Sistem Operasi

Keamanan Komputer

2016

UNIVERSITAS Telkom

Outline

- Masalah Keamanan
- Autentikasi
- Serangan dari dalam sistem
- Serangan dari luar sistem
- Mengamankan Sistem
- Deteksi Intrusion
- Enkripsi

Masalah Keamanan

- Keamanan harus dilihat sebagai lingkungan eksternal dari sistem dan melindungi sistem darinya:
  - Akses tidak sah.
  - Modifikasi merusak atau mengganggu
  - Ketidak konsistenan sistem karena kecelakaan/ketidak sengajaan.
- Lebih mudah melindungi dari kecelakaan daripada penggunaan merusak.

Autentikasi

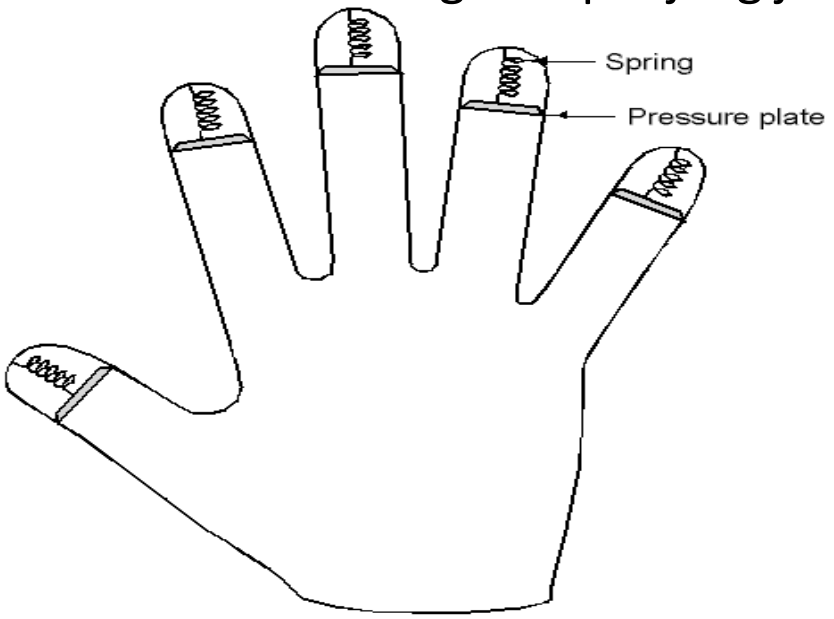
- Identitas pengguna kebanyakan diakui melalui *password*.
- Password harus dijaga kerahasiaannya.
  - Password sering diubah.
  - Menggunaan password yang “tidak bisa” ditebak.
  - Men-log semua percobaan akses yang gagal.
- Password dapat dienkripsi atau juga hanya digunakan sekali (*one time pad*).

Fungsi Satu-Arah

- Funsi seperti rumus untuk f(x)
  - Mudah untuk didapatkan y = f(x)
- Tetapi jika punya y
  - Sukar dihitung berapa x

Autentikasi Menggunakan Biometrik

Peralatan untuk mengukur panjang jari.



Serangan Dalam

- Kuda Troya
- Pencurian Login
- Pintu Jebakan (Trap Door)
- Stack dan Buffer Overflow
  - Meneksplotasi bug dalam program (overflow baik di buffer stack atau memori.)

Kuda Troya

- Program gratis (freeware) tersedia untuk pengguna yang tidak curiga
  - Didalamnya mengandung code untuk merusak
- Menempatkan program utilitas yang telah diubah di komputer korban
  - Menjebak pengguna untuk menggunakan program tersebut

Pencurian Login

(a) Layar login asli

(b) Layar login palsu

Windows: Ctrl+Alt+Del

(a)

(b)

Bom Logik

- Programer suatu perusahaan menulis program
  - Berpotensi untuk merusak
  - OK selama dia memasukkan password secara rutin
  - Jika dia dipecat, tidak ada password dan bom meledak

Pintu Jebakan (Trap/Back Door)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

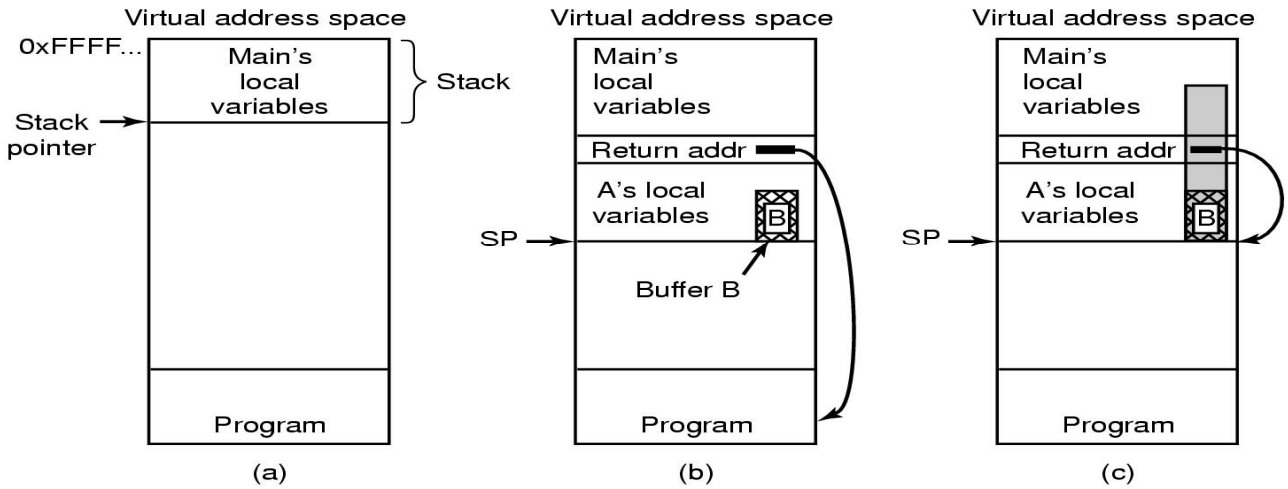
(b)

(a) Code normal.

(b) Code dengan tambahan pintu jebakan

UNIVERSITAS Telkom

Buffer Overflow



(a) Situasi ketika program utama jalan

(b) setelah program *A* dipanggil

(c) Buffer overflow diwarnai abu-abu

Contoh program ber bug

- Input a,
- Input b,
- c = a/b,
- Output c,

- Seharusnya

Contoh program fixed

- Input a,
- Input b,
- If b=0 then out
- c = a/b,
- Output c,

Serangan Luar

- Worm – menggunakan mekanisme spawn; program tunggal
- Worm Internet
  - Memanfaatkan fitur jaringan UNIX (remote access) dan bug di program *finger* dan *sendmail*.
  - Mengakses program umpan akan memuat program worm.
- Virus – potongan code yang “ada” didalam program yang sah/normal.
  - Utamanya berpengaruh di sistem mikrokomputer.
  - Mendownload program virus dari server atau bertukar data lewat media.
  - *Safe computing*.
- Denial of Service
  - Overload komputer target untuk melumpuhkan layanan

Evolusi Virus

- 1983 Periset virus Fred Cohen memakai kata virus dalam sebuah makalahnya
- 1987 Brain, virus koputer pertama dirilis. Ia menginfeksi *boot sector* floppy disk 360KB dan secara diam-diam membuat komputer kehilangan kekebalannya. Stoned, virus pertama yang menginfeksi *Master Boot Record* (MBR) dirilis. Virus ini mengacak-acak MBR harddisk dan mencegah sistem melakukan *booting*

Evolusi Virus (lanjutan)

- 1988 Software antivirus pertama dirilis oleh programmer Indonesia. Antivirus ini bisa mendeteksi Brain, membuangnya dari komputer dan membuat sistem kebal terhadap serangan Brain berikutnya. Internet Worm disebarkan ke Internet dan menyerang sekitar 6000 komputer
- 1989 Dark Avenger muncul. Virus ini cepat menginfeksi berbagai program, tetapi lama menimbulkan kerusakan, sehingga virus ini tidak terdeteksi untuk jangka waktu yang lama. IBM merilis produk antivirus pertama secara komersial. Penelitian intensif mengenai vuris dilakukan

Evolusi Virus (lanjutan)

- 1990 Jenis-jenis virus canggih seperti *polymorphic* (yang memodifikasi diri mereka saat menyebar) dan *multipartite* (yang menginfeksi berbagai lokasi pada komputer) muncul. Forum virus menjadi tempat populer bagi pembuat virus untuk bertukar kode-kode
- 1991 *Kit* membuat virus, yang memungkinkan semua orang membuat virus dengan mudah. Pada awal tahun hanya 9% perusahaan terserang virus, dan pada akhir tahun melonjak menjadi 63%

Evolusi Virus (lanjutan)

- 1992 *Michaelangelo* virus pertama yang menyebabkan kapanikan media, dirancang untuk meng*overwrite* bagian-bagian harddisk yang terinfeksi pada 6 Mei, tanggal lahir dari seniman jaman Renaissance tersebut. Penjualan software antivirus meningkat, walaupun hanya sedikit kasus yang tercatat
- 1994 Pembuat virus *Pathogen* asal Inggris berhasil dilacak oleh Scotland Yard dan dijatuhi hukuman penjara 18 bulan. Peristiwa ini merupakan pertama kalinya pembuat virus diadili

Evolusi Virus (lanjutan)

- 1995 *Concept* virus macro pertama hadir. Dibuat menggunakan bahasa Microsoft Word Basic, bekerja dimana paltform Word ada, baik di PC maupun Mac. Peristiwa ini memicu kemunculan banyak sekali virus karena virus macro mudah sekali diciptakan dan disebarkan
- 1999 Virus *Chernobyl* yang membuat harddisk dan data pengguna tidak bisa diakses menyerang pada bulan April. Walaupun menginfeksi hanya beberapa komputer di AS, virus ini menyebabkan kerusakan di seluruh dunia. Cina menderita kerugian US$291 juta, Turki dan Korsel juga mengalami kerusakan parah

Evolusi Virus (lanjutan)

- Virus *Melissa* menyerang ratusan ribu komputer di seluruh dunia. Ia menggunakan Microsoft Outlook untuk mengirimkan dirinya sendiri kepada 50 orang di buku alamat penggunannya dan menjadikannya virus pertama yang mampu melompat sendiri dari satu komputer ke komputer lain.
- 2000 Virus *Loveletter* yang berasal dari Filipina menghancurkan seluruh Eropa dan AS hanya dalam waktu 6 jam. Ia menginfeksi 3 juta komputer dan menyebabkan kerugian US$ 8,7 milyar

Ketika Cinta itu Datang (th 2000)

- 2 Mei Virus Loveletter muncul di Filipina. Tidak lama kemudian Sky Internet sebuah ISP di Filipina memberitahukan bahwa ribuan komputer yang telah terinfeksi memasuki empat halaman Web yang ditempatkan untuk mendapatkan Kuda Trojan yang diposkan oleh pembuat virus. Perusahaan itu menghapus halaman-halaman Web yang mencurigakan
- 4 Mei 04:12 Symantec dan vendor antivirus lain mulai membuat definisi untuk virus tersebut
- 4 Mei 07:00 Tim investigasi menemukan bahwa pembuat Love Letter tersebut meninggalkan nama pendeknya (Spyder), alamat email dan nama tempat tinggalnya dalam sebuah sumber code. Dia juga mengenalkan dirinya sebagai anggota kelompok programmer GrammerSoft

Ketika Cinta itu Datang

- 4 Mei 16:00 Varian LoveLetter muncul dengan kata “Very funny Joke” yang menggantikan “I Love You” dalam judul subjek email
- 4 Mei 18:40 Setidaknya 20 negara dilaporkan telah terinfeksi
- 5 Mei Lima varian dari virus tersebut muncul. Beberapa detektif amatir termasuk murid sekolah Stockholm bernama Frederick Bjorck, mencari newsgroup menggunakan keyword dan menemukan virus tersebut. Bjorck menemukan beberapa virus serupa diposkan Spyder 4 bulan sebelumnya, termasuk salah satu versi yang dikenali pembuatnya “murid dari amacc mkt.Phil” singkatan dari AMA Computer Colledge di Makati Manila

UNIVERSITAS Telkom

Ketika Cinta itu Datang

- 8 Mei Setelah mengenali nomor telpon dan dari komputer mana visur tersebut dikirim, polisi lokal menggeledah apartemen Spyder. Polisi tidak menemukan komputer, tetapi mereka menyita sebuah disket yang berisi virus serupa LoveLetter
- 11 Mei Polisi meminta keterangan Onel de Guzman yang tinggal di apartemen tersebut. Dia mengakui telah mengeluarkan virus tersebut secara tidak sengaja, tetapi menyangkal telah membuatnya
- 29 Juni Filipina tidak memiliki undang-undang anti virus, sehingga de Guzman diperiksa dengan undang-undang kejahatan kartu kredit
- 21 Agustus Penegak hukum menyimpulkan bahwa undang-undang kartu kredit tidak dapat digunakan dalam kasus ini dan dengan berat menurunkan denda

Denial of Service

A: Masihkah bisa dilihat sekarang?

B: Masihkah?!

Distributed DoS

- Penyerang akan membuat banyak komputer lain untuk menjadi budaknya (Zombie) dengan memasukkan program semacam Kuda Troya
- Pada saat tertentu penyerang akan memerintahkan komputer-komputer tersebut untuk mengirimkan data/paket sampah ke komputer yang diserang

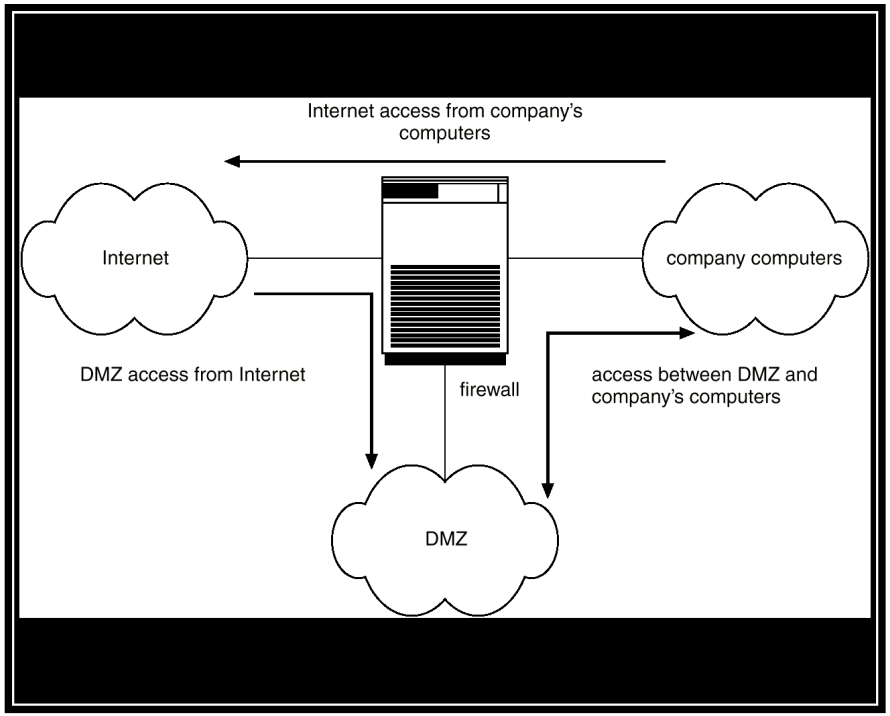
Pemeriksaan Keamanan

- Periksa:
  - Password pendek atau mudah ditebak
  - Program yang tidak terdaftar
  - Program tidak terdaftar di direktori sistem
  - Proses yang berjalan terlampau lama
  - Proteksi direktori yang tidak memadai
  - Proteksi file data sistem yang tidak memadai
  - Titik masuk program berbahaya
  - Pengubahan program sistem: monitor nilai checksum

FireWall

- Sebuah firewall ditempatkan antara host terpercaya dan tidak terpercaya.
- Firewall membatasi akses jaringan antara kedua domain keamanan.

Kam-Jar Melalui Pemisahan Domain Via Firewall



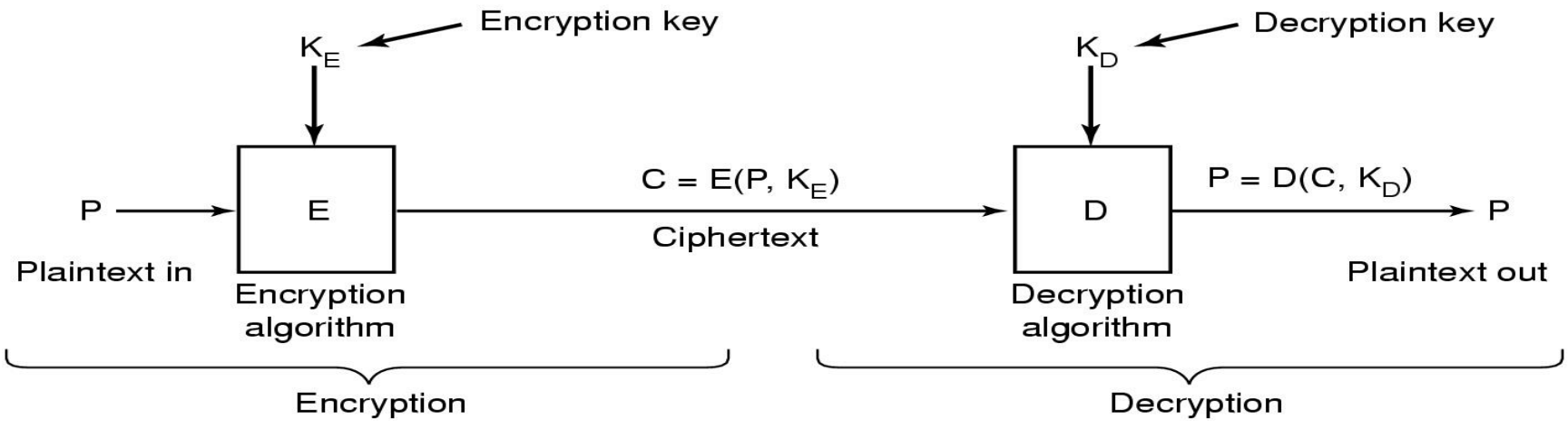
Deteksi Intrusion

- Mendeteksi percobaan untuk memasuki sistem komputer.
- Metoda deteksi:
  - Auditing dan logging.
  - Tripwire (software UNIX yang memeriksa file dan direktori tertentu yang telah diubah – misal. File password)
- Monitoring system call

Enkripsi

- Enkrip clear text ke cipher text.
- Properti dari teknik enkripsi:
  - Mudah bagi pengguna yang sah untuk menenkripsi dan mendekripsi data.
  - Skema enkripsi tidak tergantung pada kerahasiaan algoritma tetpau pada kerahasiaan parameter dari algoritma yang disebut kunci enkripsi.
  - Harus sukar bagi pihak lain untuk menemukan kunci enkripsi.

Kriptografi Dasar



Hubungan antara plaintext dan ciphertext

Kriptografi Kunci Rahasia

- Subtitusi satu demi satu huruf dengan huruf lain
  - Setiap huruf diganti dengan huruf lain
  - Hello, World ➔ Ifmmp, Xpsmf
- Kunci enkripsi = kunci deskripsi
- Disebut juga kriptografi kunci simetris

Kriptografi Kunci Publik

- Semua pengguna mengambil sepasang kunci publik dan pribadi
  - Umumkan kunci public
  - Kunci pribadi dijaga kerahasiaannya
- Kunci publik untuk mengenkripsi
  - Kunci pribadi untuk mendekripsi
- Harus sudah dicari/dihitung kunci pribadi dari kunci publiknya

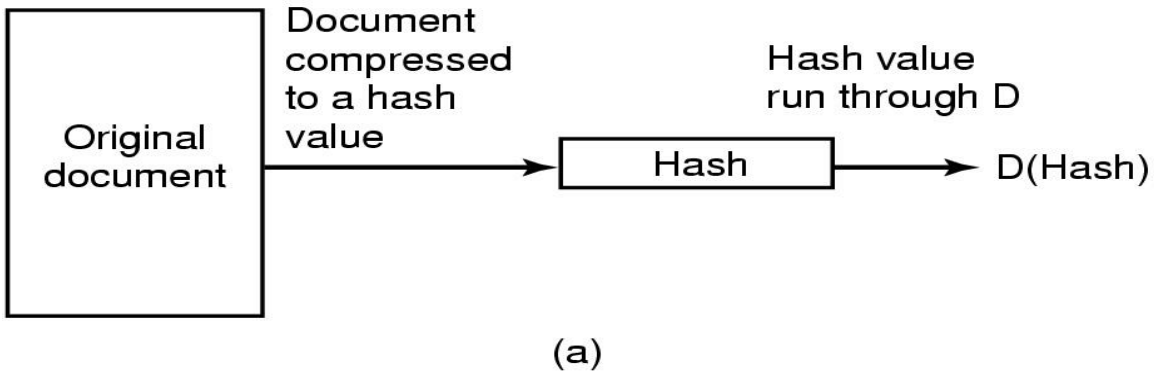
Tanda-tangan Digital

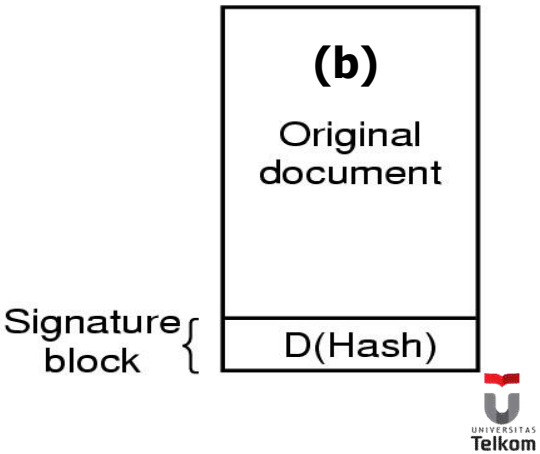
a. Hitung blok tanda-tangan

b. Penerima menerima

H1= Hash(Doc)

H2= Decode(Signature)





10 Tahap Kesehatan Microsoft

- Gunakan firewall internet
- Update software dan keamanan sistem dengan Patch Management
- Gunakan antivirus yang up-to-date
- Gunakan password yang kuat
- Pastikan keamanan fisik
- Browse web secara aman/depensif
- Gunakan email secara aman
- Backup dan restore secara reguler
- Hubungi remote user secara aman
- Kunci jaringan wireless

UNIVERSITAS Telkom