CSCI 1800 Cybersecurity and International Relations

Internet Naming and Routing

John E. Savage
Brown University
Outline

• The Domain Name System (DNS)
  – Protecting the DNS from attacks
• History of Naming Policy
• Internet routing
  – The Border Gateway Protocol (BGP)
  – Protecting BGP from attacks
• Routing Policy
The Domain Name System
The Domain Name System (DNS)

- DNS is the “telephone directory” for the Internet.
- DNS is a distributed, hierarchical, naming system.
- DNS translates host names into IP addresses.
  - www.example.com translates to the addresses 192.0.32.10 (IPv4) and 2620:0:2d0:200::10 (IPv6).
- Names are hierarchical
  - .com is a top-level domain
  - example.com is a sub-domain of .com
  - aaa.example.com is a sub-domain of example.com
Domain Names

• Four types of top-level domain:
  – **Country codes** (2 letters, e.g. .ca, .au, .de, .hu, .uk)
  – **Sponsored codes** (e.g. .edu, .coop, .gov, .mil)
  – **Generic top level** (e.g. .com, .info, .net, .org, .pro)
    - 1,544 active gTLDs, e.g. .IBM, .NYC, .REISE,, PHARMACY
  – **Test** (for testing internationalized domain names)

• Domain names are registered and assigned by **domain-name registrars**† who are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN).

† See http://www.icann.org/registrar-reports/accredited-list.html
Organization of the DNS

- The DNS resolves names into IP addresses.
- Root name servers hold IP addresses for top-level name servers, e.g. .edu, .uk. and .net.
- Top-level name servers hold IP addresses for sub-domain name servers, e.g. example.com.
Querying the DNS

• Local caches hold records mapping domain names to IP addresses. If the time to live for a domain expires, must do another lookup.

• When local cache is queried for a name that is not in the cache, it is fetched via root servers and the cache is updated with the new mapping.

• Root server is asked for IP address of authoritative name server holding requested top-level domain.

• A top-level server is asked for the IP address of the sub-domain address, etc., until found.
Poisoning the DNS Cache

- Eve sends a user to the **wrong website**:  
  - She sends local server request for name not in cache from outside the local server’s network.  
  - Local server makes request to authoritative server $S$, providing a 16-bit ID. The server responds after delay.  
  - Eve guesses 16-bit ID and before response arrives from $S$, she sends incorrect answer (resource record with IP address) to the local server.  
  - If ID guess is accurate, DNS accepts Eve’s answer and ignores later input from authoritative server.
Protecting DNS Caches

• Problems in protecting DNS caches:
  – 16 bit IDs on DNS queries are short, too easily guessed
  – Note: this can be done even if a domain name has not been officially created.

• How to harden DNS caches:
  – Only allow updates from within local network.
    • If update is from outside local network, don’t trust it.
  – Provide port number when querying root zone and require that responses have correct port no. and ID.
  – Number of choices goes from $2^{16}$ to $\sim 64,000 \times 2^{16}$. 
Public Key Cryptography

• Alice (and Bob) have public and private keys PrvA, PubA (PrvB, PubB)
• Bob encrypts a message for Alice using her public key PubA. She decrypts it using her private key PrA.
• Alice sends messages to Bob the same way.
• Using this method, they can communicate in secrete.
Cryptographic Signing of Messages

Hash function maps data of arbitrary size to fixed size. Should be difficult to invert.

Signer’s public key is attached.

If the hashes are equal, the signature is valid.
DNSSEC: Security Extensions to DNS

• To provide trust, under DNSSEC DNS replies are cryptographically signed using public key encryption.
  - A message identifying sender is encrypted by him/her.
  - Public decryption key is used to verify author.
• Difficult for an attacker to spoof a reply.
• Source has the authority granted by issuer of keys
• Chain of trust here. Ultimately, must trust root.
• DNSSEC slowly being installed.
History of Naming Policy
Names Matter

• Authority to decide mapping from domain names to IP addresses matters a lot.
  – Domain names can be expensive, insurance.com cost $35.6 million in 2010 – fees paid to ICANN
  – They involve trademark issues
  – Suffixes such as .xxx, .sucks may be controversial.

• Who should have the authority to decide on ownership and assignment of domain names and IP addresses? ICANN or some other body?
Early Days

• In early 1970s naming system consisted of small file called “hosts.txt” placed at each host.
• In 1978 Jon Postel of USC was given no-bid USG contract to run Internet naming & numbering
• By mid 1980s Postel and SRI had created the modern domain name system.
• By 1990s DoD required contract bidding.
Commercialization of Internet

• In May 1990 Government Systems, Inc. wins contract to administer the root (Postel’s job) which it hands over to Network Solutions.

• In 1995 Network Solutions wins right to charge for registering domain names.

• Domain names become very popular and Network Solutions earns fabulous profits.

• Engineers disenchanted.
First Attempt at Capturing the Root

• In June 1991 Vint Cerf and others announce formation of Internet Society (ISOC).
  – Goal: Provide Internet governing structure, home, and funding that is independent of USG
  – Mueller: An attempt to self-privatize the Internet.
• In March 1995 Aiken of US Energy Dept. asks ISOC what authority it is claiming.
• Cerf responds implying that it is preferable that Internet be run by ISOC, not USG
Role of ISOC

• ISOC writes “Generic Top-Level Domain Memorandum of Understanding” (gTLD-MoU), which looks like international legal document, designed to give Internet policy to ISOC.

• International Telecommunications Union agreed to recognize it and be repository for gTLD-MoU.
  – Formal signing ceremony on May 1, 1997
  – Group of ISPs release tentative Internet Constitution
United States Reacts

• Ira Magaziner (‘69), USG Internet policy czar, responds
  – Commercialization of Internet will be boon to US
  – To foster growth, Internet must not be regulated
  – It must be predictable and secure
  – Only the US has ultimate authority over Internet’s deep structure including naming and routing
  – USG needed to ensure Internet growth and independence

• Issue comes to head with ISOC at 12/1997 DC meeting at which Magaziner states USG case forcefully.

• 1/28/1998 Postel protests by seizing control of root but relents when Magaziner issues legal threat to USC.
ICANN Created

- Internet Corporation for Assigned Names and Numbers (ICANN), non-profit organization, is created in 1998 to oversee Internet-related tasks
  - ICANN coordinates
    - Domain name system (DNS)
    - IP addresses, allocation of addresses to Internet registrars*
    - Management of root servers and top-level domains
    - Numbers assigned to protocols and autonomous systems
  - Ensures Internet stability and security
  - Consults broadly with users, technologists, govs.

* See http://www.icann.org/registrar-reports/accredited-list.html
Major Internet Governance Event

• On 3/14/14 USG announced “its intent to transition key Internet domain name functions to the global multi-stakeholder community”* if the following goals are met:
  – “Support and enhance the multi-stakeholder model,
  – Maintain the security, stability, and resiliency of Internet DNS,
  – Meet the needs and expectations of the global customers and partners of the IANA services; and
  – Maintain the openness of the Internet.”

• No transition if the role of USG is replaced by another government or an intergovernmental organization.

Conclusion of ICANN Negotiations

• After substantial revision of its bylaws, ICANN allowed to operate without USG supervision.
• However, ICANN and its new subsidiary, PTI, are US corporations subject to US law.
Internet Routing
Autonomous System (AS)

• Each AS is a separately managed network.
• An AS is connected to a few other ASes.
• ASes decide routes packets will follow.
Intra-Network Routing

AS 1234

Intra-Network Protocols
Inter-Network Routing via BGP
Border Gateway Protocol† (BGP)

• AS announces **prefix** of IP addresses reachable via it
  – E.g. **Prefix** 129.6.0.0/16 denotes 32-bit addresses starting with first 32-16 bits of 129.6.0.0 or 10000001.

• An announcement shows destination & path.
  <129.6.0.0/16 reachable via AS-Path: [AS42,AS3,AS701,AS49]>

• (129.6.0.0/16  - first 16 bits of block are fixed.)

• An AS router uses announcements to specify which **Internet Exchange Point (IXP)** to use to send a packet to a destination.

Some Types of BGP Announcements

- **Offer to carry traffic** to a set of destinations. An AS announces paths to neighbors.

- **Withdrawal of offers.**

- **Changes in paths** for a set of destinations.

- **New path attributes.**
Some Router Actions

• Checks paths for loops.

• Impose policy constraints.
  – E.g. Packets starting in Canada must travel in Canada.

• Compute/update best paths to destinations.

• Withdraw a destination when told to do so.

• Propagate its routes to peers
BGP Threats and Risks

• **Routers are too trusting** – attackers may issue announcements that result in
  – *Eavesdropping*, delay and/or disruption of traffic.
  – *Redirection* of traffic to malicious endpoint.
  – *Hijacking* (temporarily take over) address space to launch spam, run attacks, etc.
  – *Denying* service – make an entire network disappear
Some Major BGP Routing Outages

- Feb 24, 2008 – For about two hours connection to YouTube was lost around the world due to action by Pakistan Telecom
- April 8, 2010 – For 20 mins. routes to 32,000+ networks were sent to China Telecom, taking Facebook, Twitter, etc. offline.
- November 7, 2016 – Twitter went dark for about 30 minutes
- These and many other examples illustrate fragility of BGP.
- Forbes (4/9/10) called BGP announcements cybernukes.
Spamming

- Spammers – biggest abusers of announcements
  - BGP used to “advertise” a route for a block of addresses that were allocated but unassigned.
  - Large amount of spam is sourced from bogus block
  - BGP then used to withdraw the route to the block
  - Spamming source completely disappears.
  - Untraceable, can’t be audited, not prosecutable.
Clicker Class Participation

• What does the prefix 192.2.4.5/8 means?

A. Addresses 192. -.-.-
B. Addresses -.-.-.- 5

Here – refers to an arbitrary integer in
{0, 1, 2, 3, ..., 255}
Routing Policy
Making BGP More Robust

- Many efforts made to make BG more robust.
- Latest: Resource PKI (RPKI), cryptographically signed BGP announcements.
- Would increase level of trust.
- Introduces many new issues:
  - Trust anchor has the power to withdraw certificates of trust and shut down networks.
  - Should there be one trust anchor?
  - Do we trade trust for centralized Internet control?
A Tragedy of the Commons

• BGP routing space is simultaneously
  – *Everyone's problem*, because it impacts the stability and viability of the entire Internet, and
  – *No one's problem*, in that no single entity manages this common resource

• Who’s responsible for reliability of the network?
  – End customers?
  – Service providers?
  – Somebody else?
Review

• The Domain Name System (DNS)
  – Protecting the DNS from attacks
• History of Naming Policy
• Internet routing
  – The Border Gateway Protocol (BGP)
  – Protecting BGP from attacks
• Routing Policy
DNS Attacks

• DNS cache poisoning
  – Attacker puts incorrect mapping into a cache
  – May be used to redirect traffic to a malicious site

• Sub-domain DNS cache poisoning
  – Attacker asks to resolve non-existing name, such as aaa.example.com.
  – Cache doesn’t have it. Attacker guesses cache ID and poisons cache with phony record. Adds optional glue record at same time.
    • Glue record points to attacker’s address.
  – Attempts to resolve subdomain of example.com use glue record, thereby directing traffic to attacker.
  – To guess cache ID, attack multiple times with phony subdomains until a correct cache ID is guessed.