Information security & e-government

Jazi Eko Istiyanto, Ph.D

- **Lab. Elektronika & Instrumentasi, Jurusan Fisika FMIPA UGM**
- **Program Magister Ilmu Komputer UGM**

**“it is insufficient to protect ourselves with laws;
we need to protect ourselves with mathematics.”**

Bruce Schneier

Cryptology & Hacking

- Cryptology = Cryptography + Cryptanalysis
- Cryptanalysis = Seni membobol sandi (encrypted) tanpa mengetahui kunci enkripsi-nya
- Sering disamakan dengan hacking
- Hacking lebih luas, menyangkut eksploitasi security holes pada O/S, program, protokol, dsb.

Hacker & Cracker

- Cracker = orang yang memang bermaksud jahat
- Hacker = bermaksud memperbaiki sistem
- Hacker bisa berubah menjadi cracker
- Novice hacker lebih berbahaya d/p intermediate/expert

Ancaman Security

- **Passive Attack:**
  - mencuri dengar, memonitor transmisi
  - contoh: e-mail, file transfers, client/server exchange
- **Active Attack:**
  - modifikasi data
  - contoh : akses tidak sah ke sistem komputer

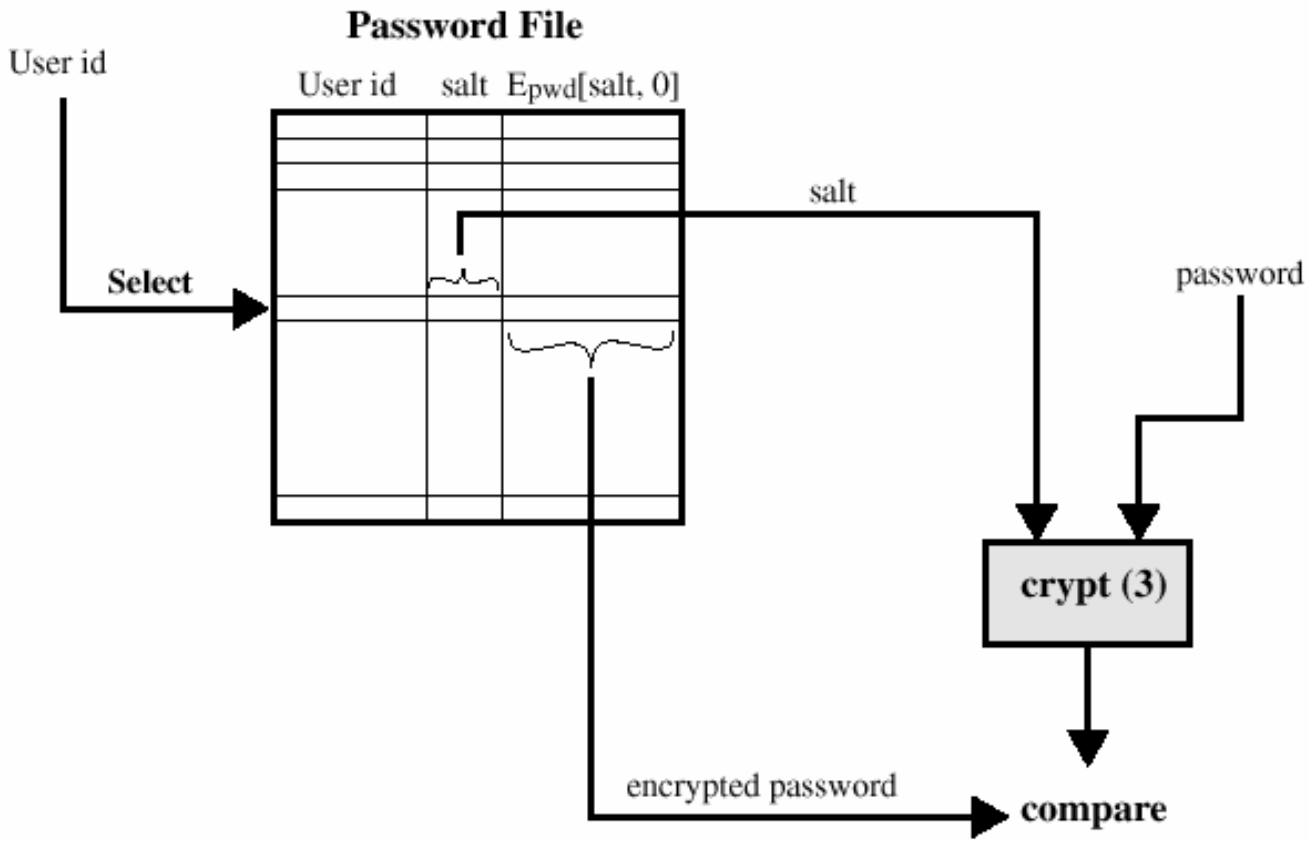
Membobol Enkripsi

- **Cryptanalysis**:
  - eksploitasi karakteristik algoritma untuk memperoleh kunci dan/atau plaintext
  - pesan selanjutnya dengan kunci sama akan mudah dibobol
- **Brute Force**:
  - coba-coba (trial & error)
  - coba semua nilai kunci yang mungkin hingga bobol.
  - rata-rata 50% dari kemungkinan nilai kunci harus dicoba.

Enkripsi Memperlambat Pembobolan

Average Time Required for Exhaustive Key Search			
Key Size (bits)	**Number of Alternative Keys**	**Time Required at 1 Decryption per us**	**Time Required at 10^6 Decryption per us**
32	2^32	35.8 mins	2.15 milliseconds
56	2^56	1142 years	10 hours
128	2^128	5.4*10^24 years	5.4*10^18 years
168	2^168	5.9*10^36 years	5.9*10^30 years

UNIX Password Scheme



Verifying a password file

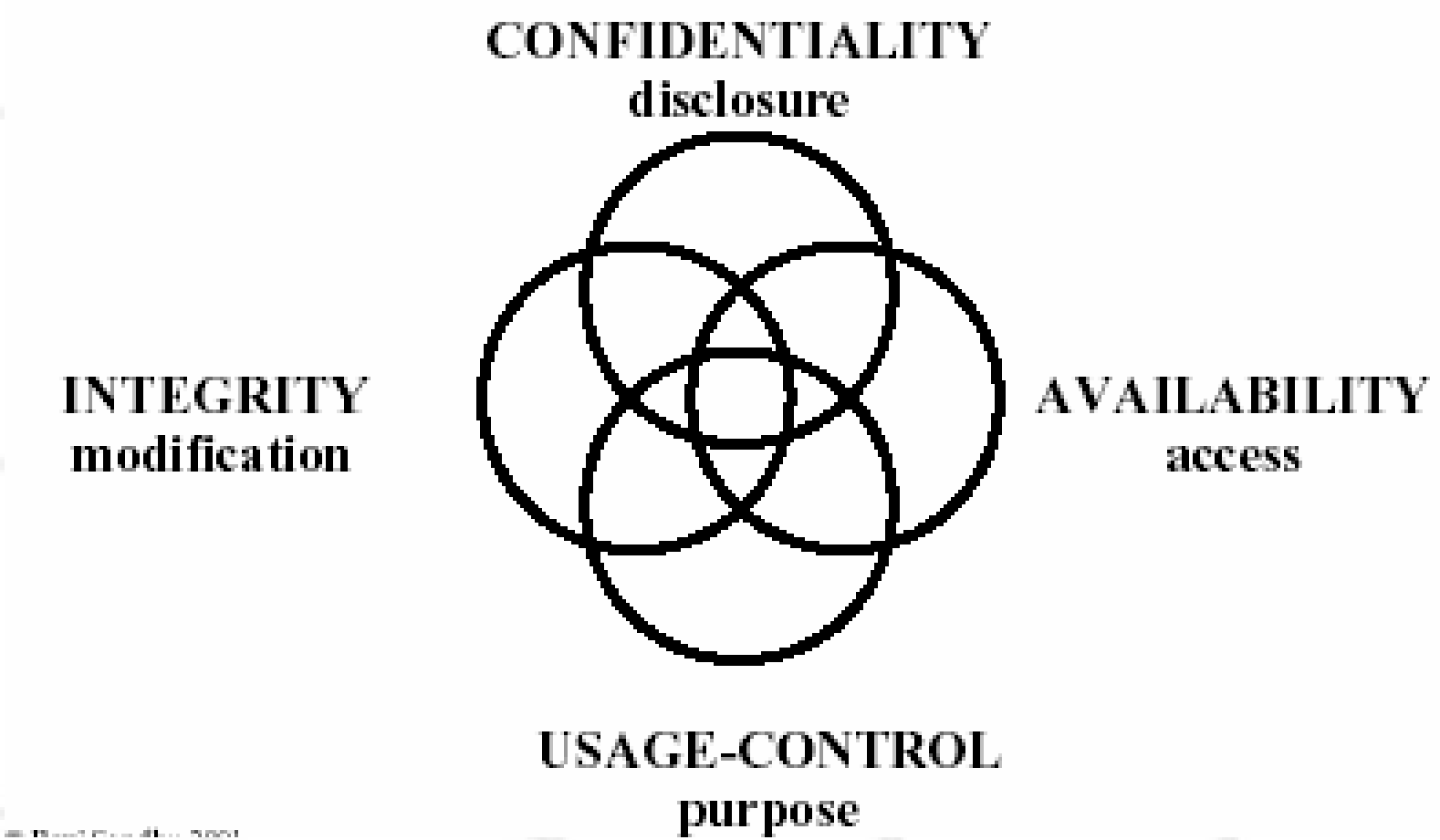
Cryptography is not Everything (1)

- Morris worm (1987)
- Password sniffing (1994)
- IP spoofing (1995)
- Denial of Services (1996)
- E-mail-borne Virus (1999)
- Distributed Denial of Services (2000)

Cryptography is not Everything (2)

- Microsoft dua kali dibobol (10/2000)
- Situs Israel dibobol (10/2000)
- Web Dept Information, Korea (8/200)
- eBay, Yahoo, Amazon, CNN (2/2000)
- I LOVE YOU (5/2000)
- 22000 serangan ke Pentagon (2000)

Security Objectives



Security

1. **Prevention**: tindakan untuk mencegah perusakan aset
2. **Detection:** tindakan untuk mendeteksi kapan, bagaimana, dan oleh siapa asset telah dirusak
3. **Reaction**: tindakan untuk mengembalikan asset dari perusakan

Security – barang pribadi

1. **Prevention**: kunci/gembok pada pintu, tralis pada jendela, tembok
2. **Detection**: barang tidak ada, alarm berbunyi, cctv
3. **Reaction:** hubungi polisi, klaim asuransi

Security e-commerce

1. **prevention**: pesanan dienkripsi, penjual mencek identitas pembeli, jangan menggunakan internet (?)
2. **detection**: transaksi yang tidak anda lakukan muncul pada credit card statement
3. **reaction**: komplain, minta nomor kartu kredit baru

Threats, vulnerabilities, assets, risks

- **Threats** : serangan yang mungkin diterima (ancaman)
- **Vulnerabilities** : kelemahan/security holes
- **Assets**: informasi dan sumberdaya yang harus diproteksi
- **Risks** : mempersyaratkan pengujian atas Threats, Vulnerabilities, dan Assets

Perspektif security

1. No silver bullets
2. Security adalah proses
3. Sikap konservatif
4. Defense-in-depth
5. Secondary objective
6. Tidak ada security mutlak
7. Security dapat ditingkatkan
8. Ketidakamanan tidak dapat ditolerir

Intrusi klasik : skenario 1

- **Insider attack** : penyerang adalah pengguna yang sah
- **Insider** memperoleh akses khusus
- Memanfaatkan bug pada program/sistem
- Memanfaatkan konfigurasi yang lemah
- Menginstal backdoor/trojan horse untuk memfasilitasi perolehan hak akses berikut

Intrusi klasik : skenario 2

- Outsider attack
- Memperoleh akses ke account yang sah
- Menyamar sebagai insider attack

Intrusi via network : skenario 3

- Outsider/insider attack
- Menspoof protokol jaringan agar secara efektif memperoleh akses ke account yang sah
- Port scanning : imap (port 143), SMB(port 139), login(port 513), http(port 80)
- DNS server = target primer untuk membangun basisdata alamat IP

Intrusion detection systems (1)

- Network Flight Recorder www.nfr.net/nfr
- TCP Wrapper (Wietse Venema) ftp.cerias.purdue.edu/pub/tools/unix
- Port didefinisikan di /etc/services
- Dibuat program untuk melakukan aksi ‘membunyikan alarm’ diset di /etc/inetd.conf

Intrusion detection systems (2)

- imap stream tcp nowait root /usr/local/bin/tcpd imap trap
- /etc/hosts.allow berisi imap.trap: ALL : spawn (/var/adm/ids.sh %d %h %H)
- Bila port discan akan mengaktifkan ids.sh untuk mengirim e-mail
- Dibuat program untuk memonitor port dan diset di /etc/inetd.conf

Intrusion detection systems (3)

Subject: ### Intrusion Detection Alert ###

You have received this alert because the network
is potentially being scanned. The information below
is the packet that was logged and dropped.

Date: Sat Jan 24
Time: 18:47:46
Source: ICARUS.CC.UIC.EDU
Destination: lisa
Service: imap

--- Finger Results ---

[ICARUS.CC.UIC.EDU]

Login Name TTY Idle When Where

Spitzner Lance Everett Spitzn pts/72 Sun 18:42 lspitz-4.soho.entera

Intrusion detection systems (4)

```
#!/bin/ksh
# Script launched by tcpd for intrusion detection purposes
USER=lance@honeynet.org
        SRV=`echo $1 | cut -f1 -d.`
        DATE=`date "+%a %b %e"`
        TIME=`date "+%T"`
        FINGER=`/usr/local/bin/safe_finger @$2`
MAIL=/usr/bin/mail
$MAIL $USER <<EOF
        Subject: ### Intrusion Detection Alert ###
You have received this alert because the network
        is potentially being scanned. The information below
        is the packet that was logged and dropped.
Date: $DATE
        Time: $TIME
        Source: $2
        Destination: $3
        Service: $SRV
--- Finger Results ---
$FINGER
EOF
##### If the service is imap, lets go ahead and snoop the session.
if [ $SRV=imap ]; then
snoop -v -c 5000 -o /var/adm/$2_snoop.$$ $2 &
fi
```

Teorema Firewall dari Bellovin (1)

- (**Murphy's Law**) Semua program mempunyai bug
- (**Law of Large Programs**) Program besar mengandung lebih banyak bug dibanding indikasi ukurannya (rumus 1 bug/ 1K baris code)
- Program untuk security juga punya bug berkaitan dengan security

Teorema Firewall dari Bellovin (2)

- Program yang tidak dijalankan, tidak penting ada bug-nya atau tidak
- Program yang tidak dijalankan, tidak penting punya security hole atau tidak
- Program yang dijalankan pada mesin yang terhubung internet harus sesedikit mungkin bugnya dan sekecil mungkin ukurannya

Open Source s/w Initiative (www.opensource.org/osd.html)

- Free redistribution
- Source code must be included
- Derived works must be allowed
- Integrity of the authors source code
- No discrimination against persons or groups
- No discrimination against fields of endeavour
- Distribution of license applies to all
- License must not be specific to a product
- License must not contaminate other software

Closed Source	Open Source
Source Code is not published	Source code is published
Companies earn money on closed source code	Companies do not earn money from sale of the code.
Not easy to see if a patent has been violated	Anyone can see if it violates a patent
There is always a company to help	There is no technical support without resorting to user groups and so forth.
You can sue the company that distributes the software	Nobody to sue. The issue of liability is still very much undecided.
Users have to wait for service pack release in order to fix bugs	Generally fast bug fixes, particularly on the more popular OSS products.

Contoh Open Source s/w

- Linux
- OpenBSD/FreeBSD
- Majordomo
- OpenPGP/PGP
- Samba

Security flaws pada OSS

- **FreeBSD** (Keyinit pada S/Key scheme)
- **Kerberos V4** (Pembangkit bil acak penghasil kunci 56-bit untuk DES)
- **Majordomo**(hacker dapat merunning perintah sebagai user ‘majordomo’)
- **PGP**(pembangkit bil acak)
- **Samba** (DoS dapat mereaktivasi smbd, buffer overflow pada message service smbd, race condition pada smbmnt

Risks and countermeasures

- Imposter connects over network
  - individual user-ids and passwords
- Network monitor reading passwords
  - encrypt password on network
- bogus replay of encrypted logon
  - strong authentication protocol e.g. krb
- insertion of packets into existing session
  - authentication codes on packets (e.g. RPC)
- Trojan Horse logon program
  - “trusted path” or SmartCard etc...

Security sistem operasi

- Sistem operasi terlalu kompleks
  - Security berbanding terbalik dengan kompleksitas
  - device drivers (dan device) biasanya ruwet
- konsep Trusted Computing Base (TCB)
  - Minimalkan komponen security yang pokok
  - Hilangkan yang tidak perlu dari TCB
  - TCB melindungi sumberdaya abstrak (file...)
  - Arsitektur komputer dipakai untuk proteksi TCB
- Security dapat menurunkan kinerja
  - Harus dilakukan kompromi desain
  - 100% security tidak mungkin

TCSEC - 1983

- Kriteria dirancang untuk persyaratan militer
  - D: no security
  - C1: basic control over subjects and objects
  - C2: individual logon, discretionary access control, accountability (audit trail)
  - B1: Mandatory access control - MLS labels
  - B2: covert channel analysis, trusted path
  - B3: minimal security kernel
  - A1: verified security
- Lemah pada jaringan, sistem khusus, tetapi masih merupakan benchmark yang berguna

Apakah linux secure?

- Untuk menunjukkan bahwa suatu O/S bersifat secure, harus dibuktikan bahwa semua loophole telah ditemukan dan telah ditutup
  - Kapan selesainya?
- Untuk menunjukkan bahwa suatu O/S tidak secure, hanya perlu menemukan sebuah hole dan mengeksploitasinya
  - Tidak begitu impresif
  - Dapat bersifat illegal.
- Tetapi kita harus melakukan apa yang kita bisa.

Tantangan

- Antarmuka untuk system call
  - Pengalamatan memori dan referensi parameter
- Verifikasi dari
  - hardware (devices dan device driver)
  - Sistem software yg kompleks (e.g. operating systems)
  - Layanan jaringan (e.g. fingerd)
  - protokol (e.g. TCP syn)
  - Protokol autentikasi (Needham/Schroeder)
- Kompromi desain dan implementasi
  - Kinerja dan kompatibilitas mundur
  - N.B. LM password dan FAT file system#
- Administrasi
  - Menggunakan mekanisme secara efektif

UK ITsec

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFICATE No. P121

This is to certify that

MICROSOFT® WINDOWS NT® WORKSTATION
and SERVER

Version 4.0 (Build 1381) Service Pack 3
on Compaq Deskpro 6400, Digital Prioris MX 6200
& Data General Aviion 6600 machines

have been evaluated under the terms of the UK ITSEC Scheme and comply with the requirements for:

E3 - Assurance Level
F-C2 - Functionality Class

date: 31 March 1999 *signed*

Dr. R PIZER
Head of the
Certification Body

E3

IT Security Certified

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME
PO BOX 152, CHELTENHAM, GLOUCESTERSHIRE
GL52 5UF, UNITED KINGDOM

CESG

dti

E-government?

- Web sites
- Intranet
- Limited interactivity
- Enterprise portals
- E-procurement
- Self-service applications
- E-business suites

E-government?

- Customer Relations Management
- Polling and Voting
- E-Market Makers
- Service Delivery
- Wireless Access
- Location –Based Services

They don't really mean 100% e-(anything)

- Paperless office
- E-learning/e-education
- E-commerce
- E-government
- Teknologi infrastruktur, security, perangkat hukum, digital forensic belum cukup matang untuk 100% e-gov

konklusi

- Bila aplikasi e-gov dibatasi tahapannya, teknologi security cukup bisa menjamin keamanan transaksi sehingga tidak perlu menjadi momok
- Masyarakat e-government dituntut tidak hanya melek IT, dan melek informasi, tetapi juga harus security-aware

Terima kasih

Science today is
technology tomorrow