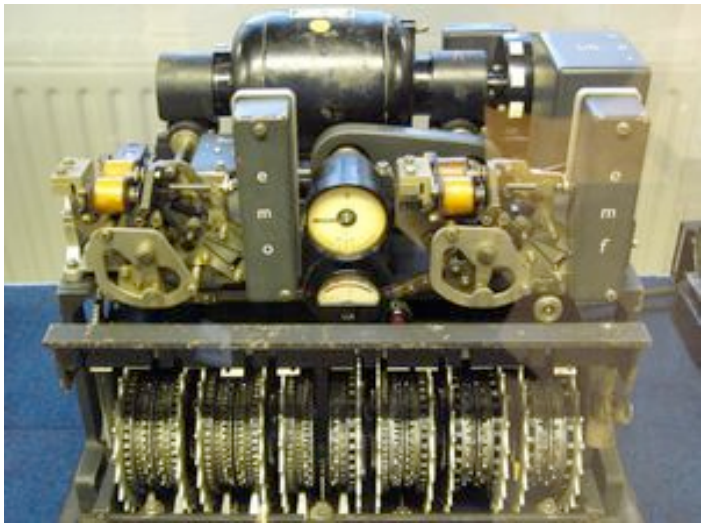


Network and Communication Security: HTTPS, IP Sec, DNS-Sec

Section 8.4

COS 461: Computer Networks

Spring 2011

Mike Freedman

http://www.cs.princeton.edu/courses/archive/spring11/cos461/

Recall basic security properties

- **Confidentiality:** Concealment of information or resources
- **Authenticity:** Identification and assurance of origin of info
- **Integrity:** Trustworthiness of data or resources in terms of preventing improper and unauthorized changes
- **Availability:** Ability to use desired info or resource
- **Non-repudiation:** Offer of evidence that a party indeed is sender or a receiver of certain information
- **Access control:** Facilities to determine and enforce who is allowed access to what resources (host, software, network, …)

Use of encryption and MAC/signatures

Confidentiality (Encryption)

Sender:

- Compute C = $Enc_K(M)$
- Send C

Receiver:

- Recover M = $Dec_K(C)$

Auth/Integrity (MAC / Signature)

Sender:

- Compute s = $Sig_K(Hash\ (M))$
- Send <M, s>

Receiver:

- Computer s' = $Ver_K(Hash\ (M))$
- Check s' == s

These are simplified forms of the actual algorithms

HTTP Security

"Securing" HTTP

- Threat model
  - Eavesdropper listening on conversation (confidentiality)
  - Man-in-the-middle modifying content (integrity)
  - Adversary impersonating desired website (authentication, and confidentiality)

- Enter HTTP-S
  - HTTP sits on top of secure channel (SSL/TLS)
  - All (HTTP) bytes written to secure channel are encrypted and authenticated
  - Problem: What is actually authenticated to prevent impersonation? Which keys used for crypto protocols?

Learning a valid public key

- What is that lock?
  - Securely binds domain name to public key (PK)
    - Believable only if you trust the attesting body
    - Bootstrapping problem: Who to trust, and how to tell if this message is actually from them?
  - If PK is authenticated, then any message signed by that PK cannot be forged by non-authorized party

How to authenticate PK

General | Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.wellsfargo.com
Organization (O)	Wells Fargo and Company
Organizational Unit (OU)	ISG
Serial Number	41:C5:CD:90:95:3C:A1:4B:C1:8A:

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	5/12/10
Expires On	5/13/11

Fingerprints

SHA1 Fingerprint	C5:EC:18:24:50:9D:90:93:96:69:
MD5 Fingerprint	1C:51:99:C9:EA:7B:FB:64:3F:92:F

Certificate Hierarchy

- Builtin Object Token:Verisign Class 3 Public Primary Certific
  - VeriSign, Inc.
    - www.wellsfargo.com

Certificate Fields

- Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Basic Constraints
  - Certificate Key Usage
  - CRL Distribution Points

Field Value

```
Modulus (1024 bits):
c9 b3 f9 c0 4a 42 be 1a c4 0a a0 b5 e0 9c 79 89
52 82 b1 89 b3 82 dc 2d 03 2b 1e 77 c3 4c 7d 97
37 62 c6 7b 31 b5 6b 25 d3 9e 7e 7e 07 95 7e f6
ab 6a 5c 88 ec 27 9d 72 3e a0 80 0c a5 ea d4 ff
```

Transport Layer Security (TLS)

(Replaces SSL)

- Send new random value, list of supported ciphers

- Send new random value, digital certificate with PK

- Send pre-secret, encrypted under PK

- Create shared secret key from pre-secret and random
- Switch to new symmetric-key cipher using shared key

- Create shared secret key from pre-secret and random
- Switch to new symmetric-key cipher using shared key

Comments on HTTPS

- Note that HTTPS authenticates server, not content
  - If CDN (Akamai) serves content over HTTPS for its customers, customer must trust Akamai not to change content
- Switch to symmetric-key crypto after public-key ops
  - Symmetric-key crypto much faster (100-1000x)
  - PK crypto can encrypt message only approx. as large as key (1024 bits – this is a simplification) – afterwards uses hybrid
- HTTPS on top of TCP, so reliable byte stream
  - Can leverage fact that transmission is reliable to ensure: each data segment received exactly once
  - Adversary can't successfully drop or replay packets

IP Security

IP Security

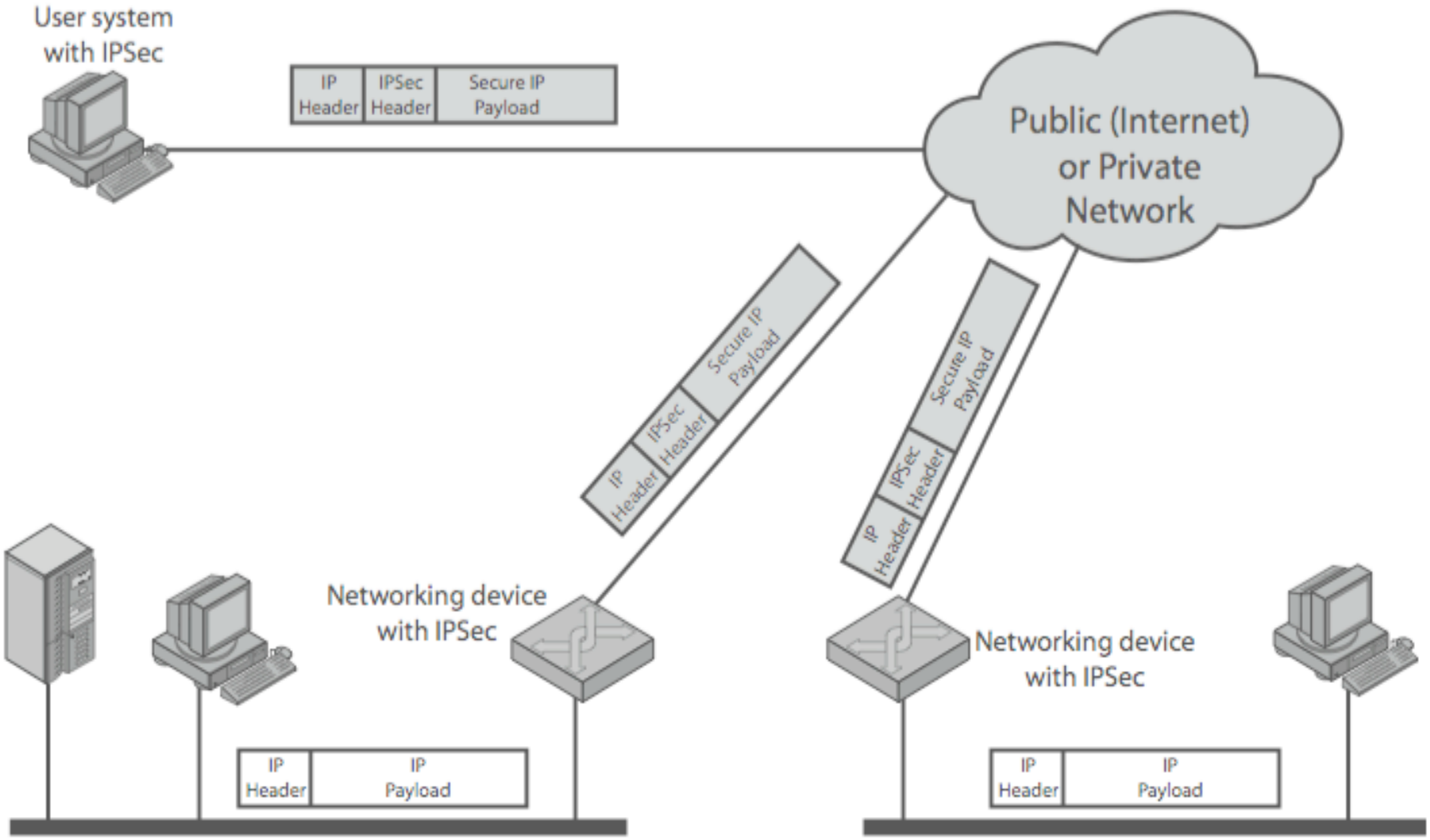
- There are range of app-specific security mechanisms
  - eg. TLS/HTTPS, S/MIME, PGP, Kerberos,
- But security concerns that cut across protocol layers
- Implement by the network for all applications?

Enter IPSec!

IPSec

- General IP Security mechanism framework
- Allows one to provide
  - Access control, integrity, authentication, originality, and confidentiality
- Applicable to different settings
  - Narrow streams: Specific TCP connections
  - Wide streams: All packets between two gateways

IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
Secure IP Payload
IPSec Header
IP Header
Secure IP Payload
IPSec Header
IP Header
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

- If in a firewall/router:
  - Strong security to all traffic crossing perimeter
  - Resistant to bypass
- Below transport layer: transparent to applications
- Can be transparent to end users
- Can provide security for individual users
- Helps secure routing architecture

IP Security Architecture

- Specification quite complex (incl. RFC 2401, 2402, 2406, 2408)
  - Mandatory in IPv6, optional in IPv4
- Two security header extensions:
  - Authentication Header (AH)
    - Connectionless integrity, origin authentication
      - MAC over most header fields and packet body
    - Anti-replay protection
  - Encapsulating Security Payload (ESP)
    - These properties, plus confidentiality

Encapsulating Security Payload (ESP)

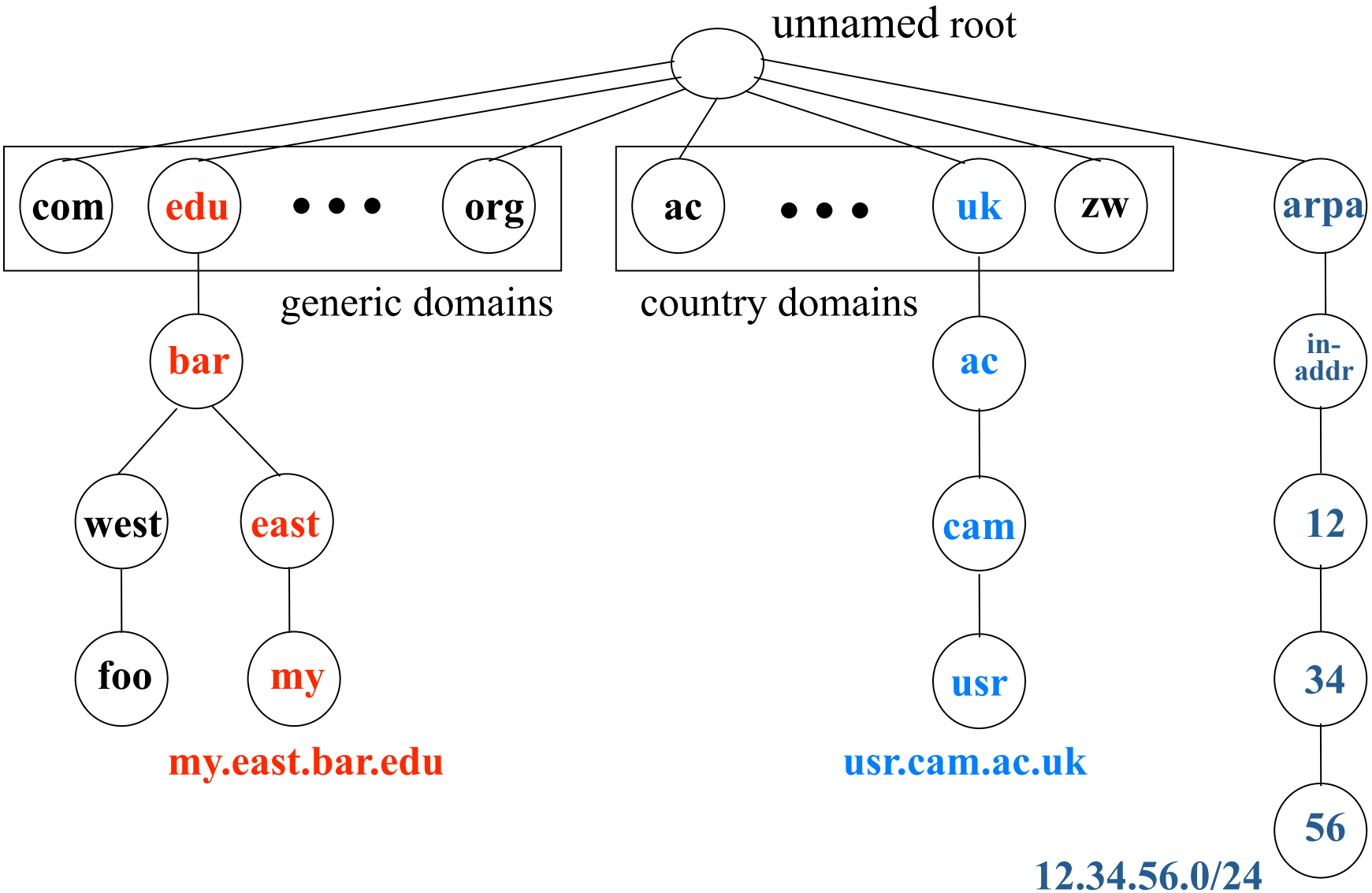
- Transport mode: Data encrypted, but not header
  - After all, network headers needed for routing!
  - Can do traffic analysis but is efficient
  - Good for host-to-host traffic
- Tunnel mode: Encrypts entire IP packet
  - Add new header for next hop
  - Good for VPNs, gateway-to-gateway security

Why is replay protection hard?

- Replay protection goal: Eavesdropper can't capture encrypted packet and duplicate later
  - Easy with TLS/HTTP on TCP: Reliable byte stream
  - But IP Sec at packet layer; transport may not be reliable
- IP Sec solution: Sliding window on sequence #'s
  - All IPSec packets have a 64-bit monotonic sequence number
  - Receiver keeps track of which seqno's seen before
    - [lastest – windowsize + 1 , latest] ; windowsize typically 64 packets
  - Accept packet if
    - seqno > latest (and update latest)
    - Within window but has not been seen before
  - If reliable, could just remember last, and accept iff last + 1
    - But IP packets can be reordered. Reordering could be particularly bad if QoS and low-priority. Hence, some windows are 1024 packets.

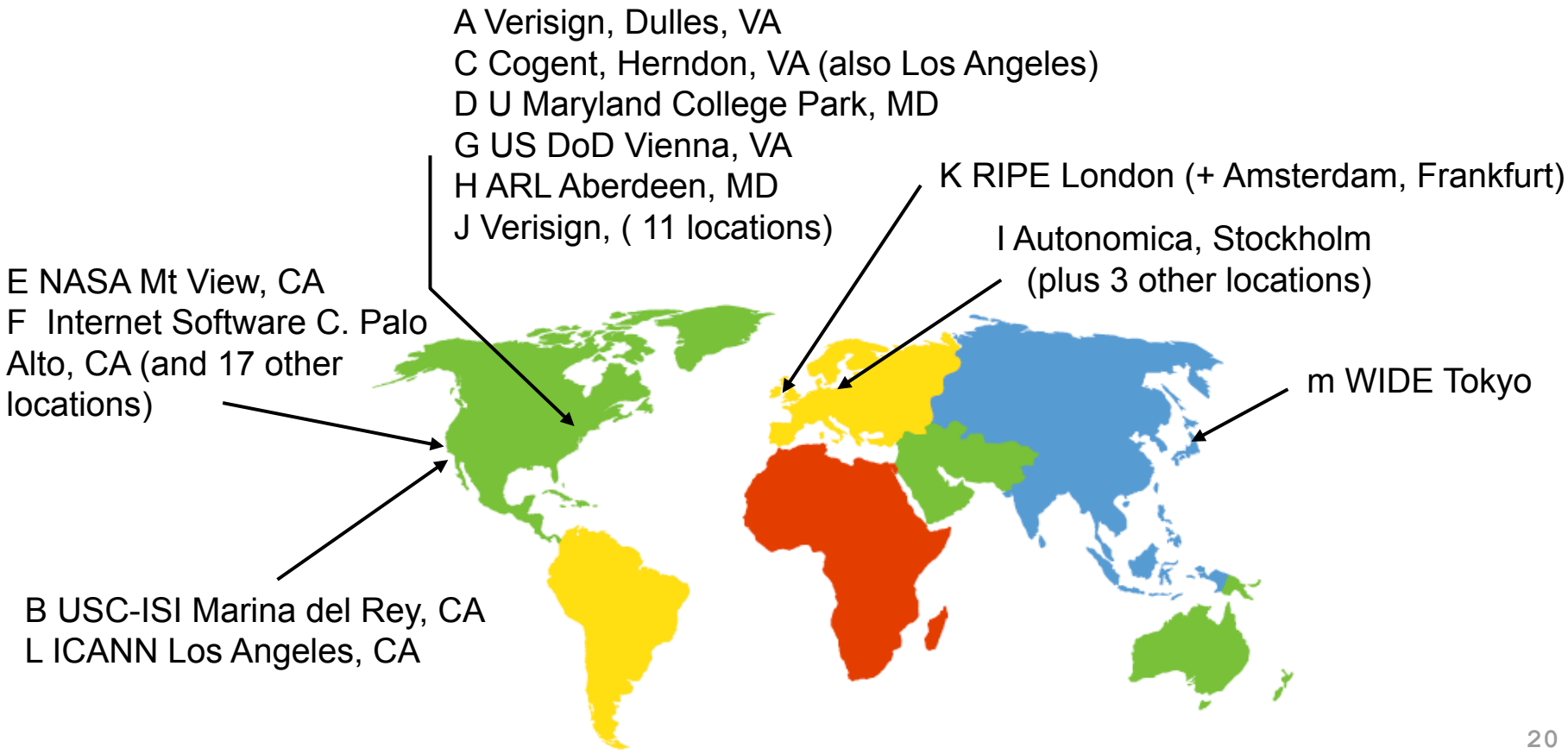
DNS Security

Hierarchical naming in DNS



DNS Root Servers

- 13 root servers (see http://www.root-servers.org/)
- Labeled A through M



DoS attacks on DNS Availability

- Feb. 6, 2007
  - Botnet attack on the 13 Internet DNS root servers
  - Lasted 2.5 hours
  - None crashed, but two performed badly:
    - g-root (DoD), l-root (ICANN)
    - Most other root servers use anycast

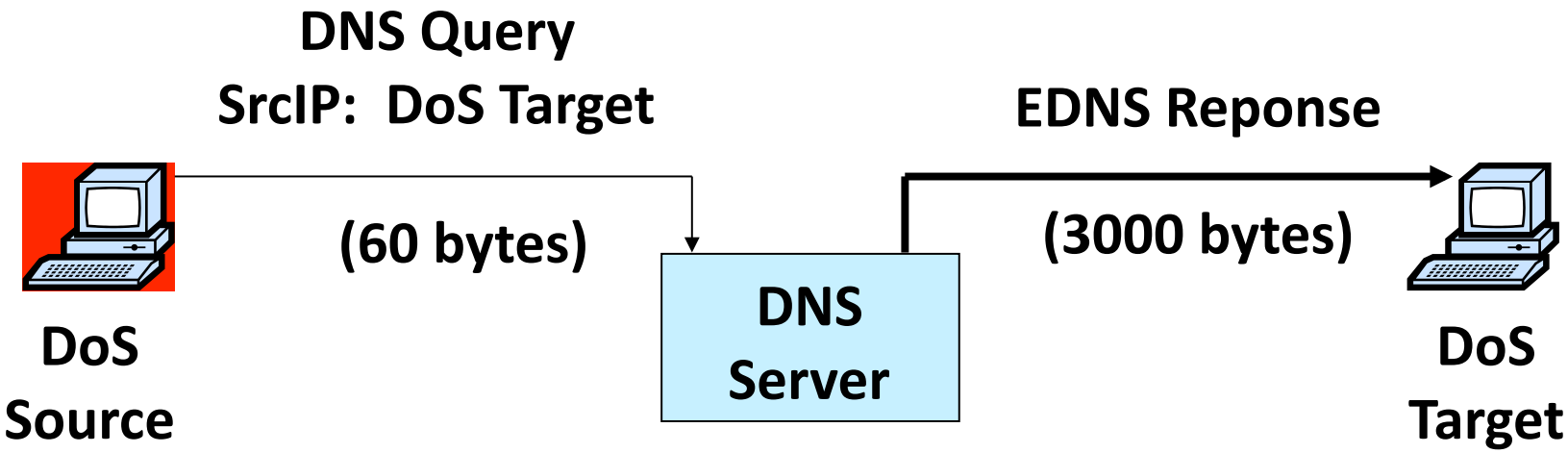
Defense: Replication and Caching

Letter	Old name	Operator	Location
A	ns.internic.net	VeriSign	Dulles, Virginia, USA
B	ns1.isi.edu	ISI	Marina Del Rey, California, USA
C	c.psi.net	Cogent Communications	distributed using anycast
D	terp.umd.edu	University of Maryland	College Park, Maryland, USA
E	ns.nasa.gov	NASA	Mountain View, California, USA
F	ns.isc.org	ISC	distributed using anycast
G	ns.nic.ddn.mil	U.S. DoD NIC	Columbus, Ohio, USA
H	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, USA
I	nic.nordu.net	Autonomica	distributed using anycast
J		VeriSign	distributed using anycast
K		RIPE NCC	distributed using anycast
L		ICANN	Los Angeles, California, USA
M		WIDE Project	distributed using anycast

source: wikipedia

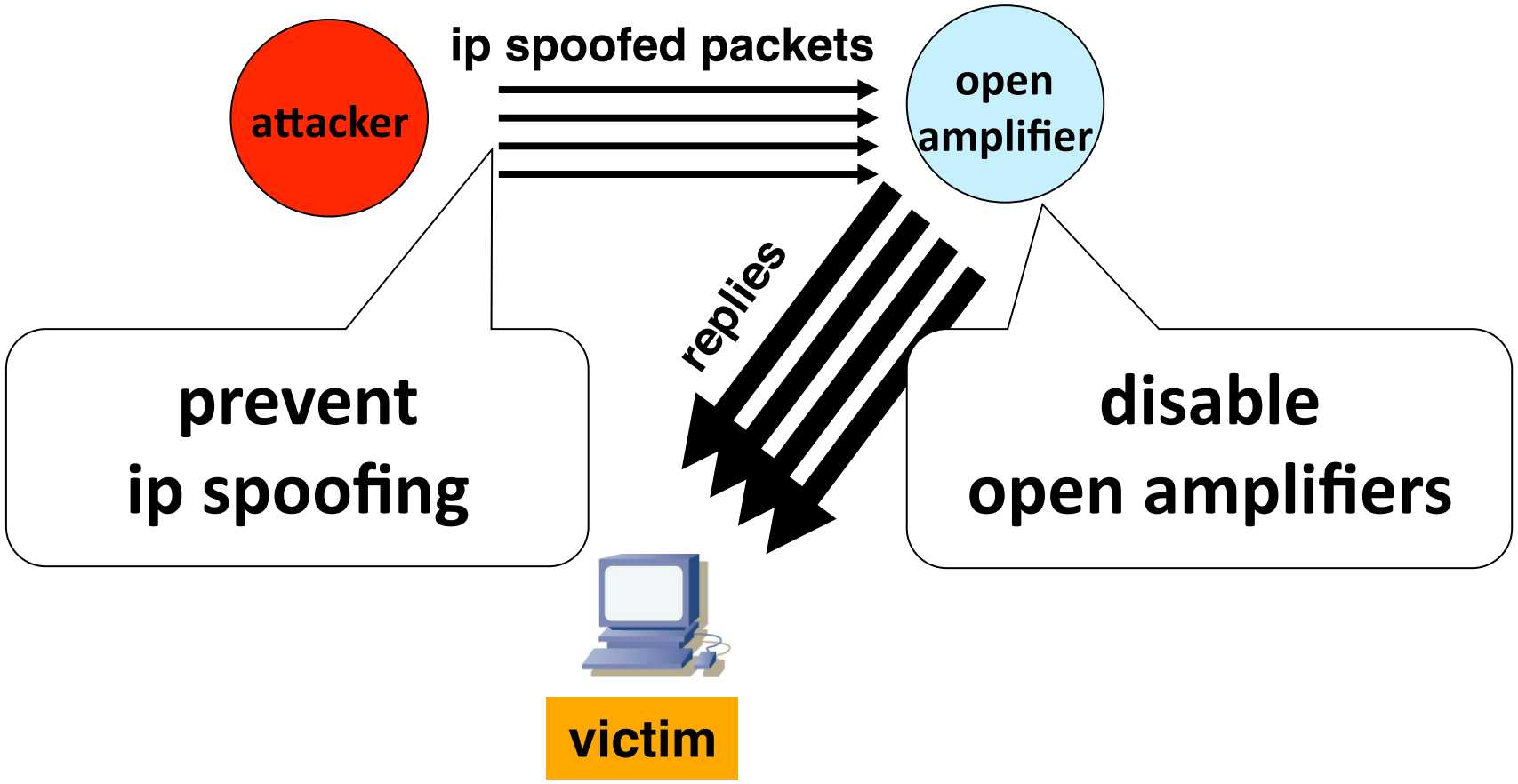
DoS attacks on end-host using DNS

×40 amplification



580,000 open resolvers on Internet (Kaminsky-Shiffman'06)

Preventing amplication attacks



DNS Integrity: Do you trust the TLD operators?

- If domain name doesn't exist, DNS should return NXDOMAIN (non-existant domain) msg
- Verisign instead creates wildcard DNS record for all .com and .net domain names not yet registered
  - September 15 – October 4, 2003
- Redirection for these domain names to Verisign web portal: "to help you search"
  - and serve you ads…and get "sponsored" search
  - Verisign and online advertising companies make money…

DNS Integrity: Was answer from authoritative server?

- DNS cache poisoning
  - Client asks for www.evil.com
  - Nameserver authoritative for www.evil.com returns additional section for (www.cnn.com, 1.2.3.4, A)
  - Thanks! I won't bother check what I asked for

DNS Integrity: Was answer from authoritative server?

- To prevent cache poisoning, client remembers domain and 16-bit request ID (used to demux UDP response)
- But…
- DNS hijacking
  - 16 bits: 65K possible IDs
    - What rate to enumerate all in 1 sec? 64B/packet
    - 64*65536*8 / 1024 / 1024 = 32 Mbps
  - Prevention: Also randomize the DNS source port
    - Windows DNS alloc's 2500 DNS ports: ~164M possible IDs
    - Would require 80 Gbps
    - Kaminsky attack: this source port…wasn't random after all

Let's strongly believe the answer! Enter DNSSEC

- DNSSEC protects against data spoofing and corruption
- DNSSEC also provides mechanisms to authenticate servers and requests
- DNSSEC provides mechanisms to establish authenticity and integrity

PK-DNSSEC (Public Key)

- The DNS servers sign the hash of resource record set with its private (signature) keys
- Public keys can be used to verify the SIGs
- Leverages hierarchy:
  - Authenticity of nameserver's public keys is established by a signature over the keys by the parent's private key
  - In ideal case, only roots' public keys need to be distributed out-of-band

Verifying the tree

Question: www.cnn.com ?