Masa Depan Sekuriti Informasi

Agus Fanar Syukri
afs@istecs.org

Abstrak:
Sejak tahun 1990-an, internet berkembang pesat ke seluruh dunia karena semakin mudahnya akses informasi ke jejaring internet, dengan menggunakan teknologi WWW (*World Wide Web*) dan juga dukungan visi PC (Personal Computer)-nya Microsoft, serta perkembangan open source OS Linux yang sangat pesat. Saat ini, internet telah menjadi bagian dari kehidupan kita sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk privat. Tetapi di balik itu masih banyak lubang kelemahan sistem di internet yang bisa dimanfaatkan oleh para *cracker* untuk tujuan tidak baik, seperti bom mail, pengacak-acakan *home page*, pencurian data, pasword ataupun nomor kartu kredit, dll. Dalam makalah ini dibahas masalah teknologi sekuriti informasi di internet, ancaman kejahatan di internet dan kiat-kiat untuk menanggulanginya, serta prakiraan perkembangan industri teknologi sekuriti informasi 10 tahun ke depan.

Kata Kunci: internet, sekuriti informasi, perkembangan industri teknologi sekuriti informasi

Pendahuluan
Sampai awal tahun 1990-an, yang dapat mengakses informasi atas perubahan dunia selama 24 jam penuh di bidang politik, ekonomi, kebudayaan, sosial dan lain-lainnya, mengumpulkan informasi, mengolahnya, kemudian memanfaatkannya untuk keuntungan perusahaan/institusi, hanyalah dimonopoli oleh perusahaan-perusahaan yang mempunyai *mainframe* yang terhubung ke jaringan komputer saja. Tetapi dengan revolusi teknologi komputer yang sangat cepat yang dimotori oleh Microsoft, kemampuan PC (Personal Computer) pun meningkat pesat, harganya semakin murah, dan pemakaiannya pun menjadi semakin mudah (*user friendly*), sehingga keberadaannya dari kebutuhan barang mewah (konsumsi *sekunder* atau *tersier*), telah cenderung menjadi barang konsumsi *primer*, yang mau tidak mau harus ada dan sangat diperlukan keberadaannya, khususnya oleh para *'netter'* (pengguna internet) dan para pebisnis.

Internet & Perkembangannya
Internet adalah jaringan informasi yang pada awalnya (sekitar akhir 1960-an, tepatnya mulai tahun 1969) dikembangkan oleh Departeman Pertahanan dan Keamanan Amerika Serikat (*DoD = Departement of Defense USA*) sebagai proyek strategis yang bertujuan untuk berjaga-jaga (penanggulangan) bila terjadi gangguan pada jaringan komunikasi umum, khususnya pengaruhnya pada sistem komunikasi militer mereka. Pada saat itu perang dingin antara Amerika Serikat dengan Uni Soviet sedang mencapai puncaknya, sehingga mereka membuat antisipasi atas segala kemungkinan akibat perang yang mungkin akan terjadi.

Pada awalnya internet hanya digunakan secara

terbatas di dan antar-laboratorium penelitian teknologi di beberapa institusi pendidikan dan lembaga penelitian saja, yang terlibat langsung dalam proyek *DARPA* (*Defence Advanced Research Projects Agency*). Tetapi 30 tahunan kemudian (sekarang ini), internet telah meluas ke seluruh dunia, dari pemerintah, perusahaan besar dan kecil, LSM hingga perorangan telah banyak yang memanfaatkannya, karena kepraktisannya sebagai sarana komunikasi dan untuk pencarian informasi

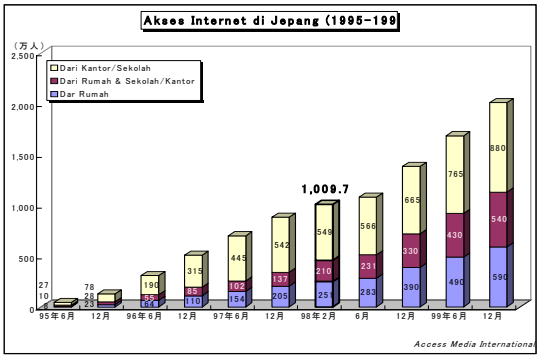
Data tentang internet tahun 1998 menyebutkan bahwa *e-mail* telah dapat dikirim ke 150 negara lebih di dunia ini, *transfer file (ftp)* dapat menjangkau ke 100-an negara, dan pengguna di seluruh dunia pun diperkirakan telah sampai 60 juta-an orang, atau 5% dari jumlah total seluruh penduduk dunia[5]. Kemudian, berdasarkan data tahun 1999, pengguna internet di seluruh dunia hingga Mei 1999 sudah mencapai 163 juta orang. Hampir sama dengan jumlah penduduk Jepang. Alamat *situs* atau *website* (*home page*) kini berjumlah sekitar 600 juta[7].

Sejak tahun 1990, *www (world wide web)* menggelobal ke seluruh pelosok dunia, menjanjikan akses informasi yang sangat mudah oleh siapa pun, termasuk oleh pemakai komputer pemula sekali pun. Ledakan *www* (sering disebut dengan *web* saja) menjadi salah satu faktor terbesar maraknya internet.

Manfaat dan Bahaya Internet

Melihat perkembangan dan pemanfaatan internet yang demikian pesat, di balik manfaat yang besar, ternyata ada bahaya yang mengancam, yang tidak banyak disadari oleh para pemakai internet, khususnya oleh para *netter* pemula. Untuk meminimalkan kemungkinan terjadinya tindak kejahatan di internet inilah diperlukan teknologi sekuriti informasi, khususnya sistem dan mesin *enkripsi* (penyandian)[4].

Dunia sandi yang berabad-abad mempunyai kesan gelap dan menakutkan, karena hanya dikuasai oleh militer, spionase ataupun kalangan diplomat saja, telah tiba saatnya untuk memancarkan sinar cerah dan kehangatannya, yaitu dengan dapat dimanfaatkannya oleh dan untuk masyarakat umum, yang dimulai dari kalangan bisnis. Bukan hanya untuk tujuan merahasiakan data dan jaringan komunikasi semata, tetapi mempunyai tujuan lebih besar, yaitu perlindungan privasi masing-masing anggota masyarakat yang terhubung ke jaringan global tanpa batas, internet.

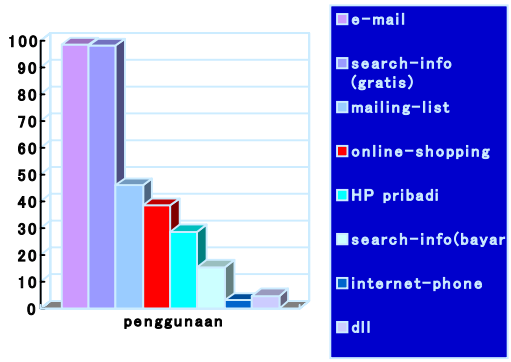


Gambar 1: Pertumbuhan Pemakai Internet di Jepang

Tetapi harus kita ingat juga, walaupun internet telah berkembang ke seluruh pelosok dunia secara global dan tidak mempunyai batas-batas negara lagi, kejahatan yang mungkin timbul masih tetap mempunyai ciri dan cara yang bergantung kepada negara/ daerah tempat si pelaku berada, yaitu cara perpikir, cara pandang, moral, norma kehidupan dan pergaulan, serta fakto-faktor lokal lainnya. Bahkan bahasa pun sangat mempengaruhinya. Pintu dan tingkat kecanggihan kejahatan di tingkat global pun berkembang bersama perkembangan jaman dan kebudayaan lokal.

Sebagai salah satu contoh perkembangan internet, kita bisa melihat salah satunya di Jepang, seperti ditunjukkan pada gambar 1. Pertumbuhan pemakai internet di Jepang adalah seperti garis linier (deret hitung), naik secara pasti dari tahun ke tahun, dan di tahun 1999, telah mencapai 15 juta orang lebih, atau 1/10 jumlah penduduk Jepang.

Kemudian, dilihat dari pemakaian internet untuk apa, seperti ditunjukkan pada gambar 2, yang terbanyak adalah untuk e-mail dan untuk mencari informasi secara gratis (masing-masing 98.5% dan 98%). Setelah itu untuk *mailing-list*, belanja secara *on-line* lewat internet, untuk membuat homepage perusahaan ataupun pribadi, menduduki peringkat berikutnya. Dari gambar 2, *on-line shopping* hanya menduduki rangking ke-4 (38.4%), menandakan bahwa belanja lewat internet masih belum dilirik oleh kebanyakan orang, mungkin karena mereka masih ragu-ragu tentang keamanan belanja di dunia maya.



Gambar 2: Pemakaian Internet di Jepang

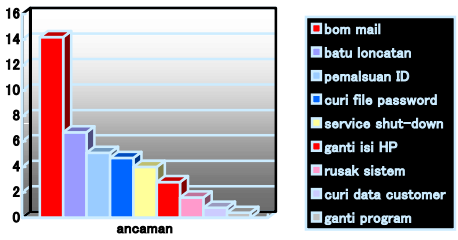
Sekuriti Internet

Dari uraian di paragraf-paragraf sebelumnya, pembaca pasti sudah tahu bahwa sebenarnya internet belumlah benar-benar aman. 2 alasan utama ketidakamanan internet adalah sebagai berikut:

1. Internet adalah wilayah bebas *tak bertuan*, tak ada pemerintahan & hukum yang mengaturnya. Manajemen dan perlindungan keamanan masing-masing jaringan diserahkan sepenuhnya kepada penanggungjawab jaringan (*administrator* jaringan internet). Dan pada kenyataannya, tidak semua administrator jaringan, mengerti dengan baik tentang keamanan internet.
2. Masih banyaknya '*hole*' (lubang) di sistem komputer dan jaringan yang dapat dimanfaatkan oleh *cracker* [1] demi keuntungan/kepuasan nafsu pribadinya.

Contoh-contoh Kejahatan di Internet dan Kiat-kiat Penanggulangannya

Dari kasus kejahatan di Jepang (gambar 3), dapat kita lihat bahwa kejahatan yang terbesar adalah bom mail, kemudian diikuti oleh batu loncatan penyerangan, pemalsuan ID dan seterusnya yang akan dijelaskan lebih detail berikut ini.



Gambar 3: Kejahatan Internet di Jepang

Bom Mail

Pengiriman bom mail ke sebuah e-mail address, biasanya dimulai oleh sentimen pribadi si pemilik e-mail address (*target*) dengan cracker. Cracker mengirimkan e-mail sebanyak-banyaknya ke komputer target, sehingga sistem di komputer target *down* (*hang-up*) karena kepenuhan e-mail.

Kiat penanggulangannya:
1. Konsultasi dengan ISP[2];
2. Protes ke pengirim & ISP pengirim;
3. Menaruh *filtering software* di mail server, untuk mencegah pengiriman e-mail oleh cracker yang sudah teridentifikasi.

Batu Loncatan Penyerangan

Sistem komputer dengan pengamanan lemah, tak jarang digunakan oleh cracker sebagai batu loncatan untuk menyerang target (komputer) lain, dengan maksud untuk lebih mengaburkan jejak si cracker .

Untuk itu, setiap penanggung jawab sistim komputer, sebenarnya tidak hanya bertanggung jawab terhadap sistimnya sendiri, tapi juga bertanggung jawab terhadap jaringan lain, baik yang terdekat maupun jaringan yang relatif jauh dari jaringan Internet wilayahnya.

Sebagai langkah preventif, penerapan sistim deteksi penerobosan merupakan suatu hal yang sangat disarankan.

Pemalsuan ID

Seorang cracker hampir dapat dipastikan tidak akan pernah memakai ID (identifitas) asli yang dimilikinya. Cracker akan berusaha menggunakan ID milik orang lain, atau membuat ID palsu dalam setiap gerakannya. Untuk mendapatkan ID orang lain, cracker dapat

[1] Yang disebut ***cracker*** adalah sebutan untuk mereka yang sangat mengerti tentang seluk-beluk komputer (software ataupun hardware-nya) beserta kelemahan-kelemahannya, yang memanfaatkan kesempatan atas kelemahan sistem yang ada untuk kepentingan yang kurang baik. Sebaliknya, bila mereka yang tahu tentang kelemahan sistem komputer dan komunikasinya, tetapi mereka berusaha memberitahukannya ke orang lain, memperbaikinya (atau secara umum untuk kepentingan yang lebih baik), disebut sebagai ***hacker***. Jadi cracker sangat lain dengan hacker.

[2] Internet Service Provider = penyedia jasa internet

mencari lewat penye-"*trap*"-an data-data yang lewat jaringan, dan menganalisanya.

Penggunaan sistim otentikasi yang baik seperti otentikasi dengan menggunakan kartu pintar (*smart card*), sidik jari dan lain-lain, merupakan salah satu jalan keluar dari masalah ini.

Pencurian File Password atau Data Customer
Salah satu cara untuk mendapatkan ID milik orang lain, tak jarang seorang cracker berusaha mencuri file password dari suatu sistem, kemudian menganalisanya. Lebih dari itu, cracker secara pribadi ataupun bersindikat, berusaha mencuri data rahasia suatu perusahaan untuk dijual ke perusahaan lawan.

Di AS, seorang cracker pernah berhasil mendapatkan ratusan ribu data kartu kredit dari hasil analisa program yang ditanamkan di server ISP-nya.

Untuk penanggulangan pencurian file password adalah dengan melakukan pencegahan penggunaan password yang mudah ditebak, sehingga biarpun file dicuri, tidak terlalu bermanfaat. Cara lainnya adalah dengan menggunakan sistim *shadowing* pada sistim password di sistim Unix, atau untuk sistim WindowNT, microsoft menerapkan sistim *enkripsi* (penyandian).

Untuk pengamanan data yang melewati jaringan terbuka seperti Internet, tidak ada jalan lain selain penggunaan enkripsi sehingga data yang lewat tidak bisa dimanfaatkan orang yang tidak berhak ataupun oleh cracker.

Shut-down Service
Seorang cracker terkadang berusaha meng-*hang-up* suatu sistem, dengan tujuan agar sistem target tidak dapat melayani service dari semua user. Kejadian ini pernah menimpa Microsoft, yang mana akses ke homepage-nya oleh semua user ditolak, karena komputer server dibuat 'sibuk' sendiri oleh si cracker.

Biasanya penyebab masalah ini adalah terletak pada program server yang menangani suatu jasa/service tertentu. Yang paling sering terjadi adalah desain program server yang tidak memikirkan/ mempertimbangkan masalah keamanan jaringan, sehingga penggunaan *buffer* (tempat penampungan sementara di memori/hard disk) tidak terkontrol dan mengakibatkan server tidak bisa menangani permintaan jasa dari pengguna yang sebenarnya.

Penanggulangannya adalah dengan penggunaan server yang didukung oleh costumer service dari pembuat program adalah suatu hal yang mutlak diperlukan oleh situs internet, terutama yang mempunyai tingkat kepopuleran yang tinggi. Sehingga setiap kelemahan yang ditemukan dari suatu sistim bisa segera didapatkan penanggulangannya. Selain itu, perlu juga dipertimbangkan pemilihan server dari pembuat program yang lebih mengutamakan kestabilan sistem daripada kelebihan fungsi-fungsi di level aplikasi.

Penggantian Isi Homepage
Masalah ini pun sering kali menimpa beberapa site di Indonesia. Contohnya oleh cracker portugis (dalam masalah Timor Timur) dan Cina (tentang kerusuhan Mei 1998 yang banyak menewaskan orang-orang Cina di Indonesia). Bahkan, di Jepang pun HP Science Technology Agency di-crack lewat penggantian halaman depan HP.
Biasanya, sistim server yang menangani jasa web ini tidak menggunakan pendekatan keamanan dalam pengoperasiannya. Padahal, walaupun suatu sistim dikatakan kuat oleh pembuatnya, kalau tidak didukung dengan *security policy* (peraturan/kebijaksanaan internal keamanan) dan pengoperasian yang baik, tidak akan bisa menghasilkan sistim yang kuat. Selain itu, hubungan dengan pihak pembuat program merupakan salah satu hal yang diperlukan dalam membangun sistim yang tahan serangan.

Program Jebakan
Trojan Horse (kuda troya) sudah dikenal sebagai salah satu teknik cracker yang sangat ampuh dan sering digunakan dalam kejahatan-kejahatan di Internet. Cracker memberikan program gratis, yang *feature*-nya bagus (banyak fungsi-fungsi program yang bermanfaat) dan penggunaanya mudah dan enak (*user friendly*), tetapi di dalam program tersebut, sebenarnya si cracker 'menanamkan' program lain yang tidak terlihat oleh user. Misalnya program untuk pencurian ID dan password, pencurian file-file tertentu dan lain-lain.

Untuk menanggulangi masalah ini, penanggung jawab sistim sebaiknya selalu melakukan pengecekan terhadap program yang dipakainya dengan melakukan pencocokan jejak (*log*) kriptografi dari programnya dengan jejak yang disediakan oleh pembuat program.

Mengapa Kejahatan di Internet Marak?
Beberapa alasan, mengapa kejahatan di internet marak adalah sebagai berikut:

1. Internet adalah wilayah bebas, tak ada pemerintahan & hukumnya;
2. Akses user dari kamar (tempat terpencil) dan lemahnya pengawasan dari orang lain, sehingga nafsu pribadilah yang akan menguasai si user;
3. Kurangnya kesadaran adanya '*hole'* kejahatan di internet oleh kebanyakan user;
4. Belum adanya standar keamanan manajemen jaringan internet.

Perkembangan Industri Sekuriti di Masa Depan
10 tahun ke depan, sampai tahun 2010 perkembangan industri sekuriti di Jepang[8] diperkirakan akan seperti daftar di bawah.

Industri	Prakiraan Pasar (milyar Yen)	Keterangan
1. Produksi Komputer	50	Asumsi perkembangan pasar komputer 3%
2. Produksi Device Penunjang Elektronik	430	Asumsi perkembangan pasar pertahun 10%
3. Network Hardware	90	Asumsi perkembangan pasar pertahun 20%
4. Network Software (S/W)	---	Tak bisa diprediksi
5. Produksi Sekuriti S/W	950	Asumsi perkembangan pasar pertahun 10~60%
6. Managemen -Network: Inspeksi Identifikasi Auto-sourching Key-manajemen	 10 10 10 10	
7. Managemen Content	11,4	
8. Back-up/Recovery	94	
9. Satpam (Industri, home-security)	7.400	Asumsi perkembangan pasar pertahun 5~15%
10. Industri Keuangan	---	Sulit diprediksi dari bidang Sekuriti Inf.
11. Industri Asuransi	110	Asumsi perkembangan pasar pertahun 3%
12. Integrasi –Sistem: Diklat Evaluasi Inspeksi Solusi	 1 3 4 190	 20% dari 5. Produksi Sekuriti S/W
Jumlah	9.370	

Penutup
Dari paparan tersebut di atas, dapat kita ambil beberapa poin keseimpulan sebagai berikut:

- Internet yang semakin meng-*global* dan menjanjikan berbagai kemudahan akses ke seluruh pelosok dunia yang terhubung lewat jaringan, **belum** benar-benar aman, khususnya untuk pemanfaatan di sektor bisnis;
- Masih adanya '*hole*' kelemahan (*bug)* di sistem komputer dan jaringan internet, yang bisa dimanfaatkan oleh *cracker;*
- Implementasi Sekuriti yang belum memadai di semua tingkat jaringan internet;
- Belum adanya UU internet di dunia global, menyulitkan penangkapan, pengadilan dan hukuman atas cracker;
- Pembuatan *security policy* (kebijakan internal keamanan) yang baik beserta penerapannya, merupakan suatu langkah yang mutlak diperlukan oleh perusahaan atau organisasi yang menghubungkan jaringannya ke Internet.
- Pasar Industri Sekuriti Informasi masih terbuka lebar, selebar pasar internet yang terus berkembang.
- Internet hanyalah ***sarana*** komunikasi, semakin bermanfaatkah atau sebalik-nya, diri & akhlaq kita sendiri-lah yang menentukan penggunaannya.

Referensi
[1] Kaufman C., Perlman R. And Spenicer M, "Network Security: Private Communication in a Public World", Prentice Hall, 1995.
[2] Schneier B, "E-mail Security", John Wiley & Sons, Inc, 1995.
[3] Schneier B, "Applied Cryptography", John

Wiley & Sons, Inc, 1996.
[4] Syukri, A.F., "Revolusi Teknologi Penyandian: Habis Gelap Terbitlah Terang", INOVASI (Media Komunikasi Sains & Teknologi PPI Jepang) vol.8, no. 2, Agustus 1998.
[5] Internet Association of Japan, "White Book of Internet 1998", Impresso, 1998.
[6] CERT, http://www.cert.org
[7] Kafi Kurnia, "Internet", GATRA Nomor 04/VI, 11 Desember 1999.
[8] JIPDEC,"Report on Security Information Technology & Industry and Future Movement", March 1999. (Berbahasa Jepang.)

Biografi Penulis

Agus Fanar Syukri
Lahir di Demak, 15 September 1969.
Afiliasi di Indonesia :
Laboratorium Industri Strategis/Lab Pengujian, KIM-LIPI Kompleks Puspiptek Serpong, Tangerang Jawa Barat, 15314 INDONESIA. Telp:021-7560562 Faks:021-7560568

Riwayat Pendidikan :

1985-1988	SMA N 1 Kudus
1989-1990	Japanese School (Kokusai Gakuyukai Nihongo Gakko)
1990-1994	S1 Saga University, Information Science.
1996-1998	S2 Japan Advanced Institute of Science & Technology (JAIST), Information Science, Security Information.

Beasiswa:

1989-1994	Science & Technology Manpower Development Program (STMDP)
1996-1997	Science & Technology A?? Indonesian Development (STAID)

Minat penelitian :
Security Information, Wireless Communication, R&D process.
Riwayat Kerja (efektif) :

1995-1996	KIM-LIPI
1998-now	NEC R&D Laboratory.

Society memberships:
ISTECS, IECI