Jaringan, Internet & E-Commerce

Pertemuan 5

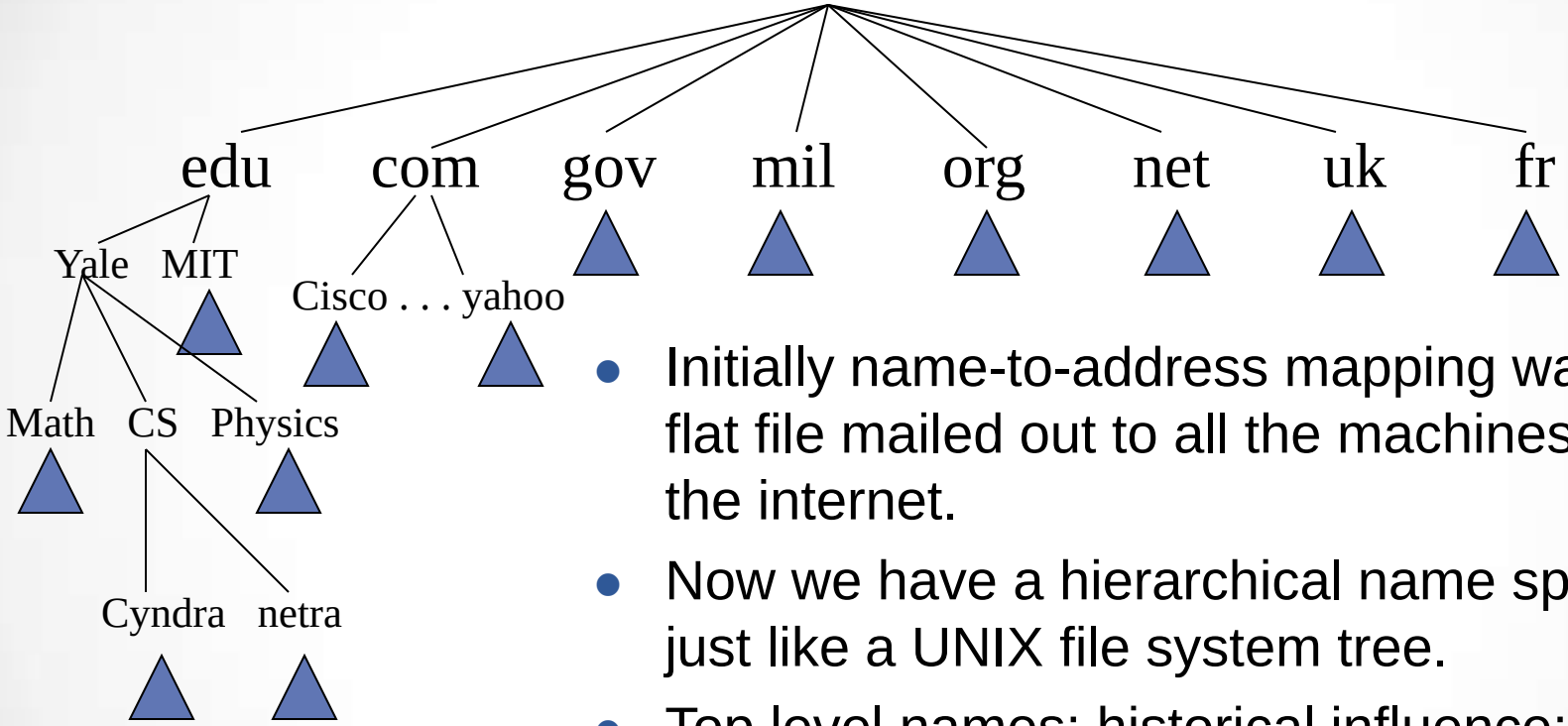
Jenis-Jenis Jaringan

- LAN (Local Area Networks)
- WAN (Wide Area Networks)
- Internet/Internet-Works

IP Address dan Host Name

- Each machine is addressed by a 32-bit integer: IP address
  - We will tell you what “IP” is later
  - Ran out of numbers and there are schemes to extend
- An IP address is:
  - Written down in a “dot notation” for “ease” of readings such as `128.36.229.231`
  - Consists of a network address and a host ID
- IP addresses are the universal IDs that are used to name everything
- For convenience, each host also has a human-friendly host name: for example “`128.36.229.231`” is “concave.cs.yale.edu”
- Question: how do you translate names into IP addresses?

Domain Hierarchy



- Initially name-to-address mapping was a flat file mailed out to all the machines on the internet.
- Now we have a hierarchical name space, just like a UNIX file system tree.
- Top level names: historical influence: heavily US centric, government centric, and military centric view of the world.

Protokol Jaringan

LANs

- Ethernet
- Token ring

WAN

- TCP/IP (4 layer)
- OSI model (7 layer)

Enkripsi

- Sistem enkripsi mentranslate data menjadi kode rahasia
- Sistem enkripsi melibatkan 4 komponen utama:
  - **Plaintext**: pesan belum terenkripsi
  - **Algoritma enkripsi**: yang berfungsi untuk mengacak pesan
  - **Kunci**: yang berfungsi sebagai kombinasi kunci
  - **Ciphertext**: pesan yang telah terenkripsi
  - **Dekripsi**: proses kebalikan dari enkripsi yang menghasilkan kembali plaintext

Teknik Enkripsi

- Dua teknik enkripsi yang digunakan:
  - **Simetris** : pengirim dan penerima menggunakan kunci yang sama
  - **Asimetris** (public key): menggunakan dua set kunci yang berbeda, disebut *public key* dan *private keys*

Enkripsi Simetris

- **Simetris** atau **private key encryption**, menggunakan algoritma dan kunci yang sama, baik untuk mengenkripsi maupun mendekripsi pesan
- Teknik enkripsi yang paling umum digunakan
- Karena kunci harus didistribusikan, maka rentan terhadap kebocoran. Ini yang menjadi kelemahan teknik ini

Enkripsi Asimetris

- Teknik yang kedua adalah asimetris atau **public key encryption** (PKE)
- PKE disebut asimetris karena menggunakan dua kunci yang berbeda:
  - public key digunakan untuk mengenkripsi pesan
  - private key digunakan untuk mendekripsi pesan
- PKE mengurangi masalah karena private key tidak pernah didistribusikan

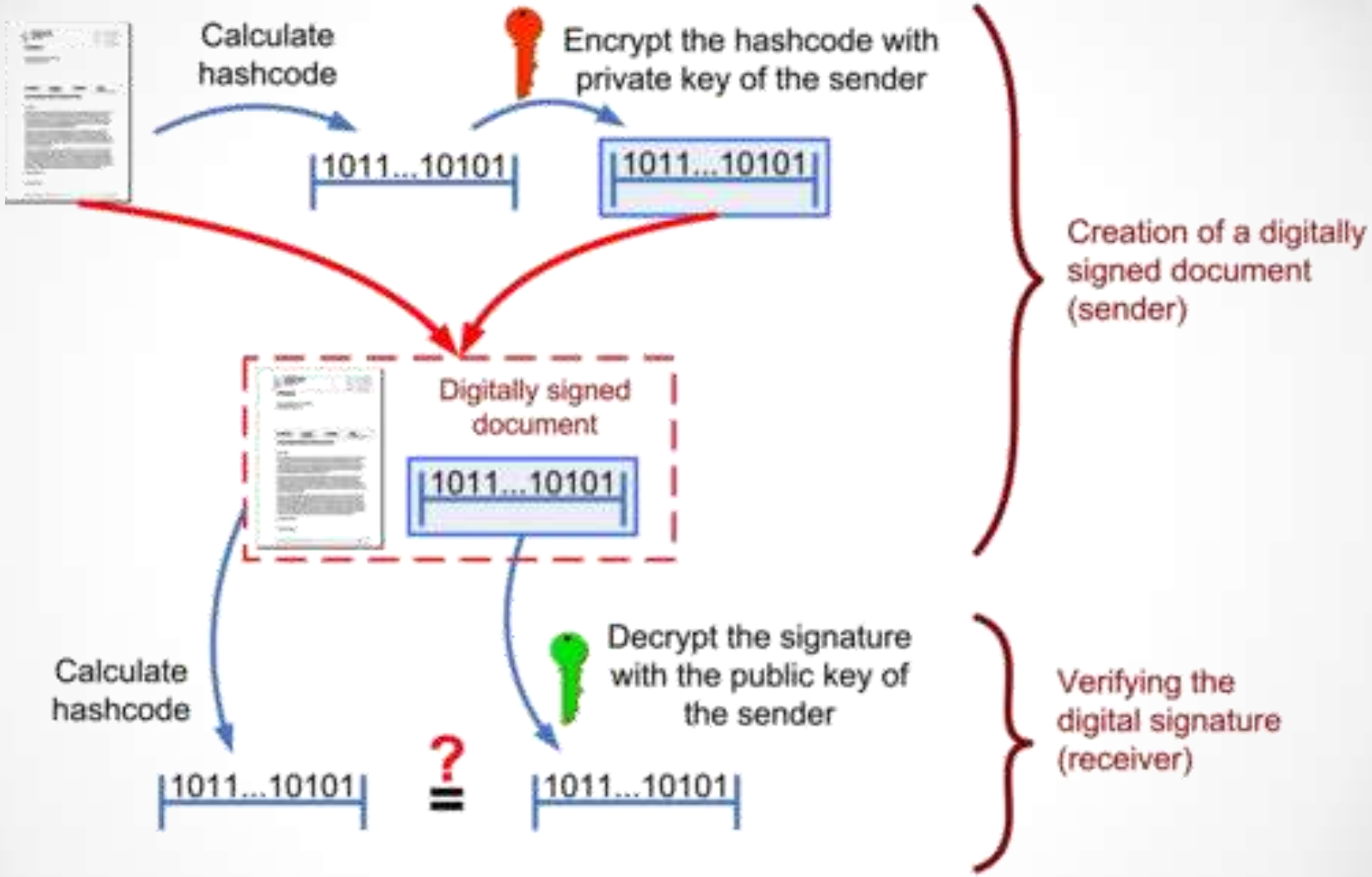
Otentikasi

- Adalah proses keamanan untuk memverifikasi bahwa user adalah mereka sebagaimana yang mereka katakan
- Password adalah metode otentikasi yang umum digunakan
- Digital signatures merupakan alternatif untuk otentikasi informasi yang dikirimkan

Digital Signature

- Digital signatures take the place of ordinary signatures in online transactions to prove that the sender of a message is who he or she claims to be
- When received, the digital signature is compared with a known copy of the sender's digital signature
- Digital signatures are also sent in encrypted form to ensure they have not been forged

Creating and verifying a digital signature



If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.

NETWORKS:

CONNECTING DEVICES

- LAN Linking Devices and Systems
  - Multiplexer
  - Hubs
    - Passive
    - Manageable
    - Switched
  - Routers
  - Switches
  - Gateways
  - Bridges

EDI

- Manfaat
  - Mengurangi input data
  - Mengurangi kertas
  - Mengurangi pengiriman
  - Mengurangi kesalahan/*error*
  - Mengurangi inventori
  - MENGURANGI BIAYA
  - EFT (*Electronic For Transactions*)
  - Rekam jejak EDI

E-Commerce

- Electronic Commerce
- Jenis-jenisnya:
  - B2C
  - B2B
  - C2C
- Komponen:
  - Sistem pembayaran elektronis (electronic payment systems)
  - SSL (secure socket layer)
  - SET (secure electronic transaction)
  - S-HTTP (secure-HTTP)

E-Commerce

- Resiko-resiko:
  - Internal
    - Kecelakaan/kegagalan sistem
    - Akuntansi yang tidak efektif
    - Aktifitas yang membahayakan
    - Penipuan
  - Eksternal
    - Intruders
      - Hackers
      - Cracker
    - Virus
    - Cyberterrorism/cybercrime

Mengendalikan E-Commerce

- Kendali atas:
  - Kebijakan dan prosedur
  - Teknik SDLC
  - Sistem anti-virus
  - Log
  - Sistem monitoring

Mengendalikan E-Commerce

- Sistem kendali akses
  - Call-back systems
  - Challenge-response systems
  - Multifaceted password systems
  - Biometrics
  - Firewalls
  - IDS (Internal Data Security)
    - Misuse detection vs. anomaly detection
    - Network-based vs. host-based systems
    - Passive system vs. reactive systems
  - Controlling DoS attacks

Tujuan Audit

- Verifikasi keamanan dan integritas transaksi
  - Dapat mendeteksi dan memperbaiki kehilangan data
  - Dapat mencegah dan mendeteksi akses ilegal, internal dan eksternal
- Verifikasi prosedur backup telah memadai
- Memastikan:
  - Tidak ada akses tanpa ijin ke database
  - Pihak berwenang hanya memiliki akses ke data yang telah disetujui saja
  - Ada kendali untuk memastikan bukti audit terhadap transaksi elektronik

Tujuan Audit

- Kendali backup untuk jaringan
- Validasi transaksi
- Kendali akses:
  - Uji kendali validasi
  - Uji kendali bukti audit

Prosedur Audit

- Memilih contoh pesan dari log transaksi dan memverifikasi integritasnya
- Meninjau ulang log transaksi pesan untuk memverifikasi bahwa semua pesan diterima sesuai dengan prosedur
- Menguji operasi fasilitas seperti call-back
- Meninjau ulang prosedur keamanan dalam pengaturan data
- Memverifikasi proses enkripsi dengan mengirim pesan teks
- Meninjau ulang kelayakan *firewall*

Sekian

&

Terima kasih