MENGAMANKAN SISTEM INFORMASI

Learning Objectives

- Mengapa sistem informasi rentan terhadap kehancuran, kesalahan, dan melanggar?
- Berapa nilai bisnis keamanan dan kontrol?
- Apa saja komponen dari suatu organisasi kerangka kerja untuk keamanan dan kontrol?
- Apa alat yang paling penting dan teknologi untuk menjaga informasi sumber daya?

Introduction

- **Facebook - jaringan sosial terbesar dunia**
- **Masalah - Pencurian identitas dan perangkat lunak berbahaya**
  - Kaspersky Labs Security menunjukkan malicious software di jejaring social seperti facebook 10 kali lebih berhasil menginfeksi pengguna dari pada penggunaan email
  - IT security firm Sophos melaporkan Facebook memiliki resiko keamanan terbasar dari Sosial Media yang lain
- **Menggambarkan:** Jenis serangan keamanan yang dihadapi konsumen

Kerentanan sistem dan penyalahgunaan

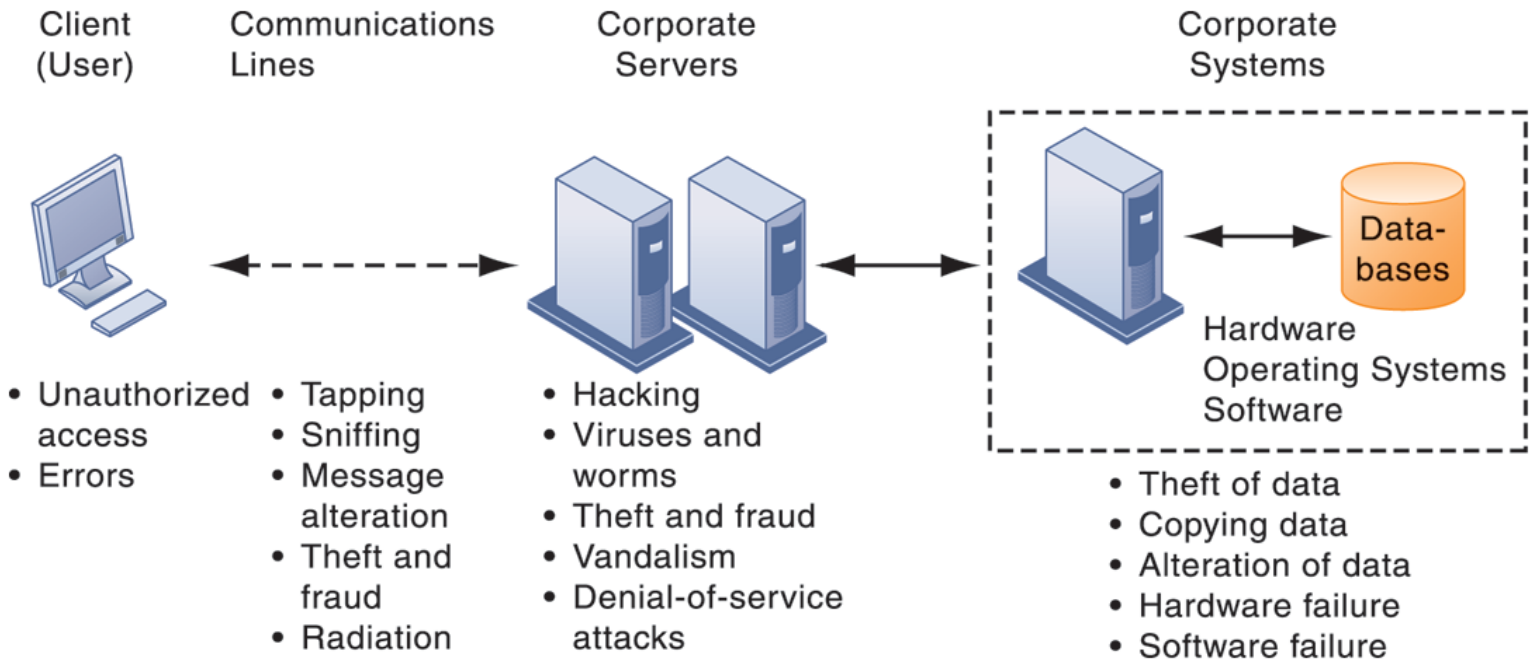
- **Keamanan (Security):**
  - ✓ Kebijakan, prosedur dan langkah-langkah teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan, pencurian, atau kerusakan fisik terhadap sistem informasi
- **Pengendalian (Control):**
  - ✓ Metode, kebijakan, dan prosedur organisasi yang menjamin keamanan aset organisasi; akurasi dan keandalan catatannya; dan kepatuhan terhadap standar operasional manajemen

Kerentanan sistem dan penyalahgunaan

- **Mengapa sistem rentan?**
  - Aksesibilitas jaringan
  - Masalah Hardware (kerusakan, kesalahan konfigurasi, kerusakan dari penyalahgunaan atau kejahatan)
  - Masalah software (kesalahan pemrograman, kesalahan instalasi, perubahan tidak sah)
  - Bencana
  - Penggunaan jaringan / komputer di luar kendali perusahaan
  - Kehilangan dan pencurian perangkat portabel

Kerentanan sistem dan penyalahgunaan

TANTANGAN KEAMANAN KONTEMPORER DAN KERENTANAN



Kerentanan sistem dan penyalahgunaan

- **Kerentanan Internet**
  - Jaringan terbuka bagi siapa saja
  - Internet begitu besar dan cepat, dampak terhadap penyalahgunaannya dapat tersebar luas
  - Penggunaan alamat Internet tetap dengan modem kabel atau DSL menciptakan target hacker tetap
  - E-mail, P2P, IM
    -Lampiran dengan perangkat lunak berbahaya
    -Mengirimkan rahasia dagang

Kerentanan sistem dan penyalahgunaan

- **Tantangan Keamanan Nirkabel**
  - Radio frequency bands easy to scan
  - SSIDs (service set identifiers)
    - Identify access points
    - Broadcast multiple times
    - **War driving**
      - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
  - WEP (Wired Equivalent Privacy)
    - Security standard for 802.11; use is optional
    - Uses shared password for both users and access point
    - Users often fail to implement WEP or stronger systems

Management Information Systems

Systems Vulnerability and Abuse

TANTANG KEAMANAN WI-FI

Banyak jaringan Wi-Fi dapat ditembus dengan mudah oleh penyusup menggunakan program sniffer untuk mendapatkan alamat untuk mengakses sumber daya jaringan tanpa otorisasi.

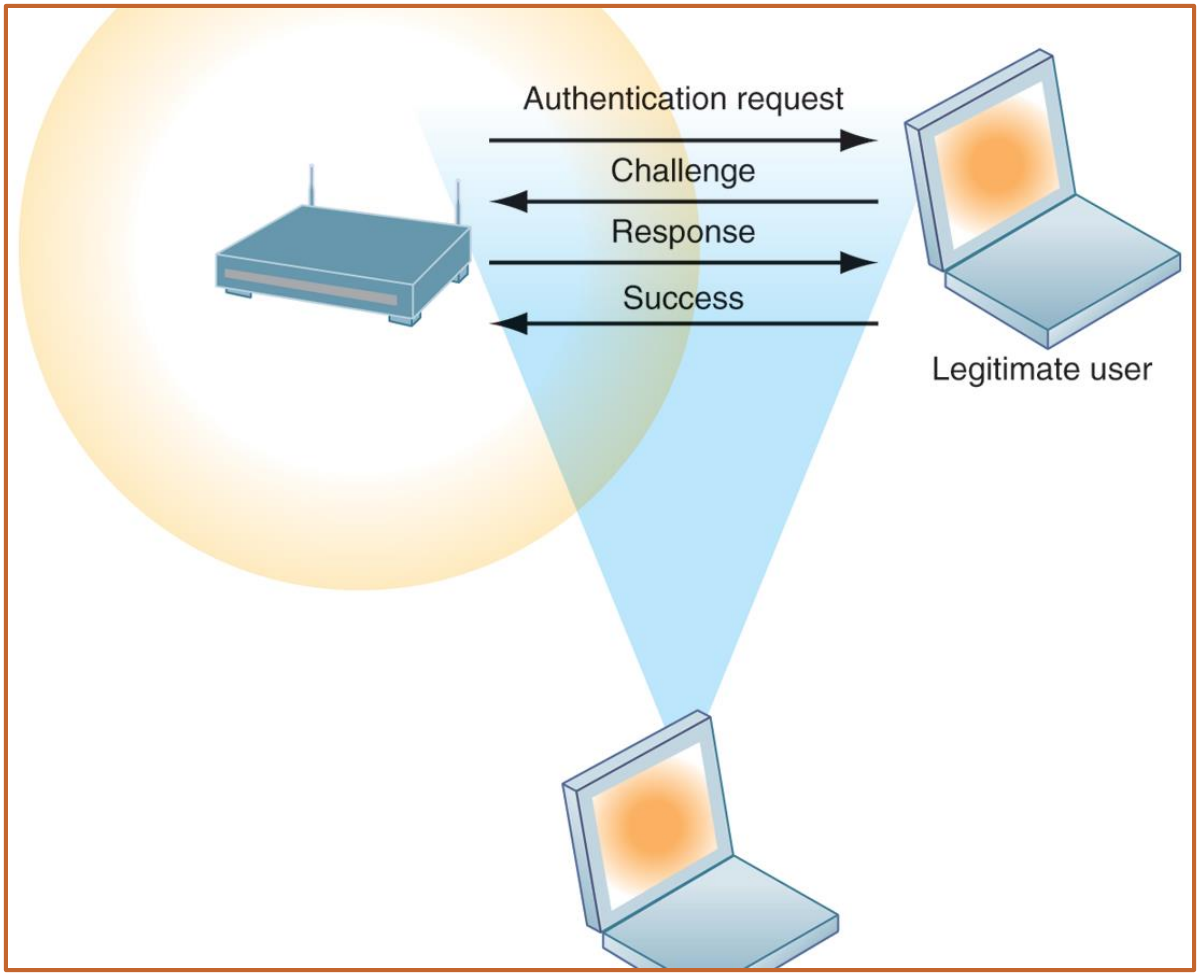


FIGURE 8-2

Management Information Systems

Perangkat Lunak Berbahaya

- **Malware (malicious software)**
  - **Viruses**
    - Program perangkat lunak berbahaya yang menempel pada program perangkat lunak lain atau file data untuk dieksekusi
  - **Worms**
    - Program komputer independen yang menyalin diri dari satu komputer ke komputer lain melalui jaringan.
  - **Trojan horses**
    - Program perangkat lunak yang tampaknya jinak tapi kemudian melakukan sesuatu yang lain dari yang diharapkan.

Management Information Systems

Perangkat Lunak Berbahaya

- **Malware (cont.)**
  - **Spyware**
    - Program kecil menginstal sendiri diam-diam pada komputer untuk memantau kegiatan penelusuran web oleh pengguna dan untuk memunculkan iklan
  - **Key loggers**
    - Mencatat setiap tombol yang diketikkan pengguna pada keyboard untuk melakukan pencurian terhadap kata sandi, no seri software, akses rekening, kartu kredit, dll

Management Information Systems

Hacker dan Kejahatan Komputer

- **Hackers vs crackers**
  - Hacker adalah seorang yg ingin mendapatkan akses tidak sah ke sebuah sistem komputer
  - Cracker istilah khusus yg digunakan untuk menunjukkan seorang hacker yg memiliki maksud kriminal
- **Activities include**
  - System intrusion, System damage,Cyber vandalism:
  - Gangguan, perusakan atau bahkan penghancuran situs atau sistem informasi perusahaan secara disengaja

Management Information Systems

Hacker dan Kejahatan Komputer

- **Spoofing**
  - Menggunakan alamat e-mail palsu atau menyamar sebagai orang lain
  - Pengalihan jalur sebuah situs ke sebuah alamat yg berbeda dari yang diinginkan dengan situs yang disamarkan
- **Sniffer**
  - Program pencuri informasi yang memantau informasi dalam sebuah jaringan
  - Memungkinkan hacker untuk mencuri informasi rahasia seperti e-mail, file perusahaan, dll

Management Information Systems

Hacker dan Kejahatan Komputer

- **Denial-of-service attacks (DoS)**
  - Suatu aktivitas untuk membanjiri server dengan ribuan permintaan palsu
  - Menyebabkan suatu layanan situs mati
- **Distributed denial-of-service attacks (DDoS)**
  - Penggunaan banyak komputer untuk meluncurkan serangan DoS
  - **Botnets**
    - Menggunakan ribuan PC yang terinfeksi oleh piranti lunak berbahaya

Management Information Systems

Hacker dan Kejahatan Komputer

- **Kejahatan Komputer**
  - **Pelanggaran hukum pidana yang melibatkan pengetahuan teknologi komputer**
  - **Komputer dapat menjadi sasaran kejahatan, misalnya:**
    - Melanggar kerahasiaan data terkomputerisasi yang dilindungi
    - Mengakses sistem komputer tanpa otoritas
  - **Komputer sebagai alat kejahatan, misalnya:**
    - Menggunakan e-mail untuk ancaman atau pelecehan

Management Information Systems

Hacker dan Kejahatan Komputer

- **Pencurian Identitas**
  - Pencurian Informasi pribadi (id jaminan sosial, lisensi atau nomor kartu kredit pengemudi) untuk meniru orang lain
- **Phishing**
  - Menyiapkan situs Web palsu atau mengirim pesan e-mail yang terlihat seperti bisnis yang sah untuk meminta pengguna untuk data pribadi rahasia.
- **Evil twins**
  - Jaringan nirkabel yang berpura-pura menawarkan dipercaya Wi-Fi koneksi ke Internet

Management Information Systems

Hacker dan Kejahatan Komputer

- **Pharming**
  - Pengalihan pengguna ke halaman Web palsu, bahkan ketika jenis individu yang benar alamat halaman Web ke browser-nya
- **ClickFroud**
  - Link yang muncul pada mesin pencarian yang berbentuk iklan yang ketika diklik tidak mengarah ke produk yg sebenarnya

Management Information Systems

Hacker dan Kejahatan Komputer

- **Global Threats: Cyberterrorism and Cyberwarfare**
  - Kerentanan internet atau jaringan lainnya membuat jaringan digital menjadi sasaran empuk bagi serangan digital oleh teroris, badan intelijen asing, atau kelompok lain
  - Cyberattacks menargetkan perangkat lunak yang berjalan pada layanan listrik, sistem kontrol lalu lintas udara, atau jaringan bank-bank besar dan lembaga keuangan.
  - Setidaknya 20 negara, termasuk China, diyakini mengembangkan kemampuan cyberwarfare ofensif dan defensif.

Management Information Systems

Hacker dan Kejahatan Komputer

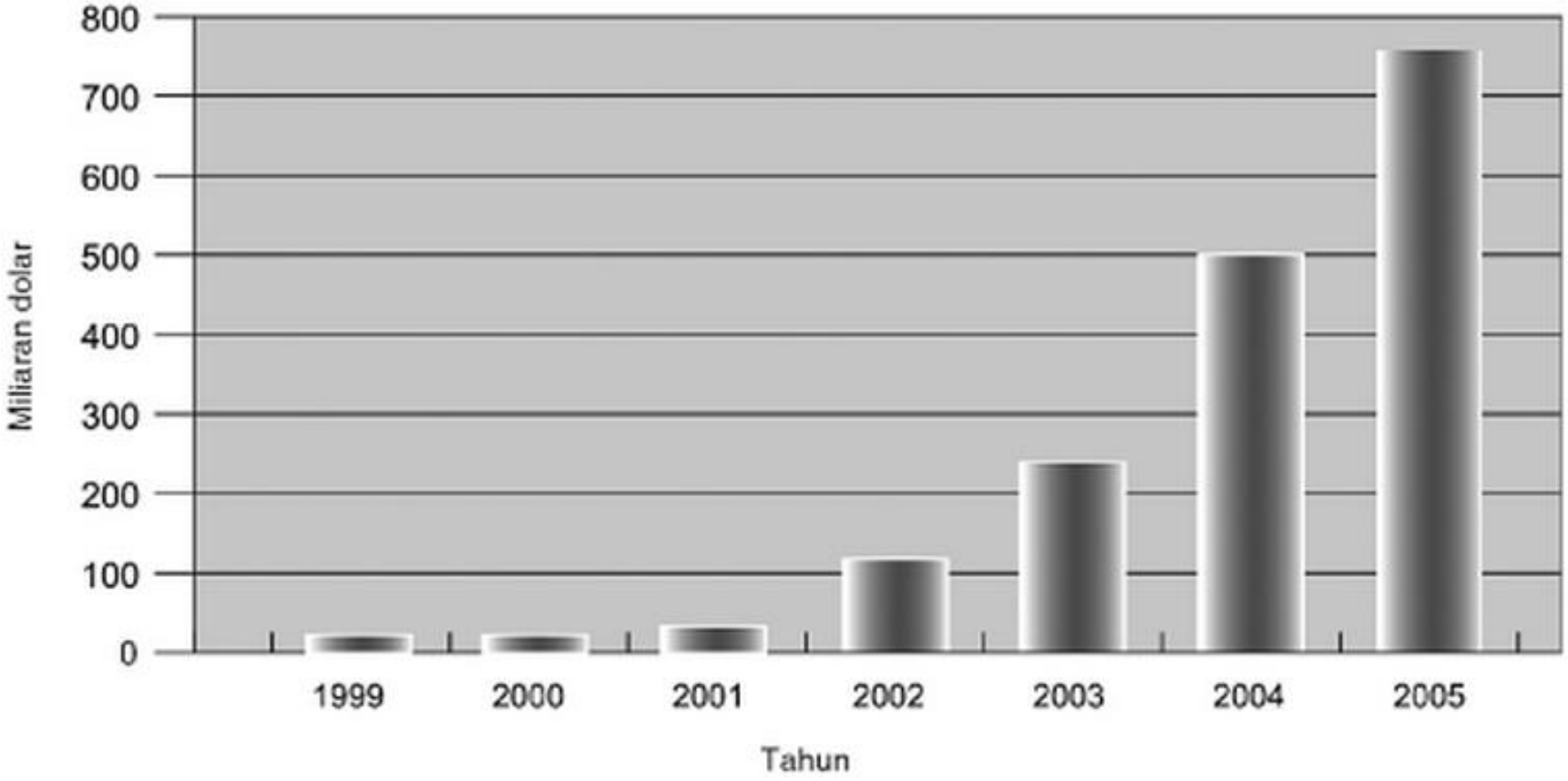


Diagram ini menunjukkan kerugian rata-rata per tahun di seluruh dunia yang disebabkan oleh *hacking*, *malware*, dan *spam*, sejak tahun 1999. Data ini didasarkan ada angka-angka dari mi2G dan penulis.

Management Information Systems

Internal Threats: Employe

- **Ancaman internal: karyawan**
  - **Ancaman keamanan sering berasal di dalam sebuah organisasi**
  - **Prosedur Keamanan Ceroboh**
    - Pengguna kurangnya pengetahuan
  - **Social engineering:**
    - Menipu karyawan untuk mengungkapkan password mereka dengan berpura-pura menjadi anggota yang sah dari perusahaan yang membutuhkan informasi

Management Information Systems

System Vulnerability

- **Kelemahan Software**
  - **Perangkat lunak komersial mengandung kelemahan yang menciptakan kerentanan keamanan**
    - Bug tersembunyi(cacat kode program)
    - Cacat dapat membuka jaringan untuk penyusup
  - **Patches**
    - Vendor melepaskan potongan-potongan kecil dari perangkat lunak untuk memperbaiki kelemahan

Management Information Systems

Nilai Bisnis Keamanan dan Kontrol

- Perusahaan sekarang lebih rentan daripada sebelumnya
  - Data pribadi dan rahasia keuangan
  - Rahasia dagang, produk baru, strategi
- Sistem komputer gagal dapat menyebabkan kerugian yang signifikan atau total dari fungsi bisnis
- Sebuah pelanggaran keamanan dapat menurunkan nilai pasar perusahaan dengan cepat
- Keamanan dan kontrol yang tidak memadai juga mendatangkan masalah

Management Information Systems

Nilai Bisnis Keamanan dan Kontrol

- **Persyaratan hukum dan peraturan untuk manajemen catatan elektronik dan perlindungan privasi**
  - **HIPAA:** peraturan dan prosedur keamanan medis dan privasi
  - **Gramm-Leach-Bliley Act:** Membutuhkan lembaga keuangan untuk menjamin keamanan dan kerahasiaan data pelanggan
  - **Sarbanes-Oxley Act:** Memberlakukan tanggung jawab pada perusahaan dan manajemennya untuk menjaga akurasi dan integritas informasi keuangan yang digunakan secara internal dan eksternal dirilis

Management Information Systems
Nilai Bisnis Keamanan dan Kontrol

- **Bukti Electronic**
  - **Bukti dalam bentuk digital**
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - Kontrol yang tepat dari data yang dapat menghemat waktu dan uang ketika menanggapi penemuan permintaan hukum
- **Computer forensics:**
  - Koleksi ilmiah, pemeriksaan, otentikasi, pelestarian, dan analisis data dari media penyimpanan komputer untuk digunakan sebagai bukti di pengadilan hukum

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Kontrol sistem informasi**
  - Kontrol manual dan otomatis
  - Pengendalian umum (*general controls*) dan aplikasi
- **Pengendalian Umum:**
  - Mengatur desain, keamanan, dan penggunaan program komputer dan keamanan file data secara umum di seluruh infrastruktur teknologi informasi organisasi.
  - Terapkan untuk semua aplikasi komputerisasi
  - Kombinasi hardware, software, dan prosedur manual untuk menciptakan lingkungan pengendalian secara keseluruhan

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Jenis Pengendalian Umum:**
  - Kontrol perangkat lunak
  - Kontrol hardware
  - Kontrol operasi komputer
  - Kontrol keamanan data
  - Kontrol implementasi
  - Kontrol administratif

- **Pengendalian Aplikasi**
  - Kontrol tertentu yang unik untuk setiap aplikasi komputerisasi, seperti gaji atau pemrosesan order
  - Memastikan bahwa hanya data berwenang yang benar-benar akurat dan diproses oleh aplikasi
  - **Memasukan:**
    - Input controls
    - Processing controls
    - Output controls

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Penilaian risiko: Menentukan tingkat risiko untuk perusahaan jika aktivitas atau proses tertentu yang tidak dikontrol dengan baik**
  - Jenis ancaman
  - Kemungkinan terjadinya selama kurun waktu
  - Potensi kerugian, nilai ancaman
  - Kerugian tahunan diperkirakan

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Penilaian risiko:** Menentukan tingkat risiko untuk perusahaan jika aktivitas atau proses tertentu yang tidak dikontrol dengan baik

TABLE 8-4 ONLINE ORDER PROCESSING RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000–$50,000 ($25,500)	$1,275
User error	98%	$200–$40,000 ($20,100)	$19,698

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Kebijakan Keamanan**
  - Peringkat risiko informasi, mengidentifikasi tujuan keamanan yang dapat diterima dan mengidentifikasi mekanisme untuk mencapai tujuan-tujuan tertentu
  - **Mengatur Kebijakan Lain**
    - Mengatur Kebijakan Penggunaan (*Acceptable use policy* -AUP)
      - Mendefinisikan penggunaan diterima sumber daya perusahaan informasi dan peralatan komputasi
    - *Authorization policies*
      - Tentukan tingkat yang berbeda dari akses pengguna ke aset informasi

Management Information Systems

Membangun Kerangka Keamanan dan Kontrol

- **Manajemen identitas**
  - **Proses bisnis dan *tools* untuk mengidentifikasi pengguna yang valid dari sistem dan mengontrol akses**
    - Mengidentifikasi dan kewenangan berbagai kategori pengguna
    - Menentukan bagian mana dari pengguna sistem dapat mengakses
    - Otentikasi pengguna dan melindungi identitas
  - **Sistem Manajemen Identitas**
    - Menangkap aturan akses untuk berbagai tingkat pengguna

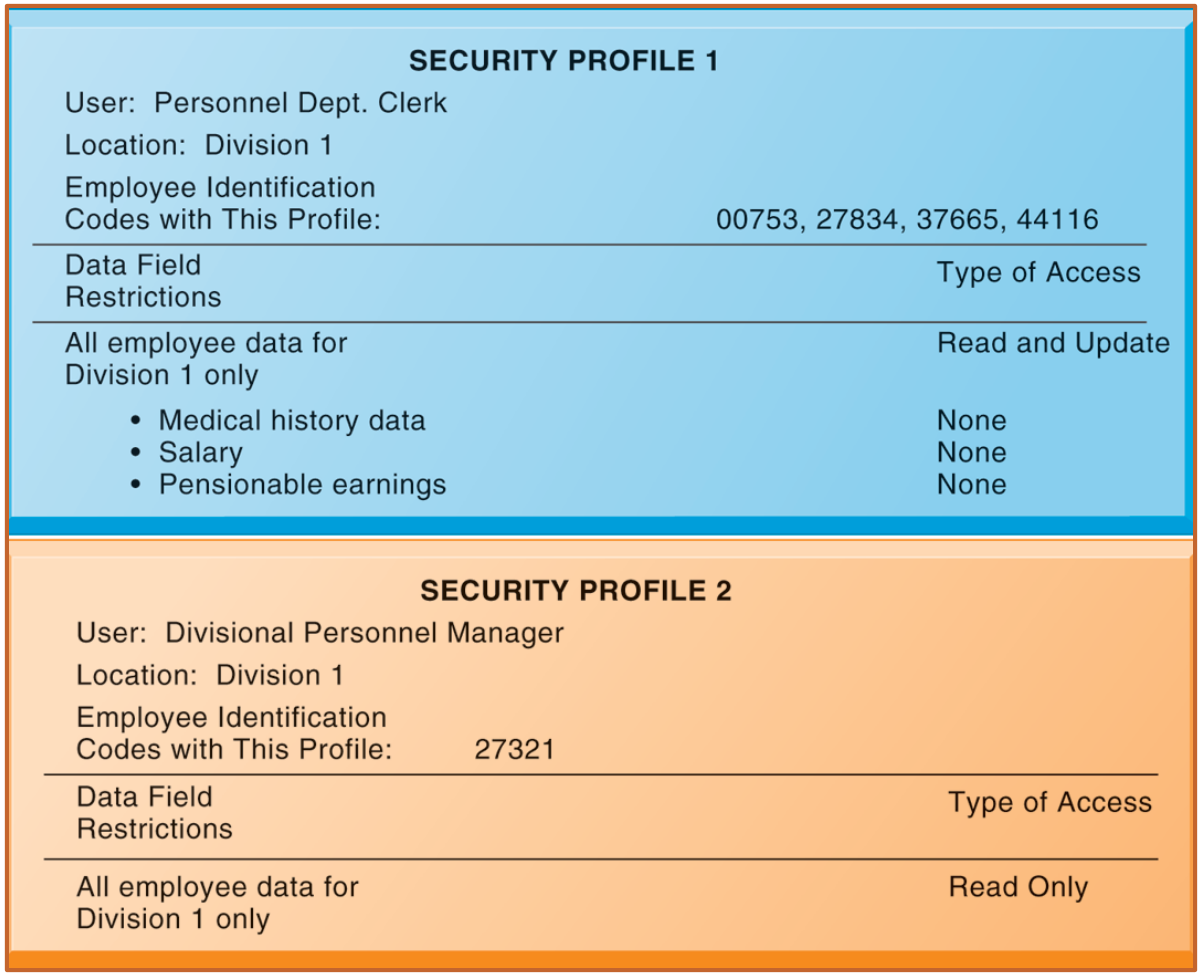
Management Information Systems

ACCESS RULES FOR A PERSONEL SYSTEM

PROFIL KEAMANAN UNTUK SISTEM PERSONIL

Kedua contoh mewakili dua profil keamanan atau pola keamanan data yang mungkin ditemukan dalam sistem personil. Tergantung pada profil keamanan, pengguna akan memiliki batasan-batasan tertentu pada akses ke berbagai sistem, lokasi, atau data dalam sebuah organisasi.

FIGURE 8-3



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

Management Information Systems

Audit Sistem Informasi Management

- **MIS audit**
  - Memeriksa lingkungan keamanan secara keseluruhan perusahaan serta kontrol yang mengatur sistem informasi individu
  - Ulasan teknologi, prosedur, dokumentasi, pelatihan, dan personil.
  - Daftar dan peringkat semua kelemahan pengendalian
  - Menilai dampak keuangan dan organisasi pada masing-masing ancaman

Management Information Systems

Audit Sistem Informasi Management

SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

FIGURE 8-4

GAMBAR 8-5 CONTOH DAFTAR KELEMAHAN PENGENDALIAN YANG DIBUAT AUDITOR

Fungsi: Pinjaman **Lokasi: Peoria, IL**	**Dipersiapkan oleh: J. Ericson** **Tanggal: 16 Juni 2007**		**Diterima oleh: T. Benson** **Tanggal: 28 Juni 2007**	
Sifat Kelemahan dan Dampaknya	Peluang Kesalahan/Penyalahgunaan		Pemberitahuan Kepada Manajemen	
	Yes/No	Alasan	Tanggal laporan	Respons Manajemen
Akun pengguna dengan kata sandi yang hilang	Yes	Meninggalkan sistem dalam keadaan terbuka bagi pihak luar yang tidak memiliki izin dan para penyerang	5/10/07	Menghapus akun yang tidak memiliki kata sandi
Jaringan dikonfigurasikan untuk mengizinkan beberapa kasus pembagian *file* sistem	Yes	Mengekspos *file* sistem yang penting kepada pihak-pihak berbahaya yang terhubung ke jaringan	5/10/07	Menjamin hanya direktori-direktori yang dibutuhkan saja yang dibagikan dan dilindungi oleh kata sandi yang kuat
Patch peranti lunak dapat memperbarui program produksinya tanpa persetujuan akhir dari kelompok Standar dan Kontrol	No	Semua program produksi membutuhkan persetujuan pihak manajemen; kelompok Standar dan Kontrol mengelompokkan kasus seperti ini pada status produksi sementara		

Management Information Systems

Audit Sistem Informasi Management

Seorang auditor sering kali menelusuri aliran transaksi sampel pada suatu sistem informasi dan akan melakukan beberapa pengujian menggunakan peranti lunak audit otomatis. Audit SIM membantu pihak manajemen mengidentifikasi kerentanan-kerentanan dalam keamanan dan menentukan apakah pengendalian sistem informasinya sudah efektif.

Technologies and Tools for Protecting Information Resources

Management Information Systems

Identity Management And Authentication

- **Identity management software**
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- **Authentication**
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication

Management Information Systems

Identity Management And Authentication

This PC has a biometric fingerprint reader for fast yet secure access to files and networks. New models of PCs are starting to use biometric identification to authenticate users.

Management Information Systems

Identity Management And Authentication

Identifikasi biometrik menggunakan teknologi yang dapat membaca dan memahami ciri-ciri khas manusia, seperti sidik jari, suara, atau wajah, untuk memberikan atau melarang akses ke suatu sistem.

Management Information Systems

Firewall, Intrusion Detection System and Antivirus Software

A. Firewall:

- Bertindak seperti penjaga gawang yg memeriksa setiap pengguna sebelum memberikan akses ke jaringan
- Mencegah pengguna yang tidak sah mengakses jaringan pribadi
- Teknologi firewall: *static packet filtering, stateful inspection, network address translation (NAT)*

Management Information Systems

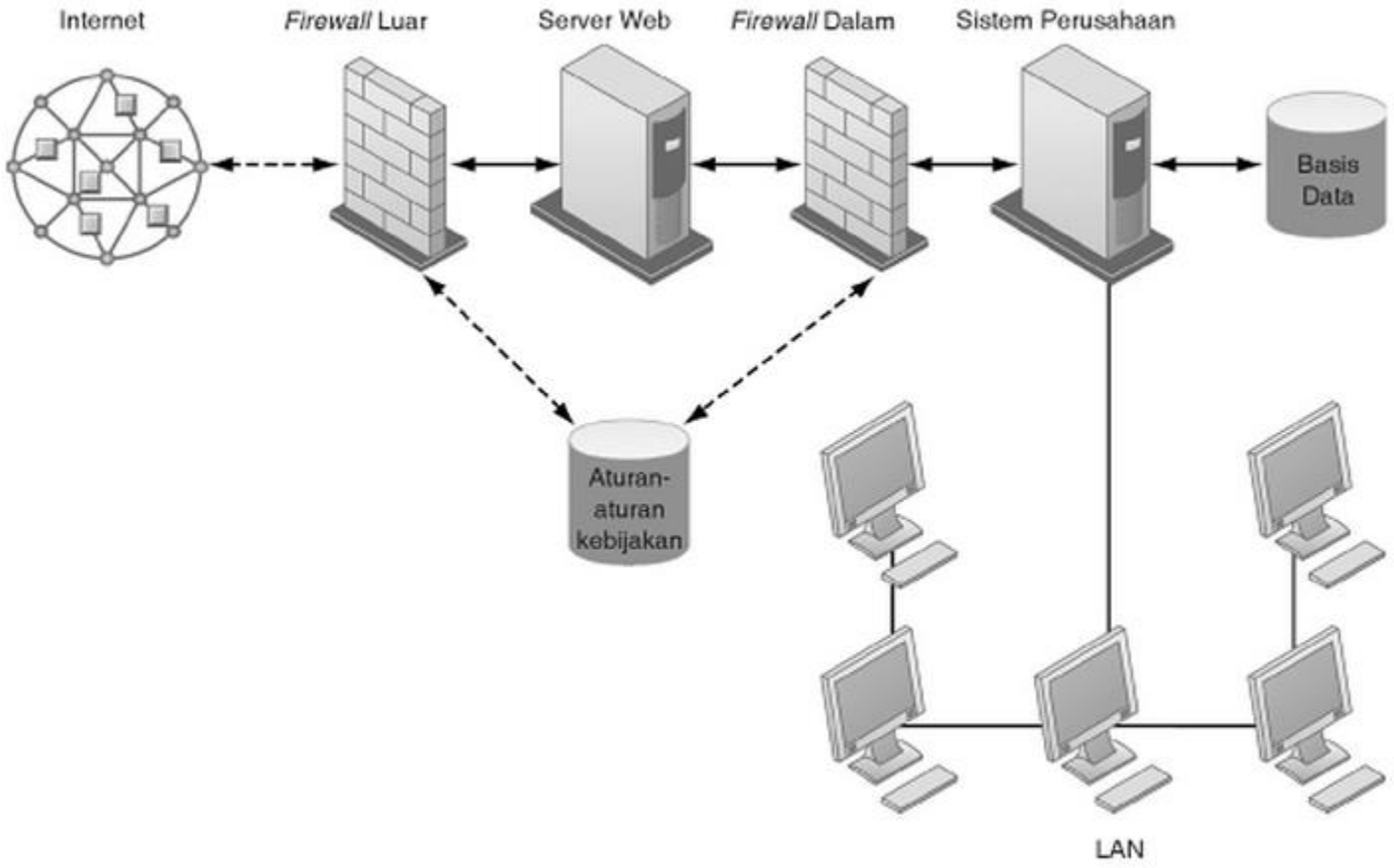
Firewall, Intrusion Detection System and Antivirus Software

- ***static packet filtering***
  - Memeriksa field terpilih di header dari paket data yg mengalir masuk dan keluar antara jaringan yg dipercaya dan internet dan memeriksa setiap paket secara terpisah
- ***stateful inspection,***
  - Menyediakan pengamanan tambahan dengan cara menentukan apakah suatu paket merupakan bagian dari dialog yg terus menerus antara pengirim & penerima

- ***network address translation (NAT)***
  - NAT menyembunyikan alamay IP komputer host internal perusahan untuk mencegah program *sniffer* di luar *firewall* mengenali dan menembus sistem

Management Information Systems

Firewall, Intrusion Detection System and Antivirus Software



Firewall diletakkan di antara jaringan perusahaan dan Internet atau jaringan yang tidak dipercaya lainya untuk melindungi jaringan perusahaan dari lalu lintas data yang tidak terotorisasi.

B. Sistem Pendeteksi Gangguan (*Intrusion detection systems*)

- Memantau hot spot di jaringan perusahaan untuk mendeteksi dan mencegah penyusup
- Memeriksa *event* yang sedang terjadi untuk menemukan serangan yg sedang berlangsung

C. Antivirus and antispyware software:

- Memeriksa komputer terhadap adanya malware dan sering kali dapat menghilangkan malware tsb
- Memerlukan *update* / pembaharuan secara terus-menerus

Unified Threat Management (UTM) Systems

- Untuk membantu bisnis mengurangi biaya dan meningkatkan pengelolaan, vendor keamanan telah menggabungkan berbagai alat keamanan ke dalam alat tunggal termasuk *firewalls, virtual private networks, intrusion detection systems, and Web content filtering* dan *anti spam software*
- *These comprehensive security management products are called unified threat management (UTM) systems*

Management Information Systems

Securing wireless networks

- **WEP security**
  - Shared Key atau WEP (Wired Equivalent Privacy) disebut juga dengan Shared Key Authentication merupakan metode otentikasi yang membutuhkan penggunaan WEP
  - Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point
  - Menggunakan kunci enkripsi statis

Management Information Systems

Securing wireless networks

- **WAP2**
  - Menggunakan kunci lebih panjang yang terus-menerus berubah (*continually changing keys*)
  - Sistem otentikasi terenkripsi dengan server otentikasi pusat untuk memastikan bahwa hanya pengguna berwenang yg dapat mengakses jaringan
  - Wi-Fi Alliance menyelesaikan spesifikasi 802.11i yang disebut sebagai Wi-Fi Protected Access 2 atau WPA2 yang menggantikan WEP dengan standar keamanan yang lebih kuat.

Management Information Systems
Encryption and Publik Key Infrastructure

- **Enkripsi / Encryption**
  - Enkripsi merupakan proses mengubah teks atau data biasa menjadi teks bersandi (*chippertext*) yang tidak dapat dibaca oleh siapa pun selain pengirim dan penerima yg dimaksud
  - Data dienkripsi menggunakan kode numerik rahasia yg dinamakan kunci enkripsi yg mengubah data biasa mjd teks bersandi, pesan harus dideskripsi oleh penerima

Management Information Systems
Encryption and Publik Key Infrastructure

- **Dua metode enkripsi pada lalu lintas di Web**
  - **SSL / Secure Sockets Layer**
    - Dirancang untuk membuat sambungan aman antara dua komputer.
    - Kegiatan saat mereka berkomunikasi satu sama lain selama sesi Web aman.
  - **S-HTTP**
    - Protokol lain yang digunakan untuk mengenkripsi data yang mengalir melalui Internet, tetapi terbatas pada individu pesan

Management Information Systems
Encryption and Publik Key Infrastructure

- **Ada dua metode alternatif enkripsi**
  - **Symmetric Key Encryption**
    - Pengirim dan penerima membuat sesi internet yang aman dengan menciptakan kunci enkripsi tunggal
    - Pengirim dan Penerima berbagi kunci yang sama
  - **Public Key Encryption**
    - Menggunakan dua kunci: satu untuk bersama (umum /public) dan satu benar-benar pribadi (private)

Management Information Systems
Encryption and Publik Key Infrastructure

PUBLIC KEY ENCRYPTION

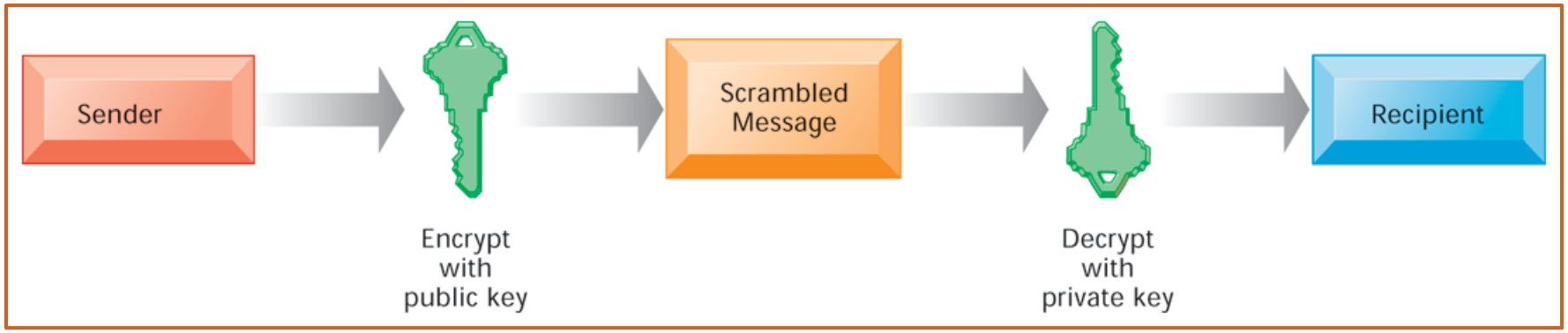


FIGURE 8-6

Sebuah sistem enkripsi kunci publik dapat dilihat sebagai rangkaian kunci publik dan private yang mengunci data bila mereka ditransmisikan dan membuka data ketika mereka diterima. Pengirim menempatkan kunci publik penerima dalam sebuah direktori dan menggunakannya untuk mengenkripsi pesan. Pesan dikirim dalam bentuk terenkripsi melalui Internet atau jaringan pribadi. Ketika pesan terenkripsi tiba, penerima menggunakan kunci pribadinya untuk mendekripsi data dan membaca pesan

Management Information Systems
Encryption and Publik Key Infrastructure

Penjelasan Gambar Public Key Encryption

- Sebuah sistem enkripsi kunci publik dapat dilihat sebagai rangkaian kunci publik dan private yang mengunci data bila mereka ditransmisikan dan membuka data ketika mereka diterima. Pengirim menempatkan kunci publik penerima dalam sebuah direktori dan menggunakannya untuk mengenkripsi pesan. Pesan dikirim dalam bentuk terenkripsi melalui Internet atau jaringan pribadi. Ketika pesan terenkripsi tiba, penerima menggunakan kunci pribadinya untuk mendekripsi data dan membaca pesan

Management Information Systems
Encryption and Publik Key Infrastructure

- **Digital certificate:**
  - File data yang digunakan untuk menentukan identitas pengguna dan aset elektronik untuk perlindungan transaksi online
  - Menggunakan pihak ketiga yang terpercaya, otoritas sertifikasi (CA), untuk memvalidasi identitas pengguna
  - CA memverifikasi identitas pengguna, menyimpan informasi di server CA, yang menghasilkan sertifikat digital terenkripsi yang berisi informasi pemilik ID dan salinan kunci publik pemilik

Management Information Systems
Encryption and Publik Key Infrastructure

- **Public key infrastructure (PKI)**
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

Management Information Systems

Technologies and Tools for Protecting Information Resources

DIGITAL CERTIFICATES

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

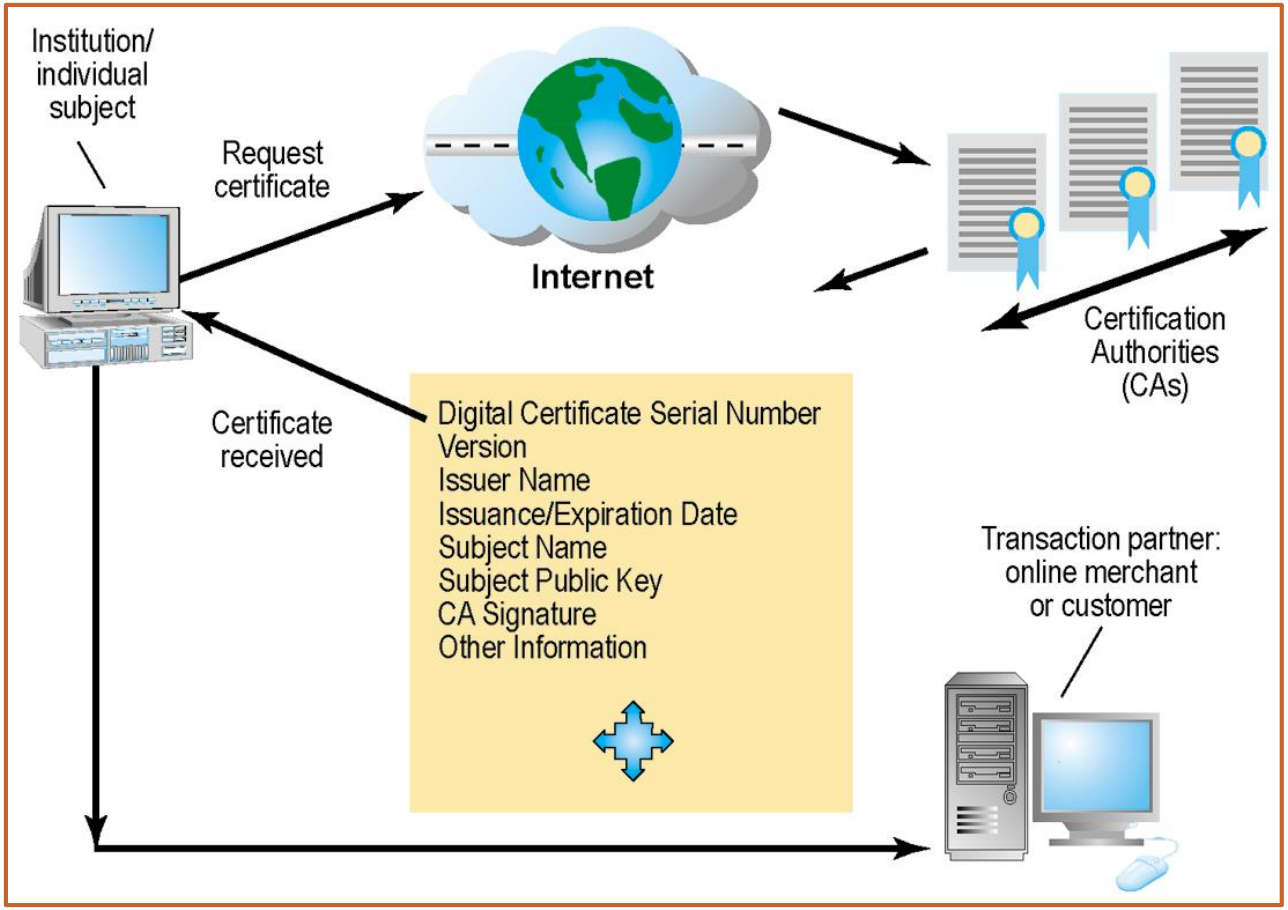


FIGURE 8-7

Management Information Systems

Technologies and Tools for Protecting Information Resources

- **Ensuring system availability**
  - Online transaction processing requires 100% availability, no downtime
- **Fault-tolerant computer systems**
  - For continuous availability, e.g. stock markets
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- **High-availability computing**
  - Helps recover quickly from crash
  - Minimizes, does not eliminate downtime

Management Information Systems

Technologies and Tools for Protecting Information Resources

- **Recovery-oriented computing**
  - Designing systems that recover quickly with capabilities to help operators pinpoint and correct of faults in multi-component systems
- **Controlling network traffic**
  - **Deep packet inspection (DPI)**
    - Video and music blocking
- **Security outsourcing**
  - **Managed security service providers (MSSPs)**

Management Information Systems

Technologies and Tools for Protecting Information Resources

- **Security in the cloud**
  - Responsibility for security resides with company owning the data
  - Firms must ensure providers provides adequate protection
  - Service level agreements (SLAs)
- **Securing mobile platforms**
  - Security policies should include and cover any special requirements for mobile devices
    - E.g. updating smart phones with latest security patches, etc.

Management Information Systems

Technologies and Tools for Protecting Information Resources

- **Ensuring software quality**
  - **Software metrics: Objective assessments of system in form of quantified measurements**
    - Number of transactions
    - Online response time
    - Payroll checks printed per hour
    - Known bugs per hundred lines of code
  - **Early and regular testing**
  - **Walkthrough: Review of specification or design document by small group of qualified people**
  - **Debugging: Process by which errors are eliminated**

Terima kasih