BUDI RAHARDJO

KEAMANAN INFORMASI

Contents

Pengantar

Buku ini muncul karena kebutuhan buku teks untuk kuliah keamanan informasi (*information security*). Jenis buku seperti ini agak langka. Bahkan dahulu ilmu yang terkait dengan keamanan - misalnya kriptografi - dianggap tidak boleh diajarkan sehingga referensi untuk hal itu sangat langka. Buku yang pertama kali terbit mengenai kriptografi adalah "Codebreakers" karangan David Kahn [1], yang diterbitkan tahun 1969. Sejak saat ini, ilmu tentang keamanan (security) mulai terbuka untuk umum.

[1] David Kahn. *Codebreakers*. Scribner, 1967

Buku teks berbeda dengan buku *how to* yang banyak beredar di toko buku. Buku tersebut biasanya hanya menjelaskan bagaimana menggunakan sebuah program tertentu, atau melakukan hal tertentu. Sementara itu buku teks digunakan untuk memberikan landasan teori sehingga pemahaman tidak bergantung kepada *tools* tertentu saja. Meskipun demikian, penggunaan *tools* sebagai contoh akan juga disampaikan dalam buku ini. Semoga dengan demikian, buku ini dapat bertahan lebih lama. (Meskipun saya agak ragu setelah melihat pesatnya perkembangan teknologi informasi.)

Urutan pembahasan juga membuat saya merenung cukup panjang. Ada beberapa hal yang disinggung di depan, tetapi pembahasan teorinya di belakang. Sementara itu kalau teorinya diletakkan di depan, maka siswa akan bosan karena terlalu banyak teori. Seharusnya memang buku ini dipaketkan dengan materi presentasi (slide) yang saya gunakan untuk mengajar. Yang itu belum saya benahi. Masih menunggu waktu.

Sebelumnya saya pernah membuat buku yang sejenis, tetapi kode sumber dari buku tersebut sudah hilang. Maklum, saya membuatnya di tahun 1990-an dengan menggunakan program FrameMaker, yang sudah tidak saya miliki lagi. Sekarang saya buat dari awal dengan menggunakan LaTeX agar lebih bisa bebas.

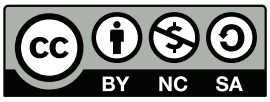
Bagi Anda yang mengajarkan kuliah *security* dan ingin menggunakan buku ini sebagai buku teks, silahkan digunakan. Bagi para mahasiswa dan peneliti yang membutuhkan referensi untuk makalah Anda, semoga buku ini dapat membantu. Selain buku ini, saya juga menulis buku lain yang dapat diunduh juga: "Keamanan Perangkat

Lunak" [2]. Yang ini saya gunakan untuk kuliah saya yang lainnya.

Selamat menikmati versi 0.1.1 dari buku ini. Semoga bermanfaat.

Bandung, 2017
Budi Rahardjo, peneliti
twitter: @rahard
blog: http://rahard.wordpress.com

Penulisan referensi:
Budi Rahardjo, *"Keamanan Informasi"*, PT Insan Infonesia, 2017.



[2] Budi Rahardjo. *Keamanan Perangkat Lunak*. PT Insan Infonesia, 2016

Pendahuluan

Selalu ada aspek negatif dari sebuah pemanfaatan teknologi. Teknologi informasi tidak lepas dari masalah ini. Ada banyak manfaat dari teknologi informasi. Sayangnya salah satu aspek negatifnya adalah masalah keamanan (*security*).

Banyak tulisan dan buku yang mengajarkan cara merusak sebuah sistem informasi. Sementara itu buku yang mengajarkan cara pengamanannya agak minim. Demikian pula, ilmu untuk mengamankan sistem berbasis teknologi informasi juga harus lebih banyak diajarkan.

Keamanan Informasi

Ketika kita berbicara tentang *security*, yang muncul dalam benak kebanyakan orang adalah *network security*, keamanan jaringan. Padahal sesungguhnya yang ingin kita amankan adalah **informasi**. Bahwa informasi tersebut dikirimkan melalui jaringan adalah benar, tetapi tetap yang ingin kita amankan adalah informasinya. Nanti akan kita bahas lebih lanjut mengapa demikian. Maka judul dari buku ini adalah "Keamanan Informasi".

Beberapa Contoh Kasus

Untuk menunjukkan betapa banyaknya masalah keamanan informasi, berikut ini ada beberapa contoh kasus-kasus. Contoh ini bukanlah daftar yang komplit, melainkan hanya sampel dari kondisi yang ada. Bahkan, kemungkinan kondisi yang ada lebih parah daripada contoh-contoh ini.

Beberapa contoh kasus di luar negeri (diurutkan berdasarkan tahun kejadiannya) antara lain dapat dilihat dari daftar berikut.

1. 2006-2008. Tahun-tahun ini ditandai dengan mulai masuknya aspek manajemen ke dalam bidang keamanan informasi. Standar ISO (mulai dari 17799 dan kemudian menjadi seri 27000) mulai digunakan di berbagai instansi. Adanya bencana alam (tsunami,

banjir, gempa, dan sejenisnya) membuat orang mulai memikirkan keberlangsungannya sistem IT. Perangkat IT semakin mengecil dalam ukuran sehingga mulai dibawa pengguna ke kantor. Misalnya pengguna membawa sendiri akses internet dengan menggunakan handphone 3G. Penggunaan kartu sebagai pengganti uang juga mulai populer. (Less cash society.)

2. 2013. Virus masih tetap mendominasi masalah. Pencurian identitas (*identity theft*) mulai marak. Cyber war mulai menjadi bagian dari diskusi.

3. 2014. Heartbleed dan Bash Bug. (Yang ini lebih mudah dijelaskan dengan menggunakan gambar. Sayangnya saya tidak memiliki hak untuk memasukkan gambar tersebut ke dalam buku ini. Di kesempatan berikutnya akan saya usahakan memberi penjelasan dengan kata-kata dulu.)

4. 2014. Bursa Singapura terganggu karena masalah software. Perdagangan saham sempat terhenti.

5. 2016. Sebuah firma hukum di Panama bernama Mossack Fonseca (MF) mengalami kebocoran data. Data yang bocor berupa tabungan / investasi orang-orang terkenal dari beberapa negara (termasuk Indonesia). Kasus ini disebut *Panama Papers Breach*. Kebocoran ini diduga karena *Slider plugin* yang digunakan oleh situsnya (yang menggunakan Wordpress) sudah kadaluawarsa dan memiliki kerentanan. Hasil eksploitasi memperkenankan orang untuk mengambil berkas sesukanya.

6. 2016. CCTV digunakan sebagai bagian dari Distributed DoS attack. Ini menunjukkan bahwa perangkat yang menjadi bagian dari Internet of Things (IoT) dapat menjadi target serangan untuk kemudian dijadikan "anak buah" (zombie) untuk menyerang tempat lain. Kode sumber Mirai yang digunakan untuk melakukan penyerangan tersedia di internet. Jika kita tidak siap, ini dapat menjadi masalah yang berikutnya.

7. 2016. Serangan DDoS terhadap berbagai DNS (Domain Name System) servers. Serangan menggunakan bantuan *botnet* sehingga menghabiskan *bandiwdth* jaringan dalam orde Gbps.

Selain contoh-contoh di atas, tentunya masih banyak kasus-kasus lain. Ada yang menganalogikan ini sebagai puncak dari *iceberg*. Di bawah laut lebih banyak lagi masalah yang tidak terlihat.

Beberapa contoh kasus yang terkait dengan Indonesia dapat dilihat dari daftar berikut.

1. 1999. Nama domain Timor Timur (.TP) diacak-acak. Diduga pelakunya adalah pemerintah Indonesia. Investigasi lebih lanjut menunjukkan bahwa ini tidak dilakukan oleh pemerintah Indonesia tetapi oleh seseorang (atau sekelompok) yang berada di Amerika Serikat.

2. 2011. Perusahaan Research in Motion (RIM) yang memproduksi *Blackberry* dipaksa untuk memiliki server di Indonesia. Alasan utama adalah agar dapat dilakukan *lawful interception*, yaitu penyadapan secara legal untuk kasus-kasus tertentu. Pihak RIM keberatan. Tidak ada server RIM di Indonesia.

3. 2015. Serangan man-in-the-browser (MITB) dilakukan terhadap berbagai layanan internet banking di Indonesia sehingga mengakibatkan hilangnya uang nasabah[3]

4. 2016. Aplikasi Pokemon Go mulai muncul dan ramai digunakan. Aplikasi ini menggunakan lokasi pengguna sebagai bagian dari permainannya, yaitu untuk menampilkan monster Pokemon sesuai dengan lokasi. Selain itu, foto dari lingkungan sekitarnya dapat juga kita ambil dan kita bagikan (share) dengan orang lain melalui media sosial. Aplikasi ini dilarang digunakan di lingkungan milter dan pemerintahan karena dikhawatirkan dapat membocorkan data rahasia. (Sebetulnya ada banyak aplikasi lain yang juga menggunakan data lokasi seperti *Waze* dan *Google Maps*, tetapi ini tidak "terlihat". Bahkan lebih berbahaya lagi adalah penggunaan layanan email gratisan untuk akun resmi pemerintahan atau instansi lain di Indonesia.)

5. 2016. Berbagai *market place* (seperti Tokopedia, Bukalapak, dll.) dan aplikasi handphone (seperti Go-Jek) diserang oleh orang yang mencoba melakukan password cracking. Asumsinya adalah seseorang akan menggunakan userid (alamat email) dan password yang sama untuk situs-situs tersebut. Identitas yang bocor di sebuah layanan (web site, application) dicoba digunakan di tempat lain.

6. 2016. Topik pembentukan "Badan Cyber Nasional (BCN)" mulai hangat dibicarakan.

[3] http://regional.kompas.com/read/2015/08/11/12185971/ Kronologi. Hilangnya. Uang. Nasabah. Bank. Mandiri. Versi. Korban

Saat ini semakin banyak lagi masalah keamanan yang ditemui. Hal ini disebabkan semakin banyak pemanfaatan teknologi informasi dan jaringan internet. Selain itu teknik untuk menemukan lubang keamanan juga semakin canggih sehingga lebih banyak ditemukan kelemahan-kelemahan tersebut.

Sebuah survey yang dilakukan oleh *Information Week* di Amerika Serikat (tahun?) menunjukkan bahwa hanya 22 persen manager

yang menganggap keamanan sistem informasi sebagai hal yang penting. Bagaimana meyakinkan mereka untuk melakukan investasi di pengamanan?

Rendahnya kesadaran atas masalah keamanan (lack of security awareness) merupakan salah satu kunci utama munculnya masalah keamanan. Para praktisi juga masih menjalankan kebiasaan buruk, seperti misalnya berbagi password admin.

Masalah keamanan informasi yang biasanya berupada data teknis harus diterjemahkan ke angka finansial agar dapat dimengerti oleh pihak pimpinan. Sebagai contoh, di Inggris ada survey mengenai berapa biaya yang dikeluarkan perusahaan jika sistem mereka tidak dapat diakses (*down*).

Security Life Cycle

Banyak orang yang beranggapan bahwa masalah keamanan informasi dapat dipecahkan dengan membeli produk keamanan, misalnya firewall, anti-virus, dan seterusnya. Kemanan informasi sebetulnya berupa sebuah siklus sebagaimana ditampilkan pada Gambar 1.

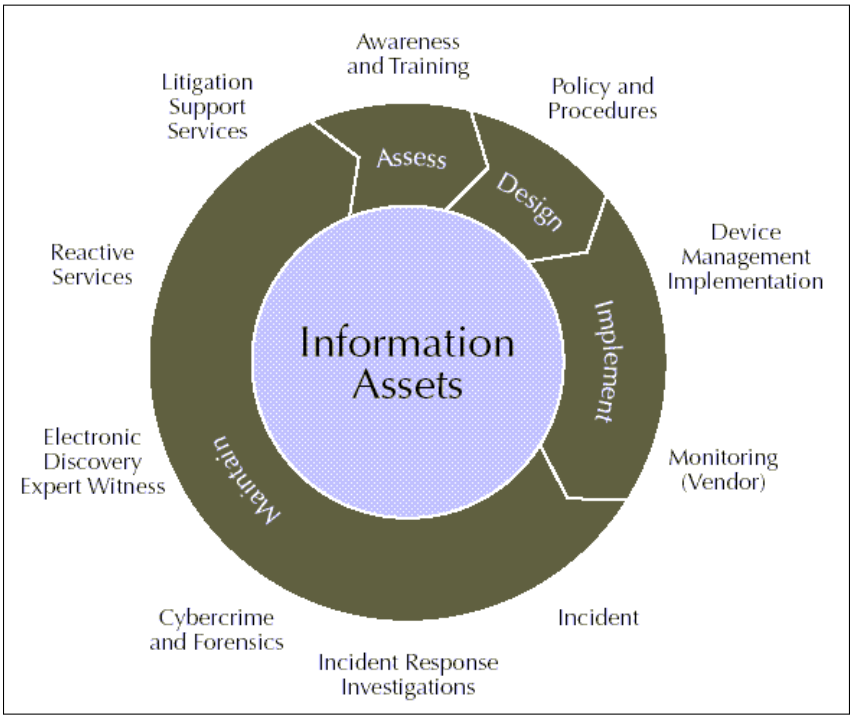


Figure 1: Security Life Cycle

Prinsip-prinsip Keamanan Informasi

Ada beberapa prinsip utama dalam keamanan informasi. Bab ini akan membahas prinsip-prinsip tersebut secara singkat. Hal-hal yang lebih rinci dan teknis, misalnya bagaimana mengimplementasikan aspek keamanan, akan dibahas pada bagian terpisah.

Aspek Keamanan

Ketika kita berbicara tentang keamanan informasi, maka yang kita bicarakan adalah tiga hal; *confidentiality*, *integrity*, dan *availability*. Ketiganya sering disebut dengan istilah **CIA**, yang merupakan gabungan huruf depan dari kata-kata tersebut. Selain ketiga hal tersebut, masih ada aspek keamanan lainnya.

Ketika kita berbicara tentang keamanan sebuah sistem - jaringan, aplikasi, atau apa pun - yang kita lakukan adalah mengevaluasi aspek C, I, dan A dari sistem tersebut. Prioritas dari ketiga aspek tersebut berbeda-beda untuk jenis sistem dan organisasi yang menggunakannya. Ada sistem yang aspek *integrity* lebih penting daripada kerahasiaannya (*confidentiality*). Untuk itu, pahami ketiga aspek ini. Ini adalah prinsip utama dari keamanan.

Confidentiality

Confidentiality atau kerahasiaan adalah aspek yang biasa dipahami tentang keamanan. Aspek confidentiality menyatakan bahwa data hanya dapat diakses atau dilihat oleh orang yang berhak. Biasanya aspek ini yang paling mudah dipahami oleh orang. Jika terkait dengan data pribadi, aspek ini juga dikenal dengan istilah *Privacy*.

Serangan terhadap aspek confidentiality dapat berupa penyadapan data (melalui jaringan), memasang *keylogger* untuk menyadap apa-apa yang diketikkan di keyboard, dan pencurian fisik mesin / disk yang digunakan untuk menyimpan data.

Perlindungan terhadap aspek *confidentiality* dapat dilakukan dengan menggunakan kriptografi, dan membatasi akses (segmentasi jaringan)

Integrity

Aspek *integrity* mengatakan bahwa data tidak boleh berubah tanpa ijin dari yang berhak. Sebagai contoh, jika kita memiliki sebuah pesan atau data transaksi di bawah ini (transfer dari rekening 12345 ke rekening 6789 dengan nilai transaksi teretentu), maka data transaksi tersebut tidak dapat diubah seenaknya.

```
TRANSFER 12345 KE 6789 100000
```

Serangan terhadap aspek *integrity* dapat dilakukan oleh *man-in-the-middle*, yaitu menangkap data di tengah jalan kemudian mengubahnya dan meneruskannya ke tujuan. Data yang sampai di tujuan (misal aplikasi di web server) tidak tahu bahwa data sudah diubah di tengah jalan.

Perlindungan untuk aspek *integrity* dapat dilakukan dengan menggunakan *message authentication code*.

Availability

Ketergantungan kepada sistem yang berbasis teknologi informasi menyebabkan sistem (beserta datanya) harus dapat diakses ketika dibutuhkan. Jika sistem tidak tersedia, *not available*, maka dapat terjadi masalah yang menimbulkan kerugian finansial atau bahkan nyawa. Itulah sebabnya aspek *availability* menjadi bagian dari keamanan.

Serangan terhadap aspek *availability* dilakukan dengan tujuan untuk meniadakan layanan atau membuat layanan menjadi sangat lambat sehingga sama dengan tidak berfungsi. Serangannya disebut *Denial of Service* (DOS).

Perlindungan terhadap aspek *availability* dapat dilakukan dengan menyediakan redundansi. Sebagai contoh, jaringan komputer dapat menggunakan layanan dari dua penyedia jasa yang berbeda. Jika salah satu penyedia jasa jaringan mendapat serangan (atau rusak), maka masih ada satu jalur lagi yang dapat digunakan.

Aspek Keamanan Lainnya

Selain ketiga aspek utama (CIA), yang sudah dibahas pada bagian sebelumnya, ada aspek keamanan lainnya. Yang ini sifatnya tambahan, meskipun kadang menjadi bagian yang cukup signifikan juga.

Non-repudiation

Aspek *non-repudiation* atau nir-sangkal digunakan untuk membuat para pelaku tidak dapat menyangkal telah melakukan sesu-

atu. Aspek ini biasanya kental di dalam sistem yang terkait dengan transaksi. Contoh penggunaannya adalah dalam sistem lelang elektronik.

Implementasi dari aspek ini dapat dilakukan dengan menggunakan *message authentication code* (dengan menggunakan fungsi *hash*) dan pencatatan (logging).

Authentication

Proses *Authentication* digunakan untuk membuktikan klaim bahwa seseorang itu adalah benar-benar yang diklaim (bagaimana membuktikan bahwa saya adalah pengguna dengan nama "budi").

Proses pembuktian seseorang ini lebih mudah dilakukan di dunia nyata dibandingkan dengan di dunia maya (siber, *cyber*). Di dunia nyata akan sulit bagi saya untuk membuat klaim palsu bahwa saya seorang wanita. (Saya memiliki kumis dan jenggot.) Namun di dunia maya, saya dapat membuat klaim bahwa saya seorang wanita dengan hanya memilih nama wanita dan memasang foto wanita.

Proses *authentication* ini dapat dilakukan dengan bantuan hal lain, yang sering disebut "faktor". (Sehingga ada istilah *two-factor authentication*.) Faktor-faktur tersebut adalah sebagai berikut.

1. Sesuatu yang diketahui. Contoh dari faktor ini adalah nama, userid, password, dan PIN.
2. Sesuatu yang dimiliki. Contoh dari faktor ini adalah kartu, kunci, dan token.
3. Sesuatu yang menjadi bagian dari fisik pengguna. Contoh dari faktor ini adalah sidik jari, retina mata, dan *biometric* lainnya.

Selain faktor-faktor di atas, ada juga yang menambahkan faktor lain seperti berikut ini:

1. orang tersebut berada di tempat tertentu. (Proximity);
2. authentication dengan menggunakan bantuan pihak lain, pihak ketiga yang terpercaya (trusted third party).

Bibliography

[1] David Kahn. *Codebreakers*. Scribner, 1967.

[2] Budi Rahardjo. *Keamanan Perangkat Lunak*. PT Insan Infonesia, 2016.