Tim PANDU

Workshop Kelautan
Hamburg, 9 Maret 2002

Pertimbangan Sekuriti Pada Sistem Informasi Kelautan Nasional

I Made Wiryana dan Avinanta Tarigan

Universitas Gunadarma

2002

Workshop Kelautan Hamburg 9 Maret 2001

Pertimbangan Sekuriti Pada Sistem Informasi Kelautan Nasional

oleh : I Made Wiryana dan Avinanta Tarigan

Penerbit : Tim PANDU

Tahun terbit : 2002

Ringkasan

Sekuriti penting untuk membangun kepercayaan (*trust*) terhadap sebuah sistem informasi. Hal tersebut harus menjadi pertimbangan pada pembangunan suatu sistem sumber daya alam kelautan nasional yang dapat dipercaya.

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, juga berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnnya, atau suatu negara terhadap negara lainnya. Beberapa aspek sekuriti yang harus dipertimbangkan diantaranya adalah *secrecy*, *integrity*, *authentication*, *non repudiatio*n, dan *accountability.*Untuk mengaplikasikan sekuriti dalam sebuah sistem informasi diperlukan juga pertimbangan lainnya misal suatu kebijakan sekuriti yang telah tertata dengan baik, teknologi yang memungkinkan diterapkannya kebijakan tersebut, serta kesepakatan sosial.

Pilihan model sekuriti dan model organisasi serta kebijakan terhadappengolahan data memiliki hubungan mutual. Sekedar menampilkan data informasi sumber daya alam di Internet tanpa pertimbangan sekuriti akan memberikan kerugian di kemudian hari. Suatu model sekuriti harus diterapkan sehingga perubahan data, serta kepemilikan data yang diberikan oleh suatu institusi tetap terjaga.

Tulisan ini berisi tentang pertimbangan yang diperlukannya komputer sekuriti dalam membangun sistem informasi kelautan, tantangan, metoda, dan teknologi yang mungkin diterapkan, serta metoda evaluasi terbuka yang sebaiknya diterapkan untuk menjaga sekuriti agar lebih baik dilaksanakan.

Pertimbangan Sekuriti Pada Sistem Informasi Kelautan Nasional

I Made Wiryana[1] - Avinanta Tarigan[2]
Universitas Gunadarma

2002

[1]Dosen Universitas Gunadarma, melanjutkan studi doktoral di RVS Arbeitsgruppe - Universitas Bielefeld. Staf redaksi majalah Infolinux, Elektro, dan Komputek. Kontributor di berbagai majalah. Aktif di Tim Pandu <http://pandu.dhs.org>

[2]Dosen Universitas Gunadarma, melanjutkan studi doktoral di RVS Arbeitsgruppe - Universitas Bielefeld. Aktif di Tim Pandu <http://pandu.dhs.org>

Daftar Isi

Daftar Gambar

Kata Pengantar

Makalah ini disajikan pada Workshop Kelautan di Hamburg pada tanggal 9 Maret 2002 yang terselenggara berkat kerjasama KJRI Hamburg, KBRI dan Ikatan Akhli dan Sarjana Indonesia (IASI) serta rekan-rekan DAAD Marine. Walaupun acara ini merupakan suatu forum diskusi antar peneliti Indonesia bidang kelautan yang sedang melanjutkan studi di Jerman, kami mencoba memberikan buah pikiran berdasarkan latar belakang disipling ilmu kami. Mudah-mudahan buah pikiran ini dapat membantu mengakselerasi perkembangan penelitian bidang Kelautan di Indonesia.

Sekuriti merupakan salah satu aspek sistem informasi yang sering diabaikan dalam pengembangan ataupun pemanfaatan Teknologi Informasi. Biasanya kebutuhan suatu sistem dengan sekuriti yang baik hanya timbul ketika dampak negatif dari kejadian sekuriti telah dirasakan. Untuk mencapai tingkat sekuriti yang baik, sekedar pembelian produk atau pemanfaatan suatu teknologi saja tidak cukup. Manajeman dan kepedulian pengguna memiliki peranan yang penting. Untuk memberikan wawasan dan kepedulian mengenai sekuriti itulah, kami mencoba menyajikan materi ini di hadapan rekan-rekan peneliti bidang Kelautan. Diharapkan dalam pemanfaatan Teknologi Informasi nantinya, kepedulian ini akan memberikan nilai positif dari sisi sekuriti sistem yang digunakan.

Akhir kata penulis ucapkan terima kasih kepada pihak yang telah memberikan kesempatan kepada penulis untuk menyampaikan buah pikiran penulis pada acara tersebut.

I Made Wiryana dan Avinanta Tarigan
Tim PANDU
`http://pandu.dhs.org`

1

Ancaman sekuriti era Internet

"Security is a chain of trust, the strength of the chain is the weakest link"

Bruce Schnier

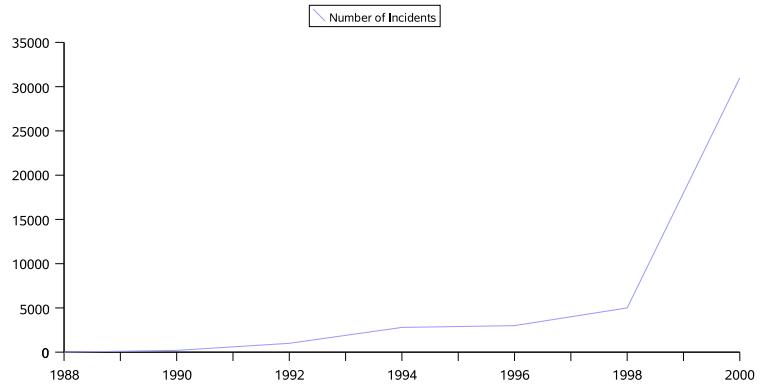
Pada tahun 80-an, komputer IBM PC yang tak dihubungkan ke jaringan (*stand alone*) mulai digunakan untuk berbagai keperluan. Saat itu, masalah keamanan merupakan masalah fisik semata. Ketika jaringan komputer mulai dikenal dan digunakan, sekuriti komputer mulai diperhatikan dan digunakan untuk mengatur hak pemakaian *resource*, baik fisik (memory, processor, disk) maupun data. Kini masalah sekuriti menjadi kompleks seiring dengan meluasnya pemanfaatan komputer, terutama setelah lahirnya Internet.

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 akademis yang serba terbuka. Sehingga pada awal perkembangannya masalah privacy bukanlah merupakan hal yang besar.

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 berupa suatu *Gemeinschaft* 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 institusi yang awalnya menganggap remeh masalah ini akhirnya mengalami kerugian yang besar akibat kelalaian ini.

Security incidents merupakan proses dan hasil pelanggaran sekuriti suatu sistem baik oleh penggunanya maupun entitas di luar sistem tersebut. Menurut **Computer Security Institute** (CSI) `<http://www.gocsi.com>`, trend terjadinya security incidents menjadi semakin tinggi pada tahun 2000 dan kerugian finansial yang diakibatkan mencapai US$ 377.828.700 pada quarter pertama tahun 2001.



Gambar 1.1: Security Incident Trend (CSI, 2001)

1.1 Motivasi serangan

Security incident merupakan hasil dari suatu ancaman digital (*digital thread*) terhadap suatu sistem oleh entitas yang sering disebut sebagai "**Cracker**". Berbeda dengan Cracker, adalah suatu entitas yang disebut dengan **hacker**. Hacker adalah entitas yang menemukan kelemahan (*vulnerability*) sistem dalam konteks security incidents. Seringkali cracker memanfaatkan hasil penemuan tersebut untuk melakukan eksploitasi dan mengambil manfaat dari hasilnya. Seorang hacker bisa menjadi seorang cracker, tetapi seorang cracker belum tentu menguasai kemampuan yang dipunyai seorang hacker.

Saat ini banyak tersedia perangkat lunak untuk melakukan eksploitasi kelemahan sistem. Software tersebut dapat didownload secara bebas dari Internet dan disebut dengan "*automate exploit tools*". Awalnya perangkat lunak ini digunakan untuk pengujian sistem (*penetration test*). Tapi dengan berbekal software ini, seorang cracker dapat melakukan exploitasi di mana saja dan kapan saja, tanpa harus mempunyai pengetahuan khusus. Cracker jenis ini dikenal sebagai "**script kiddies**".

Motivasi para hacker untuk menemukan vunerability adalah untuk membuktikan kemampuannya atau sebagai bagian dari kontrol sosial terhadap sistem. Sedangkan motivasi para cracker sangat beragam, diantaranya adalah untuk propaganda (deface web site/email), kriminal murni, penyerangan destruktif (akibat dendam atau ketidak-sukaan terhadap suatu insitusi), dan lain-lain. Apapun motif dari cracker selalu ada pihak yang dirugikan akibat tindakannya.

Pada prakteknya suatu pembentukan sistem yang aman akan mencoba melindungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain terhadap kita antara lain (Tarigan dan Wiryana, 2000):

- **Intrusion**. Pada penyerangan ini seorang penyerang akan dapat menggunakan sistem komputer yang kita miliki.
- **Denial of services**. Penyerangan jenis ini mengakibatkan pengguna yang sah tak dapat mengakses sistem.
- **Joyrider**. Pada serangan ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem.
- **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. 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.

1.2 Jenis serangan sekuriti

Serangan pada suatu sistem jaringan komputer sendiri pada dasarnya memiliki 3 gelombang trend utama yaitu (Wiryana, 2001b)

- Gelombang pertama adalah serangan **fisik** . Serangan ini ditujukan kepada fasilitas jaringan, perangkat elektronis dan komputer.
- Gelombang kedua adalah serangan **sintatik**. Serangan ini ditujukan terhadap keringkihan (*vulnerability*) pada perangkat lunak, celah yang ada pada algoritma kriptografi atau protokol.
- Gelombang ketiga adalah serangan **semantik**. Serangan jenis ini memanfaatkan arti dari isi pesan yang dikirim. Dengan kata lain adalah menyebarkan disinformasi melalui jaringan.

Masih banyak orang yang menyepelekan serangan gelombang ke tiga ini. Serangan bentuk ini dapat dilakukan, misal dengan memposting informasi yang salah ke suatu forum diskusi, mengirimkan email berantai dan sebagainya. Maraknya broker saham menggunakan media Internet untuk mencari informasi, menjadikan serangan semantik ini memberikan dampak yang besar. Sebagai contoh pada tanggal 25 Agustus 2000, Internet Wire menerima berita melalui e-mail bahwa CEO Emulex Corp telah mengundurkan diri. Tanpa memverifikasi isi dan pengirim, Internet Wire memposting berita ini, dan beberapa situs web mendistribusikan berita ini. Hal ini menyebabkan harga sahamnya turun menjadi 61%.

Akan lebih rawan lagi bila seseorang dengan melakukan serangan gelombang kedua (sintatik) dapat masuk ke database suatu media online. Lalu melakukan serangan semantik dengan mengubah berita yang ditayangkan pada media online tersebut. Karena relatif masyarakat dan pembaca mempercayai isi berita yang ditayangkan, maka serangan semantik seperti ini akan menimbulkan dampak yang lebih parah lagi. Jangankan mengubah berita baru yang sedang ditampilkan, bahkan mengubah berita lamapun sebetulnya membahayakan juga. Karena akan berakibat berkurangnya kredibilitas media online tersebut dan ini akan berdampak pada tingkat kepercayaan pembaca.

Serangan semantik ini sebetulnya sudah merupakan salah satu senjata *lumrah* dalam kegiatan dinas intelijen. Model serangan ini lazim digolongkan dalam kegiatan *active measure* (Womack, 1998). Pada dunia bisnis, penyerangan semantik ini lebih dikenal dengan istilah penyebaran berita *FUD* (*Fear, Uncertainty, and Doubt*). Hal ini sering dilakukan suatu perusahaan untuk menyebarkan keraguraguan konsumen terhadap suatu produk baru yang jadi saingannya.

2

CIA - konsep security

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

Bruce Schneier

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.

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 sebagai :

> *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*

Dengan kata lain merupakan suatu proses pencatatan yang memadai atas pemakaian resources dalam suatu sistem oleh para penggunanya. Tidak semua sistem operasi memiliki penanganan accountability yang baik. Hal ini terutama kepada sistem operasi yang bukan berkelas multiuser, misal OS/2, MS DOS, atau MS Windows 95.

Dalam membangun sebuah sistem informasi, perlu diperhatikan beberapa objektif dari sekuriti komputer untuk dipertimbangkan dalam desain, implementasi, dan operasional. Di samping hal di atas ada ada beberapa objektif sekuriti yang penting dan diperlukan sebagai pertimbangan dalam membangun sekuriti adalah :

- **Authentication**
  Sekuriti menjamin proses dan hasil identifikasi oleh sistem terhadap pengguna dan oleh pengguna terhadap sistem
- **Non Repudiation**
  Setiap informasi yang ada dalam sistem tidak dapat disangkal oleh pemiliknya

3

3M - komponen sekuriti sistem

" The moral is obvious. You cannot trust code that did not totally create yourself."

Ken Thompson - Turing Award Lecture

Pendekatan tradisional pada sekuriti komputer hanya berorientasi pada teknologi dan produk (*hardware* dan *software*). Dalam pendekatan ini, terdapat anggapan bahwa hanya sebagian orang saja yang harus mengerti dan bertanggungjawab dalam masalah sekuriti. Di samping itu, pihak manajemen menempatkan sekuriti komputer pada prioritas yang rendah. Pendekatan tradisional biasanya ditandai dengan ketidak-mengertian pengguna akan pentingnya keikut-sertaan mereka dalam membangun sekuriti. Pengguna menganggap dengan membeli dan menggunakan produk-produk sekuriti seperti firewall dan kriptografi dapat menjamin keamanan suatu sistem.

Pendekatan tradisional harus dihindari dalam membangun sekuriti. Kenyataan menunjukkan bahwa pengguna adalah mata rantai terlemah dalam rantai sekuriti itu sendiri. Oleh karena itu diperlukan pendekatan modern yang komprehensif, yang mengikutsertakan user, policy, manajemen, dan teknologi. 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.

3.1 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

Businessweek

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).

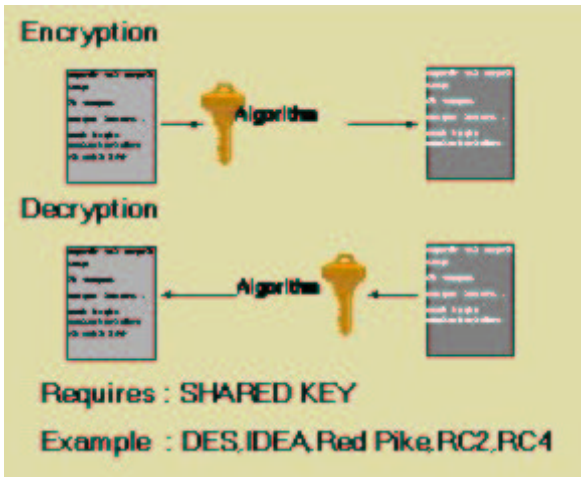
Beberapa model matematika untuk sekuriti telah dikembangkan antara lain :

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

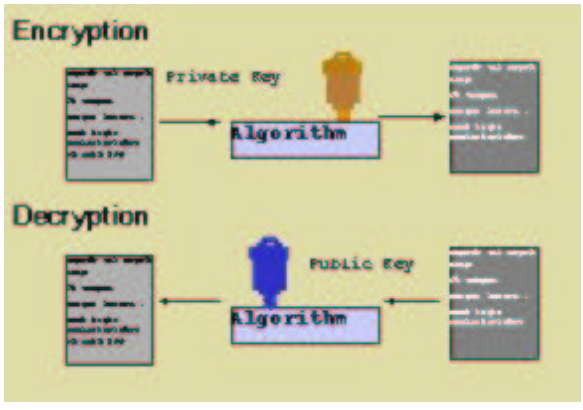
Gambar 3.1: Konsep kriptorafi

Sistem kriptografi simetris menggunakan key yang sama baik untuk pengirim data ataupun penerima data. Algoritma yang dikenal adalah DES, Blowfish. Bagaimana cara kerja kriptografi ini ditunjukkan pada Gambar 3.2. Ketika seseorang ingin mengirim pesan maka menyandikannya dengan menggunakan suatu kunci. Si penerima membuka pesan itu dengan menggunakan kunci yang sama.

Sistem kriptografi asimetris menggunakan dua buah key, yaitu *public key* dan *private key*. Salah satu key akan diberi tahu kepada publik. Mekanisme kriptografi disajikan secara sederhana pada Gambar 3.3.



Gambar 3.2: Kriptografi simetris



Gambar 3.3: Kriptografi asimetris

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. 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 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.

3.2 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 penggguna ? 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, 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 ?

3.3 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
- **Kontraktua**l, 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.

4

Komponen pembangun sekuriti

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

4.1 Sistem operasi dan aplikasi

Seringkali security incidents disebabkan oleh kelemahan akibat adanya "bug" dalam sistem operasi, aplikasi server, atau aplikasi desktop. Oleh karena itu, pemilihan sistem operasi atau aplikasi merupakan hal yang penting sebelum sistem tersebut dioperasikan. Bug dalam software tersebut muncul karena kesalahan desain dan proses pengembangan yang kurang tepat. Seringkali vendor software mengutamakan kecepatan waktu dan penghematan biaya pengembangan sehingga mengorbankan sekuriti. Selain menyebabkan kelemahan sekuriti pada sistem, bug menyebabkan sistem tidak bekerja dengan baik. Hal ini menyebabkan tidak tersedianya layanan sistem (*availability*).

- **Sebaiknya hindari penggunaan sistem operasi desktop yang tidak menjaga integritas, atau lengkapi dengan utilitas bantu**
  Seringkali masalah keamanan juga timbul akibat pengguna menggunakan sistem operasi yang tidak memiliki proteksi terhadap kernel (bagian sistem operasi). Atau tidak bersifat multi user. (Michener, 1999). Sehingga pengaruh virus, plug-in dapat menyebabkan tingkat sekuriti rendah. Bila pengguna memutuskan menggunakan sistem operasi semacam ini (misal DOS, Windows 95/98/ME), maka sudah sewajarnya tingkat pencegahan harus digunakan oleh pengguna tersebut.

- **Mewaspadai virus, plug-in, Active-X** .
  Active X dan plug-in dapat pula menyebabkan bahaya. Karena secara otomatis mereka dianggap "*trusted*" (dapat dipercaya). Untuk itu seringkali pengguna menghadapi dilema, karena seringkali suatu Internet Banking mengharapkan pengguna menginstall plug-in tertentu, atau suatu situs mendorong pengguna menginstal plug-in. Padahal penggunaan plug-in yang diperoleh dari situs di Internet, seringkali sulit diuji keamanannya, dan meletakkan sistem komputer pengguna dalam resiko yang tinggi (Wiryana, 2001c).

- **Sebaiknya pengguna selalu mencatat dan menyimpan log akses ke Internet .**
  Log ini akan sangat penting sekali ketika timbulnya suatu kasus di masa mendatang. Sayang sekali tidak semua sistem operasi di sisi desktop secara otomatis menyediakan fasilitas log ini.

4.2 Otentikasi (*authentication*)

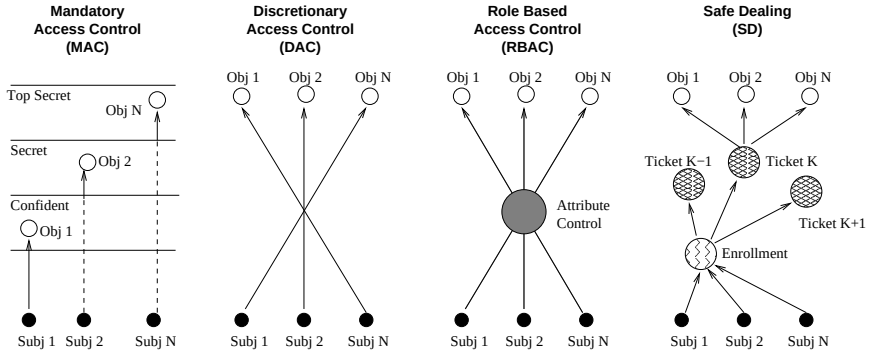
Dalam suatu sistem komputer, semua pengguna mempunyai ID sebagai identifier yang unik. Untuk dapat menggunakan sistem tersebut pengguna melakukan proses autentikasi, sehingga sistem secara dapat mengenal pengguna tersebut dan sebaliknya. Sistem sekuriti tradisional menggunakan *username* sebagai identifier dan *password* sebagai alat validasi. Teknologi berkembang sehingga saat ini terdapat beberapa mekanisme autentikasi :

- **Smartcard dan Secure Token**
  Smartcard dan secure token menyimpan digital-ID dari pengguna. Sehingga secara fisik pengguna harus mempunyai smartcard atau securetoken untuk melakukan autentikasi. Untuk mengaktifkan smartcard pengguna diharuskan untuk memasukkan PIN atau *keyphrase*.
- **Biometric authentication**
  Mekanisme autentikasi secara biologis memungkinkan sistem dapat mengenali penggunanya lebih tepat. Terdapat beberapa metode diantaranya : fingerprint scanning, retina scanning, dan DNA scanning. Dua metode terakhir masih dalam taraf penelitian, sedangkan fingerprint scanning saat ini telah digunakan secara luas dan digunakan bersama-sama dengan smartcard dalam proses autentikasi.
- **Public Key Infrastructure (PKI) dan Certification Authority**
  Public Key Infrastructure memungkinkan mekanisme yang aman untuk melakukan autentikasi, secrecy, integrity, dan non repudiation. Mekanisme PKI berdasar pada private key - public key, dan institusi Certification Authority yang akan melakukan validasi terhadap setiap pengguna dan sistem.

4.3 Akses Kontrol

Sebuah sistem komputer memerlukan akses kontrol untuk melindungi, memberikan izin, dan mengatur pemakaian sumber daya yang ada dalam sistem tersebut, baik sumber daya fisik (memory, disk, processor, jaringan komputer) maupun data/infomasi. Sumber daya yang akan digunakan disebut dengan obyek, dan yang hendak menggunakannya disebut dengan subyek (pengguna sistem, proses, atau obyek lain). Akses kontrol merupakan bagian dari implementasi policy yang diterapkan dalam organisasi. Beberapa metode akses kontrol adalah sebagai berikut :

- **DAC (Discretionary Access Control)**
  Dalam mekanisme DAC setiap objek mempunyai attribut akses berupa daftar setiap subjek dan hak aksesnya. Subjek dapat memodifikasi attribut akses (*read*, *write*, *run*) setiap objek yang dibuatnya dengan melakukan proses *granting* (mengijinkan akses) dan *revoking* (menolak akses). DAC merupakan akses kontrol yang fleksibel dan digunakan secara luas, tetapi DAC tidak menjamin tingkat sekuriti yang tinggi dalam implementasinya.

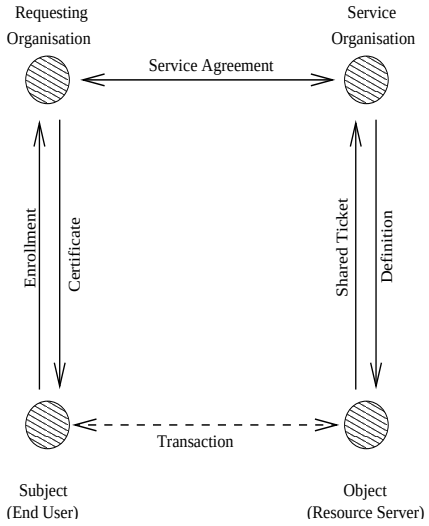


Gambar 4.1: Akses Kontrol [15]

- **MAC (Mandatory Access Control)**
  Dalam mekanisme MAC setiap subjek dan objek diklasifikasikan beradasarkan tingkat sensitifitas kerahasiaan informasi atau data yang telah didefinisikan sebelumnya. Setiap subjek hanya boleh mengakses objek yang ada di dalam level yang sama. MAC menjamin integritas dan secrecy dengan mengimplementasikan mekanisme multilevel sekuriti yang dikenal juga dengan nama Bell-LaPadulla. MAC menjamin tingkat sekuriti yang tinggi, tetapi tidak mudah dan sangat kaku dalam implementasinya. MAC diimplementasikan pada proyek-proyek sistem informasi yang membutuhkan tingkat sekuriti yang tinggi seperti pada sistem informasi militer.

- **RBAC (Role Based Access Control)**
  RBAC disebut sebagai akses kontrol yang"policy neutral", karena kemudahan dalam mengimplementasikan sekuriti policy. Setiap akses oleh subjek harus mematuhi aturan-aturan (role) yang telah didefinisikan sebelumnya. Desain dan implementasi RBAC yang tepat dan baik menjamin tingkat sekuriti MAC serta mendapatkan fleksibilitas DAC. Keterbatasan RBAC adalah pada implementasinya di tingkat inter-organisasional, karena RBAC didisain untuk diterapkan secara internal dalam suatu institusi atau organisasi.

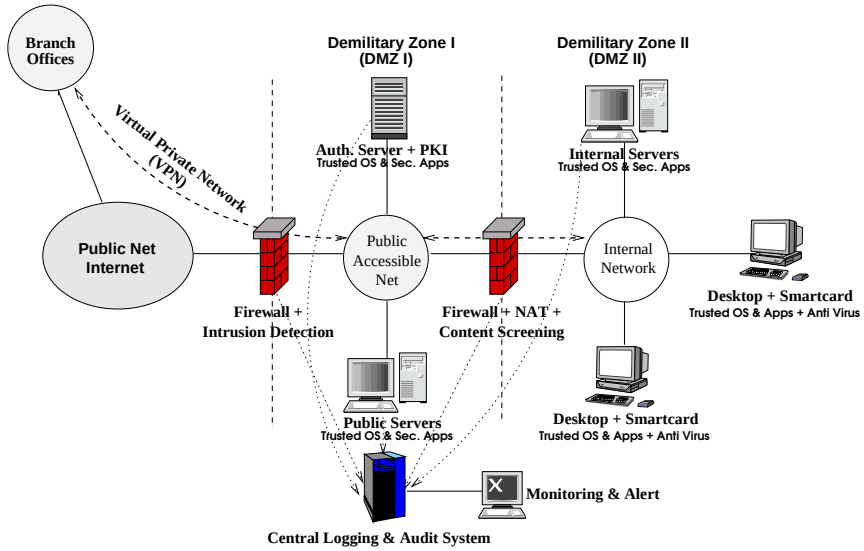
- **SD (Safe Dealing)**
  Safe Dealing (SD) merupakan akses kontrol yang didisain untuk diterapkan pada inter-organisasi atau inter-institusi. Dalam arsitektur SD terdapat dua buah institusi perantara (t*rusted intermediate institution*) yang dipercaya oleh semua pihak untuk melakukan proses yang diperlukan untuk membangun sekuriti. Setiap user (subjek) melakukan pendaftaran kepada suatu institusi (misalnya global Certification Authority) yang akan memvalidasi identitas setiap user dan memberikan digital certificate kepada user tersebut. Institusi penyedia layanan (objek) mempercayakan akses kontrol yang telah didefinisikan sebelumnya kepada sebuah institusi yang mengelola akses kontrol setiap layanan (misalnya Chamber of Commerce). Institusi penengah tersebut melakukan perjanjian layanan (*service agreement*) terhadap kelompok user dan setiap layanan. Kedua institusi tersebut dapat melakukan akses bersama terhadap masing-masing data untuk memperoleh kesepakatan dalam konteks autentikasi, validasi, dan akses kontrol. Setiap akses oleh user akan diidentifikasi oleh kedua institusi penengah tersebut dalam bentuk mekanisme pemberian akses berdasarkan karcis (*ticket-granting*).



Gambar 4.2: Safe Dealing Administration [15]

4.4 Firewall dan Intrusion Detection System

Firewall merupakan alat untuk mengatur akses kontrol pada level network di dalam suatu jaringan komputer. Firewall ditempatkan pada setiap entry-point untuk melakukan pemeriksaan serta otorisasi terhadap setiap paket transaksi yang masuk dan keluar ke dan dari jaringan tersebut berdasarkan rule atau aturan yang sudah didefinisikan sebelumnya. Firewall ini dapat dianalogikan seperti suatu pos penjagaan, yang akan memeriksa ID, memperbolehkan orang masuk, ataupun melarang seseorang masuk.



Gambar 4.3: Secure Network Architecture

Firewall terkini sudah dilengkapi dengan kapabilitas **Intrusion Detection System** (IDS) dan **Content Screening System**. Hal ini membuat sistem dapat menahan serangan pada level network. Apabila sistem mendeteksi paket transaksi yang mencurigakan (misalnya virus pada file, denial of service, atau intrusion

attempt) maka paket tersebut akan ditolak sebelum sampai kepada tujuan berikutnya.

4.5 Koneksi yang aman

SSL (Secure Socket Layer) pada dasarnya merupakan suatu mekanisme yang melindungi koneksi dari usaha penyadapan. Hal ini karena komunikasi yang terjadi antara client-server melalui suatu jalur yang dienkripsi. Tetapi sistem ini tidak melindungi dari salah masuknya pengguna ke *host* yang berbahaya, ataupun tak melindungi apakah suatu kode yang didownload dari suatu situs bisa dipercaya, atau apakah suatu situs itu bisa dipercaya. Abadi (1996) telah menunjukkan kelemahan protokol SSL versi awal secara teoritis. Jadi jelas SSL ini tidak melindungi dari beberapa hal misal (Wiryana dan Heriyanto, 2001):

- Denial of Services
- Buffer overflow
- Man-in-the-middle attack
- Cross scripting attack

Pada model SSL, **user** -lah yang harus bertanggung jawab untuk memastikan apakah server di ujung sana yang ingin diajak berkomunikasi benar-benar merupakan server yang ingin dituju. Pada dunia nyata untuk meyakinkan bahwa orang yang dihubungi adalah orang sesungguhnya, dapat dilakukan dengan mudah karena orang saling mengenal. Dengan melihat muka, suara, bau dan sebagainya kita bisa mendeteksi bahwa dia orang yang sesungguhnya.

Pada dunia Internet hal seperti itu sulit dilakukan, oleh karenanya digunakan sertifikat digital untuk melakukan hal ini. Sertifikat ini mengikat antara suatu *public key* dengan suatu identitas. Sertifikat ini dikeluarkan oleh sebuah pihak yang disebut CA (*Certificate Authority*) misal dalam hal ini Verisign atau Thawte. CA sendiri memperoleh sertifikat dari CA lainnya. CA yang tertinggi disebut root dan tidak memerlukan sertifikat dari CA lainnya. Penanganan sertifikat ini dilakukan secara hierarki dan terdistribusi.

Sayangnya sertifikat digital saja, bukanlah obat mujarab yang bisa mengobati semua jenis permasalahan sekuriti. Agar SSL dapat bekerja dengan semestinya (melakukan koneksi terenkripsi dengan pihak yang semestinya), maka penggunalah yang harus memverifikasi apakah sertifikat yang dimiliki oleh server yang ditujunya adalah benar. Berikut ini adalah beberapa hal minimal harus diperhatikan :

- Apakah sertifikat tersebut dikeluarkan oleh CA yang dipercaya.
- Apakah sertifikat tersebut dikeluarkan untuk pihak yang semestinya (perusahaan yang situsnya dituju).
- Apakah sertifikat itu masih berlaku.

Sebetulnya ketika melakukan koneksi ke sebuah situs yang mendukung SSL, hal tersebut ditanyakan oleh browser, tetapi sebagian besar pengguna selalu menekan **Yes** ketika ditanya untuk verifikasi sertifikat ini. Untuk melihat ketiga hal tersebut, dapat dilakukan dengan *double-click* pada tombol kunci yang ada di bagian kiri bawah browser. Celah ini pada dasarnya dilakukan dengan cara mengalihkan akses user dari situs aslinya ke situs palsu lainnya, sehingga dikenal dengan istilah **page hijacking**. Beberapa kemungkinan teknik yang digunakan telah dijelaskan pada (Made dan Heriyanto, 2001)

4.6 Public Key Infrastructure (PKI)

PKI merupakan teknik enkripsi public-key yang menjamin confidentiality, authentication, data integrity, dan non-repudiation. PKI merupakan pengejawantahan dari algoritma River Samir Adelmann (RSA) yang didalamnya mencakup teknologi dan fungsi legal/hukum. Digital Signature merupakan salah satu kemampuan dari teknologi PKI. Digital Signature dapat menjamin suatu dokumen elektronik otentik terhadap pembuatnya (*authentication*, *integrity*) dan mencegah terjadinya penyangkalan (*non-repudiation*) terhadap dokumen elektronik. Selain itu teknik enkripsi public mencegah terjadinya pembacaan data elektronik oleh yang tidak berhak (*confidentiality/secrecy*). Berikut ini akan dijelaskan secara singkat konsep dan prinsip dari Public Key Infrastructure (PKI) serta peran Certificate Authority (CA).

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 menegah 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.

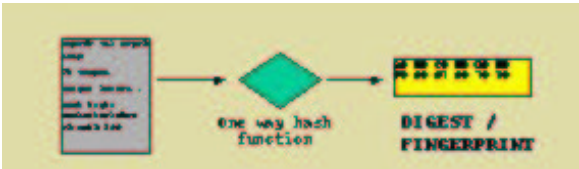
Key yang digunakan pada sistem kriptografi memegang peran yang sangat penting. Beberapa hal yang mempengaruhi ketahanan suatu key yang digunakan adalah :

- Pseudo random number. Bilangan random ini digunakan untuk menghasilkan key yang akan digunakan. Semakin random bilangan yang dihasilkan maka kemungkinan tertebaknya key akan makin kecil.
- 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.

4.7 Certificate Authority

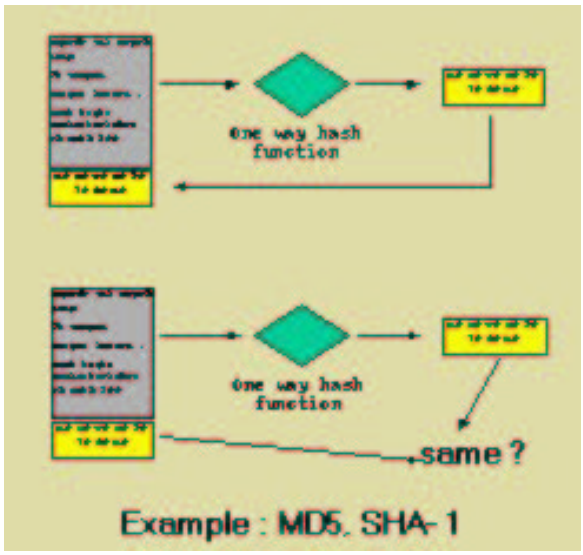
> *Does the fact that he sends out the correct answers to the questions prove that he understands Chinese ?*
>
> John Searle mengenai Chinese Room Experiment

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 4.4: One way hash function

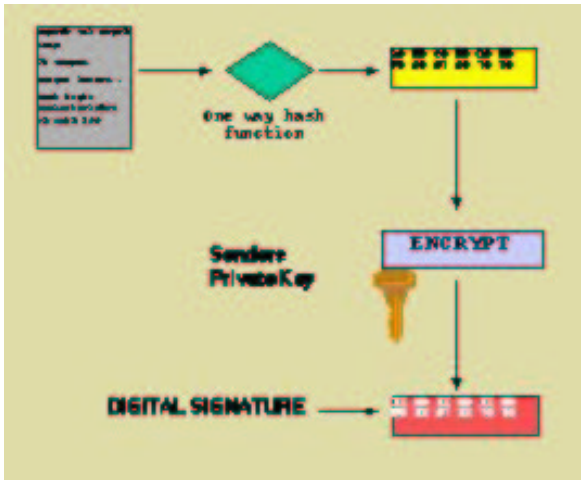
Suatu fungsi hash pada dasarnya adalah suatu fungsi sederhana yang tak bersifat reversibel. Sehingga dengan mudah kita dapat menghasilkan suatu "signature" yang khas untuk tiap deretan data. Tetapi dari signature tersebut tak dapat dilakukan pembalikan untuk memperoleh deratan data asli.



Gambar 4.5: 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 :

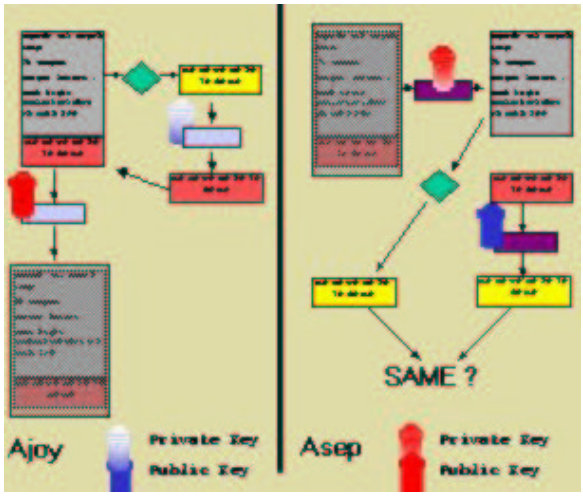
- Keterangan ditail tentang pemilik
- Keterangan tentang pihak yang mengeluarkan sertifikat (Certifier)
- Publik key itu sendiri
- Tanggal valid dan kedaluarsa
- Tanda tangan digital sertifikat tersebut yang dilakukan oleh CA
- Time stamp (penanda waktu)



Gambar 4.6: 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 4.7: Mekanisme keseluruhan

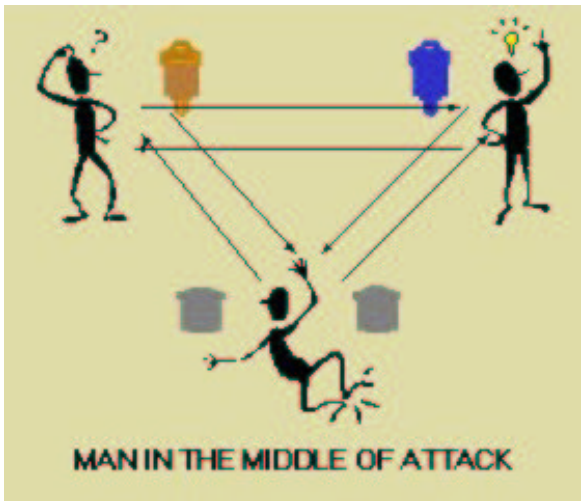
Biasanya CA disediakan oleh suatu institusi yang dipercaya oleh publik, misal suatu institusi pemerintah. Suatu Public Key Infrastructure akan terdiri dari :

- 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.

4.8 Audit dan monitor

Salah satu dari objektif sekuriti adalah accountability dan untuk mencapainya diperlukan mekanisme log (pencatatan) terhadap setiap akses / transaksi. Dalam melakukan pencatatan ini diperlukan informasi yang cukup untuk melakukan audit. Proses pencatatan ini mencakup informasi user-id (*who*), waktu akses dan durasi (*when*), tempat melakukan akses (*where*), objek yang diakses (*what*), dan aktifitas (*how*). Security indicents dapat dideteksi dengan menganalisa informasi dari hasil pencatatan tersebut (log). Untuk mencegah terjadinya security incidents, dapat dilakukan proses audit secara *real time* terhadap log-log tersebut. Untuk itu diperlukan arsip-log terpusat yang kemudian akan dianalisa dan diaudit secara *real time* sebagai proses security monitoring / surveilance yang terus-menerus (*continues*).



Gambar 4.8: Pertimbangan serangan man in the middle

4.9 Formal Method

Kriptografi merupakan buah dari teori matematika "Number of Theory". RSA, EAS, dan Quantum Cryptography merupakan hasil penelitian terkini dari metoda kriptografi. Akan tetapi, seringkali terjadi kelemahan dalam pengejawantahan (engineering process) metoda-metoda tersebut, seperti pada SSL (Secure Socket Layer) untuk mengamankan transmisi data, dan pada S/MIME (Secure/MIME) untuk mengamankan electronic document. Untuk itu setiap pengejawantahan sekuriti baik di tingkat teori, pengembangan aplikasi, dan implementasi sistem memerlukan sebuah metoda untuk melakukan proses spesifikasi, verifikasi, dan validasi. Metoda ini akan memeriksa setiap mekanisme yang ada sehingga mekanisme tersebut dapat dibuktikan berjalan seperti yang diharapkan. Metoda ini dikenal dengan Formal Method atau metoda formal. Beberapa metoda formal untuk sekuriti adalah : SPi Calculus (Martin Abadi) dan Causal Analysis (Peter B. Ladkin).

4.10 Pengguna, Security Policy, dan Manajemen

Pengguna seringkali menjadi mata rantai terlemah dalam sekuriti. Kesalahan dalam memilih password, kecerobohan pengguna dengan menuliskan password, dan mendownload file atau email bervirus sering menjadi penyebab utama security incident. Para cracker sering memanfaatkan ketidakpahaman pengguna akan sekuriti untuk mencari jalan masuk ke dalam sistem. Fenomena ini disebut dengan "social engineering" dalam teori sekuriti. Hal ini menjelaskan mengapa pengguna merupakan salah satu komponen penting dalam membangun sekuriti.

Untuk membatasi akses, mengatur pemakaian sumber daya, dan melindungi pengguna dan/atau sistem, perlu dibuat security policy yang berisi aturan-aturan komprehensif yang terdokumentasi dengan baik. Security policy harus diterapkan secara tepat dan menyeluruh kepada sistem dan penggunanya. Oleh karena itu security policy sudah seharusnya menjadi bagian dari strategi organisasi dan jajaran manajemen melakukan enforcement secara top-down dan pengguna melakukan proses feedback bottom-up untuk menyempurnakan security policy.

5

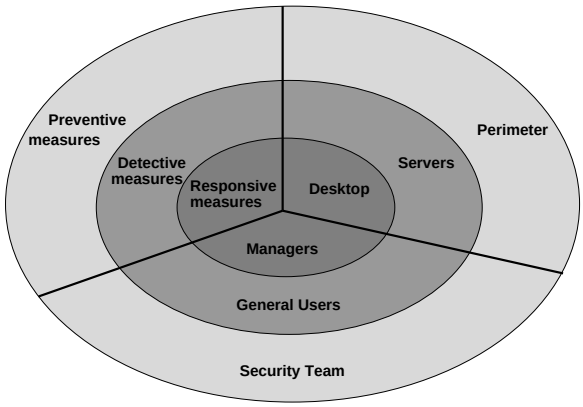
Disain dan impelementasi sekuriti

"*Security is a process, not a product*"

Bruce Schnier

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. Pendekatan multidimensi ini diketengahkan pada gambar 5.1.

5.1 Pertahanan bertingkat



Gambar 5.1: Enterprise IT security framework [32]

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.

5.2 Mekanisme sekuriti yang komprehensif

Untuk menjamin terlaksananya sistem sekuriti yang baik, maka perlu dilakukan tindakan yang menyeluruh. Baik secara preventif, detektif maupun reaktif. Tindakan tersebut dijabarkan sebagai berikut.

Tindakan preventif

Melakukan tindakan preventif atau juga lazin disebut dengan *interdiction* adalah lebih baik dari pada menyembuhkan lobang sekuriti dalam sistem. Beberapa hal yang dapat dilakukan untuk mencegah terjadinya security incidents antara lain adalah :

- Membentuk dan menerapkan security policy yang tepat
- Menanamkan pemahaman sekuriti kepada seluruh pengguna
- Mendefinisikan proses otentikasi
- Mendefinisikan aturan-aturan pada firewall dan akses kontrol
- Pelatihan dan penerapan hukum bagi terjadinya pelanggaran sekuriti
- Disain jaringan dan protokol yang aman
- Deteksi kemungkinan terjadinya vulnerability dan dilakukannya perbaikan sebelum timbul kejadian.

Tindakan detektif

Dengan melakukan deteksi terhadap setiap akses maka tindakan yang tidak diinginkan dapat dicegah sedini mungkin. Tindakan ini pada dasrnya meliputi kegiatan intelligence dan threat assesment. Tindakan detektif meliputi :

- Memasang Intrusion Detection System di dalam sistem internal. Pada sistem ini juga dapat diterapkan teknik *data-mining.* Penerapan distributed intruder detection sangat disarankan untuk sistem yang besar.
- Memasang network scanner dan system scanner untuk mendeteksi adanya anomali di dalam network atau sistem. Analasis jaringan secara real time, untuk mengetahui kemungkinan serangan melalui packet-packet yang membebani secara berlebihan.
- Memasang content screening system dan antivirus software.
- Memasang audit program untuk menganalisa semua log
- Pengumpulan informasi secara social engineering. Hal ini untuk mendengar issue-issue tentang kelemahan sistem yang dikelola.
- Perangkat monitor web dan newsgroup secara otomatis. Dapat juga dilakukan proses monitoring pada channel IRC yang sering digunakan sebagai tempat tukar-menukar infomrasi kelemahan sistem.
- Membentuk tim khusus untuk menangani kejadian sekuriti
- Melakukan simulasi terhadap serangan dan beban sistem serta melakukan analisis vulnerabilitas. Membuat laporan analisis kejadian sekuriti.
- Melakukan pelaporan dengan cara mencari korelasi kejadian secara otomatis

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).

5.3 Tahapan disain 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. Langkah-langkah tersebut disajikan pada Gambar 5.2:

- **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 pengembangan 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.

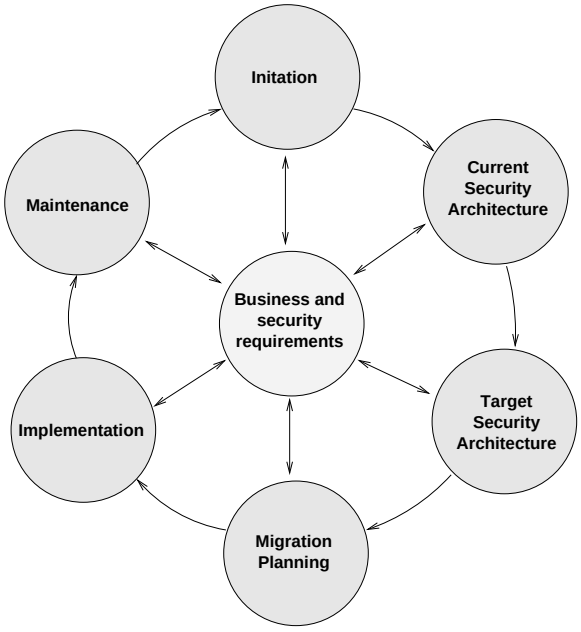
- **Maintenance**
  Sekuriti adalah hal yang sangat dinamik dan ditambah pula dengan perubahan-perubahan teknologi yang cepat. Hal ini memerlukan proses pemeliharaan (maintenance) untuk beradaptasi kepada semua perubahan-perubahan yang terjadi sehingga dapat mengantisipasi terjadinya kelemahan pada sekuriti.

5.4 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



Gambar 5.2: Pendekatan implementasi sekuriti [32]

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 terenda**h
  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.

5.5 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.

5.6 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.

Salah satu permasalahan utama dengan user di sisi sekuriti, adalah akibat komunikasi atau penjelasan yang kurang memadai pada user dan disain yang kurang berpusat pada user yang mengakibatkan lemahnya sekuriti (Adams dan Sasse, 1999). User seringkali tak menerima penjelasan yang cukup, sehingga mereka membuat atau mereka-reka sendiri resiko atau model sekuriti yang terjadi. Seringkali ini menimbulkan pengabaian dan mengakibatkan kelemahan sekuriti.

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.

5.7 Partisipasi seluruh pengguna dan manajemen

Arsitektur sekuriti yang komprehensif bukan hanya terbentuk dari security hardware, software, dan staff teknik. Tetapi melibatkan keseluruhan staff dari semua jajaran dan area di dalam organisasi. Pengalaman menunjukkan bahwa lobang sekuriti seringkali dibuat oleh pengguna yang tidak paham atas sekuriti itu sendiri. Karena itu diperlukan proses edukasi yang cukup terhadap semua pengguna dan bagaimana menjalankan security policy yang telah dibuat.

Tim Sekuriti

Meskipun teknologi untuk membangun sekuriti tersedia, tetapi dibutuhkan tim untuk mendesain dan mengimplementasikan arsitektur sekuriti pada semua level. Oleh karena itu diperlukan sebuah tim yang akan melakukan tugas-tugas sebagai berikut :

- Memformulasikan security policy
- Menganalisa resiko
- Membangun arsitektur software dan hardware
- Membangun lingkungan yang mendukung pelaksanaan sekuriti
- Memonitor operasi

Pengguna Sistem

User merupakan bagian penting dari sekuriti. Pengalaman menunjukkan bahwa seringkali kelemahan sekuriti terjadi karena kecerobohan pengguna. Untuk itu perlu dikembangkan mekanisme dan lingkungan kerja yang mendukung pelaksanaan sekuriti. Dan juga melaksanakan edukasi untuk mengembangkan pemahaman pengguna terhadap sekuriti.

Jajaran Manajerial

Komitmen dan pengertian dari jajaran manajerial bahwa sekuriti adalah bagian penting dari proses yang ada di dalam organisasi merupakan kunci pelaksanaan security policy secara menyeluruh. Jajaran manajerial diharapkan secara aktif meratifikasi dan mempromosilkan security policy, dokumen, atau juklak

6

Framework sekuriti antar-institusi

"Life was simple before World War II. After that, we had system"

Admiral Grace Hopper

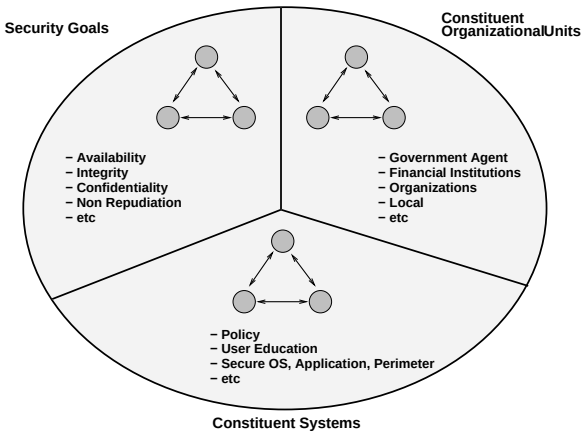
Menjamin sekuriti dalam sebuah sistem bukanlah merupakan pekerjaan yang mudah, apalagi setelah sistem tersebut berhubungan dengan sistem lain sehingga membentuk suatu sistem yang lebih besar dan kompleks. Hal ini disebabkan karena sistem tersebut mempunyai domain yang berbeda, dari perbedaan jenis dan semantik dari informasi, perbedaan operasi dan prosedur, perbedaan resiko, dan perbedaan manajerial. Pada Tabel 6.1 dijabarkan permasalahan dan solusi pada situasi ini.

Problem	Solusi
Semantic Heterogeneity / metapolicy	• Policy Neutral Akses Kontrol (RBAC / SD) • Generic formal language
Secure interoperation	Manual : need based Priority: based on voting Virtual Role in RBAC
Flexibility / Ekstensibility	Policy Library Layered Architecture
Risk Control / Assurance	Safety analysis Tampering proof
Administratif / Management	Role based auditing Risk and Vunerability Analysis Security assasement and architecture

Tabel 6.1: Problem dan solusi pada inter-institusional security framework [21]

Sistem informasi kelautan nasional tidak berdiri sendiri dan akan memerlukan keterhubungan dengan sistem lain untuk pertukaran informasi. Oleh karena itu diperlukan strategi yang tepat untuk membangun sistem tersebut. Bukan saja dari sisi teknis tetapi dari sisi kebijakan sekuritinya juga. Pada Gambar 6.1 disajikan

suatu framework yang dapat dimanfaatkan dalam suatu sistem yang melibatkan banyak instusi.



Gambar 6.1: Inter-institusional Security Framework [21]

7

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. 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

Open Source tidak menawarkan proses pengembangan software "*security through obscurity*". Dalam Open Source seluruh pengguna dan komunitas pengembang ikut menjadi kontrol dalam proses pengembangan sekuriti. Dengan mekanisme ini, sekuriti menjadi prioritas dalam proses pengembangan, dan dapat mengantisipasi adanya bug dalam software secara cepat dan tepat.

8

Penutup

"Security is a journey not a destination"

Anonymous

Semakin kompleks dan saling terhubungnya antar bagian dalam sistem, menjadikan sistem makin sulit untuk dijamin keamanannya. Sekuriti adalah suatu proses, bukan produk. Sebagai proses maka sekuriti itu memiliki banyak komponen. Sekuriti juga seperti rantai yang terdiri dari banyak mata rantai. Seperti halnya rantai, maka kekuatan sistem setara dengan kekuatan dari mata rantai yang terlemah.

Di samping itu, dampak lain akibat tingginya bandwidth dan lamanya koneksi, pengguna memiliki kemungkinan mengalami dampak **information obesity** (Shenk, 1997). Hal ini diakibatkannya lajunya informasi yang datang dan harus diserap dan diolah oleh otak pengguna. Akibat kecepatan yang mekanisme produksi dan distribusi yang hyper cepat ini dan sering lebih tinggi dari kecepatan proses pikiran orang, maka sering menimbulkan dampak yang disebut dengan information discrepancy yang diungkapkan oleh sosiolog Finlandia, Jaako Lehtonen. Efek-efek inilah yang dikenal oleh umum dalam istilah information overload yaitu dampak negatif yang timbul akibat jumlah dan laju informasi yang diterima dan harus diolah. Tak jarang mengakibatkan terbuangnya waktu, menurunnya produktifitas dan bahkan terganggunya kesehatan.

Jaringan komputer memudahkan dilakukannya serangan dan makin cepatnya penyebaran berita salah. Masyarakat sudah lama menjadi korban data statistik yang disalahkan, legenda palsu, berita bohong dan beberapa isue-isue lainnya yang sering menimbulkan kekacauan. Langkah sensor atau blokade informasi ke masyarakat relatif sudah tak dapat dilakukan lagi, maka filter yang paling efektif adalah diri sendiri.

Salah satu cara untuk mencegah dampak buruk dari ini adalah dengan pengguna memahami bagaimana kerja teknologi baru tersebut. Sekedar membawa komputer atau memberikan akses Internet ke dalam ruang kelas, tidak selalu merupakan pemecahan. Bila tidak disertai dengan persiapan kandungan informasi yang tepat, maka akan komputer di kelas akan menjadi semacam junk-food. Disantap, mengenyangkan, menghabiskan waktu dan dana, tapi kurang berisi dan terkadang dapat menimbulkan gangguan kesehatan. Banyak informasi yang diserap, tapi sedikit yang dimanfaaatkan dan menghasilkan buah pikiran.

Untuk itu proses pemahaman teknologi informasi ini haruslah perlu dipertimbangkan matang-matang mekanisme maupun pendekatan yang dilakukannya. Seperti yang diungkapkan oleh Neil Postman dalam bukunya *Technopoly* , setiap

teknologi selalu memiliki *ideologi* yang menyertainya.

> *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

Cara pandang, berfikir dan cara kerja pengguna akan secara perlahan dipengaruhi oleh teknologi ini. Sekali teknologi tersebut digunakan secara luas di masyarakat, maka akan bekerja sesuai dengan dasar disainnya dan akan bekerja sesuai dengan agenda sosialnya sendiri. Justru itu, memahami latar belakang dan dasar disain dari suatu produk teknologi sangat dibutuhkan. Karena pemahaman ini dapat membantu mengurangi dampak buruk dari pemanfaatan teknologi itu secara luas. Memahami dalam arti sekedar menguasai penggunaan dan teknik operasional suatu produk TI saja tidak cukup untuk mengendalikannya. Perlu pemahaman lebih dalam dan mendasar lagi, tentunya ini terutama bagi para praktisi TI.

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.

Sehingga di samping pertimbanga di atas, untuk menyusun strategi sekuriti yang baik bagi sistem informasi kelautan Indoensia 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.

Bibliografi

[1] Abadi, Martin (1997). Explicit communication revisited: two new attacks on authentication protocols. *IEEE Transactions on Software Engineering*, vol 23 (3), Maret 1997, 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.

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

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

[5] Adams, Anne dan Martina Angela Sasse (1999). Users are not the enemy. *Communication of the ACM* . Desember 1999, vol 42 (12), 41-45.

[6] Bellovin, Steven M. (1995). Using the Domain Name System for Sytem Break-ins. *Proceedings of the Fifth Usenix UNIX Security Symposium, Hune, Salt Lake City* . Tersedia di `ftp://ftp.research.att.com`

[7] Butler, Randy, Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Carl Kesselman (2000). A national scale authentication infrastructure. *IEEE Computer* , Desember 2000, 60-64.

[8] Cybenko, George, Guofei Jiang (2000). Developing a distributed system for infrastructure protection. *IT Pro* , July/Agustus 299 hlm. 17 - 22.

[9] *Computerzeitung*, Interview Dirk Henz-BSI : Opensource ist positiv. Nr. 22/31 Mei 2001.

[10] Edwards, John (2001). Next-generation viruses present new chanllenges, IEEE Computer, May 2001, hlm. 16-18.

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

[12] Felten, Edward W, Dirk Balfans, Drew Dean, Dan S Wallach (1997). Web Spoofing : An Internet Con Came. Technical Report 540-96. Department of Computer Science, Princeton University

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

[14] Gutzmann, Kurt (2001). Access Control and Session Management in the HTTP Environment. *IEEE Internet Computing*, January-February 2001, hlm 26-35.

[15] H.M. Gladney and Arthur Cantu. Authorization Management for Digital Libraries. *Communications Of The ACM*, May 2001/Vol. 44. No. 5, hlm 63-65.

[16] 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.

[17] ICE-TEL homepage . `http://www.darmstadt.gmd.de/ice-tel/ice-home.html`

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

[19] James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford (2001). Security Models for Web-Based Applications. *Communications of the ACM*, February 2001/Vol. 44. No 2, page 38-44.

[20] James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford (2001). Digital Government Security Infrastructure Design Challenges. I*EEE Computer*, February 2001, hlm 66-72.

[21] Joshi, Ghafoor, Aref, Spafford, "Digital Government Security Infrastructure Design Challenges"

[22] Kessler, Gary C (2001). Nontechnical Hurdles to Implementing Effective Security Policies. *IT Professional,* March-April 2001, hlm 49-51.

[23] Ladkin, Peter B (1999). *Comment on security.* Lecture material.

[24] Lampson, Buttler W (1994). Authentication in distributed system.

[25] Madsen, Mark, Andrew Herbert (1997). A guide to secure electronic bussiness using the E2S architecture. *Web Security : A matter of trust* . USA : O Reilly.

[26] Michener, John (1999). System Insecurity in the Internet Age. *IEEE Software* , July/August 1999, 62-68.

[27] Ronald, Edmund M.A, Moshe Sipper (2000). The challenge of tamperproof Internet Computing. *IEEE Computer.* Oktober 2000, hlm 98-99.

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

[29] Schneier, Bruce (2000). Semantic Network Attacks. *Communications of the ACM* vol 43(12), Desember 200.

[30] Schneier, Bruce (2000). *Secrets & Lies.* USA : John Willey and Sons.

[31] Shenk, David (1997). *Data Smog : Surviving the information glut* , London : Abacus.

[32] Simon Liu, John Sullivan, Jerry Ormaner. A Practical Approach to Enterprise IT Security. *IT Pro*, September-Oktobe 2001, 35-42.

[33] White House (2000). *National Plan for Information System Protection ver 1.0*

[34] Wiryana, I Made, Avinanta Tarigan (2000). Public Key Infrastructure dan Open Source. *Seminar : Secure your Future.* Tersedia di `http://pandu.dhs.org/Security/artikel-01`

[35] Wiryana, I Made, Tedi Heriyanto (2001). *Resiko Internet Banking telah tampak.* Diterbitkan di DETIK.COM. Tersedia di `http://pandu.dhs.org/Security/artikel-03`

[36] Wiryana, I Made (2001b). *Jangan angap enteng virus SMS.* Tersedia di `http://pandu.dhs.org/Security/artikel-02`

[37] Wiryana, I Made (2001c). *Berbahayanya modem booster.* Tersedia di `http://pandu.dhs.org/Security/artikel-04`

[38] Womack, Helen (1998). *Under Cover lives : Soviet spies in the cities of the world* . London : Weidenfeld Nicholson : London, 1998.

[39] Zwicky, Elizabeth D, Simon Cooper, D. Brent Chapman (2000). *Building Internet Firewall.* OReilly and Associates