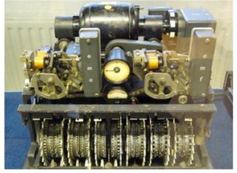


Naming Security

Mike Freedman

COS 461: Computer Networks

http://www.cs.princeton.edu/courses/archive/spr20/cos461/

Network Security

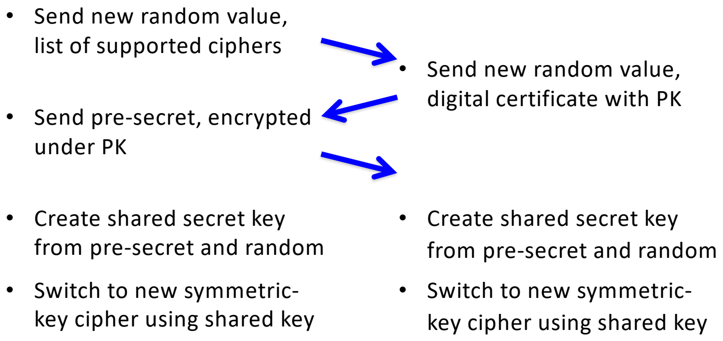
- Application layer
  - E-mail: PGP, using a web-of-trust
  - Web: HTTP-S, using a certificate hierarchy
- Transport layer
  - Transport Layer Security/ Secure Socket Layer
- Network layer
  - IP Sec
- Network infrastructure
  - DNS-Sec and BGP-Sec

Continuation of Lec 18

Transport Layer Security (TLS)

Based on the earlier Secure Socket Layer (SSL) originally developed by Netscape

TLS Handshake Protocol



- 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

TLS Record Protocol

- Messages from application layer are:
  - Fragmented or coalesced into blocks
  - Optionally compressed
  - Integrity-protected using an HMAC
  - Encrypted using symmetric-key cipher
  - Passed to the transport layer (usually TCP)
- Sequence #s on record-protocol messages
  - Prevents replays and reorderings of messages

Comments on HTTPS

- HTTPS authenticates server, not content
  - If CDN (Akamai) serves content over HTTPS, customer must trust Akamai not to change content
- Symmetric-key crypto after public-key ops
  - Handshake protocol using public key crypto
  - Symmetric-key crypto much faster (100-1000x)
- 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

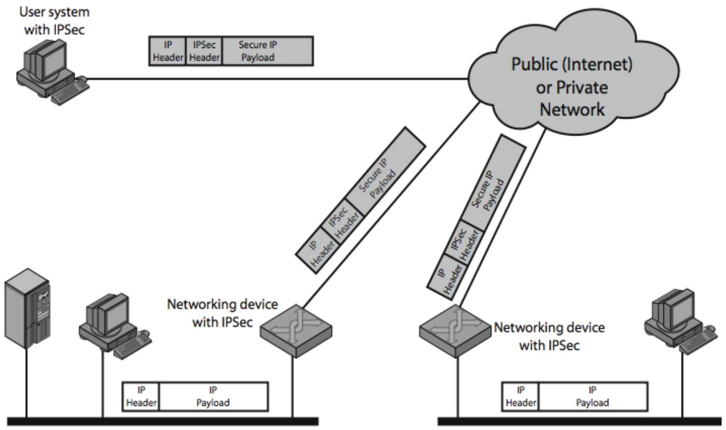
- There are range of app-specific security mechanisms
  - eg. TLS/HTTPS, S/MIME, PGP, Kerberos, …
- But security concerns that cut across protocol layers
- Implement by the network for all applications?

Enter IPSec!

IPSec

- General IP Security 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



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

13

IP Security Architecture

- Specification quite complex
  - 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

14

Encapsulating Security Payload (ESP)

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

15

Replay Protection is Hard

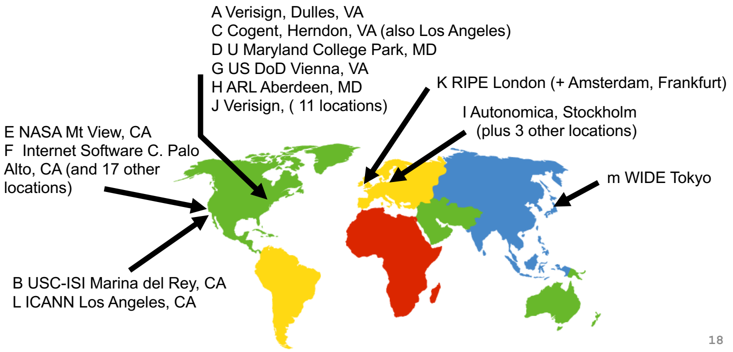
- Goal: Eavesdropper can’t capture encrypted packet and duplicate later
  - Easy with TLS/HTTP on TCP: Reliable byte stream
  - But IP Sec at packet layer; transport may not be reliable
- IP Sec solution: Sliding window on sequence #’s
  - All IPSec packets have a 64-bit monotonic sequence number
  - 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

16

DNS Security

DNS Root Servers

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



A Verisign, Dulles, VA
C Cogent, Herndon, VA (also Los Angeles)
D U Maryland College Park, MD
G US DoD Vienna, VA
H ARL Aberdeen, MD
J Verisign, (11 locations)

K RIPE London (+ Amsterdam, Frankfurt)

I Autonomica, Stockholm
(plus 3 other locations)

E NASA Mt View, CA
F Internet Software C. Palo Alto, CA (and 17 other locations)

m WIDE Tokyo

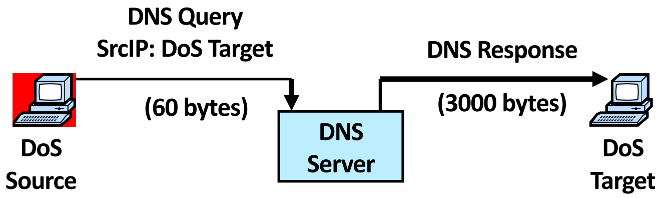
B USC-ISI Marina del Rey, CA
L ICANN Los Angeles, CA

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

Denial-of-Service Attacks on Hosts

×40 amplification



DNS Query
SrcIP: DoS Target

(60 bytes)

DNS Response

(3000 bytes)

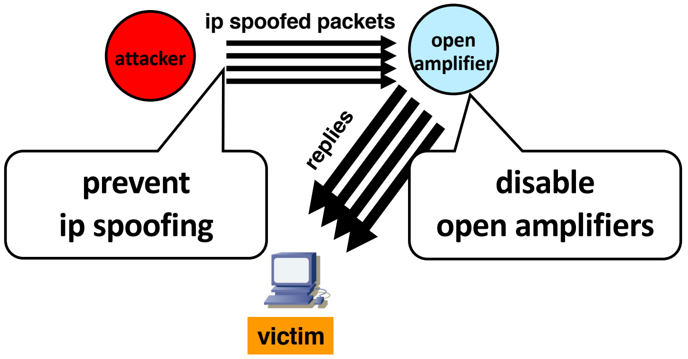
DoS Source

DNS Server

DoS Target

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

Preventing Amplification Attacks



ip spoofed packets

attacker

open amplifier

replies

prevent ip spoofing

disable open amplifiers

victim

23

DNS Integrity and the TLD Operators

- If domain name doesn't exist, DNS should return NXDOMAIN (non-existant domain) msg
- Verisign instead creates wildcard records for all .com and .net 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 $$

24

DNS Integrity: Cache Poisoning

- Was answer from an authoritative server?
  - Or from somebody else?
- 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

25

DNS Integrity: DNS Hijacking

- To prevent cache poisoning, client remembers:
  - The domain name in the request
  - A 16-bit request ID (used to demux UDP response)
- 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 DNS source port
  - Kaminsky attack: this source port… wasn't random

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

26

Let's strongly believe the answer! Enter DNSSEC

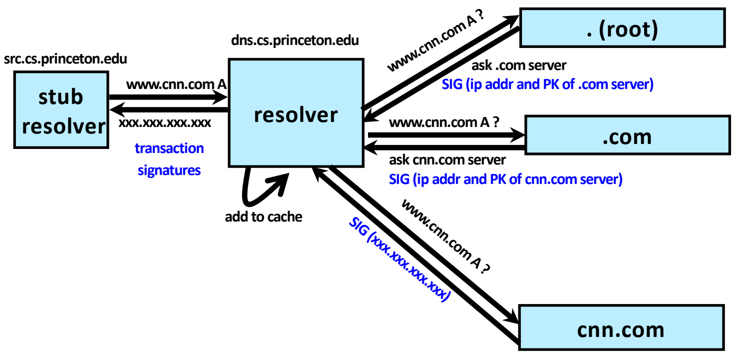
- DNSSEC protects against data spoofing and corruption
- DNSSEC also provides mechanisms to authenticate servers and requests
- DNSSEC provides mechanisms to establish authenticity and integrity

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 name server'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 ?



Conclusions

- Security at many layers
  – Application, transport, and network layers
  – Customized to the properties and requirements
- Exchanging keys
  – Public key certificates
  – Certificate authorities vs. Web of trust
- Next time
  – Interdomain routing security
- Learn more: take COS 432 next year!