Understand the history, actors, and issues in the DNS Ecosystem.
Questions from Last Class

Does Safari use the OS Stub Resolver? -- Yes.

Why not just return an IP address for a nameserver? -- Nuanced.

What recursive resolver does Stanford use? -- 8.8.8.8 only for visitor network.

RCODE for responses -- Implementation and network dependent

When is an answer authoritative? -- Flags in the header + Delegation
DNS Query Life Cycle Recap

1. **Client Stub Resolver** (IP: 137.110.222.10)

2. **CPE Forwarder** (IP: 137.110.222.10)

3. **Recursive Resolver**

   - Ask ns[1,2].ucsd.edu
   - sysnet.ucsd.edu?
   - 137.110.222.10

4. **TLD Authoritative NS**

   - sysnet.ucsd.edu?
   - Ask edu Auth NS

5. **Root Authoritative NS**

   - sysnet.ucsd.edu?
Discussion: Integrity

Can DNS responses be modified?
Can one tell if the responses are modified?
Does it matter if they are modified?
Discussion: Integrity

Can DNS responses be modified?
Can one tell if the responses are modified?
Does it matter if they are modified?
SSL Certificates to the rescue(?)!
DNS Interception

- Intercept DNS Queries
  - Exploit lack of integrity check on DNS responses

- Interception by whom?
  - ISPs
  - Governments
  - Companies

- Interception where?
Where can Interception occur?
DNS Interception: Why?

- Censorship
- Parental Controls/Firewalls/Security
- Advertising
  - Take over NXDOMAIN queries.
Discussion: Confidentiality

Are DNS queries confidential?
QName Minimization
Encryption: DoH/DoT

DNS over HTTPs
DNS over TLS
Encrypted queries to recursive resolver?
Confidentiality? From whom?
What about ECS?
Mystery #1: Nameserver Change Whodunnit?

White County, Georgia Official Domain: whitecounty.net

whitecounty.net

Parent Zone
ns1.hemc.net
ns2.internetemc.com

Child Zone
ns1.hemc.net
ns2.internetemc.com
Mystery #1: Nameserver Change Whodunnit?

White County, Georgia Official Domain: whitecounty.net

Parent Zone
ns1.hemc.net
ns2.internetemc.com

Child Zone
ns1.hemc.net
ns2.internetemc.com

Parent Zone
ns1.hemc.net
ns2.internetemc1aj2tkdy.biz

Child Zone
ns1.hemc.net
ns2.internetemc.com

July 01, 2019
Mystery #2: DROPTHISHOST Anomaly

33% of nameservers in the last 9 years ending in .biz are dropthishost-xxxx.biz
Mystery #2: DROPTHISHOST Anomaly

33% of nameservers in the last 8 years ending in .biz have dropthishost substring

Parent Zone
ns1.knowanewbie.com
ns2.knowanewbie.com

Jan 09, 2016

Parent Zone
dropthishost-e06eed78-1098-41db-9964-f13d6f032d52.biz
dropthishost-e6a1816-88a8-455b-b20d-e4aeef79ed9e.biz
DNS Administration: A Simplified History

● Before 1999, Department of Commerce, SRI-NIC, Network Solutions
● After 1999, Department of Commerce identified Internet Corporation for Assigned Names and Numbers (ICANN) to administer the DNS
  ○ gTLDs have to obey rules set forth by ICANN
  ○ ccTLD rules are determined by each country
● Four Principles
  ○ Competition
  ○ Representation
  ○ Stability
  ○ Private, Bottom-Up Coordination
Actors in the DNS Ecosystem

- DNS Root
- ICANN

TLD
- com.
- edu.
- xyz.
- us.

Registries

Domain
- google.com.

Registrant

Subdomain
## Actors in the DNS Ecosystem

<table>
<thead>
<tr>
<th>DNS Root</th>
<th>TLD</th>
<th>Domain</th>
<th>Subdomain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>edu.</td>
<td>Registrant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>xyz.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>us.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICANN</td>
<td>Registries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Questions:**
- Domains purchased through registrars?
- What role do registrars play?
Actors in the DNS Ecosystem

DNS Root

ICANN

TLD

com.
edu.
xyz.
us.

Registries

Domain
google.com.

Registrant

Subdomain

* Not all TLDs have registrars. .gov and .edu do not have registrars.

Domains purchased through registrars?

What role do registrars play?
Actors in the DNS Ecosystem: DNS Configuration

Parent Zone

Registry

Registrar

Registrant

Child Zone
How do updates to DNS Configuration propagate?
Actors in the DNS Ecosystem: DNS Configuration

How do updates to DNS Configuration propagate?

Parent Zone

Registry

Registrar

Child Zone

Registrar

Registrant

EPP

Web Portal / API
Potential Theories on the Mysteries?
Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

Registry  Registrar  Registrant

Child Zone

EPP  Web Portal / API
Extensible Provisioning Protocol: Mental Model

TLD DNS Configuration == Database

EPP == API
EPP Mental Model
EPP Mental Model
EPP Mental Model

foo.com

foo.com

ns1.foo.com

ns2.foo.com

bar.com

ns1.bar.com

Registrar A

Registrar B

Subordinate Relationship

Delegated Nameserver

Host Object

Domain Object

Host Object
EPP Mental Model

foo.com expires.

Registrar A  Registrar B

Subordinate Relationship  Delegated Nameserver

Host Object  Domain Object  Host Object
EPP Mental Model
Limitations on Host Object Renaming

**Local Consistency:** If renamed within the same TLD the domain object must exist. However, EPP cannot check external references.

- ns1.foo.com **CANNOT** be renamed to ns1.blahblah.com if blahblah.com does **NOT** exist
- ns1.foo.com **CAN** be renamed to ns1.blahblah.biz even if blahblah.biz does **NOT** exist
EPP Mental Model

foo.com expires.

Registrar A

Registrar B

Host Object

Domain Object

Host Object

Subordinate Relationship

Delegated Nameserver
Limitations on Host Object Renaming

Registrar A Options

1. Rename NS to a “sink” domain owned by Registrar A
   a. Network Solutions uses lamedelegation.org
   b. Registrar A is responsible for queries and upkeep of sink domain.

2. Rename NS to a “random” domain in a different TLD
   a. Different TLD bypasses EPP check.
   b. Registrar does not have to handle queries or upkeep any domains.
   c. Potential security risk.
EPP Mental Model
EPP Mental Model

[Diagram showing relationships between domain and name server objects, with labels for Registrar A and Registrar B.
Well meaning standards might promote non-optimal behavior.
Risky BIIZness 10000ft Summary

- Well meaning standards might promote non-optimal behavior.
- We were able to hijack .edu and .gov domains!
Risky BIZness 10000ft Summary

- Well meaning standards might promote non-optimal behavior.
- We were able to hijack .edu and .gov domains!
- But they do not have registrars? So how?
EPP Mental Model: Multiple TLDs

Verisign EPP Repository

Afilias EPP Repository
EPP Mental Model: Multiple TLDs
EPP Mental Model: Multiple TLDs

Verisign EPP Repository

Afilias EPP Repository

sacrificial nameserver

ns2.fooxxxx.biz

ns1.qux.gov

qux.gov

ns2.foo.com

ns1.baz.org

baz.org

delegation

lame
Risky BIZness 10000ft Summary

- Well meaning standards might promote non-optimal behavior.
- We were able to hijack .edu and .gov domains!
- But they do not have registrars? So how?
- Many domains affected -- including courthouses, law enforcement, local healthcare, local administration, and many more.
- Domain owner is not aware that nameserver has changed! Re-registration does not fix it!
You own a domain *example.com*.

- Webpage on [www.example.com](http://www.example.com) does not load
- You see your mail at [you@example.com](mailto:you@example.com) stop.

What are potential root causes?
It's not DNS

There's no way it's DNS

It was DNS
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.

What are potential root causes?

- Lame Delegation
  - Typo in A/NS Records
  - Misconfiguration
  - example.com NS not working
  - IP addresses unreachable
- Domain expired?
- Hijack?
DNS Cache Poisoning

- Attack that exploits implementation
- Vulnerability in old implementations
  - Client used same UDP Port
  - If attacker guessed 16 bit ID then they could poison cache.
  - “Fixed” by randomizing UDP source port.
DNS Configuration

- DNS Configuration is Critical Infrastructure
  - NS Records, A/AAAA Records

- Control over DNS Configuration == Full Domain Control

- Not only redirect users, but also obtain SSL certificates.
  - Some Certificate Authorities (CAs) now use DNS to prove ownership.
  - Makes DNS integrity even more important.
Ecosystem Threat Model

Parent Zone

Registry

Registrar

Child Zone

EPP

Web Portal / API
Ecosystem Threat Model

Parent Zone

Registry

Registrar

EPP

Web Portal / API

Child Zone

Registrant

Registrant Compromise

Attacker can modify domains owned by the registrant
Ecosystem Threat Model

**Parent Zone**

**Registry**

**Registrar**

EPP

**Web Portal / API**

**Child Zone**

**Registrant**

**Registrant Compromise**

Attacker can modify domains owned by the registrant.

**Registrar Compromise**

Attacks typically compromise EPP credentials.

Attacker can modify *all* domains managed by the registrar.
Ecosystem Threat Model

Parent Zone

Registry

Registrar

Child Zone

Registrant

EPP

Web Portal / API

Registry Compromise
Attacker can modify *all* domains in the TLDs managed by the registry

Registrar Compromise
Attackers typically compromise EPP credentials.
Attacker can modify *all* domains managed by the registrar.

Registrant Compromise
Attacker can modify domains owned by the registrant
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.
- The authoritative nameservers have changed.

Potential root causes?
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it?
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it? -- Registrars!
You own a domain *example.com*.

- Webpage on **www.example.com** does not load
- You see your mail at **you@example.com** stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it? -- Registrars!

What do attackers do to offload the domain?
Always has been

timeouts
bad certs
intermittent
API failures
mystery
service errors

Wait, it's all DNS?
Moar DNS
Discussion: Integrity

- Minimal security considerations in original DNS design.
- How to guarantee integrity of response?
  - Guarantee response has not been modified.
- But in order to do that, how to extend DNS?
Extension Mechanisms for DNS (EDNS)

Add additional section to the end of a DNS packet.

EDNS sections skipped in old resolvers, and nameservers.

Used to implement DNSSEC, and ECS.
DNS Security Extension (DNSSEC)

- Add signature to DNS Records
  - Validate signature to ensure integrity of response

- Low adoption rate
  - Complicated to deploy

- Not all resolvers support DNSSEC.
  - Public DNS Resolvers support DNSSEC
EDNS Client Subnet (ECS)

CDNs with large number of PoPs.

How to ensure response is mapped to closest PoP for client?

ECS allows recursive resolvers to supply the prefix of client IP

137.110.222.10 → 137.110.222.0/24

https://blog.cloudflare.com/introducing-regional-services/
DNS Tunneling

- DNS is typically not blocked at organizational firewall
- Some organizations block .xyz TLD
  - But do not block DNS queries
- Can use DNS queries to exfiltrate data!
Alternative Root
Blockchain DNS