EECS 388:
Introduction to Computer Security

Network Attacks and Defenses, Part 2

Feb 23, 2015

1

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 information 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, …)

2

Network protocols with built-in security support

- Many original network protocols did not originally implement security.
  - HTTP, SMTP, BGP, DNS, ARP, IP
- In many cases added on later (e.g. HTTPS)
- When developing secure protocols, assume that your network provides no security

3

Network Security

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

4

Broad types of network vulnerabilities

- Unencrypted Transmission
  - Passive attacker can eavesdrop on any communication
- No source authentication
  - Do not know the source of any packet you receive
- No integrity
  - Protocols do not prevent modification
  - assume that an attacker can modify headers and data
  - checksums in network protocols are to assure no corruption, not prevent attacks
- No built-in bandwidth control

5

Attack model

- Two general types of attackers we consider
  1. passive eavesdropper
  2. active main-in-the-middle (MITM)

6

Eavesdropping/MITM Attacks

- How can attacker intercept and read traffic?
- Wireless networks
  - open networks -- anyone in range can listen
  - secure protocols added
    - WEP -> now completely broken, do not use
    - WPA -> WPA2
- Wired networks
  - hub versus switch: broadcast vs. forward to a specific port
    - switch under attack becomes a hub when overloaded
  - possible to trick client into sending you traffic using ARP spoofing

7

Wired network tricks

- DHCP: how does a client know its gateway to the Internet?
- What is ARP (address resolution protocol) and how does it work?
- How do you trick a client into using you as a GW?
  - ARP spoofing, gratuitous arp

8

Network attacks

- What tools do people use?
  - wireshark, tcpdump, dsniff
- what can an attacker do in these situations?
  - capture content
    - sensitive data, session (cookies)
  - replay, drop, etc, etc.
  - modify content: infect executables, inject ads (evidence in real life even at ISP level)
  - What is NSA attack model here?
    - What can you learn if you passively read all data that goes through an ISP?

9

Defense against network attacks

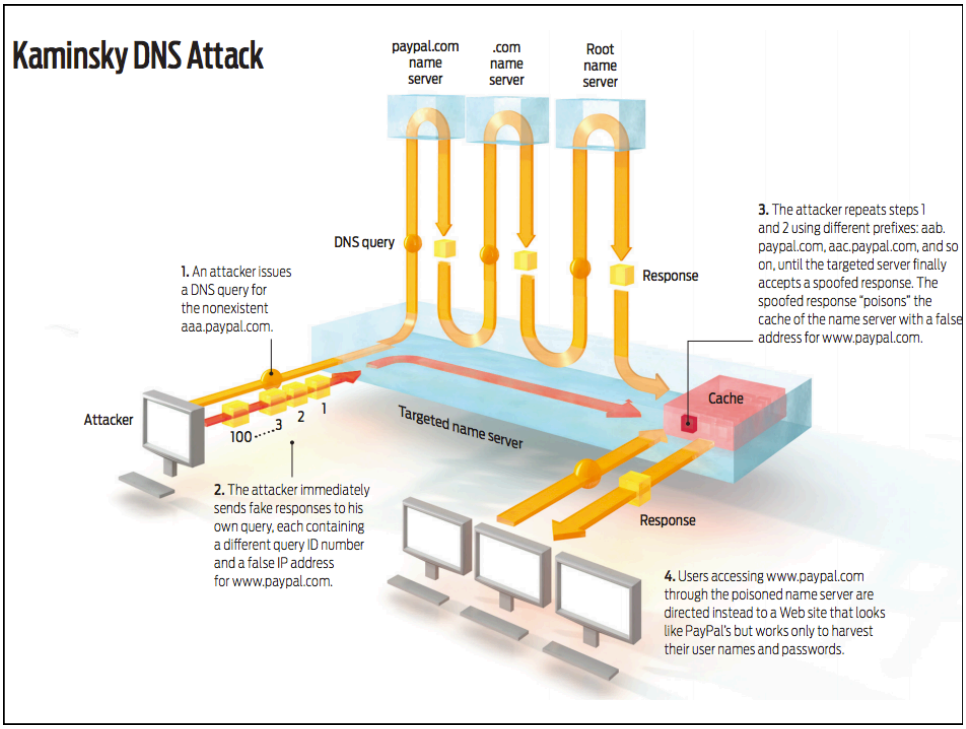
- secure protocols (e.g. TLS, SSH)
- VPNs: tunnel all content back to your home organization
- wireless: WEP, WPA, WPA2
- Anything else?

10

No Source Authentication in IP

- Cannot trust source IP
- RAW sockets: can send **anything**!
- egress filtering/bullet-proof hosting
- What about TCP? Why is this different than UDP?
  - what does 3-way handshake prevent?
- Kaminsky Attack against DNS.
  - only 2^16 transaction IDs
  - fixed with port randomization -> how many possibilities now? (about 134 million: 2^16*2^11)
- What else does IP spoofing allow?
  - DDoS reflection attacks

11



Weaknesses in Routing

- What is BGP?
  - How do you decide your best route?
- Sometimes wrong routes get announced
  - Pakistan Youtube announcement of 2012
    - Nothing prevents this from happening
- Why aren't we using signed routes?
- What is DNSSEC?

13

Exploits

- Virus, worms, trojans
  - virus: exploit that attaches onto another file or program
  - worm: self-propagating exploit
- How do worms work?
  - scanning for other vulnerable hosts, AIM/email contacts
- What do worms do?
  - blackmail (encrypt files) , steal data , corrupt files , send SPAM, carry out DoS attacks
- A permanently compromised system is more useful -> rise of the botnet
  - bot = servant

14

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?

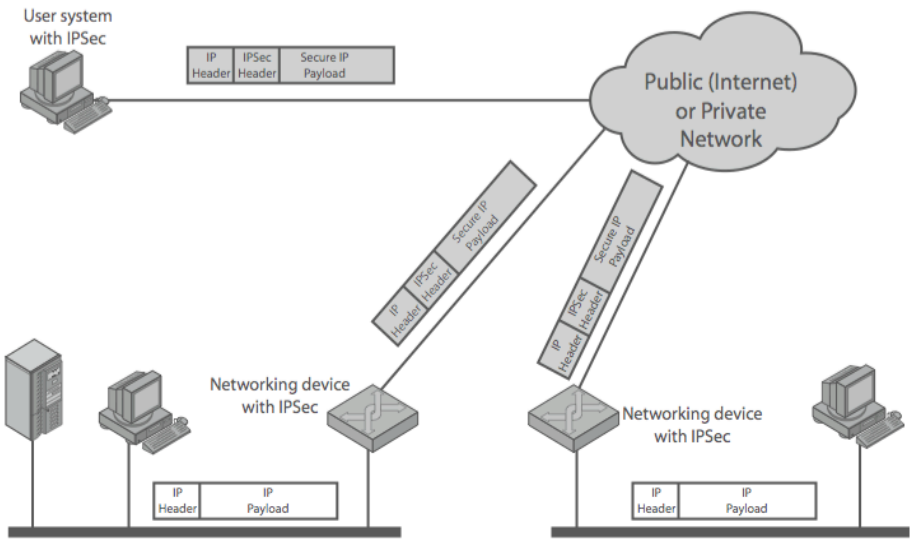
Enter IPSec!

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

17

IPSec Uses



18

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

19

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

20

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: Encrypts entire IP packet
  - Add new header for next hop
  - Good for VPNs, gateway-to-gateway security

21

Replay Protection is Hard

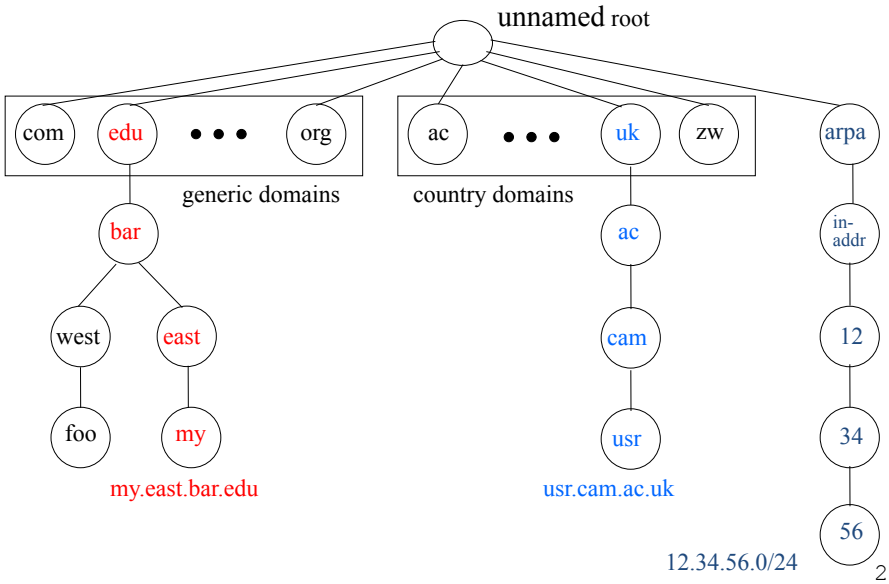
- Replay protection goal
  - Eavesdropper can't capture encrypted packet and duplicate later
- Easy with TLS/HTTP on TCP
  - Reliable byte stream
- Hard for IP Sec
  - Transport may not be reliable
  - Sketch of solution: sequence numbers on packets

22

DNS Security

23

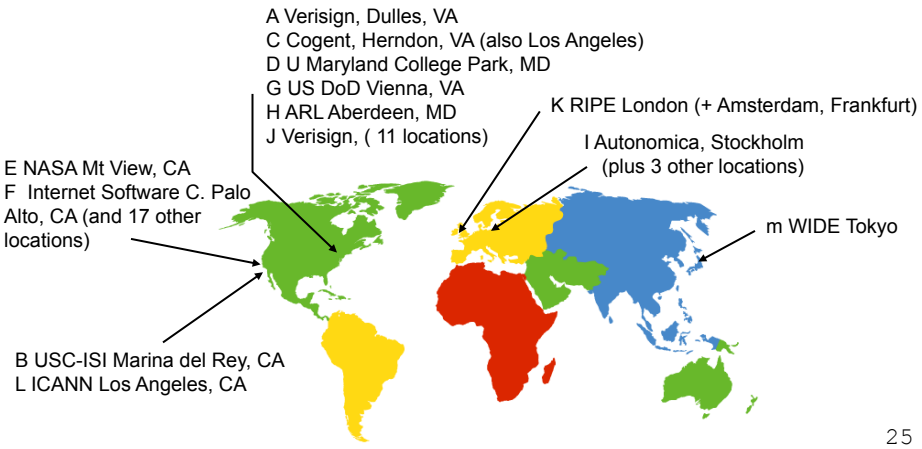
Hierarchical Naming in DNS



24

DNS Root Servers

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



25

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

26

Defense: Replication and Caching

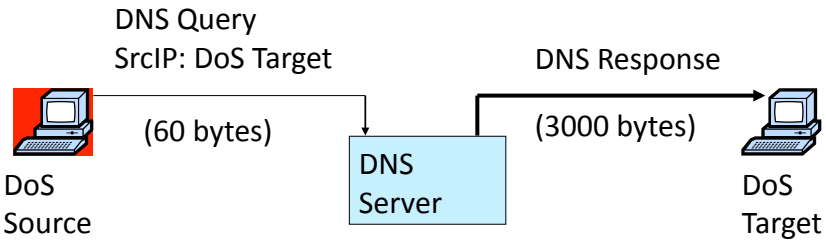
Letter	Old name	Operator	Location
A	ns.internic.net	VeriSign	Dulles, Virginia, USA
B	ns1.isi.edu	ISI	Marina Del Rey, California, USA
C	c.psi.net	Cogent Communications	distributed using anycast
D	terp.umd.edu	University of Maryland	College Park, Maryland, USA
E	ns.nasa.gov	NASA	Mountain View, California, 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

27

Denial-of-Service Attacks on Hosts

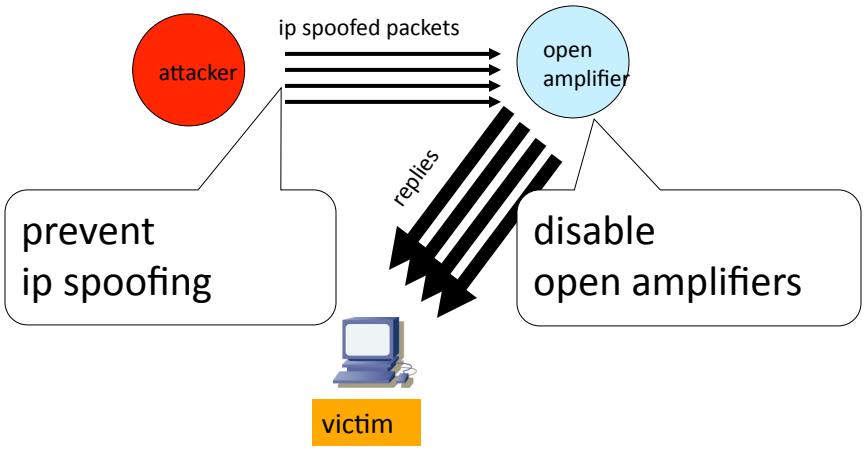
×40 amplification



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

28

Preventing Amplification Attacks



29

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 $$

30

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

31

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

32

DNS Sec

- Protects against data spoofing and corruption
- Provides mechanisms to authenticate servers and requests
- Provides mechanisms to establish authenticity and integrity

33

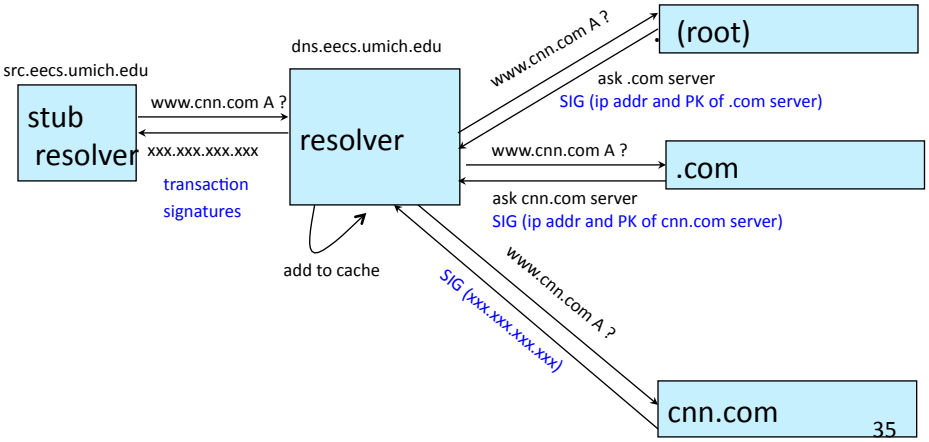
PK-DNSSEC (Public Key)

- 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

34

Verifying the Tree

Question: www.cnn.com ?



35

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

36