Keamanan dalam *Electronic Commerce*

Outline

- Electronic Commerce
- Contoh kasus masalah keamanan
- Dasar-dasar keamanan
- Upaya untuk meningkatkan keamanan
- Sumber informasi

Electronic Commerce

- Ecommerce akan berlangsung jika tingkat keamanan sudah dalam batas yang dapat diterima
- Sudahkah?
- Masalah: bisnis tidak dapat menunggu
  - New economy, digital economy: membingungkan semua orang
  - Bubbles? Atau nyata? Global 1000 companies

Contoh kasus keamanan di Indonesia

- Penjebolan web site (yang baru)
  - www.RedHat.or.id
  - Satelindo.co.id
  - Polri.go.id
  - FKP.or.id
  - BEJ, dst.
  - http://www.2600.com

Statistik & contoh

- Angka pasti, sulit ditampilkan karena kendala bisnis. Negative publicity.
- 1996. FBI National Computer Crime Squad, kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan.
- 1996. American Bar Association: dari 1000 perusahaan, 48% telah mengalami computer fraud dalam kurun 5 tahun terakhir.
- 1996. Di Inggris, NCC Information Security Breaches Survey: kejahatan komputer naik 200% dari 1995 ke 1996.
- 1997. FBI: kasus persidangan yang berhubungan dengan kejahatan komputer naik 950% dari tahun 1996 ke 1997, dan yang convicted di pengadilan naik 88%.

Statistik & contoh (2)

- 1988. Sendmail dieksploitasi oleh R.T. Morris sehingga melumpuhkan Internet. Diperkirakan kerugian mencapai $100 juta. Morris dihukum denda $10.000.
- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi sebuah airport lokal (Worcester, Mass.) sehingga memutuskan komunikasi di control tower dan menghalau pesawat yang hendal mendarat.

Statistik & contoh (3)

- 1999 CSI/FBI Computer Crime and Security Survey

Disgruntled employees	86%
Independent hackers	74%
US Competitors	53%
Foreign corp.	30%
Foreign gov.	21%

http://www.gosci.com

Statistik & contoh (4)

- Electronic banking hacked by Chaos club (Jerman)
- Survey *Information Week* (di USA, 1999), 1271 system or network manager, hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting.
- Kesadaran akan masalah keamanan masih rendah!

Dasar-dasar keamanan

- Aspek dari keamanan
  - privacy / confidentiality
  - integrity
  - authentication
  - availability
  - non-repudiation
  - access control

Dasar-dasar keamanan (2)

- Potensi lubang keamanan
  - disain kurang baik
  - implementasi kurang baik
  - salah konfigurasi
  - salah menggunakan

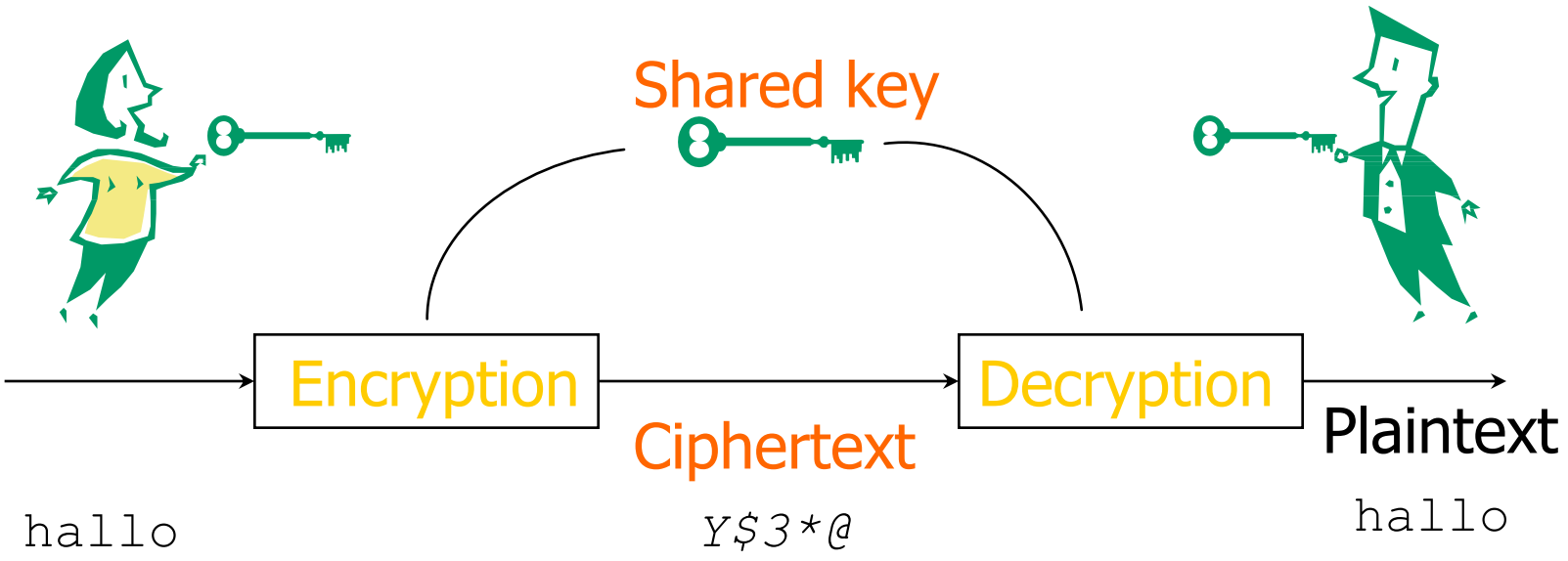
Meningkatkan keamanan (sisi bisnis)

- *Risk analysis* anda untuk menentukan aset dan resiko
- Bagaimana dampak lubang keamanan terhadap bisnis?
- Buat rencana (plan) dan alokasikan dana (budget)!
- Tentukan kebijakan

Meningkatkan keamanan (sisi teknis)

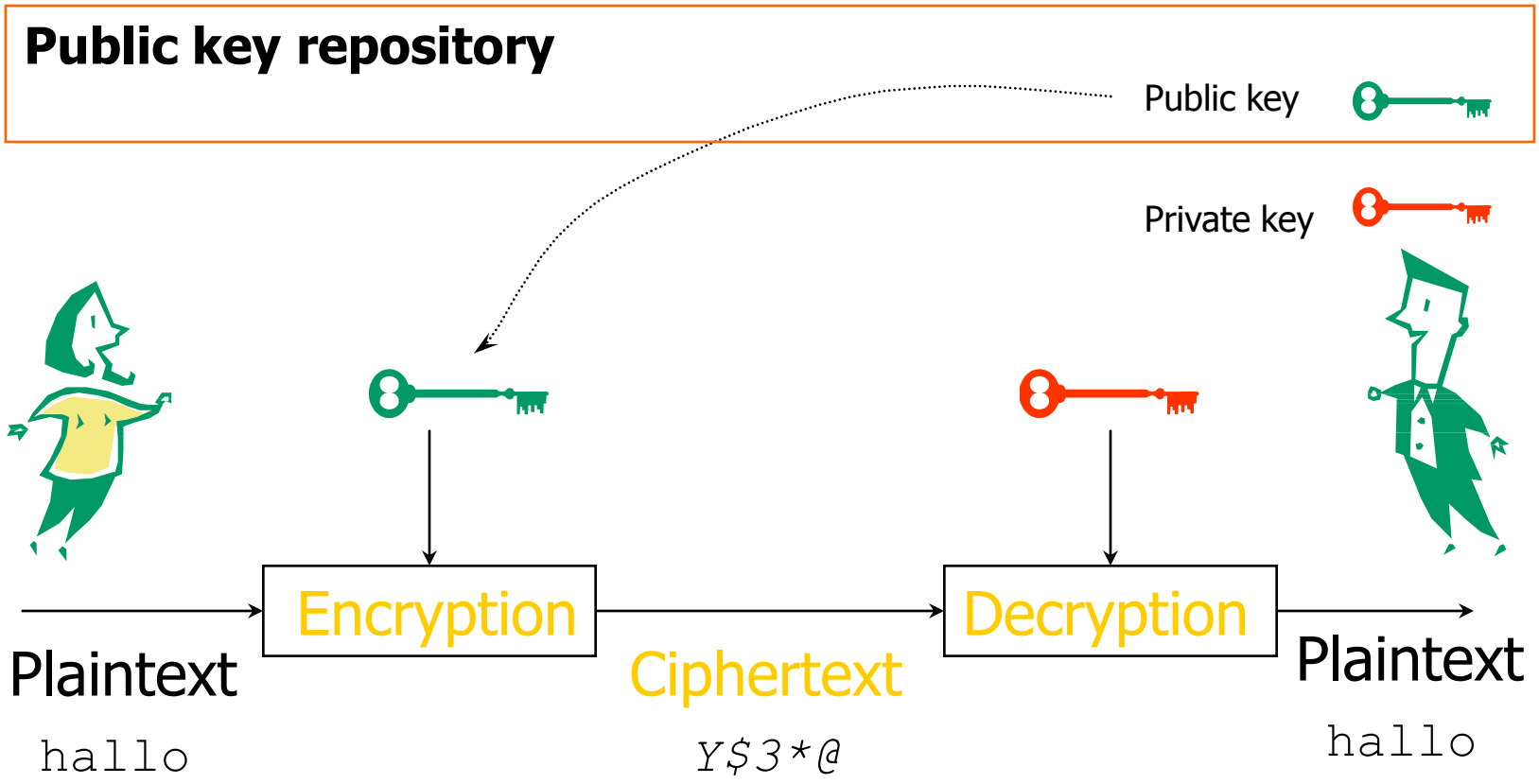
- Penggunaan teknologi kriptografi, enkripsi
  - mengatasi masalah *privacy, integrity, authentication, non-repudiation, access control* (kecuali *availability*)
  - mengubah data menjadi sulit dibaca oleh orang yang tidak berhak
  - *private key* vs *public key system*

Private key



Kunci yang digunakan untuk enkripsi dan dekripsi sama!

Public key


Public key repository
Public key
Private key
Encryption
Decryption
Plaintext
hallo
Ciphertext
Y$3*@
Plaintext
hallo

... sisi teknis (2)

- Penggunaan kunci publik (*public key*)
  - RSA, ECC
- Kebutuhan Infrastruktur Kunci Publik (IKP) *[Public Key Infrastructure - PKI]*
  - *Certification Authority (CA)*
  - *Public key server, Certificate Repository*
  - *Certificate Revocation Lists (CRL)*
- Penggunaan smartcard dapat membantu

... sisi teknis (3)

- Keamanan negara?
- Masalah larangan ekspor USA
  - Hanya kualitas rendah yang boleh dijual, misalnya enkripsi dengan 40-bit
  - RSA 512-bit sudah pecah!
    http://www.cwi.nl/~kik/persb-UK.html

... sisi teknis (4)

- Masalah HaKI (*intelectual property rights*)
- Masalah hukum (*legal aspects*)
- *Playing field* harus sama (*level*)

Kemanan *Indonesian cyber*

- Dibutuhkan kerjasama industri (bisnis), perguruan tinggi, dan pemerintah.
- Pengembangan resources (SDM, tools, funding)
  - Pentingnya perguruan tinggi: riset
  - Masih banyak yang harus dikuasai! (lihat makalah)
  - Contoh hasil penelitian yg dapat diakses

ID-CERT

- Public services
  - Mailing list: id-cert@paume.itb.ac.id
    Langganan: id-cert-subscribe@paume.itb.ac.id
  - Kirimkan alamat email + nomor telepon anda:
    br@paume.itb.ac.id
- Research
  - Kuliah S2 di ITB, EL 776 (Keamanan Sistem Informasi)
  - Evaluasi: public key server, CA, SSL
  - Contoh makalah
- Commercial Services

Contoh hasil riset (1)

- Abdus Somad Arief, "Tinjauan Tentang Undang-Undang Hak Cipta Indonesia dalam Dunia Cyberspace”
- Agus Fikri Hadi, "Studi Tentang Set dan Contoh Implementasinya”
- Bagus FW Hidayat, "Proteksi Software (Perangkat Lunak) dan Kajian Implementasinya”
- Bayu Suharso, "Keamanan EDI Over Internet”
- Budi Rahayu, "Fraud di Bidang Telekomunikasi”
- Charindra Purnomo, "Konsep Pengamanan Data Billing Dengan Public Key”
- Charles Mankin, "Program Aplikasi Analisa 'Log File' Server”
- Eddy Supriadi, "Security Audit dengan Menggunakan Santa/Satan”
- Ferdinal, "Studi Tentang Virtual Private Network”
- Hepta Yuniarta, "Disaster Recovery Plan”
- Imam Adi Siswanto, "Penandatanganan Kontrak Via Network”

Contoh hasil riset (2)

- Imam Pradja Laksono, "Analisa Kejahatan Cyber Terhadap Infrastruktur Sistem Informasi”
- Imam Rijanto, "Aspek Ketahanan pada Jaringan Komputer"
- I Wayan Sukerta, "Studi Sistem Pembayaran Elektronik (Electronic Payment) dan Pengkajian Implementasinya di Indonesia”
- Joko Supriyanto, "Implementasi RC5 menggunakan VHDL”
- Kartitah Yulianti, "Studi Kasus Social Engineering Pada Sistem Keamanan di Suatu Perusahaan"
- Luki Ardiantoro, "Komunikasi Anonim (Anonymity) melalui Jaringan Internet”
- Mohammad Firdaus, "Aspek Keamanan pada Sistem Kartu Chip”
- Nugroho Satriyo Utomo, "Teknik Kriptografi Komunikasi Wireless dengan Algoritma Elliptic Curve Cryptography (EEC) Berbasis Key Authentication dan Key Agreement"
- Nurhasan, "Perancangan dan Implementasi Perangkat Keras Pengaman Informasi Data”
- Sasmito, "Analisis Ancaman dan Resiko dalam Sistem Keamanan Informasi"
- Suhartono, "Analisa Statistik dan Estimasi Performansi Penggunaan Sidik Jari sebagai Sistem Informasi"

Sumber informasi

- Makalah / tulisan
  - Budi Rahardjo, “Mengimplementasikan eCommerce di Indonesia”, Technical Report, PPAU Mikroelektronika, TR-PPAUME-1999-02, 1999. http://www.paume.itb.ac.id/tr/1999-02.pdf
  - Budi Rahardjo, “Keamanan Sistem Informasi Berbasis Internet”, 1999. Http://www.paume.itb.ac.id/rahard/id-cert/handbook.pdf

Sumber informasi

- System Administration, Networking and Security
  http://www.sans.org
- Computer Security Institute
  http://www.gocsi.com
- News, dsb.
  http://securityportal.com
- Tools:
  http://www.opensec.net
- Hacking tools:
  http://www.rootshell.com
- ID-CERT
  http://www.paume.itb.ac.id/rahard/id-cert

Kontak

Budi Rahardjo

- MIS Director
  Pusat Penelitian Antar Universitas
  bidang Mikroelektronika (PPAUME), ITB
  br@paume.itb.ac.id
  http://www.paume.itb.ac.id/rahard
  Fax: (022) 250-8763
- GM Information Technology Services
  UPT PIKSI ITB
  budi@piksi.itb.ac.id
  http://www.piksi.itb.ac.id/~budi
  Fax: (022) 250-0940
- Insan Komunikasi - vision, attitude, relationship!
  High performance, secure services
  Rahardjo@insan.co.id