eecs489 COMPUTER NETWORKS

Lecture 13: Application-layer Security

At Which Layer to Put Security?

Link-oriented vs. end-to-end

Which layer?

- application layer: secure email (PGP), SSH, DNSSec
- above TCP: Secure Socket Layer (SSL) Netscape, 1994, used by HTTPS
- IPsec: Authentication Header (AH) and Encapsulating Security Payload (ESP)

Pretty Good Privacy (PGP)

Internet e-mail encryption scheme, de facto standard

Uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described previously

Provides secrecy, sender authentication, data integrity

Inventor, Phil Zimmerman, was target of 3-year federal investigation

A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob: IOU $100.

Sincerely yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ
+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

SSH [RFC 4251]

Establishes a secure channel between a local and a remote computer

Uses public-key cryptography to authenticate remote host and user

Provides confidentiality and data integrity with symmetric cryptography and digital signature

Authentication

- password-based, or
- public-key based
  - public and private key pair generation using `ssh-keygen`

Secure Sockets Layer (SSL)

Transport layer security for TCP-based apps

Used between Web browsers and servers (HTTPS)

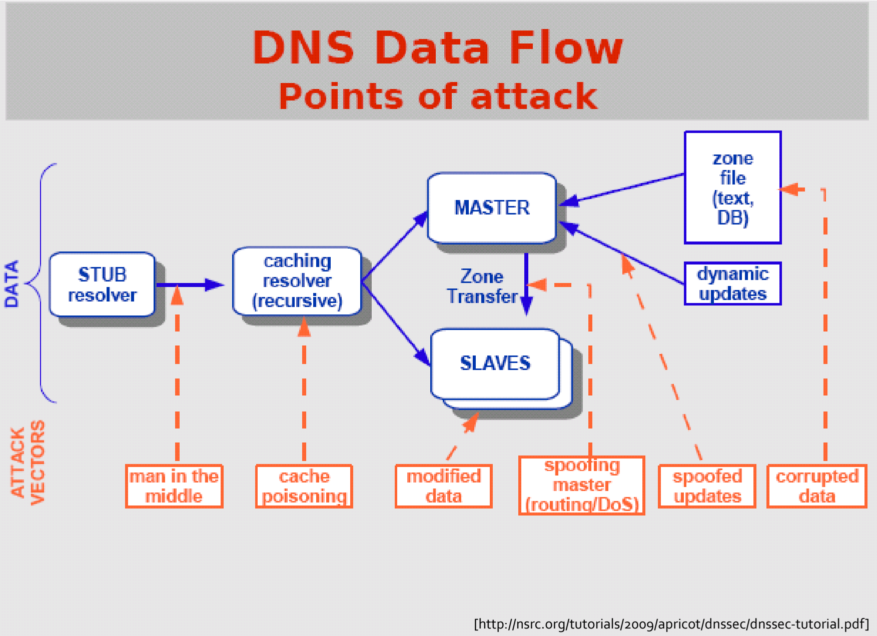
Security services:

- server authentication (is it really your bank's server?)
- data encryption (keep card# secret, transaction not altered)
- client authentication (optional)

SSL can be used for non-Web applications, e.g., IMAP

SSL v3 is IETF's Transport Layer Security (TLS)

SSL Programming Tutorial (on course's Links page):
`http://h71000.www7.hp.com/doc/83final/ba554_90007/ch04s03.html`



DNS Data Flow
Points of attack

[http://nsrc.org/tutorials/2009/apricot/dnssec/dnssec-tutorial.pdf]

DNSSEC

Security services provided:

- authenticates servers and requests
- protects against data spoofing and corruption

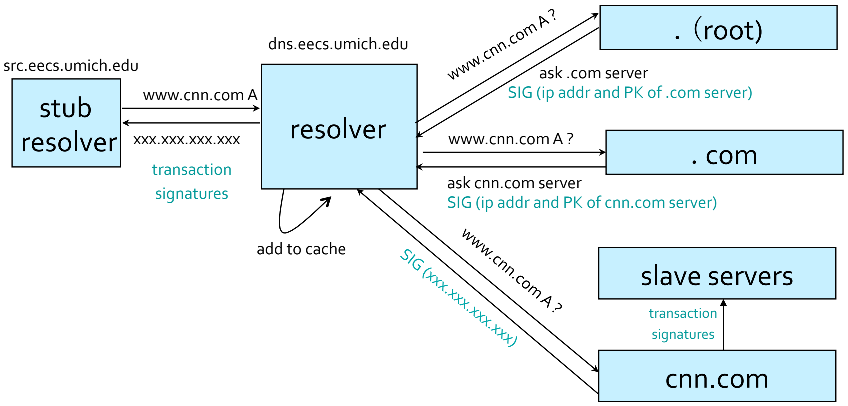
PK-DNSSec:

- nameservers sign the hash of resource records with private keys
- nameservers' public keys used to verify the signatures
- leverages the DNS hierarchy as PKI, to establish chain of trust:
  - a nameserver's public key is signed by the parent's nameserver, e.g., umich.edu nameserver signs the eecs.umich.edu nameserver's public key
  - ideally, only roots' public keys need to be distributed out-of-band

[Rexford]

Verifying the Tree

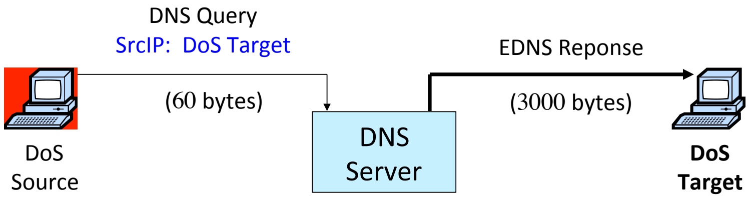
Resolve: `www.cnn.com`



[Rexford]

DNS as DDoS Tool

DNS Amplification Attack (40× amplification)



580,000 open resolvers on Internet [Kaminsky-Shiffman '06]

EDNS: Extension Mechanism for DNS, allows for larger than 512-byte UDP packet

[Rexford]

Root-level DNS DDoS Attack

Feb. 6, 2007:

- botnet DDOS attack on the 13 Internet DNS root servers
- lasted 2.5 hours;
  plus, 3.5 hours later, another one that lasted 5 hours
- no root server crashed, but two performed badly (slowly):
  - G-root (DoD), L-root (ICANN)
  - F-root and M-root also saw heavy traffic, but mitigated by use of anycast

[Rexford]

Limitations of DNS-based Failover

DNS failover/load balancing: via multiple A records

```
;; ANSWER SECTION:
www.cnn.com.            300    IN     A      157.166.255.19
www.cnn.com.            300    IN     A      157.166.224.25
www.cnn.com.            300    IN     A      157.166.226.26
www.cnn.com.            300    IN     A      157.166.255.18
```

If server fails, service unavailable for TTL

- if TTL set very low: extra load on DNS
- anyway, even if TTL at resolver is set low,
  browsers still cache DNS mappings ☹

What if root NS fails? All DNS queries take > 3s?

[Rexford]

Motivation for IP Anycast

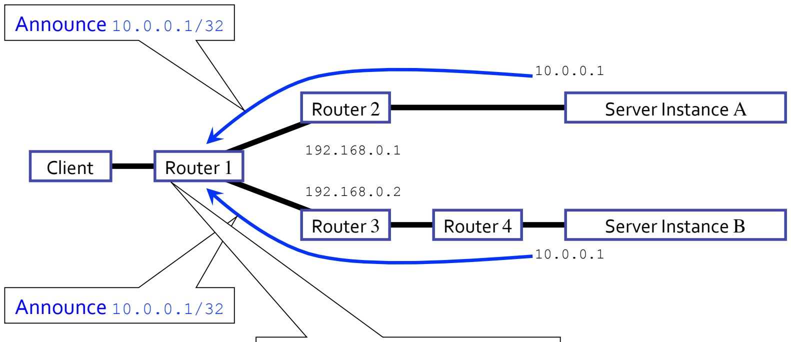
If an IP address can represent many servers, prefer to do load-balancing/failover at the network layer, rather than the application layer (DNS)

IP anycast is appealing because it simply re-uses existing protocols:

- multiple instances of a service share the same IP address
- each instance announces the same IP address/prefix in the routing protocol
- routing infrastructure directs packets to nearest instance of the service
  - can use the same selection criteria used to populate forwarding tables
- no special capabilities in servers, clients, or network

[Rexford]

IP Anycast in Action

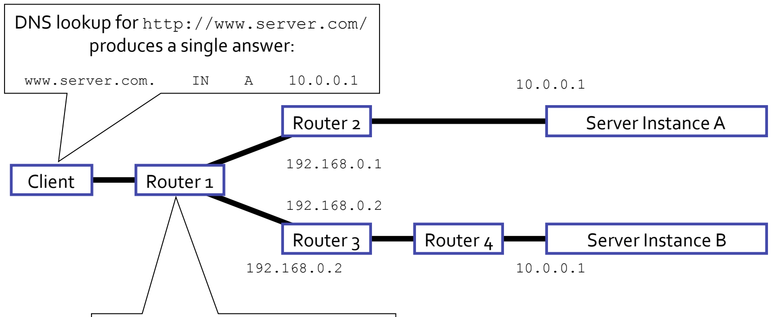


Routing Table from Router 1:

Destination	Mask	Next-Hop	Distance
192.168.0.0/29		127.0.0.1	0
10.0.0.1	/32	192.168.0.1	1
10.0.0.1	/32	192.168.0.2	2

[Rexford]

IP Anycast in Action



DNS lookup for `http://www.server.com/` produces a single answer:

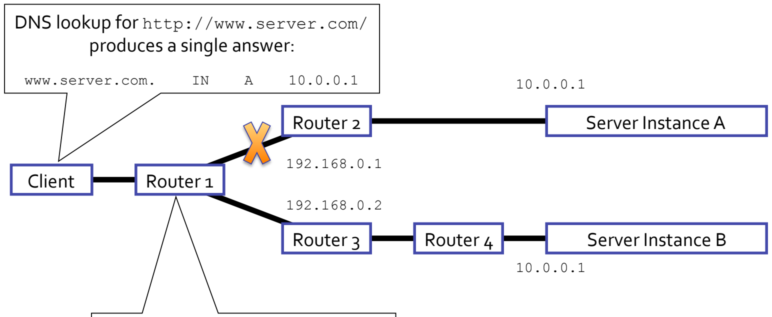
```
www.server.com.    IN    A    10.0.0.1
```

Routing Table from Router 1:

Destination	Mask	Next-Hop	Distance
192.168.0.0/29		127.0.0.1	0
10.0.0.1	**/32**	**192.168.0.1**	**1**
10.0.0.1	/32	192.168.0.2	2

[Rexford]

IP Anycast Failover



DNS lookup for `http://www.server.com/` produces a single answer:

```
www.server.com.    IN    A    10.0.0.1
```

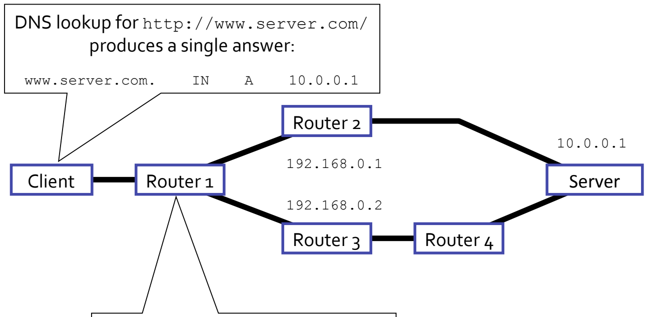
Routing Table from Router 1:

Destination	Mask	Next-Hop	Distance
192.168.0.0/29		127.0.0.1	0
~~10.0.0.1~~	~~/32~~	~~192.168.0.1~~	~~1~~
10.0.0.1	**/32**	**192.168.0.2**	**2**

[Rexford]

IP Anycast in Action

From client/router perspective, topology could as well be:



DNS lookup for `http://www.server.com/` produces a single answer:

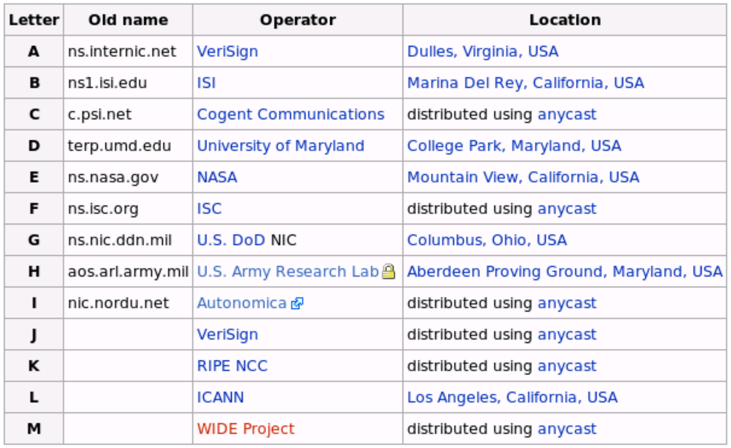
```
www.server.com.    IN    A    10.0.0.1
```

Routing Table from Router 1:

Destination	Mask	Next-Hop	Distance
192.168.0.0/29		127.0.0.1	0
10.0.0.1	/32	192.168.0.1	1
10.0.0.1	/32	192.168.0.2	2

[Rexford]

DNS Root Servers and IP Anycast



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

[wikipedia]

Downsides of IP Anycast

Many Tier-1 ISPs' ingress routers block prefixes > /24

- work around: publish a /24 for each anycast address ⇒ poor address space utilization

Scales poorly with number of anycast groups

- each group needs entry in global routing table

Not trivial to deploy

- need to obtain an IP prefix and AS number
- must speak BGP

Subject to the limitations of IP routing

- no notion of load or other application-layer metrics
- convergence time can be slow (as BGP or IGP converges)

[Rexford]

Downsides of IP Anycast

Failover doesn't work with TCP

- TCP is stateful ⇒ other server instances will just respond with RSTs
- anycast may react to network changes, even though server is still online

Currently, only root name servers (UDP) are anycasted, nothing else is

[Rexford]

Do You Trust the TLD Operators?

Redirection of all .com and .net domain names not yet registered by others to "search page"

- Versign's SiteFinder "helps you search" . . . and serves you ads...and helps you get "sponsored" results
- February 2004: Verisign sued ICANN for having violated antitrust laws by preventing it from adding "features" to Top Level Domains

[Rexford]