Ir. Budi Rahardjo, M. Sc., Ph.D

Teknik Komputer – STEI ITB

Keamanan Informasi

Pengantar Nama Domain

II3230 - Keamanan Informasi

Latar Belakang

- Komputer bekerja berdasarkan dengan **angka**
  - Bilangan biner: **1010 0101**
  - Nomor IP: **167.205.21.82**
  - Semua diterjemahkan menjadi angka (biner), baru kemudian diproses
- Manusia memiliki kelemahan dalam mengingat angka
  - **167.205.59.96** vs "**www.itb.ac.id**"
  - Mana yang lebih mudah diingat?
- Domain juga menjadi identitas:
  - Google, Amazon, Facebook, ...

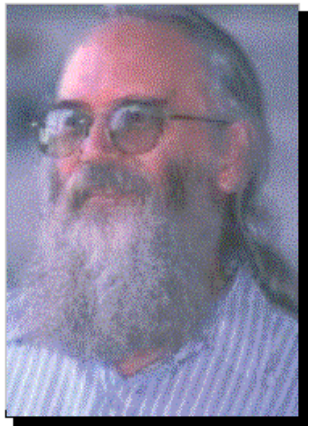
Solusi?

- Diperlukan sebuah konversi dari nama ke angka dan sebaliknya
- Cara paling mudah adalah dengan menggunakan tabel
  - Di sistem UNIX ada berkas "**/etc/hosts**"
  - Contoh isinya

```
167.205.21.81     router
167.205.21.82     www.paume.itb.ac.id
167.205.21.83     mail-server
167.205.21.84     asimov
```

Pengaturan Nomor IP dan Nama

- Sejarahnya pengaturan nomor IP dan nama host diatur secara tersentral oleh IANA (Internet Assigned Numbers Authority)
  - Dimotori oleh Jon Postel
  - Daftar tabel diunduh secara berkala



Situs web
IANA – http://www.iana.org
Jon Postel – http://www.postel.org

iana
Internet Assigned Numbers Authority

Masalah Mulai Muncul

- Sistem tabel dapat digunakan untuk jumlah mesin yang tidak terlalu banyak
- Masalah
  - Internet berkembang. Jumlah hosts bertambah. Tabel bertambah besar dan repot untuk dikelola secara manual
  - Perebutan nama yang “favorit”
    - Nama fungsi: server, router, ...
    - Nama tokoh: kartun, pengarang science fiction, ...
    - Nama lokasi: kota, negara, ...

Domain Name System (DNS)

- “Tabel” yang dikelola secara terdistribusi
- Seorang administrator mengelola sebuah domain tertentu.
  - Domain dapat memiliki sub domain
- DNS inventor: Paul Mockapetris
  - http://en.wikipedia.org/wiki/Paul_Mockapetris
- Data-data di DNS tidak hanya sekedar nomor IP tapi juga: MX record, jenis komputer, OS, lokasi, dll.

Mekanisme Query DNS

- *Query* DNS sama seperti menelusuri alamat pos biasa
- Untuk menelusuri alamat di bawah ini, alamat dibaca dari belakang (mulai dari Indonesia)

```
Budi Rahardjo
Pusat Mikroelektronika ITB
Gedung PAU ITB
Jalan Ganesha 10
Bandung 40132
Indonesia
```

Query DNS

- Name server (NS): server yang mengelola database domain ybs
  - Mencari NS dengan menggunakan tools
- Query ke “www.itb.ac.id” dilakukan dengan urutan
  - . → a.root-servers.net (198.41.0.4)
  - .id → b.dns.id (103.19.179.179) ← **name server dari .id**
  - .ac.id → b.dns.id (103.19.179.179) ← **name server dari .ac.id**
  - .itb.ac.id → ns1.itb.ac.id (167.205.23.1) ← **name server ITB**
  - **www.itb.ac.id = 167.205.59.96**
- Ada proses *cache* untuk mempercepat query
  - Domain yang sering (baru saja) dicari disimpan di cache

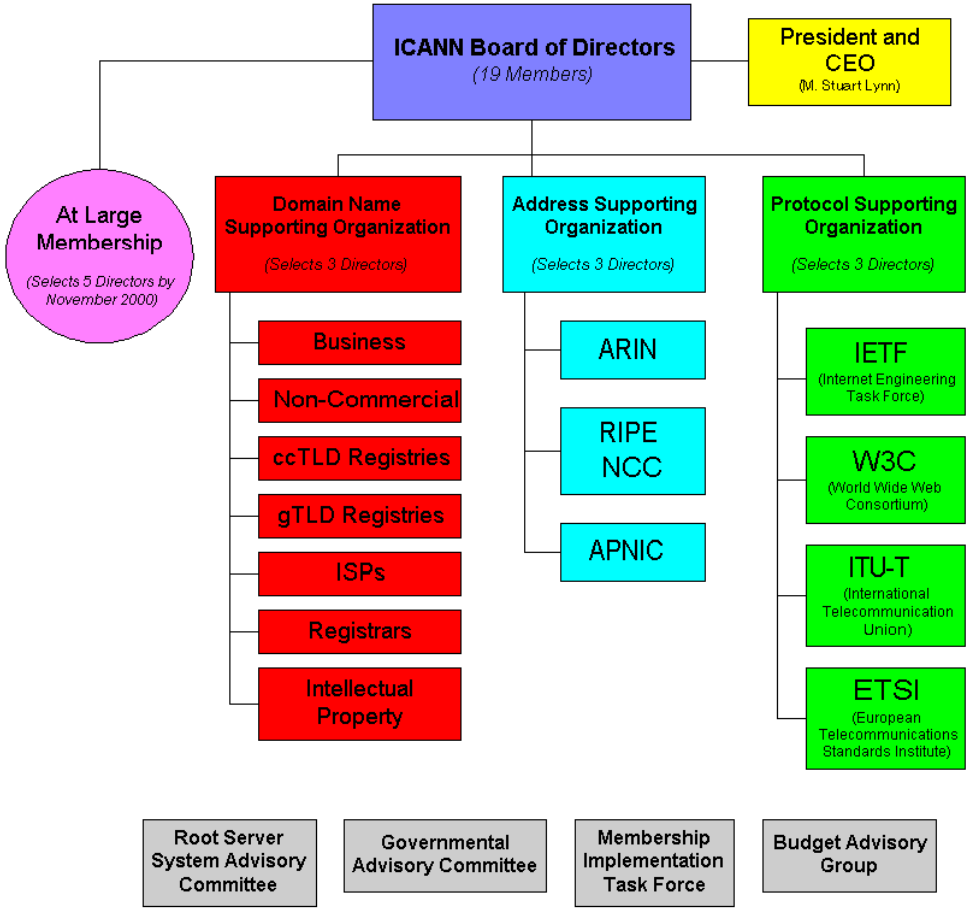
Klasifikasi Nama Domain

- gTLD (generic Top Level Domain)
  - Domain yang populer: .com, .net, .org, .gov, .mil, .edu, .int
  - Sudah ditambah dengan domain-domain lain
    - .aero, .biz, .coop, .info, .museum, .name, .pro
    - http://www.iana.org/gtld/gtld.htm
- ccTLD (country code Top Level Domain)
  - .ID, .JP, .SG, .US, dll.
  - Masing-masing dikelola oleh seorang administrator yang ditunjuk oleh IANA

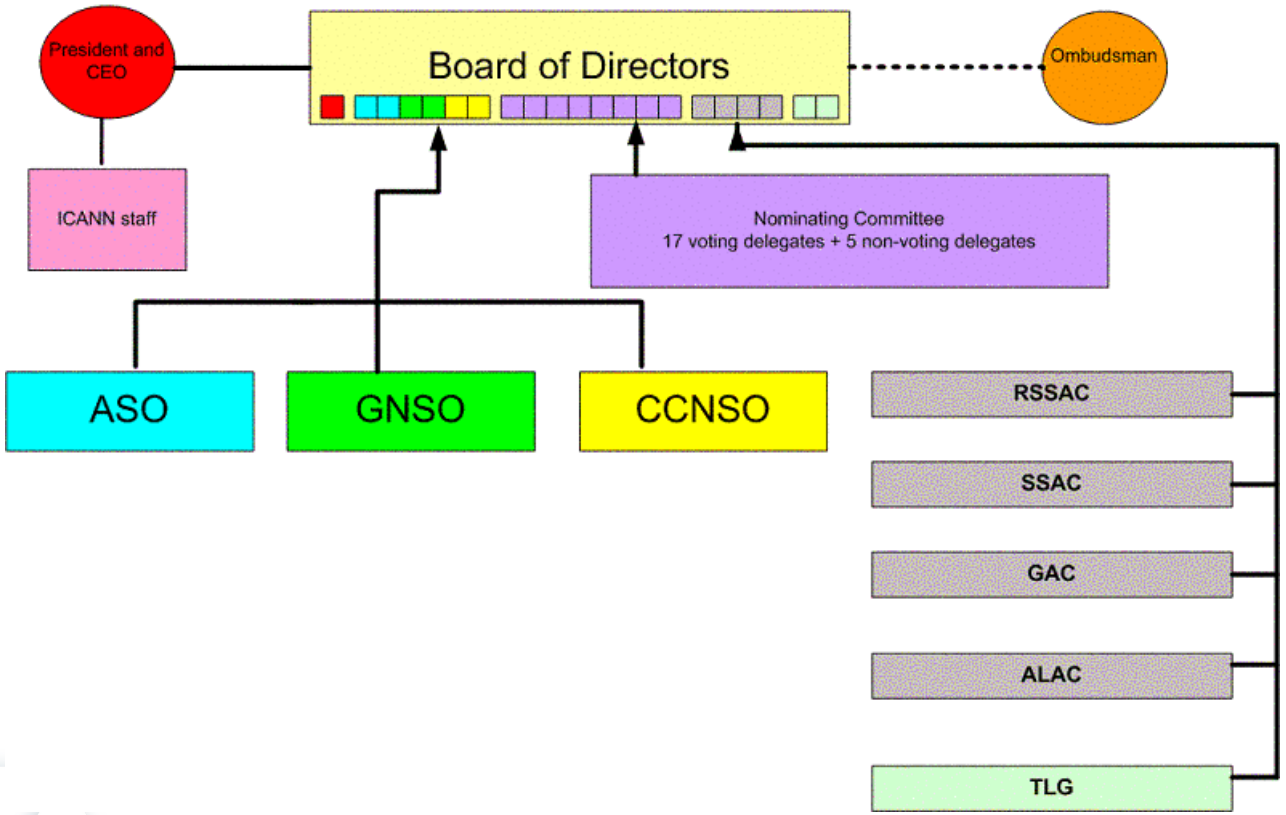
Organisasi terkait dengan DNS

- Global:
  - Pada mulanya: IANA (www.iana.org)
  - Sekarang: ICANN (Internet Corporation For Assigned Names and Numbers) www.icann.org
- Regional
  - APTLD, CENTR, AFNIC, ...
- Negara
  - Berbeda-beda. Di Indonesia: IDNIC / ID DOMREG / Pengelola Nama Domain Indonesia

ICANN Organizational Chart



ICANN Organizational Chart



Pengelola Nama Domain Indonesia

- Sejarah
  - Dimulai dari individual: Didik Partono ke Rahmat Samik Ibrahim dan kemudian ke Budi Rahardjo (beserta Maman Sutarman)
  - Awalnya menggunakan nama IDNIC (Indonesia Network Information Center), ID DOMREG, ccTLD ID
  - Menjadi “Pengelola Nama Domain Indonesia” (PANDI)
  - Terdaftar di IANA/ICANN

Sejarah Struktur Domain .ID

- Domain harus di bawah second level domain
  - .ac: academic
  - .co: company
  - .or: others
  - .net: net
  - .go: government
  - .mil: military
  - .sch: school
  - .web: web
- Khusus:
  - .war.net.id: warnet

Topik Seputar DNS

- Teknis
  - Tools, server, setup, query, dll.
  - Support: internasionalisasi (IDN), IPv6, secure DNS
- Non-teknis
  - Aturan penamaan dan persyaratan pendaftaran

Data DNS lainnya

Selain nomor IP, DNS dapat digunakan untuk menyimpan data lainnya

- Mail server: MX record
  Server mail yang berhak menerima/mengirim mail untuk domain tersebut
  `host -t mx itb.ac.id`

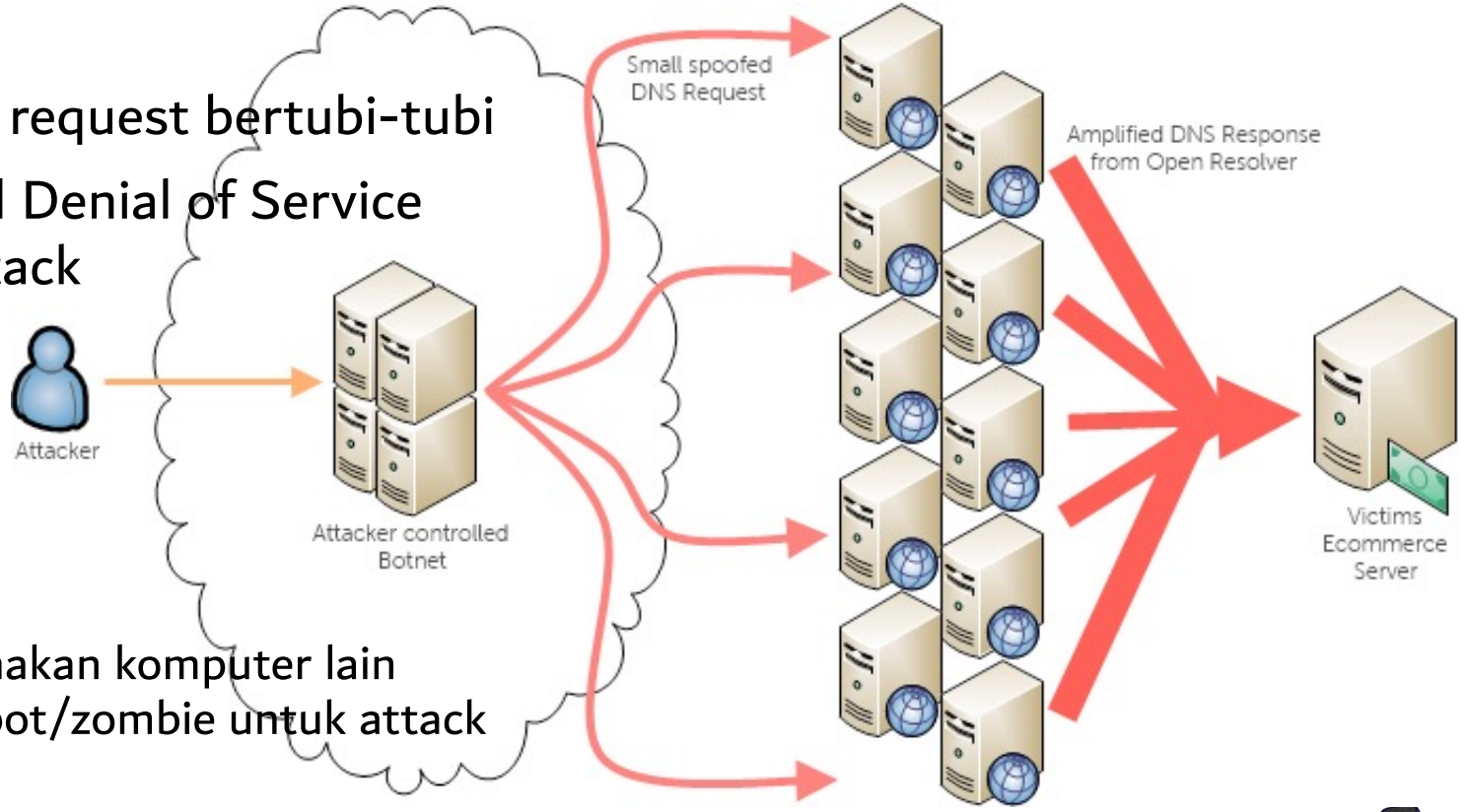
- Kunci publik
- Data server lainnya: OS, dll.
- Lokasi (jarang dilakukan karena kebocoran data)

Serangan Terhadap DNS

- Melakukan ***zone transfer*** terhadap data DNS
  - *Zone transfer* seharusnya dibatasi (tidak diperbolehkan untuk orang luar)
  - Tidak semua subdomain harus diketahui
  - *Zone transfer* juga dapat menghabiskan bandwidth karena ada faktor amplifikasi
    - Request hanya membutuhkan *x* bytes
    - Jawaban dari request jauh lebih besar dari *x* bytes tersebut

Serangan DoS Terhadap DNS

- Melakukan request bertubi-tubi
- Distributed Denial of Service (DDoS) attack



- Menggunakan komputer lain sebagai bot/zombie untuk attack

Serangan Terhadap DNS

- Random label attack
  - Melakukan query DNS dengan subdomain yang **random** (yang kemungkinan besar tidak ada) sehingga server DNS sibuk menjawab request ini
    - **xyz123**.itb.ac.id?
    - **xyz124**.itb.ac.id?
    - **xyz12345**.itb.ac.id?
    - dst
  - Tidak ada di **cache** (karena random)
- DNS spoof
  - Menyadap DNS query dan menjawab dengan data palsu

DNS dan Hukum

- Masalah HaKI dari nama domain
  - Trademark
  - Cybersquating
- Dispute Resolution Policy?