INTRODUCTION TO NETWORK SECURITY

REFERENCES :

ANOTHER PERSPECTIVE ON NETWORK SECURITY; WILLIAM STALLINGS; UNIVERSITY OF WASHINGTON; 2011

NETWORK SECURITY; JUSTIN WEISZ, SRINIVASAN SESHAN; CARNEGIE MELLON UNIVERSITY; 2002

INTRODUCTION TO SECURITY; BUDI RAHARDJO; INSTITUT TEKNOLOGI BANDUNG; 2016

SEJARAH SINGKAT PERADABAN

KERANGKA

- WHAT IS SECURITY?
- WHY DO WE NEED SECURITY?
- WHO IS VULNERABLE?
- COMMON SECURITY ATTACKS AND COUNTERMEASURES
  - FIREWALLS & INTRUSION DETECTION SYSTEMS
  - DENIAL OF SERVICE ATTACKS
  - TCP ATTACKS
  - PACKET SNIFFING
  - SOCIAL PROBLEMS

APA ITU "SECURITY"

- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

…etc.

SEGITIGA PERSYARATAN SECURITY

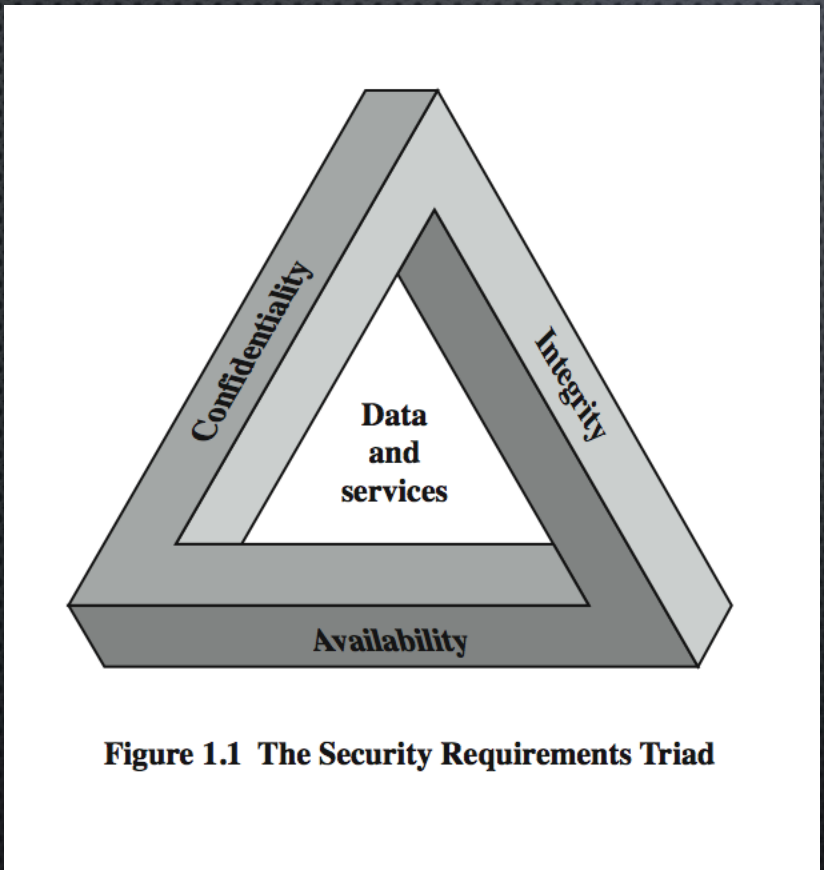


Figure 1.1 The Security Requirements Triad

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Computer Security
The protection afforded to an automated information system in order to attain the applicable objectives of preserving the ***integrity***, ***availability*** and ***confidentiality*** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

SYARAT SECURITY

- **CONFIDENTIALITY**
  - PRESERVING AUTHORIZED RESTRICTIONS ON INFORMATION ***ACCESS*** AND ***DISCLOSURE***, INCLUDING MEANS FOR PROTECTING PERSONAL PRIVACY AND PROPRIETARY INFORMATION.
- **INTEGRITY**
  - GUARDING AGAINST INFORMATION ***MODIFICATIONS*** OR ***DESTRUCTION***, INCLUDING ENSURING INFORMATION NON-REPUDIATION AND AUTHENTICITY.
- **AVAILABILITY**
  - ENSURING TIMELY AND RELIABLE ACCESS TO AND ***USE*** OF INFORMATION

SERANGAN, MEKANISME, & LAYANAN SECURITY

- **Security *Attack***
  - Any action that compromises the security of information
- **Security *Mechanism***
  - A process / device that is designed to detect, prevent or recover from a security attack.
- **Security *Service***
  - A service intended to counter security attacks, typically by implementing one or more mechanisms.

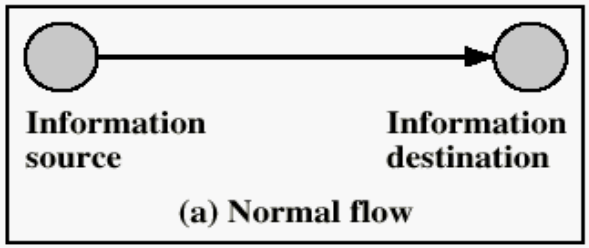
ANCAMAN DAN SERANGAN

Table 1.1 Threats and Attacks (RFC 2828)

Threat A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
Attack An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

… but *threat* and *attack* used nearly interchangeably

ANCAMAN/SERANGAN SECURITY



... ...

ANCAMAN/SERANGAN SECURITY

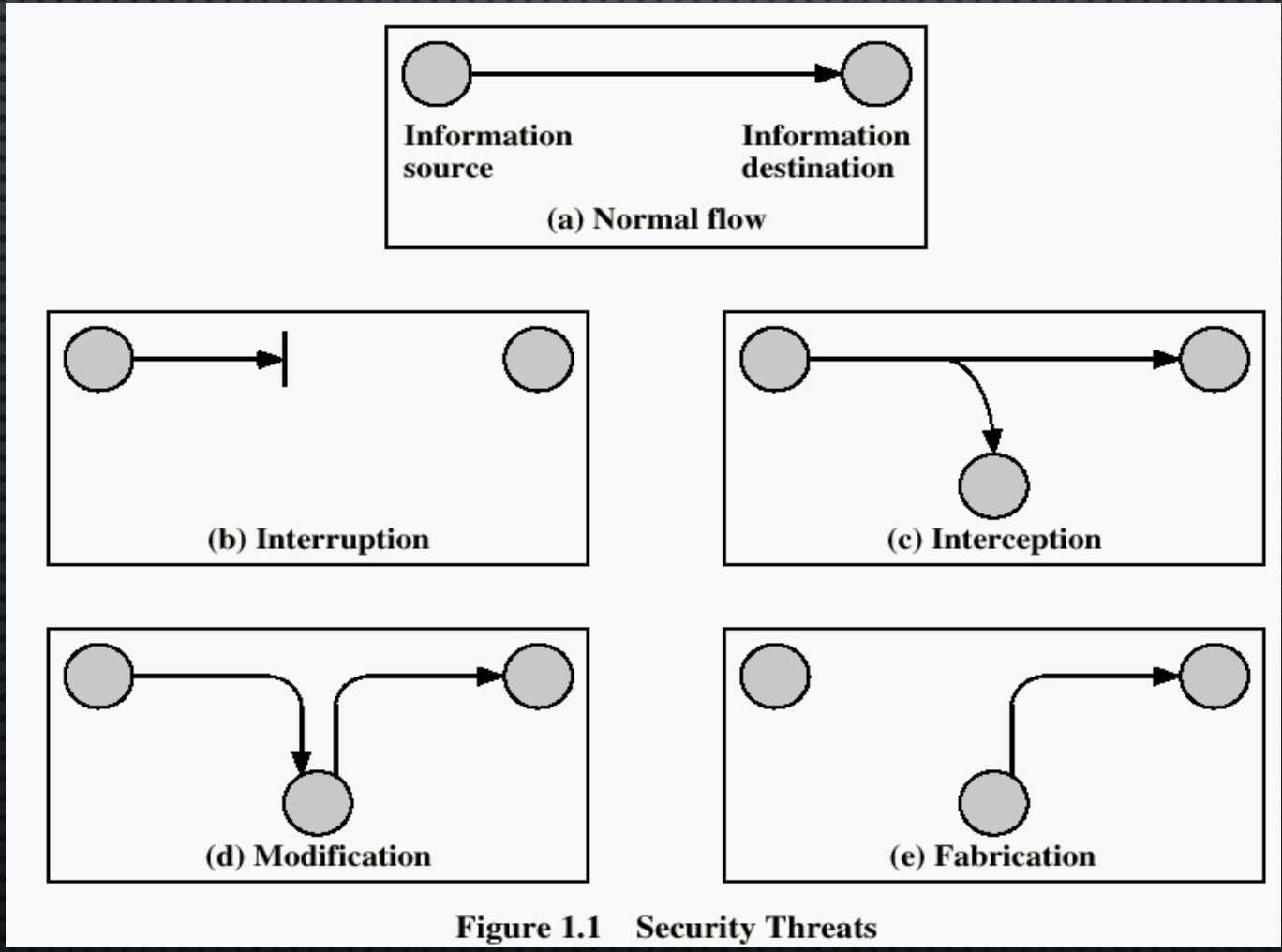
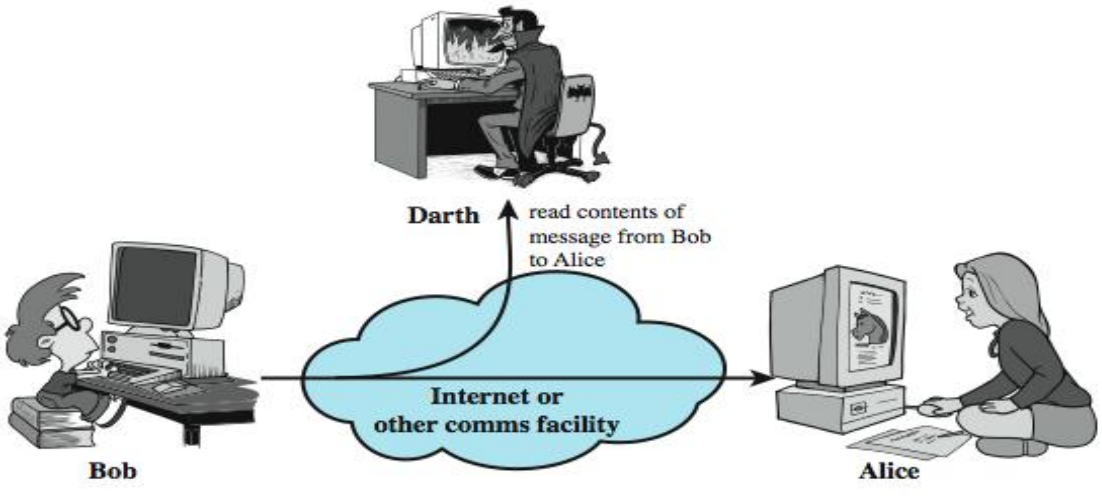
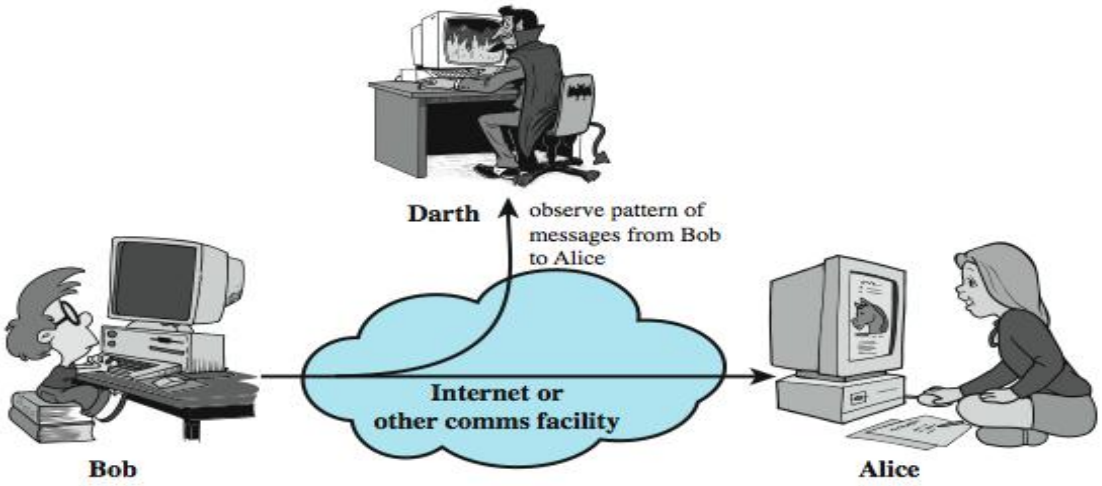


Figure 1.1 Security Threats

SERANGAN PASIF



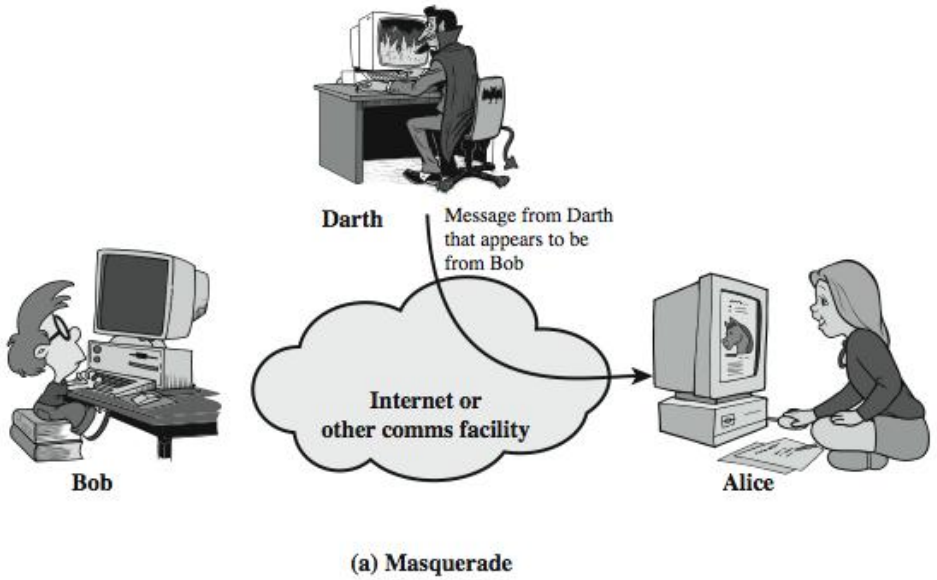
(a) Release of message contents



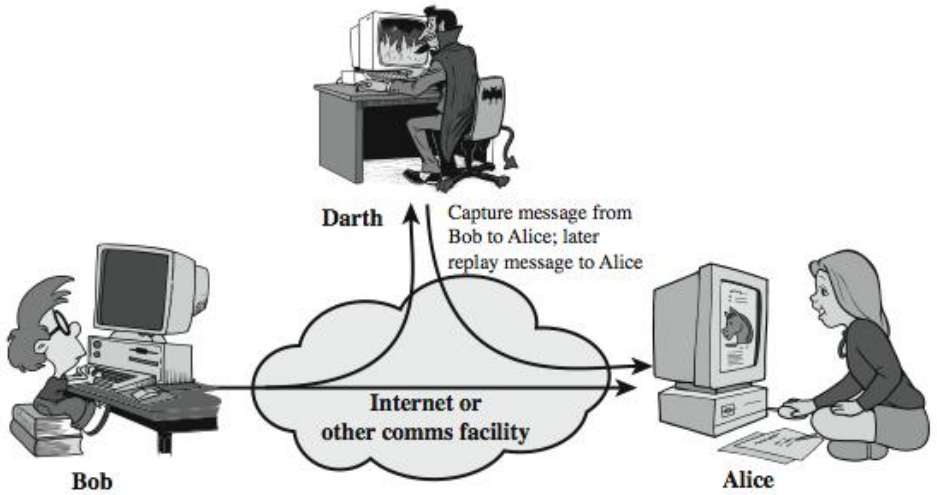
(b) Traffic analysis

Figure 1.2 Passive attacks.

SERANGAN AKTIF (1)



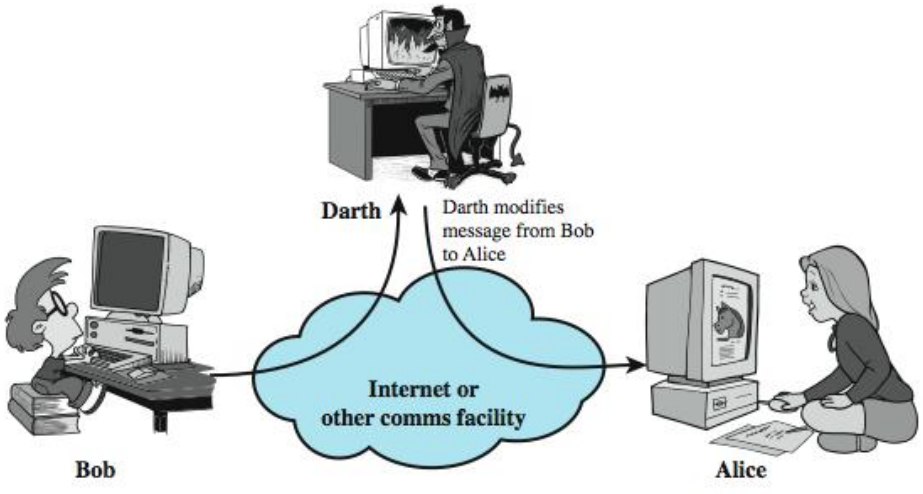
(a) Masquerade



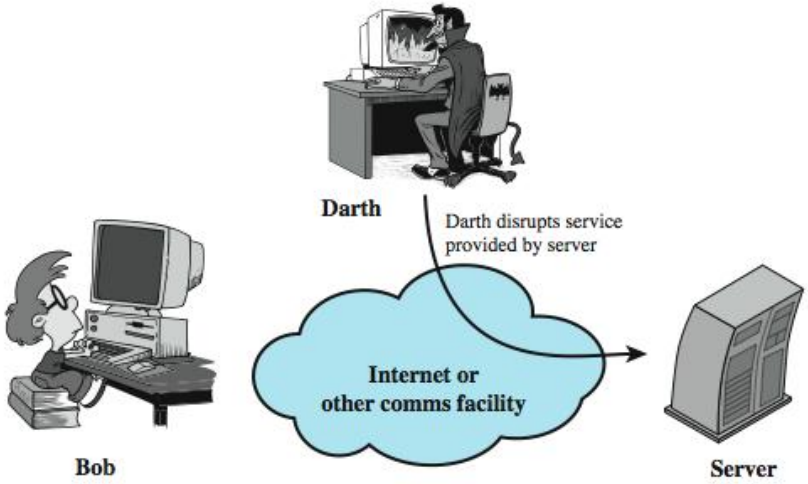
(b) Replay

Figure 1.3 Active attacks (page 1 of 2)

SERANGAN AKTIF (2)



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active Attacks (page 2 of 2)

LAYANAN KEAMANAN (X.800)

- **Authentication**
  - The assurance that the communicating entity is the one it claims to be
- **Access Control**
  - The prevention of unauthorized use of a resource
    - who can have access to a resource,
    - under what conditions access can occur,
    - what those accessing the resource are allowed to do
- **Data Confidentiality**
  - The protection of data from unauthorized disclosure
- **Data Integrity**
  - The assurance that data received are exactly as sent by an authorized entity (i.e., contains no modification, insertion, deletion or replay).
- **Non-Repudiation**
  - Provides protection against denial by one of the entities involved in a communication of having participated in all/part of the communication.

MODEL KEAMANAN JARINGAN

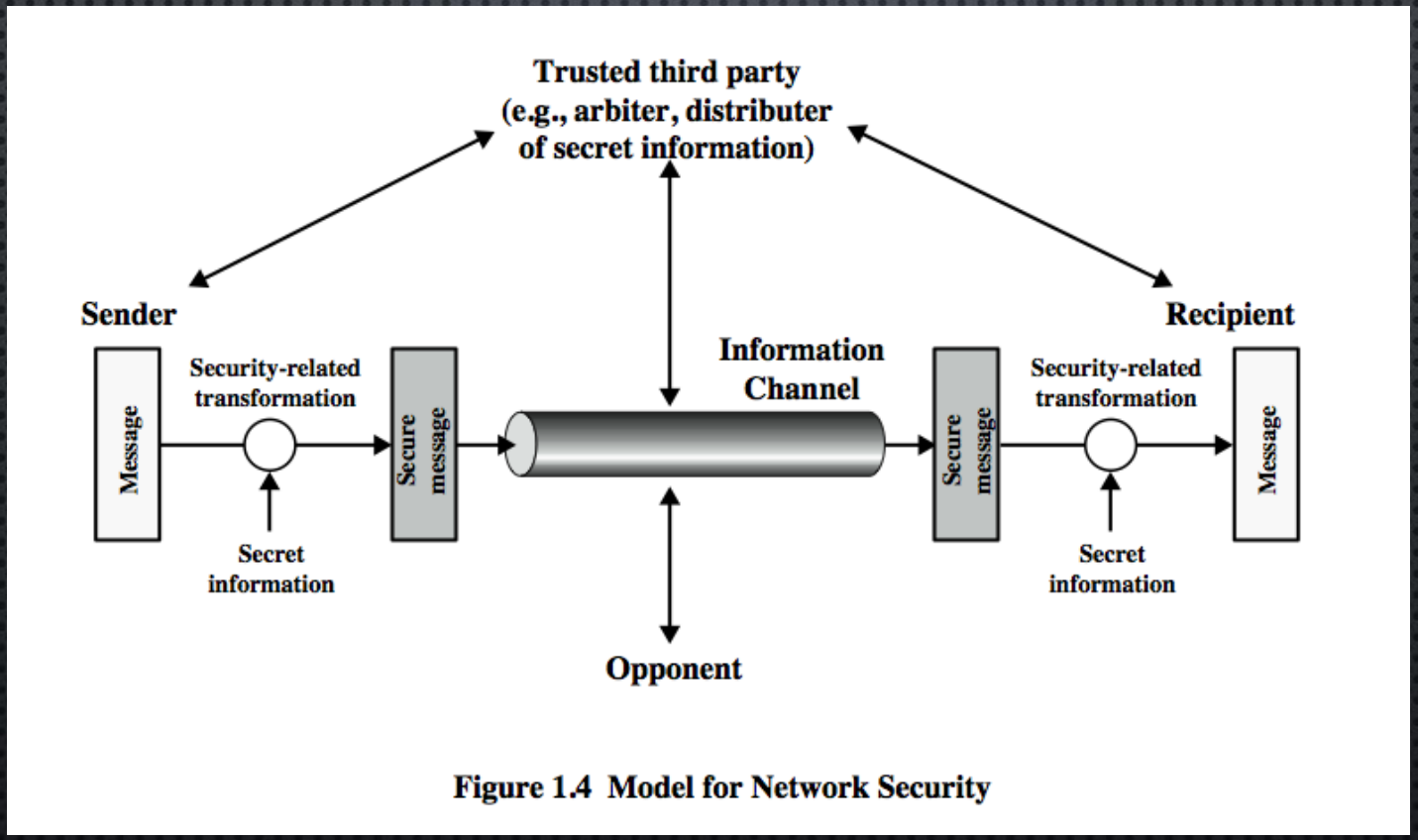
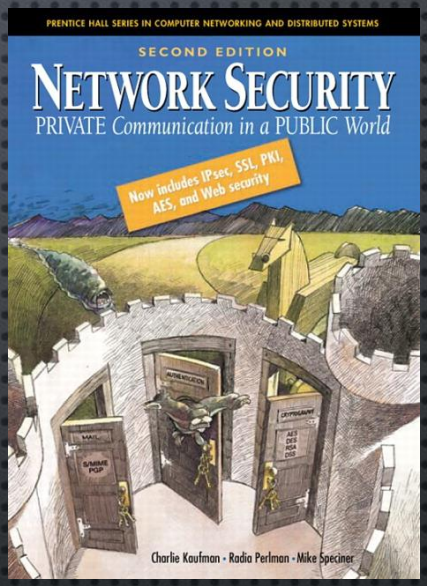


Figure 1.4 Model for Network Security

UNSUR MANUSIA

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

-- C. Kaufman, R. Perlman, and M. Speciner.



Network Security: Private Communication in a Public World, 2/E
Kaufman, Perlman & Speciner
Prentice Hall, 2003

2016

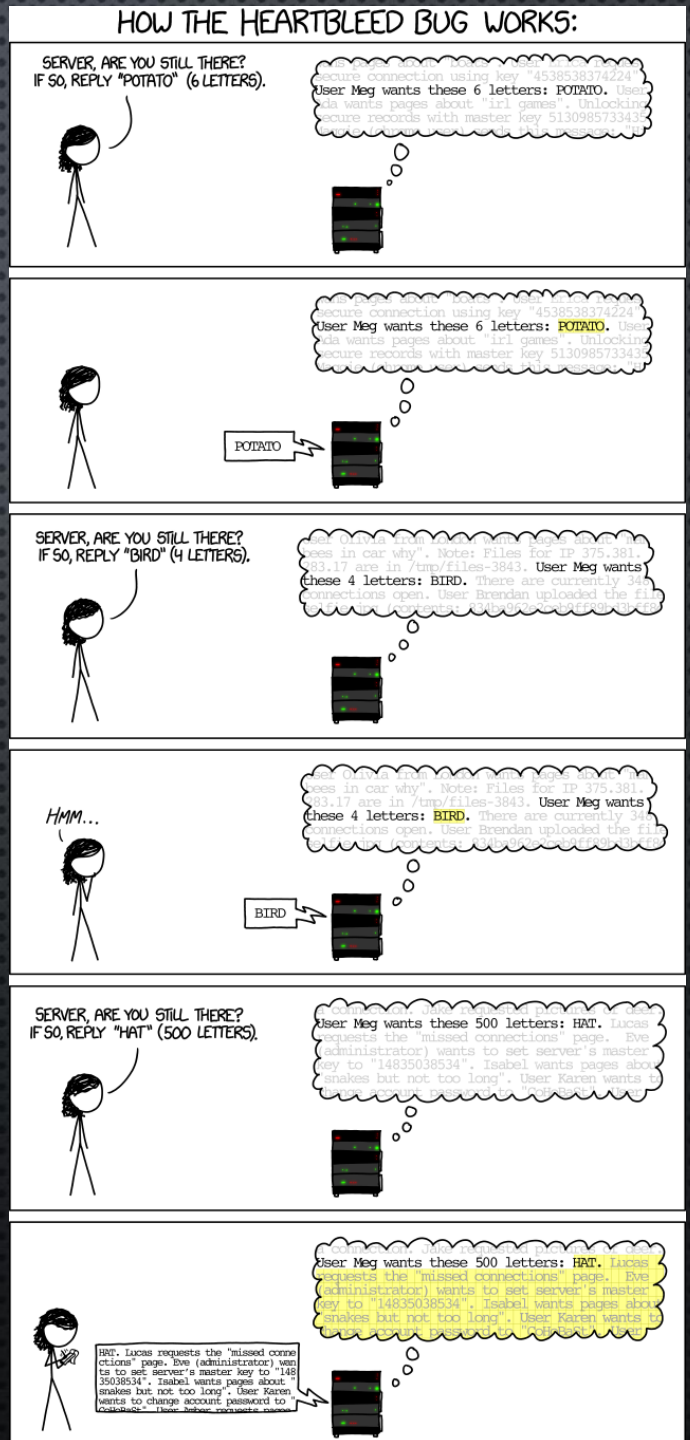
- HTTPS://WWW.THEGUARDIAN.COM/NEWS/2016/APR/03/WHAT-YOU-NEED-TO-KNOW-ABOUT-THE-PANAMA-PAPERS

2015

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

2014

- HEARTBLEED



2014

Bursa Singapura Terganggu

Perdagangan di bursa saham Singapura sempat macet karena software ngadat. **Halaman 24**

KOMPAS GRAMEDIA

HOT SECURITY ISSUES 2012-2013

- Masih tetap didominasi virus / worm / malware / spam
- *Identity theft* (individu & perusahaan)
- Cyberwar mulai menjadi topik diskusi
- Penipuan-penipuan di jejaring sosial, SMS

PRESIDENSBY.INFO ... HACKED AGAIN (2013)

LONDON RIOTS – AGUSTUS 2011

BLACKBERRY DIGUNAKAN UNTUK MENGORGANISIR?

HOT ISSUES 2011

- **Research In Motion** (RIM) – pembuat **BlackBerry** – dipaksa untuk memiliki server di Indonesia.
  - Salah satu alasan yang digunakan adalah agar Pemerintah dapat melakukan penyadapan (*interception*)

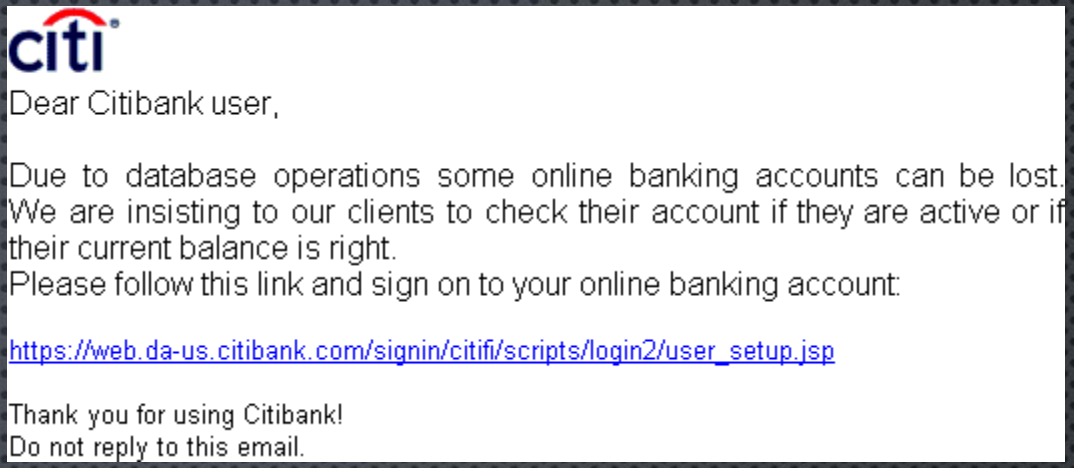
HOT ISSUES 2010

- Mulai populernya social network (web 2.0)
  - Facebook, Friendster, Orkut, ...
- Masalah
  - Pencurian identitas (*identity theft*)
  - Penurunan produktivitas kerja
  - Masalah etika dan legal

"Lack of internal security awareness is still one of our biggest threats. Technology can reduce risks to a point but it is people who are the weakest link."

Deloitte Global Security Survey 2004 Respondent

PHISING


citi

Dear Citibank user,

Due to database operations some online banking accounts can be lost. We are insisting to our clients to check their account if they are active or if their current balance is right.
Please follow this link and sign on to your online banking account:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you for using Citibank!
Do not reply to this email.

From: <USbank-Notification-Urgecq@UsBank.com>
To: …
Subject: USBank.com Account Update URGEgb
Date: Thu, 13 May 2004 17:56:45 -0500

USBank.com

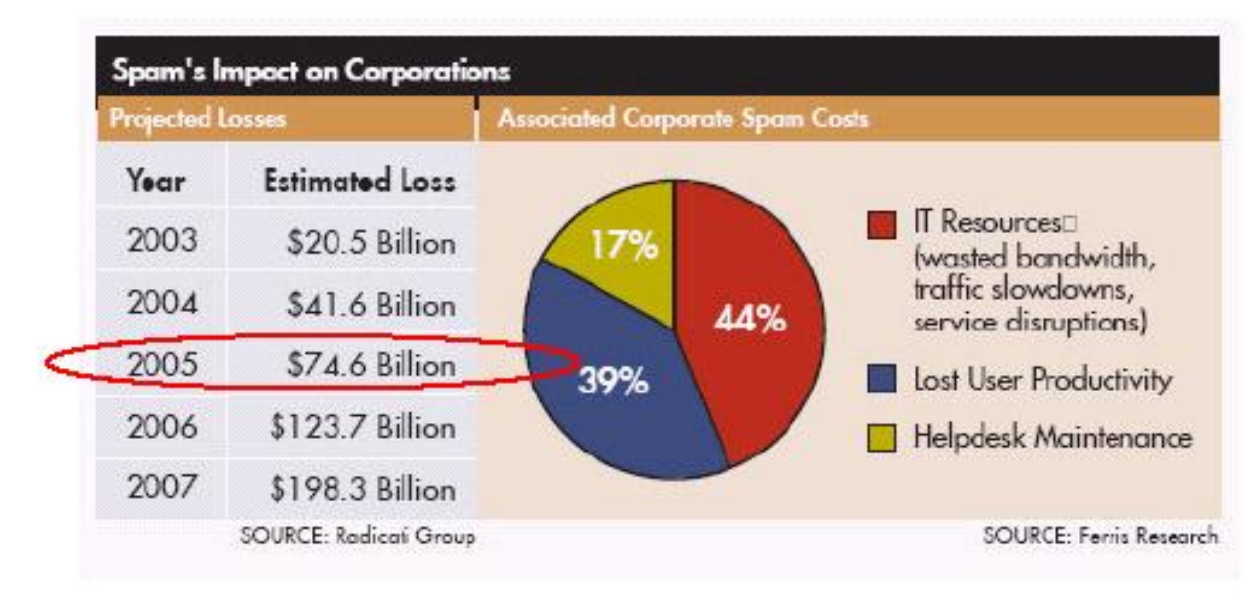
Dear US Bank Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
http://www.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage

Note: Requests for information will be initiated by US Bank Business Development; this process cannot be externally requested through Customer Support.

SPAM



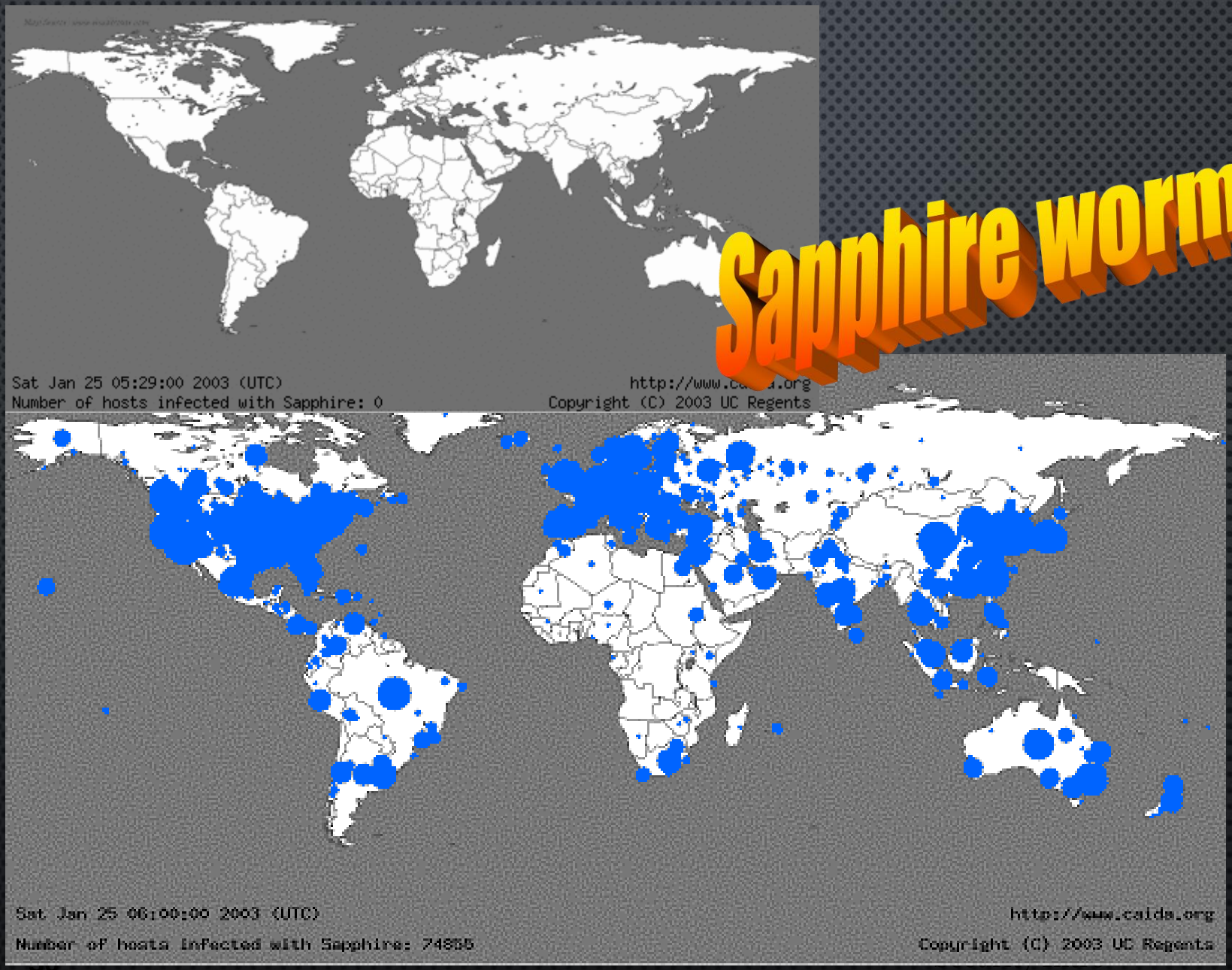
- Email yang berisi sampah (umumnya iklan)
- Menghabiskan jaringan, disk, waktu pekerja
- Spam merugikan bisnis

TERLUPAKAN … ABUSE DARI DALAM!

- **1999 Computer Security Institute (CSI) / FBI Computer Crime Survey** menunjukkan beberapa statistik yang menarik, seperti misalnya ditunjukkan bahwa "disgruntled worker" (orang dalam) merupakan potensi attack / abuse.
  http://www.gocsi.com

Disgruntled workers	**86%**
Independent hackers	74%
US competitors	53%
Foreign corporation	30%
Foreign government	21%

Sapphire worm



STATISTIK DI INDONESIA (SAMBUNGAN)

- Agustus 2005. Listrik dari PLN mati beberapa jam untuk Jakarta dan sekitarnya
  - KRL terhenti. Penumpang terlantar.
  - Operasi di rumah sakit di tunda dan hanya operasi yang serius dilakukan.
  - PLN tidak mengganti rugi.
  - Bagaimana perusahaan yang tidak memiliki cadangan (backup) catu daya?

STATISTIK DI INDONESIA (SAMBUNGAN)

- JANUARI 2010. DIMULAI DARI ATM DI BALI, BEBERAPA ATM DIDAPATI DIPASANG ALAT SKIMMER.
  - BANYAK NASABAH YANG UANGNYA DIAMBIL MELALUI PENGGANDAAN KARTU ATM
  - MASALAH KEMUDIAN MEREBAK KE BERBAGAI TEMPAT
  - MENJADI ISYU UTAMA DI BERBAGAI MEDIA

tro

KEJAHATAN ATM

KEJAHATAN ATM

Menyadap PIN dengan wireless camera

- September 2015. Akun twitter palsu @indosatcare (perhatikan bahwa itu huruf “L” kecil) menjawab pertanyaan pelanggan indosat dengan guyonan / celaan
  - *"@lndosatCare: @boo_kepo Hai, silahkan registrasi muka anda dengan air kobokan ya. Thanks ^HB”*

Location: http://www.bri.co.id/

buwakakakakakakakakakakaakakakakaakakakakakakakakakaak

```
                    :::!~!!!!!:.
                  .xUHWH!!  !!?M88WHX:.
                .X*#M@$!!   !X!M$$$$$$WWx:.
               :!!!!!!?H! :!$!$$$$$$$$$$8X:
              !!~  ~:~!! :~!$!#$$$$$$$$$$8X:
              !!~  ~:~!! :~!$!#$$$$$$$$$$8X:
             ~!~!!!!~~ .:XW$$$U!!?$$$$$$RMM!
               !:~~~ .:!M"T#$$$$WX??#MRRMMM!
               ~?WuxiW*`   `"#$$$$8!!!!??!!!
             :X- M$$$$       `"T#$T~!8$WUXU~
            :%`  ~#$$$m:         ~!~ ?$$$$$$
          :!`.-   ~T$$$$8xx.  .xWW- ~""##*"
.....   -~~:<` !    ~?T#$$@@W@*?$$      /`
W$@@M!!! .!~~ !!       .:XUW$W!~ `"~:    :
#"~~`.:x%`!!  !H:   !WM$$$Ti.: .!WUn+!`
:::~:!!`:X~ .: ?H.!u "$$$B$$$!W:U!T$$M~
.~~   :X@!.-~   ?@WTWo("*$$$W$TH$! `
Wi.~!X$?!-~    : ?$$$B$Wu("**$RM!
$R@i.~~ !     :   ~$$$$$B$$en:``
?MXT@Wx.~    :     ~"##*$$$$M~
-= Hi Mom ! I told u i can hack ! =-
```

A Firewall is
it detects and
in or out of the network.
But security i
You can't just

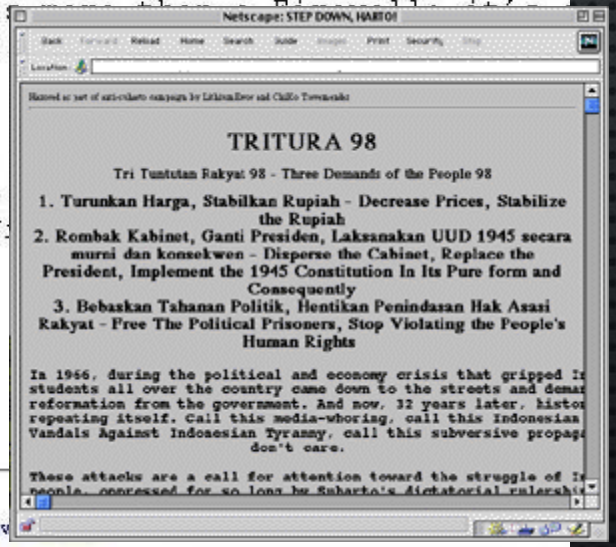
Anti-CyberLaw,
so you have to
Dont stop us f

Thu, 03 Oct 2002 06:45:18 GMT

Bosen

#hackers@centrin.net.id - #hackers@austnet.org - #antihackerlink@dal.net - #rsjiv

sakitjiwa - syzwz - madya - AresU - TioEuy - undee



Karyawan BNI Cabang Serang Tilap Rp 1,2 Miliar Uang Nasabah ONH

SERANG — Sekitar 42 orang jemaah asal Kabupaten Serang, Banten gagal berangkat ke Mekkah. Mereka menjadi korban penipuan Alamsyah Rambe, pegawai Bank BNI 46 Cabang Serang. Kini, Alamsyah, yang menangani urusan penerimaan jemaah haji, kabur membawa uang nasabah senilai Rp 1,2 miliar.

Beberapa karyawan BNI Serang kepada *Tempo News Room* kemarin mengatakan, Rambe tidak pernah masuk kerja sejak para korban menuntut uang mereka dikembalikan. "Manajemen BNI sendiri kebingungan mengembalikan uang mereka, lah 42 orang dari Kabupaten Serang batal berangkat karena tidak mendapat kuota. Mereka sebelumnya dijanjikan berangkat ke Tanah Suci pada 3 Februari, bersamaan dengan keberangkatan rombongan Wakil Presiden Hamzah Haz.

Pada 2 Februari, mereka menuju penampungan jemaah haji di Bekasi. Namun, dua hari kemudian, mereka mendapat kepastian batal berangkat karena tidak mendapat kuota. Akibat kejadian ini, para korban dirugikan Rp 1,2 miliar—total ongkos naik haji (ONH) yang disetorkan melalui Alamsyah Rambe.

Pimpinan Wilayah BNI Regio- [illegible] dia meminta waktu sebulan untuk memeriksa ke mana raibnya dana tersebut.

Susilo juga berjanji akan memeriksa kemungkinan keterlibatan Kepala Cabang BNI Serang, Mahfud. "Jika Alamsyah Rambe terbukti, akan dipecat, dan kami serahkan ke kepolisian," katanya.

Susilo memastikan dana [illegible] disetorkan para nasabah it[illegible] Rambe tidak masuk BNI. "Sebab, bila dana itu m[illegible] kas BNI, setoran y[illegible] disa[illegible] kan akan tercatat," ka[illegible]

Amin, salah seorang K[illegible] bersama istrinya, Arnah [illegible] Kampung Kramat, Desa S[illegible] Kecamatan Curug, Se[illegible] setoran tabungan haji BN[illegible] bagai tanda terima.

Yakin tak ada masalah[illegible] dan istrinya meninggalkan [illegible] pung halaman pada 2 Feb[illegible] ke Bekasi. Namun, dua ha[illegible] mudian, mereka balik lagi [illegible] na tidak bisa berangkat. K[illegible] an sempat dialami Misbah, [illegible] hun, warga Kampung Kr[illegible]

Bank BNI Dituding Bobol Dana Nasabah Rp 700 Juta

MAKASSAR — Bank BNI 1946 Makassar, Sulawesi Selatan, di[illegible] demo oleh sekitar 20 orang, Rabu (5/2). Mereka meminta pihak bank membayar ganti rugi atas [illegible] tabungan seoran[illegible] nasabah sekitar Rp 700 juta. Para pendemo itu bukanlah piha[illegible] yang tabungannya mengalami kebobolan. Mereka mengaku se[illegible] bagai mitra kerja Debby Chandrawaty, nasabah yang disebut menjadi korban pembobolan itu.

Pemimpin Bank BNI 1946 Makassar Muchlis Abdussalam m[illegible] nyatakan, pihaknya tidak mungkin mengganti uang nasabah yang diduga bobol tanpa alasan yang kuat. "Tidak bisa dibaya[illegible] kan sebelum ada putusan pengadilan siapa yang benar dan si[illegible] pa yang salah," katanya. ● muanas

Transaksi RTGS Mencapai Rp 64,9 Triliun per Hari

MALANG — Transaksi harian antarbank yang dilakukan melalui sistem Bank Indonesia *Real Time Gross Settlement* (BI-RTGS) atau layanan transfer dana antar bank secara seketika, telah mencapai lebih dari 13.735 dengan nilai sekitar Rp 64,9 triliun per hari.

Deputi Gubernur Bank Indonesia Aulia Pohan di sela peresmian penerapan RTGS di Malang, akhir pekan lalu mengatakan jumlah tersebut meliputi lebih dari 95 persen transaksi pembayaran antarbank.

Tingginya penggunaan sistem RTGS, menurut Aulia, karena sistem ini mampu mengatasi risiko sistemik dari transaksi tersebut. "Risiko dapat dikurangi karena sistem ini pun membuat bank peserta dapat mengelola likuiditas dana secara cermat."

Sistem RTGS pertama kali diterapkan di Jakarta pada 17 November 2000. Hingga kini telah 29 wilayah kantor Bank Indonesia yang menerapkan sistem ini. Malang merupakan wilayah ke-29.

Dengan penerapan sistem ini masyarakat atau perbankan di wilayah tersebut dapat melakukan transfer dalam jumlah besar atau bersifat mendesak hanya dalam hitungan waktu sekitar 4 detik. Untuk transfer dana dalam jumlah relatif kecil, tidak mendesak, atau bersifat rutin, masyarakat dapat memanfaatkan layanan kliring yang telah ada saat ini. ● anne

PIKIRAN RAKYAT, 14 FEB 2003 12 ZULHIJAH 1423 H - RAYAGUNG 1935

Hj. Eman Dibacok Perampok

Kawanan Maling Bobol ATM Bank Mandiri

BANDUNG, (PR).-
Anjungan tunai mandiri (ATM) Bank Mandiri yang [illegible] letak di depan Kantor [illegible] Telkom Jalan [illegible] No. 1 Bandung dibobol maling, dahan dalam waktu dekat kita dapat meringkus pelakunya," tegasnya.

Perampokan

Sementara itu, aksi perampokan di siang bolong kembali terjadi. Kali [illegible]dalah Dewan [illegible]sat, Hj. Eman [illegible]mar Jalan Pa[illegible] Balong Gede [illegible]ota Bandung. [illegible]itu, Hj. Eman [illegible]an gelang dan [illegible] gram, juga [illegible]n cukup parah [illegible] harus dirawat [illegible]h Bandung. [illegible]kan yang ter[illegible]), sekira pukul [illegible]at menggem[illegible] itu terjadi be[illegible] banyak warga [illegible]pokan setelah [illegible]lagi sendirian [illegible]ı tetangganya [illegible]n sudah berlu[illegible]

[illegible]awa ke rumah [illegible]t sedikit saja, [illegible]ak akan terto[illegible]rga yang eng[illegible]tasnya. [illegible]ngan yang [illegible]'R" di Tempat [illegible]'KP) menye[illegible]erampokan di [illegible] sedang sepi. [illegible] yang bersebe[illegible]ı korban pun [illegible]pencurian de[illegible]val terjadi per[illegible]ı sekira pukul 13.00 WIB ada seorang pemuda bertamu ke rumah korban dengan pura-pura untuk ikut sembahyang. Saat itu korban tidak curiga dan membawa sejadah untuk diberikan ke pelaku. Baru juga sejadah itu akan digelar oleh korban, pelaku tiba-tiba memukulnya dari arah belakang dengan benda keras, dan berusaha merebut perhiasan emas yang dipakai oleh korban. Rupanya korban sempat melawan dan mempertahankan barang miliknya, akhirnya pelaku membacoknya dengan senjata tajam kearah kepala, setelah itu merampas gelang dan kalung kurang lebih seberat 40 gram.

Pelaku kabur melalui pintu depan. Sebelum kabur, rupanya pelaku sempat mengunci pintu depan rumah korban sehingga korban susah untuk keluar. Ini terbukti saat korban akan keluar untuk minta tolong, ternyata pintu depanya dalam keadaan terkunci. Namun dengan sekuat tenaga, korban berusaha mendekati pintu dan minta tolong dengan mengetuk-ngetuk pintu kaca dan diketahui oleh salah seorang tetangga korban, Ny. Fatah.

Melihat korban berlumuran darah itu, pintu didobrak dan korban saat itu juga dibawa ke rumah sakit RS Muhammadiyah untuk diberikan pertolongan. Saat terjadi perampokan di rumah tersebut, hanya ada korban. Sementara itu, petugas kepolisian hingga kemarin belum berhasil mengungkap kasus perampokan di siang bolong tersebut. (A-72/A-125)***

BANK YANG NAKAL?

'Dua bank lakukan kecurangan rugikan nasabah'

JAKARTA (Bisnis): Dua bank diketahui melakukan penurunan suku bunga tabungan tanpa diketahui oleh nasabahnya sehingga memperoleh tambahan pendapatan yang cukup besar.

Anggota DPR Dradjad HA Wibowo menjelaskan BI telah mengetahui kecurangan yang dilakukan oleh dua bank tersebut.

"Pada akhir tahun ada bank yang mempunyai kecenderungan memotong bunga tabungan sebesar 2% selama beberapa hari. Nasabah tidak merasakan adanya kerugian karena uang yang hilang sangat kecil sekitar Rp2000-Rp3000 per rekening,"ujarnya akhir pekan lalu.

Namun, tambahnya, uang ini kalau diakumulasikan dengan jumlah rekening maka bisa mencapai miliaran rupiah. Dia memaparkan praktek-praktek itu masuk dalam pemeriksaan BI namun belum terlihat jelas upaya hukuman yang ditempuh oleh bank sentral terhadap bank-bank yang melanggar ketentuan tersebut.

Bisnis mencoba menghubungi beberapa pejabat BI yang terkait dengan pengawasan perbankan namun mereka mengatakan akan memeriksa kemungkinan itu.

Dradjad menjelaskan struktur kepemilikan bank di Indonesia memudahkan terjadinya kejahatan perbankan.

"Adanya pemegang saham mayoritas akan memudahkan pembuatan keputusan operasional bank yang berpotensi menjadi kejahatan perbankan," katanya.

Dia membandingkan di AS dan Australia terjadi pembatasan kepemilikan bank tidak hanya oleh asing tetapi juga oleh warga negaranya sendiri.

"Lihat saja di AS maupun Asutralia hanya dibatasi 15%. Rata-rata pembatasan kepemilikan di suatu bank berkisar 20%-25% di beberapa negara," katanya.

Dia mengingatkan dominasi kepemilikan asing di beberapa bank akan menyulitkan BI dalam melakukan konsolidasi perbankan yang akan diluncurkan dalam waktu dekat.

"Ada amandemen UU Perbankan yang bisa dimanfaatkan untuk pembatasan meskipun sudah terlanjur bank-bank di Indonesia dimiliki oleh pemegang saham mayoritas. Tidak ada masalah karena pemegang saham yang sudah terlanjur memiliki saham bank diminta melepas kepemilikannya kepada pasar," katanya.

Dia menuturkan BI juga perlu mengeluarkan aturan mengenai merger dan akuisisi untuk mendukung rencana bank sentral melakukan konsolidasi perbankan.

"Harus ada kejelasan pembelian bank dilakukan dengan transaksi yang sehat bukannya rekayasa keuangan tanpa ada uang segar yang masuk. Jangan sampai bank dalam satu grup usaha melakukan merger sebatas rekayasa keuangan tanpa adanya uang keluar,"paparnya. **(mmh)**

KEJAHATAN DI ATM

Transaksi Butik ATM Citibank

Apabila bertransaksi di mesin ATM mana pun, hendaknya jangan mau dipandu atau dibantu oleh petugas sekuriti yang bertugas di sana. Karena oknum tersebut bisa menggunakan nomor PIN anda dan melakukan transaksi penarikan dari rekening anda.

Berikut adalah pengalaman saya. Pada tanggal 2 April 2003 saya bermaksud mencari ATM BCA yang berada di lokasi Hero Tomang, Jakarta Barat. Namun, sesampainya di sana saya disambut oleh petugas sekuriti ATM Citibank dan mempersilakan masuk ke dalam butik ATM Citibank. Saya menolak, namun petugas tersebut terus memaksa dan mengatakan tidak ada ATM BCA dan kartu BCA juga bisa digunakan di butik ATM Citibank tersebut.

Pada saat saya melakukan transaksi, petugas tersebut berdiri di samping saya dan bermaksud untuk memberitahukan cara menggunakan mesin ATM tersebut. Pada dua transaksi pertama, mesin tidak berhasil mengeluarkan uang yang saya minta, namun pada transaksi ketiga dan keempat berhasil.

Saya meninggalkan mesin tersebut setelah berhasil mendapat jumlah yang saya maksud (setelah transaksi ketiga dan keempat). Namun, setelah melakukan pencetakan buku tabungan, saya baru sadar, ada transaksi kelima dan keenam yang tidak saya lakukan. Hal ini bisa dilihat dengan interval waktu yang tertera pada lembar konfirmasi penarikan uang dari BCA, yang menunjukkan bahwa transaksi kelima terpaut dengan jangka waktu lebih kurang 2 menit dari transaksi keempat.

Sedangkan waktu normal untuk transaksi dengan kartu yang sama adalah lebih kurang 40 detik saja, seperti terlihat dari transaksi ke 1 s/d 4. Waktu saya meminta pertanggungjawaban dari pihak Citibank, dengan enaknya mereka menga- ransaksi sudah tidak bisa ber- Padahal, pihak ik biaya admi- Rp 30.000 untuk setiap transaksi. Untuk apa Citibank menggunakan nama butik ATM dan membuat propaganda tentang kemewahan dalam bertransaksi apabila fasilitas video rekamannya saja tidak jalan?

SUSILO SUNDARIWATI
Jl Mandala Raya No 8 RT 001/005 Tomang, Jakarta Barat

Pemalsuan Struk Transfer BCA

Tanggal 21 Mei 2003, kami memasang iklan penjualan sepeda motor (B 6156 IP) di surat kabar. Keesokan harinya (22/5) sekitar pukul 17.30, kami kedatangan dua pembeli yang mengaku masing-masing bernama Robby Wijaya (sekitar 35 tahun) beralamat Meruya, Jakarta, dan Hadi Gunawan (sekitar 45 tahun). Melihat penampilan, kedua orang itu tidak

Saat itu kami sempat konfirmasi ke BCA Hot Line dan mendapatkan jawaban bahwa transaksi sekitar pukul 18.00 akan efektif keesokan harinya. Setelah mendapatkan jawaban itu, tanpa berpikir curiga, kami menyerahkan surat-surat sepeda motor tersebut dengan pemikiran struk asli transfer ATM BCA sudah kami terima. Kedua orang tersebut sempat memberikan kartu nama kepada kami. Keesokan harinya (23/5), kami mengecek kembali dan ternyata hingga saat ini uang tersebut tidak pernah masuk ke rekening kami. Ciri-ciri sepeda motor

Sumber:
Surat Pembaca, Kompas, 2003

PENIPUAN LAIN

- Penipuan melalui SMS
  - Anda menang sebuah undian dan harus membayarkan pajaknya. Pajak dapat dibayarkan melalui mesin ATM (transfer uang, atau dengan membeli voucher yang kemudian disebutkan nomornya)
  - Banyak yang percaya dengan modus ini
  - Social Engineering
  - Hipnotis?

Mungkinkah aman?

- Sangat sulit mencapai 100% aman
- Ada timbal balik antara keamanan vs. kenyamanan (security vs convenience)
  - Semakin tidak aman, semakin nyaman
  - Juga "security vs performance"
- Definisi computer security:
  (Garfinkel & Spafford)

  A computer is secure if you can depend on it and its software to behave as you expect

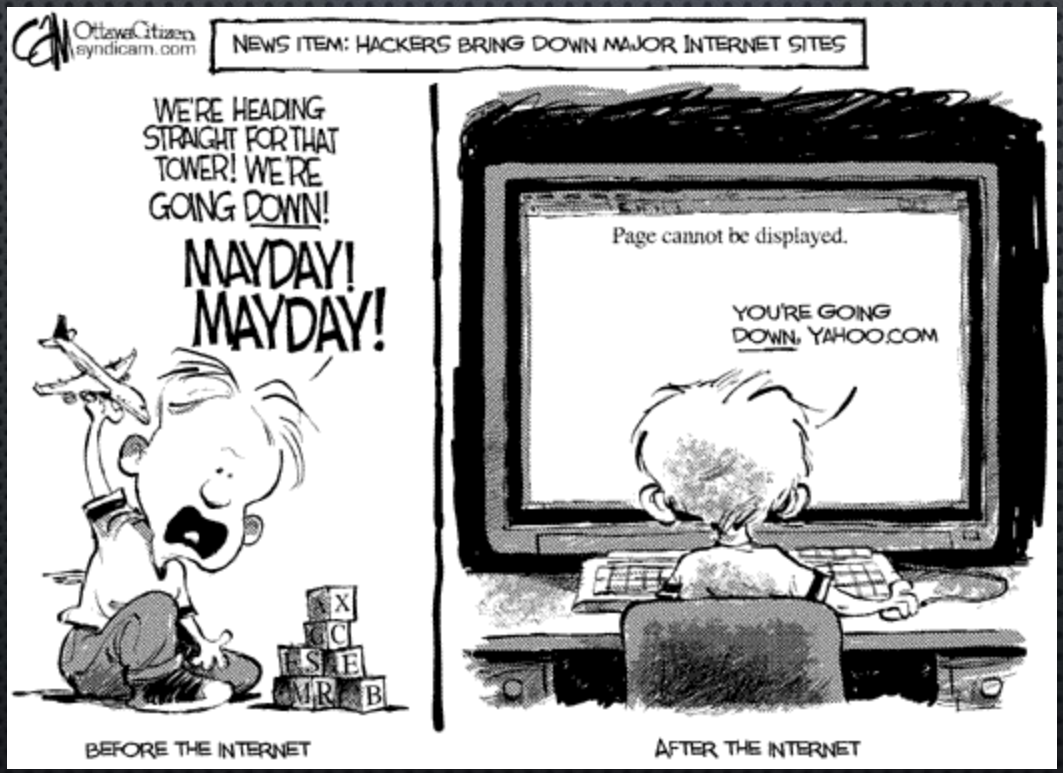
PENINGKATAN KEJAHATAN KOMPUTER
BEBERAPA SEBAB

- **APLIKASI BISNIS YANG BERBASIS KOMPUTER / INTERNET MENINGKAT.**
  - INTERNET MULAI DIBUKA UNTUK PUBLIK TAHUN 1995
  - ELECTRONIC COMMERCE (E-COMMERCE)
- STATISTIK E-COMMERCE YANG MENINGKAT
- SEMAKIN BANYAK YANG TERHUBUNG KE JARINGAN (SEPERTI INTERNET).

PENINGKATAN KEJAHATAN KOMPUTER

- **PEMAKAI MAKIN MELEK TEKNOLOGI DAN KEMUDAHAN MENDAPATKAN SOFTWARE.**
  - ADA KESEMPATAN UNTUK MENJAJAL. TINGGAL DOWNLOAD SOFTWARE DARI INTERNET.
    (SCRIPT KIDDIES)
  - SISTEM ADMINISTRATOR HARUS SELANGKAH DI DEPAN.

HACKER KECIL



Introduction of Cryptography

References:

1. Applied Cryptography, Bruce Schneier
2. Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell

DEFINITIONS

The Concise Oxford Dictionary (2006)

- Cryptography was the art of writing or solving codes.

Until 20th century

- Cryptography was an art to construct and break good codes.

The late 20th century

- Cryptography was a science.

Now

- Cryptography encompasses much more than secret communication.

MODERN CRYPTOGRAPHY

It's the scientific study of techniques for securing digital information, transactions, and distributed computations.

CLASICAL CRYPTOGRAPHY VS MODERN CRYPTOGRAPHY

Classical Cryptography

- Cryptography was in military and intelligence organizations.

Modern Cryptography

- Cryptography is everywhere!

TERMINOLOGY

Plaintext (cleartext)	• Message
Encryption	• The process to disguise message
Ciphertext	• Encrypted message
Decryption	• The process to turn back ciphertext into plaintext
Cipher	• The algorithm of cryptography
Cryptosystem	• A cipher with plaintext, ciphertext, and key.

TERMINOLOGY (CONT'D)

Cryptography

- The art and science to make message secure

Cryptographers

- People who practice cryptography

Cryptanalysis

- The art and science to break ciphertext

Cryptanalysts

- People who practice crypanalysis

Cryptology

- The branch of mathematics involving cryptography and cryptanalysis

Cryptologists

- People who practice cryptology

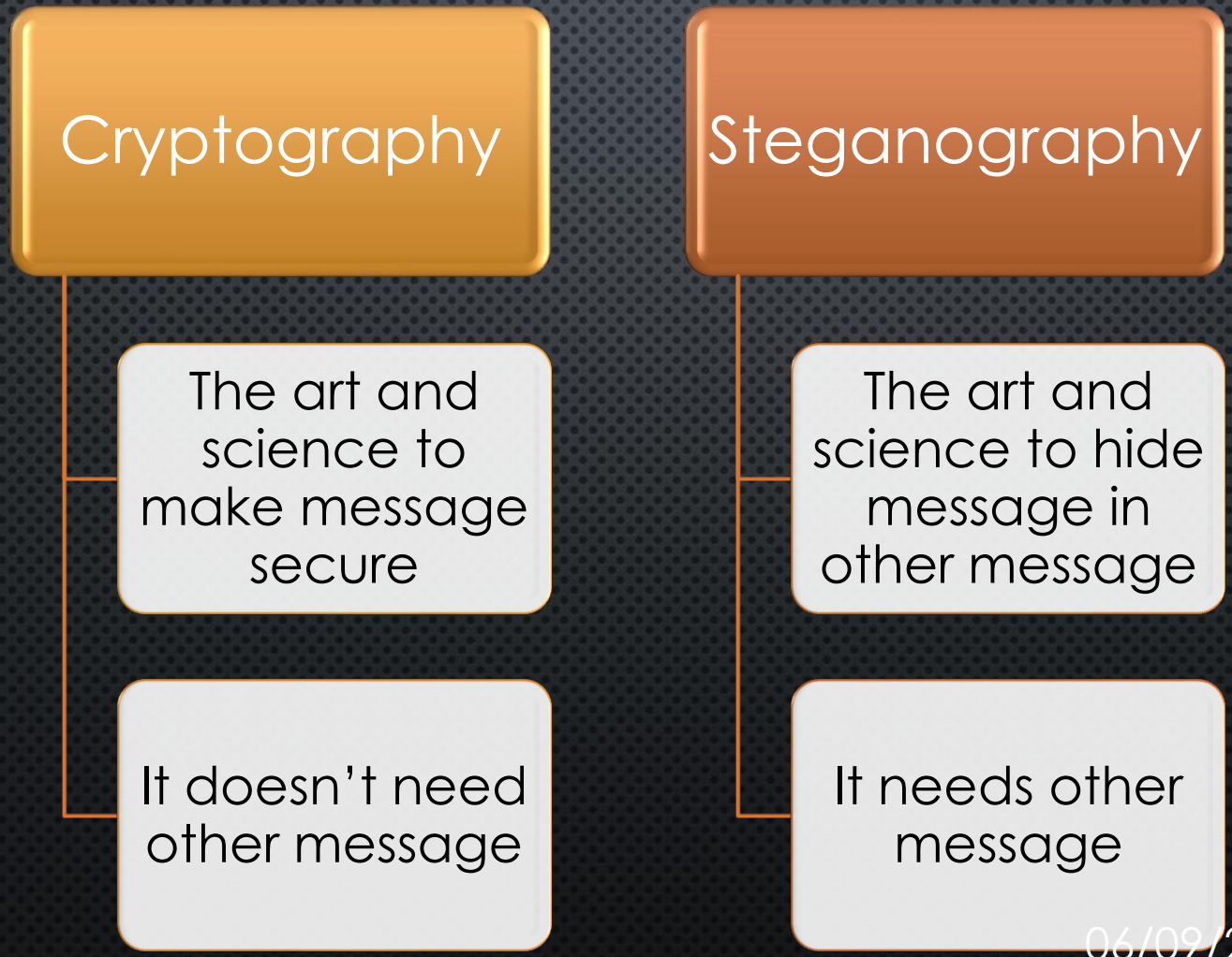
Kerckhoffs' Principle

- The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

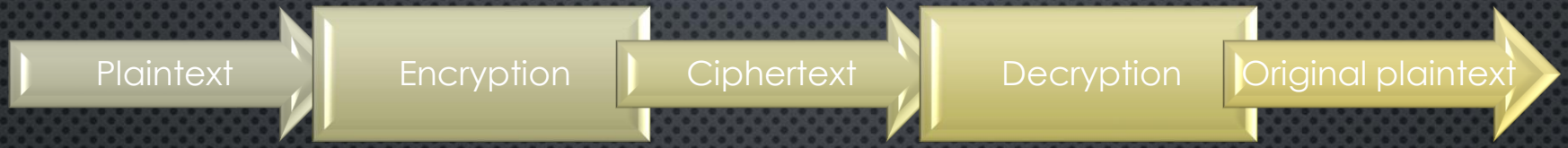
Why?

- It is more easy to keep the secrecy of key than cipher.
- It is more easy to change the key than cipher.

CRYPTOGRAPHY VS STEGANOGRAPHY



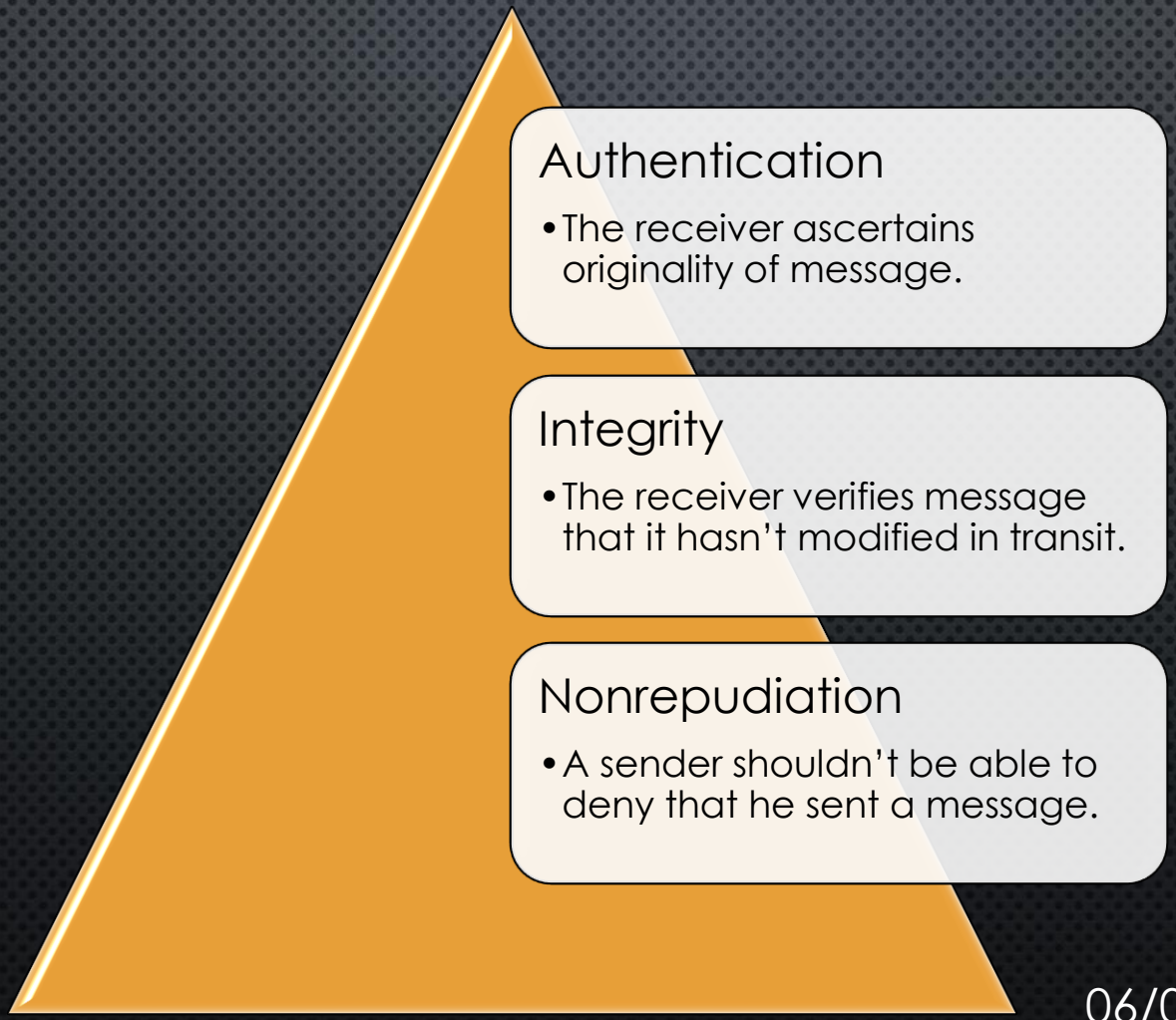
ENCRYPTION – DECRYPTION PROCESS



E(M) = C
D(C) = M
D(E(M)) = M

M : message/plaintext
C : ciphertext
E : encription process
D : decription process

CYPTOGRAPHY'S JOBS



Authentication

- The receiver ascertains originality of message.

Integrity

- The receiver verifies message that it hasn't modified in transit.

Nonrepudiation

- A sender shouldn't be able to deny that he sent a message.

CRYPTOGRAPIC ALGORITHM

- A CYPTOGRAPHIC ALGORITHM (CIPHER) IS THE MATHEMATICAL FUNCTION FOR ENCRIPTION AND DECRIPTION.
- A RESTRICTED ALGORITHM IS THE CRYPTOGRAPHIC ALGORITHM BASED ON KEEPING THAT IT WORKS A SECRET. THIS ALGORITHM HAS NO QUALITY CONTROL OR STANDARDIZATION.
- KEY-BASED ALGORITHMS CONSIST OF SYMMETRIC ALGORITHM AND ASYMMETRIC ALGORITHM.

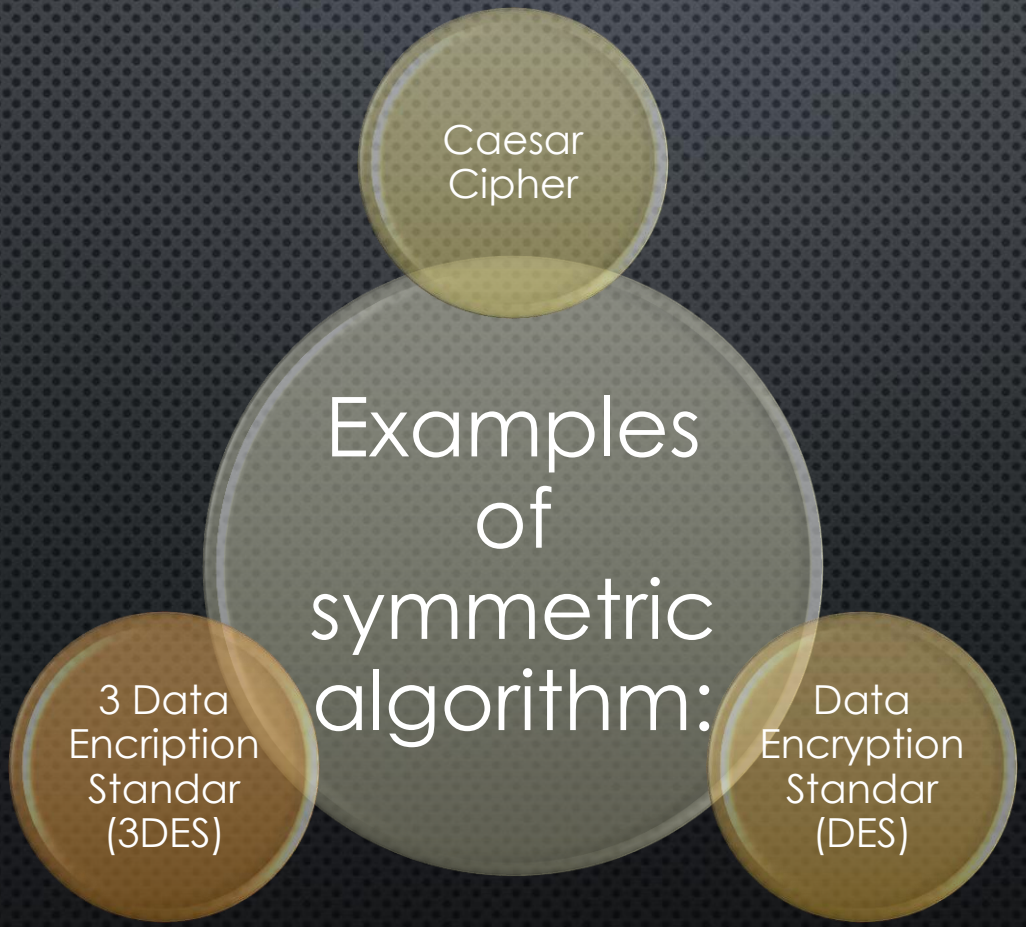
SYMMETRIC ALGORITHM

- It's also called conventional algoritm or private-key algorithm.
- The decryption key can be calculated from the encription key and vice versa. The decryption key and ecnryption key are the same.
- Encryption and decryption process can be denoted by:

$E_K(M) = C$

$D_K(C) = M$

SYMMETRIC ALGORITHM (CONT'D)



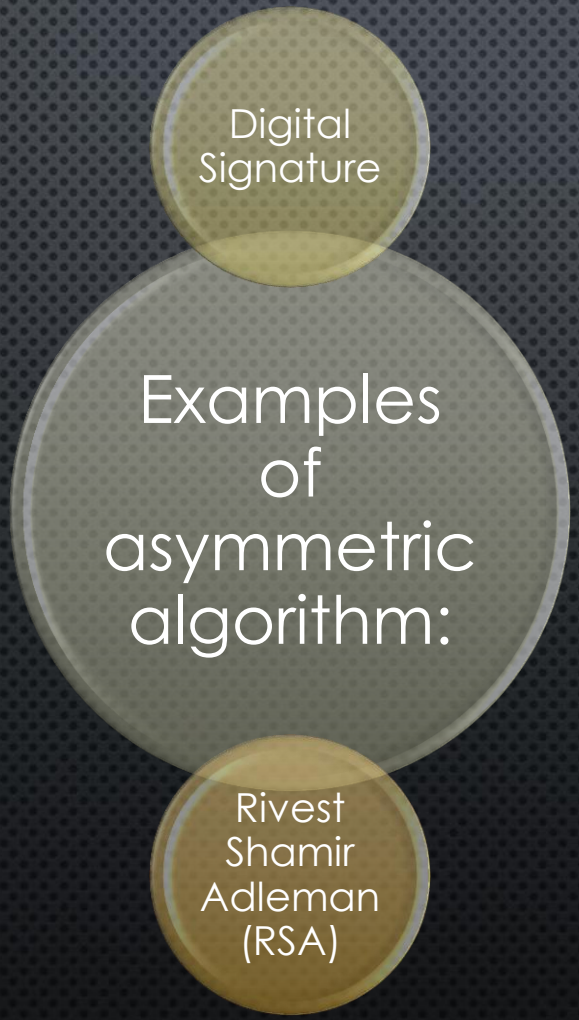
Asymmetric Cryptography

- It's also called public-key algorithm.
- The decryption key cann't be calculated from the encription key and vise versa. The decryption key and encryption key aren't the same.
- Encryption and decryption process can be denoted by:

$E_{K1}(M) = C$

$D_{K2}(C) = M$

ASYMMETRIC CRYPTOGRAPHY (CONT'D)



PROTOCOL OF CRYPTOGRAPHY

Protocol is a series of steps between two or more parties to do the task.

Characteristics of protocol:

- It has a sequence from start to finish
- It involves two or more parties
- It achieves something

Protocol for symmetric cryptography

- Alice and Bob agree on a cryptosystem.
- Alice and Bob agree on a key.
- Alice encrypts plaintext using the encryption algorithm and the key. The result is ciphertext.
- Alice sends ciphertext to Bob.
- Bob decrypts ciphertext using the same algorithm and key and reads it.

Protocol for asymmetric cryptography (1)

- Alice and Bob agree on a cyptosystem.
- Bob sends Alice his public key.
- Alice encrypts plaintext using Bob's public key and sends it to Bob.
- Bob decrypts Alice's ciphertext using his private key.

Protocol for Asymmetric Cryptography (2)

- Alice gets Bob's public key from database. All public keys are published on database.
- Alice encrypts plaintext using Bob's public key and sends it to Bob.
- Bob decrypts Alice's ciphertext using his private key.

Protocol for Hybrid Cryptography

- Bob sends Alice his public key.
- Alice generates a random session key, encrypts it using public key, and sends it to Bob.
- Bob decrypts ciphertext using private key to recover session key.
- Alice and Bob encrypt their communications using the same session key.

TERIMA KASIH