PENGANTAR

KULIAH KRIPTOGRAFI DAN KEAMANAN JARINGAN

OUTLINE

- **Pengenalan**
- **Sejarah**
- **Motivasi: contoh-contoh pelanggaran keamanan jaringan**
- **Konsep keamanan komputer**
- **Arsitektur keamanan OSI**

APAKAH KRIPTOGRAFI?

- **Dari kata-kata Yunani:**
  - κ ρ υ π τ ός: tersembunyi, rahasia.
  - Γ ρ ά φ ε ι ν (graphein): tulisan; or λ ο γ ί α (logia): studi.
- **Kriptografi: penerapan dan studi terhadap teknik-teknik untuk keamanan komunikasi dari pihak ketiga.**
- **Berhubungan dengan kriptoanalisis dan kriptologi:**
  - Kriptografi mengacu pada ilmu dan seni untuk mendisain penyandian.
  - Kriptoanalisis mengacu pada ilmu dan seni untuk memecahkan penyandian.
  - Kriptologi: studi tentang keduanya.
- **Kapan kriptografi diperlukan? → komunikasi dengan medium yang tidak aman.**

- **Kriptografi dapat digunakan untuk:**
  - Autentikasi: membuktikan identitas suatu pihak.
  - Confidentiality (kerahasiaan): hanya penerima yang dituju (intended receiver) yang membaca pesan.
  - Integritas: tidak ada modifikasi pesan.
  - Non-repudiation: untuk membuktikan bahwa pengirim (sender) pesan benar-benar mengirim pesan.

ALGORITMA KRIPTOGRAFI

- **Kriptografi pada umumnya mengacu pada enkripsi (*encryption)*.**
- **Enkripsi: proses mengkonversi informasi biasa menjadi teks yang tidak dapat dimengerti (terbaca).**
  - Plaintext: data tak terenkripsi (asli)
  - Ciphertext: data terenkripsi
  - Enkripsi dilakukan oleh pengirim
- **Dekripsi: mengubah kembali unintelligible ciphertext menjadi plaintext.**
  - Dekripsi dilakukan oleh receiver
- **Cipher (penyandian): sepasang algoritma untuk melakukan enkripsi dan pasangan dekripsinya.**
- **Tiga macam algoritma kriptografi:**
  - Secret key cryptography (SKC) (kriptografi simetris)
  - Public key cryptography (PKC) (kriptografi asimetris)
  - Hash functions (one-way cryptography / kriptografi satu arah)

SEJARAH KRIPTOGRAFI

- **Kriptografi klasik:**
  - Non-standard hieroglyphs dipahat ke monumen pada masa Old Kingdom of Egypt sekitar 1900 BC.
  - Semacam tablet clay dari Mesopotamia: satu di antaranya tertanggal sekitar 1500 BCE untuk mengenkripsi resep pemahat untuk pembuatan tembikar.
  - Yunani Kuno: pesan rahasia yang menjadi tato pada kepala budak, tertutup rambutnya yang telah tumbuh. → steganografi.
  - (Julius) Caesar cipher: D untuk A, E untuk B dst.,
    - Diubah menjadi C untuk A, D untuk B, dst. oleh Augustus Caesar.

- **Kriptografi jaman menengah (Medieval):**
  - Al-Kindi: *Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*)
    - Teknik-teknik kriptoanalisis: polyalphabetic ciphers, cipher classification, Arabic phonetics and syntax, deskripsi pertama untuk frequency analysis
    - Metode-metode penyandian, kriptoanalisisnya, analisis statistik untuk huruf dan kombinasi huruf pada bahasa Arab.
  - Monoalphabetic substitution oleh orang-orang Arab: suatu keyword digunakan untuk melakukan permutasi terhadap cipher alphabet.

    abcdefghijklmnopqrstuvwxyz → plaintext

    SECURITYABDFGHJKLMNOPQVWXZ → ciphertext
  - Polyalphabetic cipher oleh Leon Battista Alberti (sekitar 1467) → "father of Western cryptology".
  - Johannes Trithemius, dalam tulisannya *Poligraphia*, menemukan tabula recta, merupakan komponen penting dalam the Vigenère cipher.
  - Kriptografer dari Prancis Blaise de Vigenere menemukan polyalphabetic system yang disebut dengan Vigenère cipher.
  - Babington plot pada saat pemerintahan Queen Elizabeth I yang menyebabkan dieksekusinya Mary, Queen of Scots.
  - Pesan terenkripsi pada zamannya Man in the Iron Mask (terdekripsi pada 1900 oleh Étienne Bazeries) mengungkap sedikit identitas dari tawanan tersebut.

- **Kriptografi dari 1800 sampai WW II**
  - Charles Babbage's Crimean War melakukan penelitian pada kriptoanalisis matematika dan polyalphabetic ciphers
  - Edgar Allan Poe menggunakan metode sistematis untuk memecahkan ciphers pada tahun1840an → menantang kriptografer untuk mengirimkan ciphers
  - Pada WW I Admiralty's Room 40 memecahkan sandi-sandi kelautan Jerman
  - Tahun 1917, Gilbert Vernam mengusulkan teleprinter cipher di mana kunci yang sudah disiapkan sebelumnya, disimpan pada paper tape, dikombinasikan karakter demi karakter dengan plaintext untuk menghasilkan ciphertext.
  - Pasukan Jerman membuat mesin rotor elektromekanikal yang disebut Enigma.
  - Kriptografer US Navy memecahkan beberapa sistem kripto AL Jepang. Salah satu di antaranya berujung pada kemenangan US pada Battle of Midway.
  - Mesin cipher Sekutu yang digunakan pada WWII : British TypeX dan American SIGABA → didesain dengan semangat mirip dengan Enigma.

- **Kriptografi modern**
  - Claude E. Shannon: A mathematical theory of cryptography (1945)
    - 2 tipe dasar sitem kerahasiaan: (1) melindungi dari hackers dan attackers yang memiliki resource tidak terbatas untuk men-decode pesan (unconditional security); (2) melindungi dari hackers dari attackers yang memiliki resource terbatas untuk men-decode pesan (computational security).
  - Draft of Data Encryption Standard (US Federal Register, 1975):
    - Untuk mengembangkan fasilitas komunikasi elektronik yang aman untuk bisnis seperti bank dan organisasi keuangan yang besar lainnya.
    - Advanced Encryption Standard (2001)
  - New Direction of Cryptography (Whitfield Diffie, Martin Hellman, 1976)
    - Algoritma kunci asimetris.
    - Pasangan kunci yang berhubungan secara matematika, satu sebagai kunci enkripsi, yang lain sebagai kunci dekripsi.

MOTOVASI: CONTOH-CONTOH PELANGGARAN KEAMANAN JARINGAN

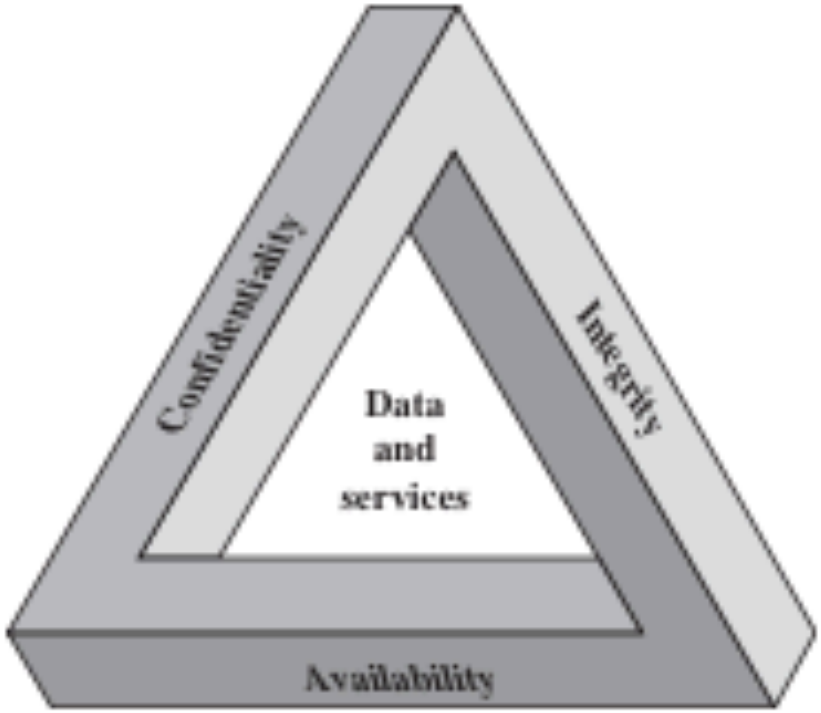
- **A mengirim berkas rahasia ke B. C berhasil memonitor transmisi dan mendapatkan salinan berkas, padahal dia tidak berhak membaca berkas.**
- **Network manager D mengirim perintah ke komputer E. Isi perintah untuk mengupdate file autorisasi sehingga beberapa user baru diberi hak akses. User F mengintersep pesan, mengubah isi data dan meneruskannya ke komputer E. E menerima pesan tersebut sebagai pesan dari D.**
- **User G membuat pesan dan meneruskan pesan ke komputer H sedemikian hingga seolah-olah pesan tersebut dari pihak yang mempunyai hak akses. Komputer H melakukan perubahan sesuai dengan isi pesan dari G.**

KONSEP KEAMANAN KOMPUTER

- **Computer security: nama generik untuk sekumpulan tool yang dirancang untuk melindungi data dan melawan hacker.**
- **Definisi (National Standard of Institute and Technology):**
  - 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).
- **Tiga kata kunci:**
  - Integrity
  - Availability
  - Confidentiality
- **CIA triad → tujuan keamanan paling dasar untuk data dan services.**

CIA TRIAD

- **Merupakan tujuan keamanan paling dasar untuk data dan services.**



CONFIDENTIALITY / KERAHASIAAN

- **Meliputi 2 hal:**
  - Data: informasi pribadi atau rahasia tidak dibocorkan kepada pihak-pihak yang tidak berhak mengetahuinya.
  - Privasi: individu berhak mengontrol informasi yang mana yang berhubungan dengan mereka yang boleh diambil atau disimpan oleh pihak-pihak tertentu dan kepada siapa informasi tersebut boleh dibuka.
- **Standar no. 199 FIPS (Federal Information Processing Standard):**
  - Tujuan: menjaga pembatasan akses dan pembukaan informasi, termasuk penjagaan privasi individu.
  - Kerahasiaan hilang berarti terjadi pembukaan informasi oleh pihak yang tidak mempunyai hak.

INTEGRITY / INTEGRITAS

- **Meliputi 2 hal:**
  - Data: informasi dan program hanya dipertukarkan dengan cara yang sudah ditentukan.
  - Sistem: sistem berlaku sesuai fungsinya, tidak ada manipulasi yang tidak diperbolehkan.
- **Standar no. 199 FIPS (Federal Information Processing Standard):**
  - Tujuan: melindungi dari modifikasi/perusakan informasi yang tidak diijinkan, termasuk memastikan validitas informasi.
  - Integritas hilang berarti terjadi modifikasi yang tidak diijinkan atau perusakan terhadap informasi.

AVAILABILITY / KETERSEDIAAN

- **Memastikan bahwa sistem bekerja dengan baik dan service tidak ditolak untuk user yang mendapatkan hak akses.**
- **Standar no. 199 FIPS (Federal Information Processing Standard):**
  - Tujuan: memastikan akses dan penggunaan informasi yang cepat dan reliable.
  - Ketersediaan hilang jika terjadi gangguan terhadap akses atau penggunaan informasi atau sistem informasi.

KONSEP-KONSEP LAIN

- **Autentikasi:**
  - Keaslian dapat diverifikasi dan dipercaya.
  - Keyakinan terhadap validitas dari transmisi, pesan, dan asal pesan.
  - Verifikasi bahwa user adalah benar-benar sesuai dengan apa yang diakuinya dan semua input berasal dari sumber yang terpercaya.
- **Akuntabilitas:**
  - Actions dapat dilacak secara unik.
  - Mendukung: deteksi dan pencegahan terhadap gangguan, after-action recovery, tindakan hukum.
  - Sistem harus menyimpan catatan aktivitasnya → analisis forensik, transaction disputes.

3 LEVEL DAMPAK TERJADINYA GANGGUAN KEAMANAN (FIPS 199)

- **Rendah:**
  - Berdampak terbatas terhadap operasional dan aset organisasi atau individual.
  - Contoh:
    - Organisasi tetap dapat menyediakan fungsi pokoknya, tetapi efektivitas terganggu.
    - Menyebabkan gangguan minor terhadap aset perusahaan.
    - Menyebabkan kerugian finansial kecil.
    - Menyebabkan gangguan kecil terhadap individu.

- **Moderat:**
  - Berdampak serius terhadap operasional dan aset organisasi atau individual.
  - Contoh:
    - Organisasi dapat menyediakan fungsi pokoknya, tetapi efektivitas sangat jauh menurun.
    - Menyebabkan gangguan signifikan terhadap aset perusahaan.
    - Menyebabkan kerugian finansial yang signifikan.
    - Menyebabkan gangguan signifikan terhadap individu, tetapi tidak termasuk hal-hal yang membahayakan jiwa.

- **Tinggi:**
  - Berdampak kerusakan terhadap operasional dan aset organisasi atau individual.
  - Contoh:
    - Organisasi tidak dapat menyediakan satu atau lebih fungsi pokoknya.
    - Menyebabkan gangguan sangat besar terhadap aset perusahaan.
    - Menyebabkan kerugian finansial yang besar.
    - Menyebabkan gangguan besar terhadap individu, termasuk hal-hal yang membahayakan jiwa.

CONTOH LEVEL GANGGUAN KEAMANAN

- **Kerahasiaan:**
  - Tinggi: nilai mahasiswa.
  - Moderat: data pengambilan mata kuliah.
  - Rendah: daftar mahasiswa, daftar staf akademik.
- **Integritas:**
  - Tinggi: data rekam medis pasien.
  - Moderat: forum web.
  - Rendah: anonymous online poll.
- **Ketersediaan:**
  - Tinggi: sistem yang menyediakan service autentikasi.
  - Moderat: website universitas.
  - Rendah: aplikasi pencarian nomor telepon online.

TANTANGAN KEAMANAN KOMPUTER

- **Security tidak sederhana.**
- **Serangan terhadap kelemahan mekanisme keamanan yang tidak terantisipasi.**
- **Di mana harus menempatkan mekanisme keamanan.**
- **Penyerang hanya memerlukan satu kelemahan, sedangkan desainer harus mengantisipasi semua kemungkinan kelemahan.**
- **Keamanan dipikirkan setelah desain sistem selesai.**
- **User memandang keamanan sebagai hal yang mengurangi kenyamanan penggunaan sistem.**

LATIHAN

1. **Misalkan terdapat alat kesehatan yang memonitor dan mencatat data pasien dan menyimpannya secara lokal. Untuk mengakses data, user harus memasukkan PIN ke alat tersebut dan kemudian mengakses data yang diperlukan. Tunjukkan contoh kebutuhan kerahasiaan, integritas, dan ketersediaan yang berhubungan dengan sistem, dan level dari pentingnya kebutuhan tersebut.**
2. **Untuk organisasi berikut ini, tentukan level dari dampak gangguan kerahasiaan, ketersediaan dan integritas sistem.**
   a. Organisasi yang mengelola informasi publik pada web servernya.
   b. Organisasi yang mengelola informasi investigasi yang sangat sensitif.
   c. Organisasi yang mengelola distribusi energi listrik di suatu kota.

3. **Misalkan terdapat DBMS untuk suatu department store.**
   - Berikan contoh database di mana kerahasiaan data adalah kebutuhan yang paling penting.
   - Berikan contoh database di mana integritas data adalah kebutuhan yang paling penting.
   - Berikan contoh di mana ketersediaan sistem adalah kebutuhan yang paling penting.
4. **Ulangi masalah no 1 untuk sistem telepon yang meneruskan panggilan telepon berdasarkan nomor telepon yang diminta oleh pengguna.**

ARSITEKTUR KEAMANAN OSI

- **Security attack:**
  - Tindakan membahayakan keamanan informasi yang dipunyai organisasi.
- **Security mechanism:**
  - Proses atau alat untuk mendeteksi, mencegah, atau recover dari serangan keamanan.
- **Security service:**
  - Service untuk menjaga keamanan pemrosesan data dan transfer informasi di organisasi.
  - Tujuan: meng-counter security attack.
  - Alat: satu atau lebih security mechanism.

SECURITY ATTACK

- **Ada 2 istilah:**
  - 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.

TIPE ATTACKS

- **Ada 2 macam serangan (X.800 dan RFC 2828):**
  - Serangan pasif
  - Serangan aktif

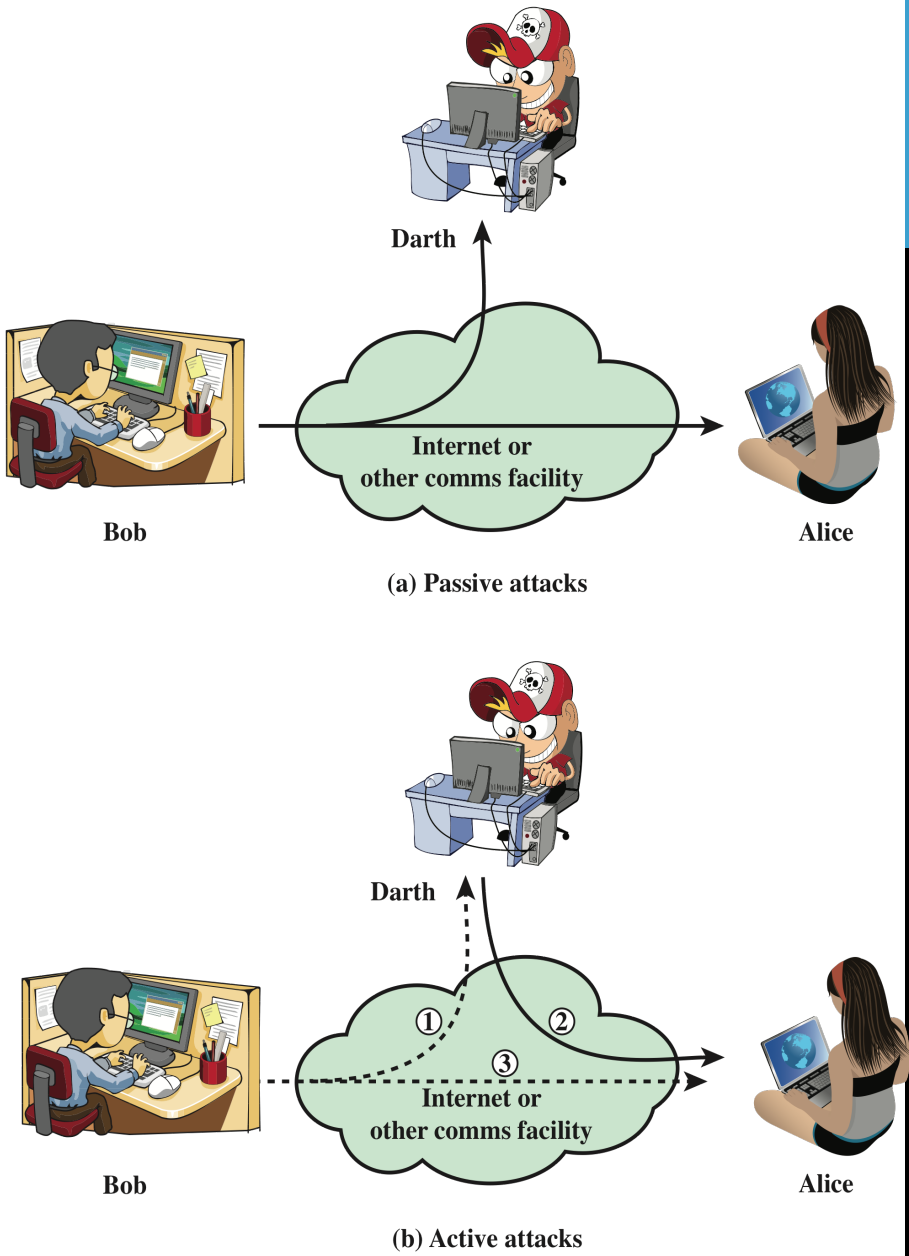
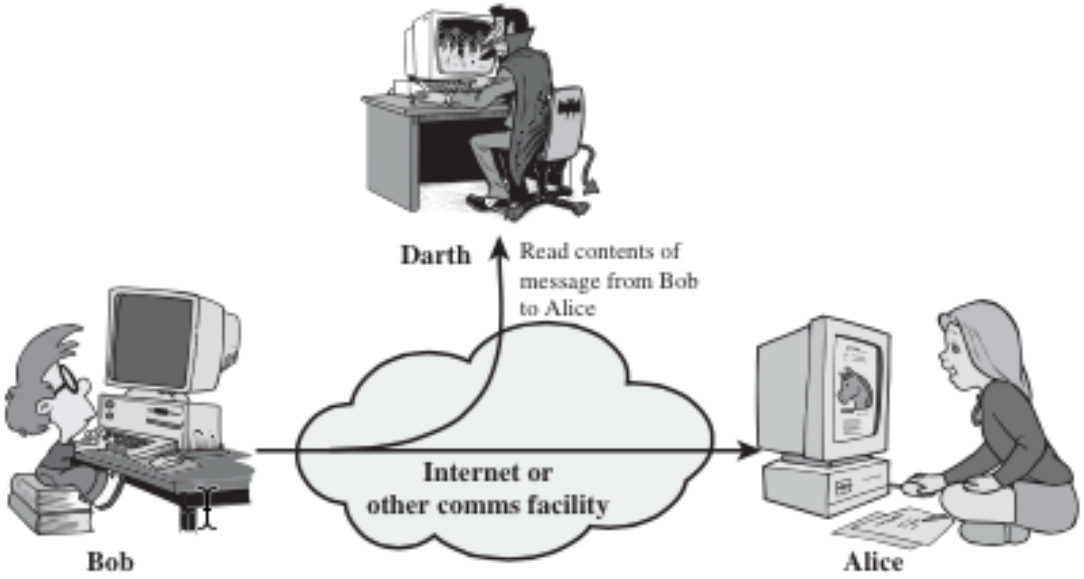
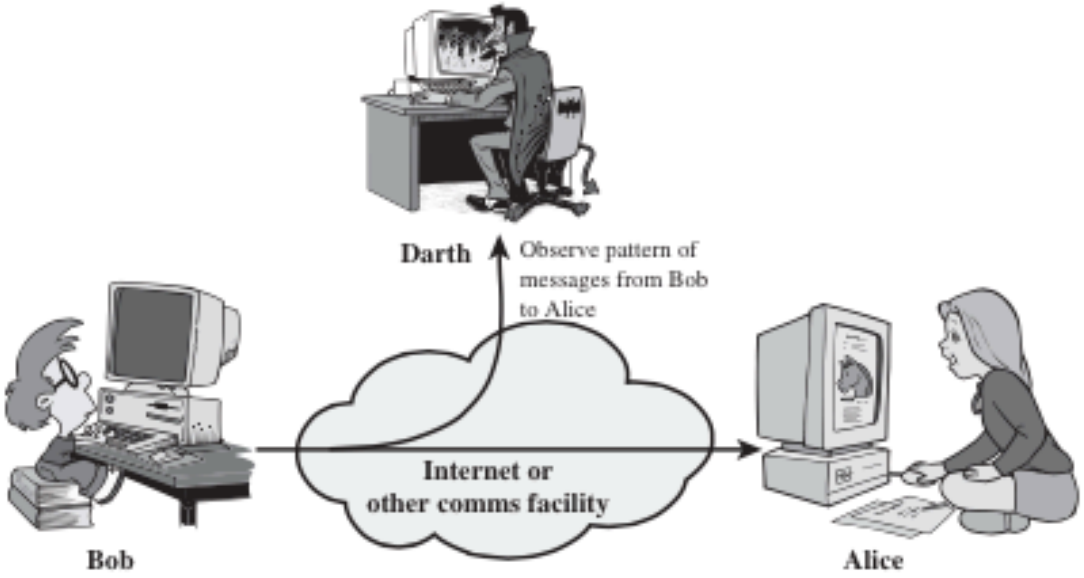


Figure 1.1 Security Attacks

- **Serangan pasif:**
  - Tujuan: mendapatkan informasi.
  - Ada 2 macam:
    - Release of message content
    - Traffic analysis
  - Sulit dideteksi.
  - Contoh pencegahan dengan enkripsi.

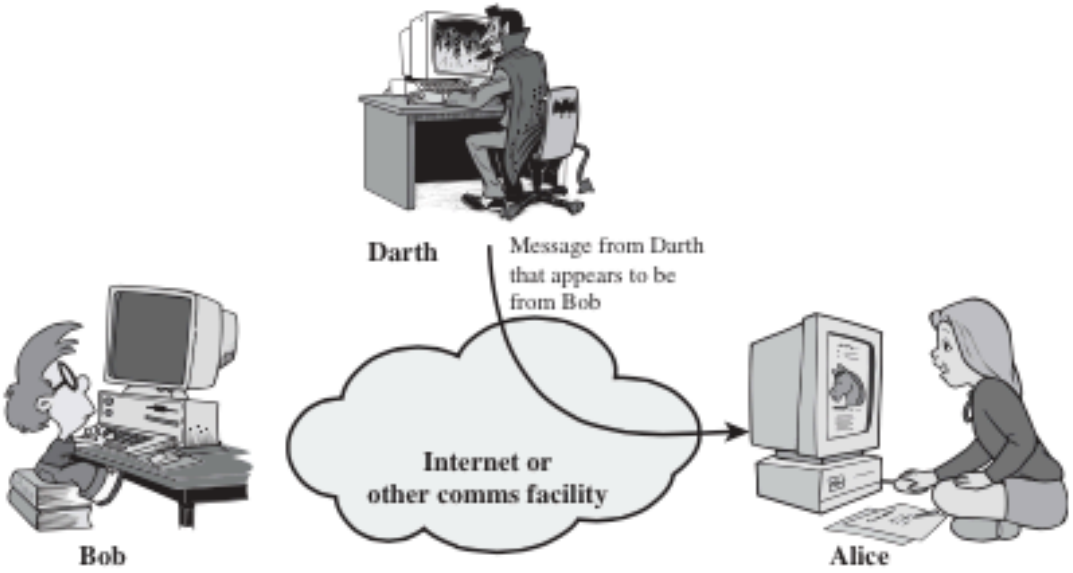


(a) Release of message contents

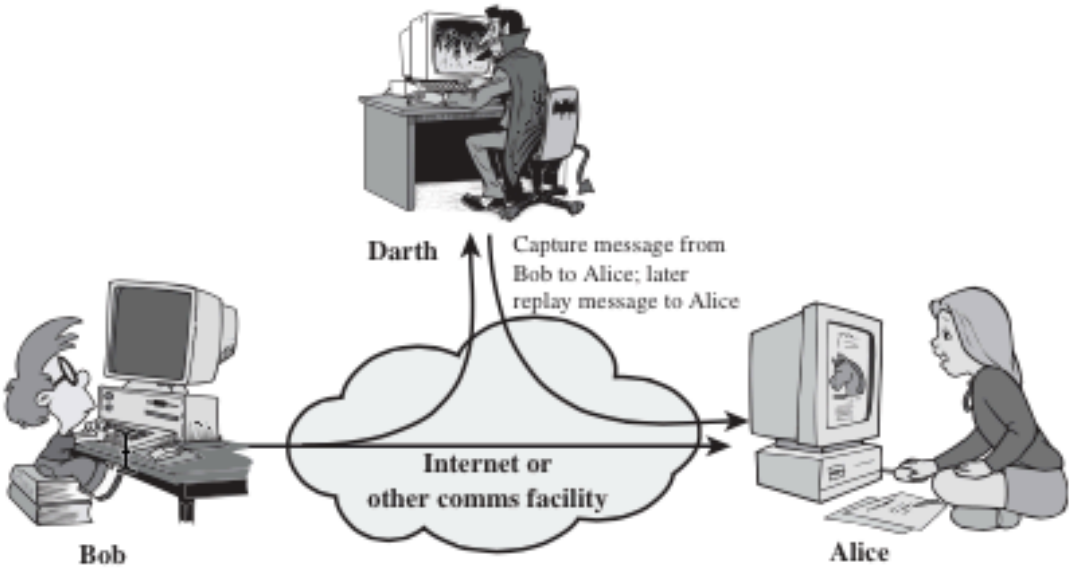


(b) Traffic analysis

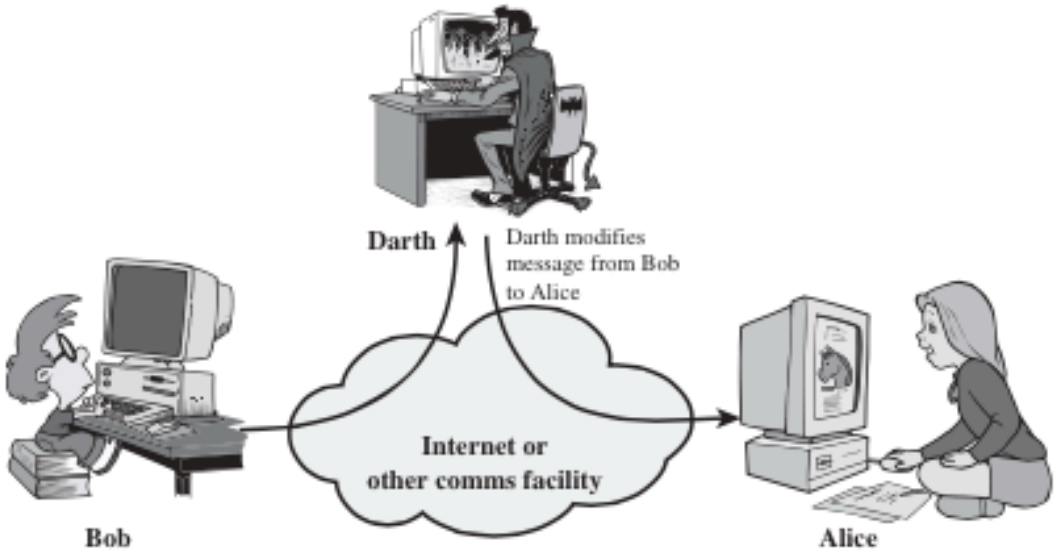
- **Serangan aktif:**
  - Tujuan: modifikasi data
  - 4 macam:
    - Masquarade: berpura-pura menjadi entity lain.
    - Replay: menangkap data, kemudian mentransmisi.
    - Modification of message.
    - Denial of service.



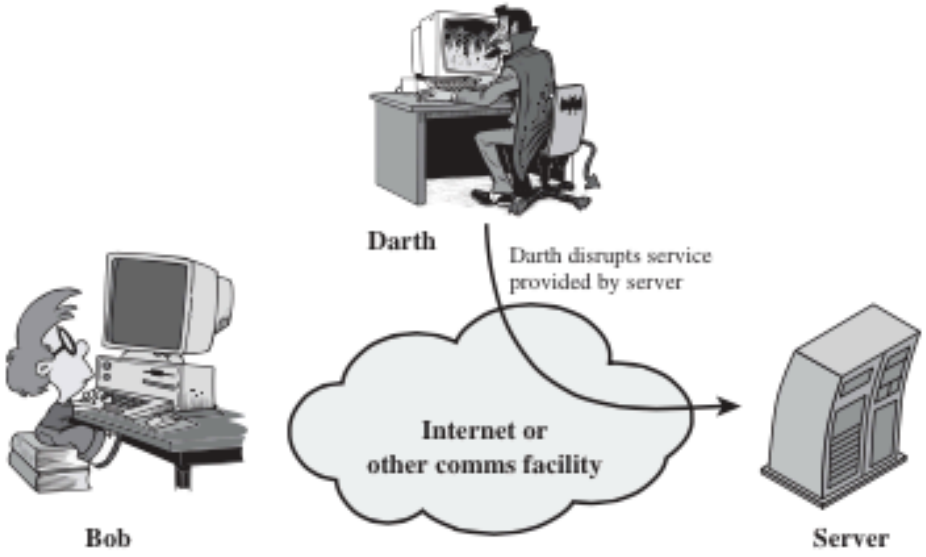
(a) Masquerade



(b) Replay



(c) Modification of messages



(d) Denial of service

SECURITY SERVICES

- **Definisi menurut X.800 (ITU) (International Telocommunication Union):**

  A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

- **Definisi menurut RFC 4949 (IETF-Internet Engineering Task Force):**

  A processing or communication service provided by a system to give a specific kind of protection to system resources

SECURITY SERVICE: KATEGORI MENURUT X.800

- **Autentikasi: menjamin bahwa komunikasi benar-benar otentik**
  - Peer entity
  - Data origin
- **Kontrol akses: mencegah penggunaan yang tidak legal**
- **Kerahasiaan data: proteksi dari serangan pasif.**
- **Integritas data: data benar-benar sama dengan yang dikirim.**
- **Nonrepudiation: proteksi dari denial oleh salah satu entity.**
  - Origin
  - Destination
- **Availability: properti bahwa sistem dan sumber daya akan selalu tersedia**

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

SECURITY MECHANISMS

- **Encipherment: algoritma untuk menyandikan**
- **Digital signature: membuktikan asal dan integritas data**
- **Access control: meng-enforce access rights**
- **Data integrity: memastikan integritas data**
- **Authentication exchange: memastikan identitas suatu entitas**
- **Traffic padding: penyisipan bit ke data asli**
- **Routing control: pemilihan jalur dan penyesuaiannya jika terjadi serangan**
- **Notarization: penggunaan trusted third party untuk memastikan dipenuhinya properti pertukaran data**

SECURITY MECHANISMS

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

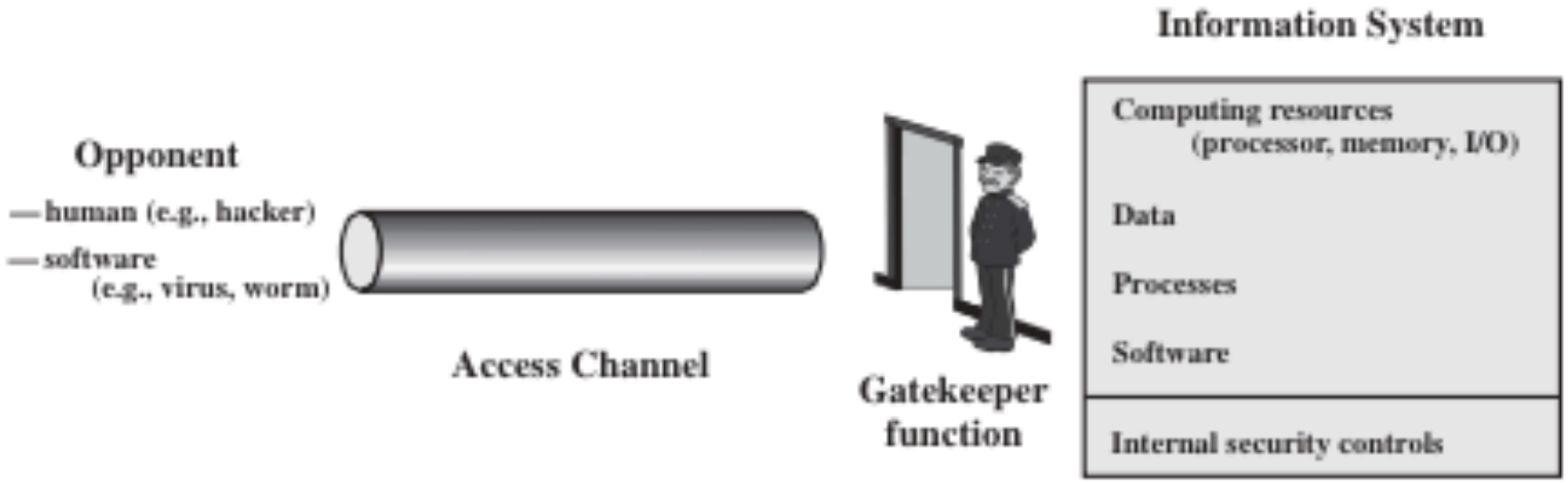
Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

HUBUNGAN ANTARA SECURITY SERVICES DAN SECURITY MECHANISMS

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer Entity Authentication	Y	Y			Y			
Data-Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic-Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

MODEL KEAMANAN JARINGAN

MODEL KEAMANAN AKSES JARINGAN



STANDARDS

NIST

National Institute of Standards and Technology

U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation

NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

ISOC

Internet Society

Professional membership society with worldwide organizational and individual membership

Provides leadership in addressing issues that confront the future of the Internet

Is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB)

Internet standards and related specifications are published as Requests for Comments (RFCs)

LATIHAN

1. **Buatlah matriks serupa dengan hubungan antara security services dan security mechanisms untuk:**
   a. Security service dengan attacks
   b. Security mechanisms dengan attacks