga berbentuk pasar bebas.

Pada bentuk pertama bisa dikatakan tak ada batasan antara privat dan publik, sedang pada yang kedua terjadi perbedaan secara jelas. Dengan adanya pergeseran tersebut dan makin banyaknya penggunaan eCommerce kebutuhan akan sekuriti mulai tampak dengan jelas. Banyak perusahaan yang awalnya menganggap remeh masalah ini akhirnya mengalami kerugian yang besar akibat kelalaian ini.

Sekuriti komputer juga sudah sering dimanfaatkan untuk sarana iklan yang seringkali memakan korban akibat kurangya pemahaman pengguna. Pertama adalah issue firewall, lalu sistem deteksi intrusi, kemudian Virtual Private Network (VPN), dan yang sekarang sering digunakan dalam produk yang berkaitan dengan sekuriti adalah Certificate Authority (CA) dan Public Key Infrastructure (PKI). Sehingga sering digunakan sebagai peralatan marketing yang berujung pada pernyataan untuk membujuk pembeli :

> ‘‘*Bila anda membeli produk A maka anda akan aman*’’.

Tetapi kenyataannya tak seindah itu, terutama dalam era Internet yang serba cepat ini. (Schneier, 1999). Sekuriti terbentuk dari suatu mata rantai yang akan memiliki kekuatan sama dengan mata rantai yang terlemah. Sistem sekuriti berbasiskan CA akan memiliki rantai yang tak seluruhnya hanya merupakakn sistem kriptografi. Manusia akan banyak terlibat,

Sekuriti komputer memiliki definisi yang beragam, sebagai contoh berikut ini adalah definisi sekuriti komputer yang sering digunakan (Gollmann, 1999) :

Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

Tetapi dengan makin pentingnya eCommerce dan Internet, maka masalah sekuriti tidak lagi sekedar masalah keamanan data belaka. Berikut ini dikutipkan salah satu pernyataan Erkki Liikanen Commissioner for Enterprise and Information Society European Commission yang disampaikan pada **Information Security Solutions Europe** (ISSE 99), Berlin 14 October 1999. Berikut ini adalah cuplikan utama :

1. *Security is the key to securing users trust and confidence, and thus to ensuring the further take-up of the Internet. This can only be achieved if security features are incorporated in Internet services and if users have sufficient safety guarantees*

2. *Securing the Internal Market is crucial to the further development of the European security market, and thus of the European cryptographic industry.This requires an evolution of mentalities: Regulation in this field transcends national borders. Let's "think European".*

3. *European governments and the Commission now have a converging view on confidentiality. We see this in Council, in Member State policies and in the constructive discussions we have. We must take this debate further and focus of the potential of encryption to protect public security rather than mainly seeing it as a threat to public order.*

4. *Finally, **the promotion of open source** systems in conjunction with technology development is certainly one important step towards unlocking the potential of the desktop security market for the European cryptographic industry.*

Jadi masalah sekuriti pada infrastruktur eCommerce dan Internet tidak saja terletak pada masalah teknologi dan ekonomi saja, tetapi juga menyangkut dengan keamanan suatu negara atau ketergantungan negara terhadap negara lain. Bukan saja sistem sekuriti dengan teknologi yang aman, tetapi juga pertimbangan bahwa pemanfaatan suatu teknologi tidak dibatasi oleh negera lain. Sebagai contoh USA dengan ITAR-nya membatasi pemanfaatan jenis teknologi kriptografi tertentu.

Pada prakteknya suatu pembentukan sistem yang aman akan mencoba melindungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain terhadap kita antara lain :

- **Intrusion**. Pada penyerangan ini seorang penyerang akan dapat menggunakan sistem komputer yang kita miliki. Sebagian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang memiliki hak untuk mengakses sisttem.

- **Denial of services**. Penyerangan jenis ini mengakibatkan pengguna yang sah tak dapat mengakses sistem. Sebagai contoh adalah Distributed Denial of Services (DDOS) yang mengakibatkan beberapa situs Internet tak bisa

diakses. Seringkali orang melupakan jenis serangan ini dan hanya berkonsentrasi pada intrusion saja.

- **Joyrider**. Pada serangan ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem. Mereka masuk ke sistem karena beranggapan bahwa mungkin data yang di dalamnya menarik. Rata-rata mereka karena rasa ingin tahu, tapi ada juga yang menyebabkan kerusakan atau kehilangan data.

- **Vandal**. Jenis serangan ini bertujuan untuk merusak sistem. Seringkali ditujukan untuk site-site besar.

- **Scorekeeper**. jenis serangan in hanyalah bertujuan untuk mendapatkan reputasi dengan cara mengcrack sistem sebanyak mungkin. Sebagian besar dari mereka tertarik pada situs-situs tertentu saja. Sebagian dari mereka tak begitu peduli dengan data yang ada di dalamnya. Saat ini jenis ini lebih dikenal dengan istilah **script kiddies**

- **Mata-mata**. Jenis serangan ini bertujuan untuk memperoleh data atau informasi rahasia dari pihak kompetitor. Saat ini semakin banyak perusahaan yang memanfaatkan jasa ini.

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.

2 CIA dan 3M

Perlindungan data adalah hal yang penting dalam masalah sekuriti. Pada bahasan sekuriti data didefinisikan sebagai :

> *Phsical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meanings we assign to data are called information. Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules*

Dengan definisi di atas, maka data dianggap merepresentasikan informasi. Pada bahasan sistem sekuriti data dapat dikategorikan menjadi

- Data publik, yaitu data yang dapat dikomunikasikan dengan siapa saja
- Data rahasia, yaitu data yang tak boleh bocor ke tangan yang tak berhak
- Sebarang data

Seringkali orang sering mempertimbangkan masalah akses yang tidak sah saja dalam sekuriti. Sebetulnya hal yang perlu dipertimbangkan adalah lebih luas. Dalam perancangan dan pembahasan sistem sekuriti kazimnya kita akan dihadapkan pada pertimbangan yang dikenal dengan istilah **segitiga CIA**

- **Confidentiality,** yang akan berkaitan dengan pencegahan akan pengaksesan terjadap informasi yang dilakukan oleh pihak yang tak berhak.

- **Integrity**. yang akan berkaitan dengan pencegahan akan modifikasi informasi yang dilakukan oleh pihak yang tak berhak.

- **Availability,** pencegahan akan penguasaan informasi atau sumber daya oleh pihak yang tak berhak.

Disain suatu sistem sekuriti akan mencoba menyeimbangkan ke tiga hal di atas.

Confidentiality akan berkaitan dengan privacy (data personal) dan secrecy (kerahasiaan). Privacy lebih berkaitan dengan data pribadi, sedang secrecy terhadap data yang dimiliki oleh suatu organisasi. Kerahasiaan dan keamanan saling berhubungan.

Secara umum integrity berkaitan dengan jaminan bahwa sesuatu berada dalam kondisi seharusnya. Pada sekuriti ini akan berkaitan dengan proses pengubahan data. **Integrity** didefinisikan oleh Clark and Wilson adalah :

> *No user of the system, even if authorized, may be permitted to modify data items in such a way that asses or a accounting records of the*

company are lost or corrupted.

Dalam **Orange Book** (panduan untuk evaluasi sekuriti) didefinisikan **data integrity** adalah :

> *The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.*

Dalam hal ini jelas bahwa integrity berkaitan dengan konsistensi eksternal. Suatu data yang disimpan dalam sistem komputer harus benar menggambarkan realita yang ada di luar sistem komputer. Sedangkan dalam hal communication security, integrity sendiri memiliki definsi sebagai :

> *The detection and correction of modification, insertion, deletion or replay of transmitted data including both intentional manipulations and random transmission errors.*

Sedangkan **availability** didefinisikan oleh **ISO 7498-2** adalah :

> *The property of being accessbile and useable upan demand by an authorized entity.*

Salah satu kasus yang sering terjadi pada aspek ini adalah adanya **Denial of Service**, yang didefinisikan sebagia :

> *The prevention of authorized access to resources or the delaying the time-critical operations.*

Setiap user harus bertanggung jawab terhadap aksi yang dilakukan pada sistem . Untuk itulah konsep accountability menjadi penting pada sistem komputer. **Accountability** :

> *Audit information must be selectively kept and protected so that action affecting security can be traced to the responsible party*

Pada hakekatnya seringkali orang melupakan bahwa dalam pelaksanaan sekuriti akan melibatkan **3 M** yaitu :

- Matematika
- Manajemen
- Manusia

Berikut ini akan dibahas lebih dalam mengenai pertimbangan tersebut.

2.1 Matematika

> *Since mathematics is the foundation of all digital advances, nations well versed in that discipline - including China, India and the nations of Southeast Asia - could turn their homelands into formidable technology power*

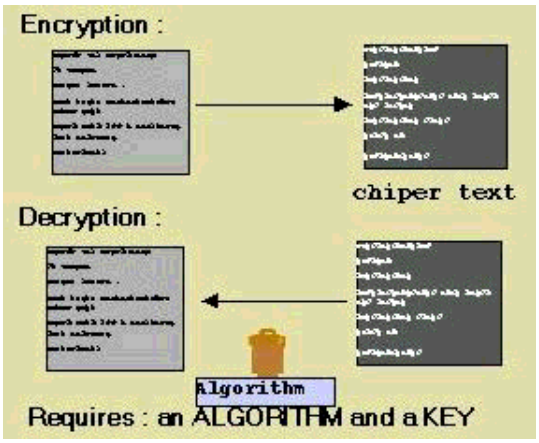
Pada penyusunan suatu sistem sekuriti tidak terlepas dari kebutuhan pemahaman matematis yang mendasari penyusunan algoritma yang nantinya diimplementasikan baik dalam bentuk perangkat keras ataupun lunak. Beberapa konsep matematika yang sering dimanfaatkan misal :

- **Number theory**, mendasari berbagai algoritma kriptografi seperti DES, RSA dan lain sebagianya.

- **Formal model**, digunakan untuk melakukan pengujian apakah suatu protokol dapat dijamin keamanannya. Pengembangan dari berbagai jenis kalkulus sepertri SPI Calculus (Abadi dan Gordon, 1999) lazim digunakan untuk menganalisis suatu protokol yang digunakan untuk sekuriti. Metoda formal matematis ini sering digunakan secara formal untuk membuktikan celah yang ada pada protokol SSL (Abadi dan Needham, 1996), SSH dan AKA (Abadi, 1997).

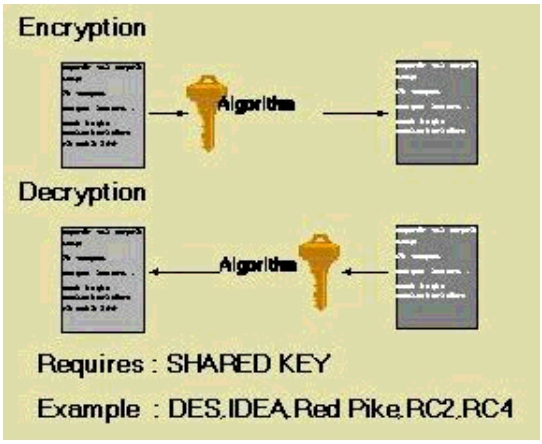
Beberapa model matematika untuk sekuriti telah dikembangkan antara lain :

- Model Bell-LaPadula (BLP)
- Model Harrison-Ruzzo-Ullman (HRU)
- Model Chinesse Wall
- Model Biba
- Model Clark Wilson



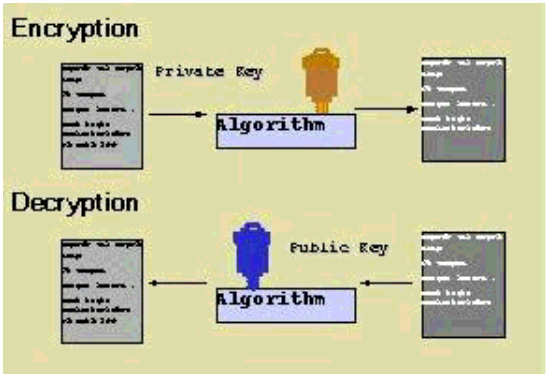
Gambar 1. Konsep kriptorafi

Sistem kriptografi **simetris** menggunakan key yang sama baik untuk pengirim data ataupun penerima data. Algoritma yang dikenal adalah DES, Blowfish.



Gambar 2. Kriptografi simetris

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



Gambar 3. 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:

$$\begin{array}{lll} Message\,1 & A \rightarrow B: & \{K_{ab}\}_{K_b} \\ Message\,2 & B \rightarrow A: & \{N_b\}_{K_{ab}} \\ Message\,3 & A \rightarrow B: & \left\{CA, \{N_b\}_{K_a^{-1}}\right\}_{K_{ab}} \end{array}$$

- Pada pesan pertama *A* mengirimkan session key K_{ab} ke server *B* dengan menggunakan publik key K_b
- Kemudian *B* akan menghasilkan "tantangan" (*challenge*) N_b
- *A* akan melakukan "sign" dan akan mengirimkan kembali ke *B* dengan sertifikat *CA*

Versi SSL di atas tidak memiliki otentikasi client seperti yang diharapkan.

Sehingga dapat menimbulkan suatu "attack". Perbaikan dari masalah ini dilakukan dengan mengubah tahapan ke tiga menjadi :

$$Message\,3 \quad A \rightarrow B: \quad \left\{CA, \{A, B, K_{ab}, N_b\}_{K_a^{-1}}\right\}_{K_{ab}}$$

Dalam bahasan ini tidak dibahas lebih dalam lagi mengenai pemanfaatan matematika dalam sekuriti, karena sudah merupakan suatu syarat mutlak yang lazim diketahui.

2 Manajemen

> *The technology, however is only a tool.. it cannot solve social and economic problem in the absence of social and economic policy..... Technology cannot balance the budget, although with creative thinking it can be used to improve the efficiency of government and minimize the cost*
>
> Daniel Burnstein dan David Kline dalam Road Warrior

Pada dasarnya untuk membuat suatu sistem yang secure tidak lepas dari bagaimana kita mengelola suatu sistem dengan baik. Sehingga persyaratan *good practice* standard seperti Standard Operating Procedure (SOP) dan *Security Policy* haruslah diterapkan di samping memikirkan hal teknologinya.

Suatu security policy sebaiknya berisi :

- **Penjelasan.** Suatu kebijakan haruslah eksplisit dan jelas dipahami dan menerangkan mengapa kebijakan tersebut diterapkan. Karena sebagian besar orang cenderung tak mengikuti aturan bila tak diberikan alasannya.

- **Tanggung jawab tiap pihak yang terlibat** Suatu kebijakan memaparkan secara eksplist harapan dan tanggung jawab setiap pihak, pengguna, pengelola dan pihak manajemen. Dengan cara ini dihindari harapan serta melepaskan tanggung jawab pada pihak lain.

- **Bahasa yang biasa.** Karena yang membaca dokumen ini adalah semua pengguna, maka kebijakan harus ditulis dengan bahasa yang dipahami oleh semua kalangan.

- **Otoritas yang menerapkan**. Harus juga ditentukan tindakan yang perlu dilakukan bila terjadi pihak yang tak mematuhi kebijakan tersebut. Kebijakan juga harus menentukan siapa yang akan memutuskan mengenai keputusan hukuman ketika terjadi pelanggaran.

- **Perkecualian.** Tak ada kebijakan yang sempurna, terutama untuk perubahan di masa mendatang. Sehingga perlu dilakukan penentuan bilamana diperlukan suatu pengecualian. Siapa dan bagaimana yang mendapat pengecualian tersebut.

- **Penilaian ulang.** Karena sistem terus berevolusi, maka kebijakan perlu juga direvisi pada masa mendatang. Sebagai contoh perubahan ukuran organisasi (orang yang terlibat) akan menyebabkan perubahan policy ini juga.

Sebaiknya security policy **TIDAK** berisi hal berikuti ini :

- **Ditail teknis.** Karena suatu kebijakan haryus menjelaskan apa yang akan dilindungi dan mengapa, maka tidak perlu ditail teknis tentang bagaimana melakukan hal tersebut dijabarkan. Akan lebih bermanfaat menuliskan dokumen pendek yang dapat dipahami semua pihak daripada dokumen panjang yang bersifat teknis yang hanya dipahami oleh bagiam teknis saja.

- **Permasalahan pihak lain.** Setiap situs memiliki kebijakan yang berbeda karena perbedaan contraint, pengguna, dan juga kemampuan. Kebijakan ini juga berubah sejalan dengan waktu. Sehingga janganlah selalu sekedar mengikuti kebijakan yang dilakukan oleh pihak lain belaka dalam membuat policy ini.

- **Masalah yang bukan merupakan masalah sekuriti komputer.** Seringkali permasalahan non sekuriti dianggap permasalahan sekuriti, sebagi contoh pengguna menampilkan gambar porno (ini permasalahan sumber daya manusia). Pengguna bermain game sepanjang hari juga bukan masalah sekuriti (kecuali game tertentu yang memanfaatkan jaringan). Sehingga batasan mana yang merupakan permasalah sekurit dan mana yang bukan harus cukup dijelaskan.

Berikut ini adalah contoh suatu policy yang kurang cocok (sengaja ditulis dalam kutipan aslinya) :

> *OTP will be used for all incoming connections*

Policy di atas terlalu spesifik dan teknis, sehingga sulit untuk dipahami, sehingga seringkali tak diterapkan. Berikut ini adalah perbaikan :

> *Nonreusable passwords shall be used to authenticate all incoming connections from the outside world, in order to prevent potential attackers from being able to capture reusable passwords by monitoring such connections.*

Policy di atas sudah lebih baik karena telah menjelaskan APA yang harus dilindungi, dan MENGAPA. Policy tersebut tetap memberikan opsi terbuka BAGAIMANA hal tersebut diimplementasikan, sehingga staf teknis dapat memilih implementasi yang terbaik. Policy di atas dapat ditulis lebih baik menjadi :

> *Regular passwords are often stolen and reused when they pass across networks. We won't use passwords that can be reused across networks our company doesn't control.*

Policy hanya memberikan panduan dalam implementasi tapi tak menjelaskan secara speisifik implementasi yang dilakukan.

Sangat sulit untuk menentukan suatu guideline seragam yang berkaitan dengan sekuritini ini. Hal ini juga disebabkan oleh beragamnya bentuk organisasi yang memanfaatkan IT. Akan tetapi berikut ini diberikan beberapa hal mendasar yang sebaiknya disertakan dalam penulisan kebijakan sekuriti (security policy) :

- Siapa saja yang diperkenankan memiliki account pada situs anda ? Apakah ada account untuk guest ? Bagaimana dengan kontraktor, vendor dan client yang terlibat dengan sistem anda ?

- Apakah sebuah account dapat digunakan bersama oleh beberapa pengguna ? Bagaimana dengan sekretaris yang menggunakan account seorang eksekutif untuk membaca emailnya ? Bagaimana dengan proyek bersama ? Apakah penggunaan suatu workstation sebentar tergolong pemakaian account bersama ?

- Kapan seseorang dapat kehilangan hak atas accountnya, dan apa yang dilakukan ?

- Siapa yang dapat menggunakan modem dial in ? Apakah ada pertimbangan khusus untuk line SLIP, PPP, atau ISDN ?

- Apa yang harus dilakukan orang sebelum menghubungkan komputernya ke jaringan utama ?

- Bagaimana membuat komputer cukup aman sebelum komputer tersebut memperoleh layanan dari mesin utama ?

- Bagaimana membuat komputer aman agar dapat dikoneksikan jaringan dengan akses tak terproteksi ke Internet

- Bagimana data keuangan harus dilindungi ?

- Bagimana informasi rahasia mengenai pegawai dilindungi ? Bagaimana dengan kantor di negara lain yang berada di bawah hukum yang berbeda ?

- Apakah yang perlu dilakukan oleh tiap orang untuk melindungi sistemnya ? Bagaimana model password yang harus digunakan dan bagaimana proses penggantiannya ?

- Apakah tindakan pencegahan yang perlu dilakukan terhadap virus ?

- Siapa yang dapat melakukan koneksi ke network eksternal ? Bagaimana definisi network eksternal ini ? Apakah diperbolehkan seorang manajer proyek menghubungkan network internal dengan situs lainnya ? Bagaimana dengan koneksi dari partner bisnis ? Bagaimana koneksi lainnya ke Internet ?

- Bagaimana komputer di rumah diamankan ? Bagaimana komputer tersebut memperoleh akses yang aman ke jaringan kantor ?

- Bagaimana pegawai yang sedang dalam perjalanan memperoleh akses yang aman ke jaringan kantor ?

- Informasi manakah yang tergolong informasi rahasia bagi suatu perusahaan ? Bagaimana informasi tersebut dilindungi ? Apakah boleh informasi tersebut dikirm ke luar melalui e-mail ?

- Apakah persyaratan untuk suatu sistem agar dapat melakukan electronic commerce ?

- Jika suatu kantor memiliki situs remote, bagaimana dibuat akses yang aman ke jaringan utama di kantor pusat ?

Dalam mendisain sekuriti dapat dipakai 5 tahapan dasar berikut ini :

1. Pada aplikasi yang bersangkutan, manakah mekanisme proteksi difokuskan, apakah pada data, operasi, atau pengguna

2. Pada layer manakah dari 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 ?

2.3 Manusia

> *... we can make machines smarter and smarter, but their value will be in how much smarter they make people*
>
> Doug Engelbart dalam Dr Dobb Journal

Manusia adalah salah satu faktor yang sangat penting tetap sering kali dilupakan dalam pengembangan Teknologi Informasi. Begitu juga dalam mengembangkan sistem sekuriti. Sebagai contoh karena penggunaan password yang sulit sehingga menyebabkan pengguna malah menuliskannya pada kertas yang ditempel dekat komputer. Sehingga dalam menyusun kebijakan sekuriti faktor manusia dan budaya setempat haruslah sangat dipertimbangkan.

Seperti yang diungkapkan oleh **Kevin Mitnick** (seorang cracker yang terkenal), sebagian besar celah diperoleh melalui rekayasa sosial yang menunjukkan kelemahan pengguna. Saat ini di Indonesia masih banyak praktek dari pengguna yang sangat mengabaikan faktor sekuriti (bahkan di bank pun masih berlangsung). Banyak pengguna komputer yang tergolong sensitif (misal Bank) saling menukar password, bahkan sering menuliskan password dan menempel di

dekat monitornya. Salah satu serangan yang sering dilakukan terhadap kelengahan pengguna adalah kasus ‘‘impersonate’’ pada Internet Banking.

Komunitas internet yang tadinya merupakan komunitas sejenis (para ilmuwan) yang berdasarkan rasa percaya dan keinginan berkolaborasi, kini menjadi komunitas yang majemuk, dan penuh dengan orang asing. Sehingga mirip dengan jalanan yang rawan akan tindak kejahatan. Hukum (apalagi di Indonesia) sepertinya belum bisa mengikuti kecepatan perubahan internet. Sehingga langkah paling tepat untuk melindungi sistem, adalah dari diri pengguna sendiri. Baik secara aktif menjaga pesan yang dikirimkan, teliti dalam menerima pesan, maupun berhati-hati dalam menggunakan fasilitas atau jasa di internet. Kasus virus-worm seperti I LOVE U yang mengirimkan pesan seakan-akan dari pengguna dengan tujuan yang ada di address book pengguna, sudah merupakan suatu contoh nyata begitu mudahnya kasus pelanggaran keamanan dan pencurian identitas dilakukan. Ini juga berawal dari ketakpedulian pengguna terhadap permasalahan ini.

Sistem komputer client yang digunakan pengguna saat ini sering tidak dianggap sebagai sumber kelemahan sistem sekuriti. Padahal ini salah satu penyebab beberapa kasus keamanan. Untuk beberapa sistem yang mensyaratkan keamanan (misal perbankan, data organisasi) maka perlu digunakan client yang memiliki sistem log dan multi user yang baik. Sehinga accountibility dari tiap pengguna akan tetap terjaga.

Pada dasarnya seorang pengguna memiliki tanggung jawab penggunaan sumber daya komputasinya. Tanggung jawab ini berdasarkan konvensi yang berupa (Ladkin, 1999) :

- Legal, sebagai contoh tak mengancam orang lain, tak menyaru sebagai orang lain, jangan merusak pekerjaan orang lain
- Kontraktual, sebagai contoh tak bermain game, tak menulis email pribadi, menjaga kontrak bisnis tetap bersifat rahasia.
- Sosial, tak menunjukkan gambar porno, atau tak membaca email milik orang lain.

3 PKI dan CA

> *Modern society is imposed not by the personal presence and brute force of an elite caste but by the way each individual learns the art of self-surveilance*
>
> Michel Foucault

Berikut ini akan dijelaskan secara singkat konsep dan prinsip dari Public Key Infrastructure (PKI) serta peran Certificate Authority (CA).

3.1 Public Key Infrastructure

Perdagangan tradisional berbasiskan kertas dan ‘‘trust’’. Dalam perkembangan perdagangan tradisional telah dikenal sistem EDI yang bersifat : secure, closed,

dan menggunakan sistem yang proprietary. Sedangkan saat ini eCommerce yang menggunakan Internet relatif bersifat tak aman, open dan memanfaatkan open system.

Di dunia Internet relatif sulit sekali memastikan apakah seseorang itu benar personal yang dimaksud. Sehingga timbul permasalahan mendasar dalam pemanfaatan eCommerce.

- **Authentication** : untuk mengidentifikasi pihak yang terlibat. Dalam perdagangan tradisional hal tersebut dilakukan dengan surat yang ditanda-tangani.

- **Confidentiality** : untuk menjaga informasi agar tetap privat. Dalam perdagangan tradisional surat ditulis dalam amplop dan lalu ditanda-tangani lalu di-‘‘seal’’.

- **Integrity**: untuk melindungi manipulasi informasi. Hal ini dilakukan pengiriman dengan surat tercatat, lalu dibuat salinannya dan dikirimkan dua kali.

- **Non repudiation** : untuk mencegah pengingkaran informasi oleh pemilik. Hal ini dapat dilakukan dengan adanya saksi yang menguji keabsahan tanda tangan tersebut.

Agar hal tersebut dapat tercapai dalam eCommerce maka perlu diterapkan langkah-langkah :

- **Kriptografi standard** (simetrik dan asimetrik). Kriptografi simetrik cepat, aman tetapi memiliki permasalahan pengelolaan key. 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.

- **One way hashing**. Menggunakan fungsi satu arah, dan tanpa key. Digunakan untuk menghasilkan suatu sidik data khas terhadap suatu kumpulan data. Digunakan untuk menentukan apakah suatu data telah berubah.

- **Tanda tangan digital.** Beberapa negara telah mensahkan penggunaan tanda tangan digital dalam transaksi elektronis. Tanda tangan digital ini akan menjamin otentikasi suatu dokumen.

- **Certificate Authority.** Suatu sistem yang mengikat kepemilikan public key dan pengguna sesungguhnya.

Langkah di atas dapat digunakan untuk membentuk ‘‘trust’’ dalam transaksi di Internet :

- **Authentication** : publik key digunakan untuk membuat digest dari pesan. Hanya dengan menggunakan private key dari pengirim maka dapat

didekrip.

- **Confidentiality** : Pesan dienkripsi dengan menggunakan publik key dari penerima. Hanya dengan menggunakan private key dari pengirim pesan dapat didekripsi.

- **Integrity:** Membandingkan digest dengan tanda tangan digital yang didekripsi.

- **Non repudiation** : tanda tangan digital melakukan hal ini.

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

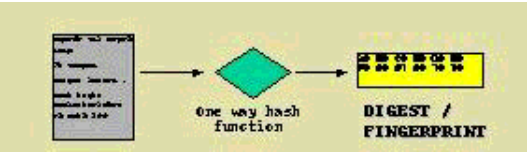
- Pseudo random number
- Panjangnya key, semakin panjang semakin aman. Tetapi perlu diingat bahwa membandingkan dua buah sistem kriptografi yang berbeda dengan berdasarkan panjang keynya saja tidaklah cukup.
- Private key harus disimpan secara aman baik dalam file (dengan PIN atau passphrase) atau dengan smart card.

3.2 Certificate Authority

Does the fact that he sends out the correct answers to the questions prove that he understands Chinese ?

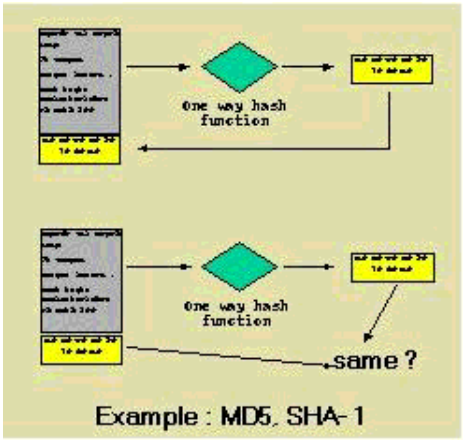
John Searle mengenai Chinese Room Experiment

Penggunaan public key memang akan memudah proses manajemen key yang digunakan dalam suatu eCommerce. Tetapi bagaimana mengetahui suatu publik key adalah milik seseorang ? Untuk itu akan dimanfaatkan digital signature dan Certifcate Authority (CA).



Gambar 4. One way hash function

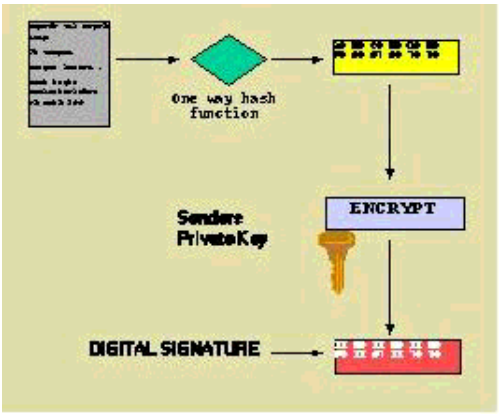
Suatu fungsi hash pada dasarnya adalah suatu fungsi sederhana yang tak bersifat reversibel. Sehingga dengan mudah kita dapat menghasilkan suatu ‘‘signature’’ yang khas untuk tiap deretan data. Tetapi dari signature tersebut tak dapat dilakukan pembalikan untuk memperoleh deretan data asli.



Gambar 5. Pemanfaatan hash

Suatu CA akan mengikat (bind) suatu publik key dengan pemiliknya. Melakukan penyampulan untuk mendistribusikan publik key. CA yang dipercaya akan melakukan tanda tangan digital untuk menguji kepemilikan kunci tersebut. Suatu Certificate pada dasarnya akan berisi :

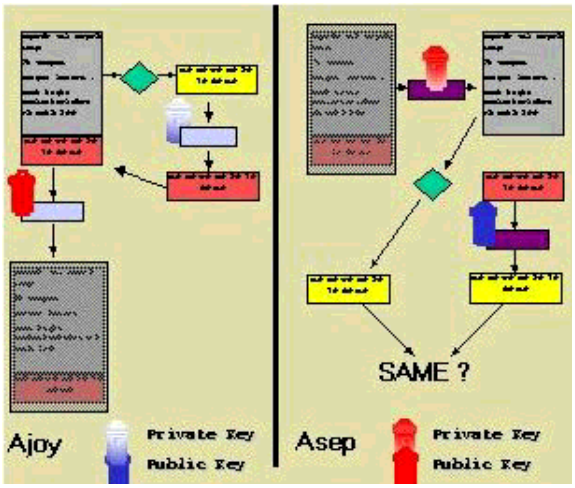
- Keterangan ditail tentang pemilik
- Keterangan tentang pihak yang mengeluarkan sertifikat (Certifier)
- Publik key itu sendiri
- Tanggal valid dan kedaluarsa
- Tanda tangan digital sertifikat tersebut yang dilakukan oleh CA
- Time stamp (penanda waktu)



Gambar 6. Tanda tangan digital

Suatu CA akan melakukan beberapa hal mendasar :

- Membuat sertifikat
- Bertanggung jawab memvalidasi pemilik dari suatu public key.
- Mendistribuskan CA dengan direktori server
- Membuat Certification Revocation List (CRL)

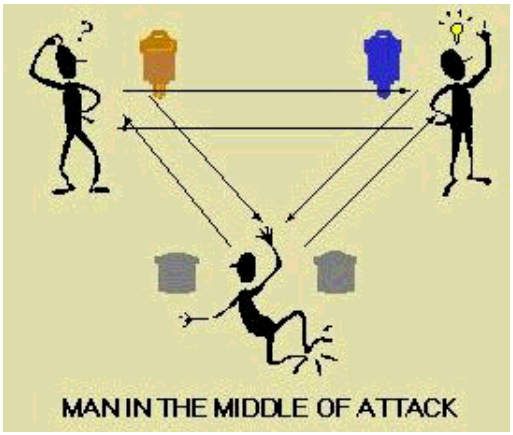


Gambar 7. Mekanisme keseluruhan

Biasanya CA disediakan oleh suatu institusi yang dipercaya oleh publik, misal suatu institusi pemerintah. Suatu Public Key Infrastructure akan terdiri dari :

- Certification Authority (CA)
- Registratraion Authority (RA)
- Direktori
- Aplikasi yang mendukung PKI !!!!!
- Prosedur dan policy

Yang perlu dipahami adalah kenyataan bahwa biasanya dalam penyusunan PKI maka akan melibatkan **20% teknologi dan 80% policy**. PKI adalah salah satu infrastructure eCommerce yang penting.



Gambar 8.Pertimbangan serangan man in the middle

4 Open Source dan Security

> *Over the next decade the development of application software will shift from the technological elite to the software proletariat*
>
> Scott Brown dalam The Future of Software

Dengan tersedianya source code para open source sering pihak merasa ragu akan

keamanan sistem tersebut. Sudah barang tentu pendekatan dengan konsep security through obscurity ini kurang tepat. Pada saat ini Open Source merupakan salah satu kandidat untuk penyediaan infrastruktur sistem yang aman. Tidak saja aman dari sisi teknologi tapi juga dari sudut pandang ketergantungan suatu negara. Beberapa negara di Eropa telah memutuskan pemanfaatan Open Source dalam pembentukan infrastruktur eCommerce mereka.

Pemerintah Jerman melalui *Bundesminister für Wirtschaft und Technologi* (*BMWi*). menyatakan bahwa selama ini pengembangan infrastruktur Internet sering dilakukan dengan menggunakan pendekatan security through obscurity. Sehingga banyak orang menutup mata terhadap resiko yang mungkin terjadi pada sistem operasi yang dominan. Berdasarkan alasan inilah maka BMWi mendukung pengembangan Open Source, karena menjanjikan keamanan yang lebih baik. Paling tidak memungkinkan para ekspert di luar perusahaan penyedia sistem tersebut untuk memeriksa secara lebih seksama dan menyeluruh.

BMWi sejak tahun 1999 telah mulai mengembangkan komponen untuk sistem sekuriti dengan perangkat lunak Open Source. Di samping itu, BMWi menganggap Open Source menawarkan solusi yang lebih aman, lebih user friendly dan inovasi yang lebih baik serta interoperabilitas yang baik dengan produk lain. Dengan ketersediaan source code maka diharapkan para developer di Jerman dapat bekerja lebih cepat tanpa bergantung pada vendor negara lain. Saat ini telah banyak developer Open Source yang berasal dari Jerman. Menurut perkiraan BMWi, Jerman pada tahun 2000 akan menghabiskan sekitar 200 milliard DM untuk kebutuhan komputer sehingga langkah-langkah penghematan seperti penggunaan Open Source dan teknologi baru perlu dilakukan. Dukungan pemerintah Jerman terhadap Open Source memang sungguh-sungguh tercermin pada studi yang dilakukan *der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung* (*KBSt*), yang menyarankan penggunaan perangkat lunak Open Source di lingkungan kementerian dalam negeri Jerman. Hal ini juga didukung oleh kajian *Institut für Rechtsfragen der Open Source Software* suatu LSM yang memfokuskan pada aspek hukum dari Open Source. Hal ini tak mengherankan sebab sejalan dengan yang diutarakan oleh Erkki Liikanen - Commissioner for Enterprise and Information Society European Commission yang disampaikan pada Information Security Solutions Europe (ISSE 99), bahwa berdasarkan alasan keamanan dan menghindari ketergantungan pada negara lain, maka sangat penting mempertimbangkan penggunaan Open Source dalam teknologi kriptografi.

Negara-negara Eropa telah juga mengembangkan proyek yang dikenal dengan nama Interworking Public Key Infrastructure for Europe. Proyek ini juga berusaha mengembangkan teknologinya dengan pendekatan Open Source. Dengan telah diakuinya secara hukum tanda tangan digital ini, maka sudah saatnya Indonesia mempertimbangkan pembangunan PKi yang mempertimbangkan aspek non teknis dan teknis secara lebih seksama.

5 Penutup

> *Each new tool comes to us with its own particular embedded technology. The way we perceive the world around us depends largely*

on which tool is apparently at our disposal. Once a technology is admitted into societ it plays out its own hand. It does what it is designed to do. Our task is to understand what the design is.

Neil Postman, in Technopoly

Perubahan fungsi serta komunitas pengguna internet tampaknya belum diikuti dengan perubahan drastis teknologi jaringan yang mendasarinya. Teknologi yang digunakan relatif masih memanfaatkan TCP/IP yang serba terbuka. Terbuka di sini bukan berarti source code atau standarnya diketahui banyak orang, tetapi dalam mekanismenya yang masih membuka alamat tujuan dan pengirimnya. Ketertutupan informasi yang berkaitan dengan suatu protokol bukan merupakan suatu jaminan bahwa protokol itu akan lebih aman. Seperti diketahui, algoritma atau mekanisme kriptografi yang menjadi sandaran usaha penyusunan jalur komunikasi aman pun menggunakan algoritma yang mekanismenya diketahui oleh orang banyak.

Beberapa protocol telah dikembangkan untuk mengatasi kekurangan protokol TCP/IP, seperti IPSEC (IP Secure), IP-NG (IP New Generation). Di samping faktor teknologi, masalah security ini juga disebabkan perilaku pengguna dalam memanfaatkan internet itu sendiri, hingga menyebabkan mudahnya lubang security terjadi. Perilaku ini sendiri tak terlepas dari cara pandangan pengguna terhadap komunitas internet itu sendiri dan terhadap security itu sendiri.

Untuk menyusun strategi sekuriti yang baik perlu difikirkan pertimbangan dasar berikut ini :

- Kemungkinan dipenuhinya (ekonomis dan pertimbangan waktu)
- Apakah sistem tetap dapat difungsikan
- Kesesuaian kultur
- Hukum setempat yang berlaku

Dengan makin pentingnya infrastruktur sosial seperti SDM, perangkat hukum maka dalam mengembangkan dan memasyarakatkan penggunaan Internet sebaiknya tidak hanya berhenti pada aspek teknologi saja, dan melupakan aspek non teknis. Semakin banyaknya orang menggunakan Internet, atau kantor terhubung ke Internet maka akan makin harus makin diperhatikan permasalahan sekuriti ini.

Even if computer/Internet literacy was a mandate, the correct curriculum path would not be Internet first. It might be something like : Reading/writing literacy, typing/keyboarding/general computer literacy, a variety computer application programs, computer mechanism and ETHICS, then the Internet

Tom Harrion dalam Computer and Society, June 1997

Bibliografi

1 Abadi, Martin (1997). Explicit communication revisited: two new attacks on authentication protocols. *IEEE Transactions on Software Engineering*,

vol 23 (3), Maret 1997, hlm. 185 - 186.

2 Abadi, Martin (1997b). Secrecy by typing in security protocols. *Theoretical Aspects of Computer Software*, third International Symposiumm TACS 97. hlm. 611 - 637.

2 Abadi, Martin, Andew D. Gordon (1999). A calculus for cryptographic protocols : the spi calculus. *Information and Computation*, 148, hlm 1-70.

2 Abadi, Martin, Roger Needham (1996). Prudent engineering practice for Cryptographic Protocols. *IEEE Transactions on Software Engineering*, vol 22 (1), Januari 1996, hlm. 6 - 15.

2 Feiertag, Richard J, Peter G Neumann (1979). *The Foundation of Provable Secure System*.

3 Gollmann, Dieter (1999). *Computer Security*. England : John Willey & Sons Inc.

4 Heintze, Nevin, J. D. Tyger (1996). A model for secure protocols and their compositions. *IEEE Transactions on Software Engineering*, vol 22 (1), Januari 1996. hlm. 16 - 30.

4 Ladkin, Peter B (1999). *Comment on security. Lecture material*.

5 Lampson, Buttler W (199). *Authentication in distributed system*.

5 Ronald, Edmund M.A, Moshe Sipper (2000). The challenge of tamper proof Internet Computing. *IEEE Computer*. Oktober 2000, hlm 98-99.

3 Schneier, Bruce (1996). *Applied Cryptography*. Canada : John Willey & Sons Inc.

6 **Information Security Solutions Europe** (ISSE 99), Berlin 14 October 1999 dapat dibaca di http://europa.eu.int/comm/commissioners/liikanen/speeches/051099_en.htm

7 ICE-TEL homepage . http://www.darmstadt.gmd.de/ice-tel/ice-home.html

6 White House (2000). *National Plan for Information System Protection ver 1.0*

6 Zwicky, Elizabeth D, Simon Cooper, D. Brent Chapman (2000). *Building Internet Firewall*. O'Reilly and Associates

---

Penulis :

Avinanta Tarigan SKom[1]
Dosen Universitas Gunadarma, aktif di Tim Pandu, Depok Valley

Technology (DVT) dan KPLI Jakarta

I Made Wiryana, SSi, SKomp, MSc[2]

Dosen Universitas Gunadarma sedang melanjutkan program doktoral di RVS Arbeitsgruppe Bielefeld, aktif di Tim Pandu, Depok Valley Technology (DVT) dan KPLI Jakarta