Lec 26: Naming & Encryption

- DNS (domain name service)
- TLS
  - key exchange
  - digital certificates
ICANN
International corps for address names and numbers
- Control root name servers.

authoritative Name servers

find www.cs.cornell.edu
where is www?
where is cs?
where is cornell.edu?
where is 10.1.2.4?

Caching nameserver

10.1.2.3
10.1.2.4

Cornell.edu NS
Cornell.edu NS/CS/IR
Caching...
Public key signatures

\[ \text{msg} \rightarrow \text{sign} \rightarrow \text{verify} \]

Yes: signature valid
No: invalid.

Recipient buys public keys, tells everyone public key, never loses anyone's key

Comp. expensive

Computationally cheap

Sender

Recipient

From "scan key" of public key for this message

Public key encryption (expensive)

Secret/shared key encryption (cheap)
TLS: transport layer security
- establish a TCP connection
- use connection to establish shared key $k_s$
- use $k_s$ to encrypt further traffic.

Sender $k_{rec}$

Form session key $k_{enc}$ for this message

For the message $msg$:

$k_s$ → $Enc_{k_s}(msg) ← msg$

Secret/Shared key encryption (cheap)

Recipient $k_{send}$

Public key encryption (expensive)

$k_{pub}$ → $Enc_{k_{pub}}(k_s)$ → $k_s$

$msg' ← Enc_{k_{send}}(msg) ← msg'$

TCP
IP
eth

Encrypted data

Header fields:
- length
- src/dst IP addr.
- src/dst port
- protocol
- source address
- destination address
Man in the middle attack

to prevent: some kind of "out of band" communication - very expensive.
KCA can grant authority to other CAs for subdomains

- e.g. Cornell CA, responsible for cornell.edu keys.

KCA

KCA sends

KCA says cornell.edu is KCA.

KCA

KCA says cornell.edu is KCA.

Enc_{KCA}(k_B)

Enc_{KCA}(k_S)
VPN (virtual private network)

- User
  - Traffic flows through proxy server
  - Source: me, Destination: bad.com
  - Data: x
- Proxy server
  - Source: proxy, Destination: bad.com
  - Data: x
- Wireless router
  - Encrypted data