Perils of Transitive Trust in the Domain Name System

Emin Gün Sirer
joint work with Venugopalan Ramasubramanian

Cornell University
How to Own the Internet via DNS

Emin Gün Sirer
joint work with Venugopalan Ramasubramanian

Cornell University
Introduction

- **DNS is critical to the Internet**

- **DNS architecture is based on** delegations
  - Control for names is delegated to name servers designated by the name owner

- **Delegations decentralize administration and improve fault tolerance**
  - But create a dependence
Dependencies for www.fbi.gov

- www.fbi.gov
- fbi.edgesuite.net
- a33.g.akamai.net
- gov
- gov.zoneedit.com
- zoneedit.com
- zoneedit.com
- com
- gtld-servers.net
- nstld.com
- net
- dns[2].sprintip.com
- ns[3,4,5,6].vericenter.com
- sprintip.com
- ns[1,2,3]-auth.sprintlink.net
- reston-ns[1,2,3].telemail.net
- edgesuite.net
- akam.net
- g.akamai.net
- akamai.net
- akamaitech.net
- fbi.gov
- ns[1-6].vericenter.com
Subtle Dependencies in DNS

DNS dependencies are subtle and complex

- www.fbi.gov
  - 86 servers, 17 domains
- www.cs.cornell.edu
  - cs.rochester.edu  cs.wisc.edu  itd.umich.edu
  - 48 nameservers, 20 domains

Conventional wisdom says “add redundant nameservers to mask failures, at no cost”

- Conventional wisdom is wrong
  - Increases risk of domain hijacks
Dependencies for www.fbi.gov
Dependencies for www.fbi.gov
Servers with Security Loopholes

www.fbi.gov → fbi.gov → sprintip.com

dns[2].sprintip.com
ns[3,4,5,6].vericenter.com

ns[1,2,3]-auth.sprintlink.net
reston-ns[1,3].telemail.net
reston-ns[2].telemail.net
Lessons

- DNS delegations create a directed acyclic graph of dependencies.
- This graph forms the trusted computing base for that name.
- This graph is often large and includes many vulnerable hosts, making domain hijacks possible.
Goals

- Identify **vulnerable assets**
  - Which domain names have large dependencies and entail high risk?
  - Which domains are affected by servers with known security holes and can be easily taken over?

- Identify **valuable assets**
  - Which servers control the largest portion of the namespace and are thus likely to be attacked?
Survey Methodology

- Collected 593160 domain names
  - Visible names people care about from Yahoo & DMOZ
  - Separately examined the Alexa Top-500

- Traversed 166771 name servers
  - Large set of important nameservers

- Examined the dependence graphs for 535036 domains, 196 top-level-domains
How vulnerable is a typical name?

How big is the average TCB?

Which domains have the largest TCBs?

What are the chances of a successful domain hijack?
TCB Size

Number of Dependencies

<table>
<thead>
<tr>
<th></th>
<th>All</th>
<th>Top 500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>46</td>
<td>68</td>
</tr>
<tr>
<td>Max</td>
<td>604</td>
<td>342</td>
</tr>
<tr>
<td>Median</td>
<td>26</td>
<td>22</td>
</tr>
</tbody>
</table>

CDF (%) vs. size of TCB

All Names
Top 500 Names
Dependencies by TLD

- aero: 466
- int: 390
- mil: 366
- info: 353
- edu: 349
- biz: 15
- gov: 15
- org: 15
- net: 8
- com: 5
Most Vulnerable Name

- Roman Catholic Church website in the Ukraine depends on nameservers in
  - Berkeley, NYU, UCLA, Russia, Poland, Sweden, Norway, Germany, Austria, France, England, Canada, Israel, Australia

- An attacker in Monash, Australia could redirect the IP binding for a website in Ukraine

- It’s a small world after all…
Lessons for TLD Operators

Some TLDs are set up such that all names in them are dependent on many nameservers
- AERO, Ukraine, Malaysia, Poland, Italy…

Some TLDs have few dependencies
- Japan

Possible to achieve high failure resilience without depending on lots of hosts
Vulnerable Names

- Surveyed BIND version numbers
  - Queried public version numbers
  - 40% response rate

- Compared against database of known vulnerabilities from ISC
  - Many have well-known exploit scripts available

- Examined the dependency graphs to determine how vulnerable names are
Chances of domain hijacks

- Not all vulnerabilities are equal

- An attacker can compromise a name completely (Own it) if it can acquire a graph cut
Chances of domain hijacks

Not all vulnerabilities are equal

An attacker can compromise a name completely (Own it) if it can acquire a graph cut

If a full cut is not vulnerable, attacker must combine compromise with DoS
Due to large TCBs for names, an attacker can use vulnerable servers and small DoS attacks to own many names.
Vulnerable Names

- 17% of servers have known loopholes
- 30% of names are directly vulnerable
- 84% are vulnerable with 2-host DoS
- An attacker that can DoS 8 hosts can own almost any name
- DNS dependencies expand the impact of vulnerabilities
Where are the valuable nameservers?

“Ok, I want to take over the Internet. Where do I start?”
Most Valuable Nameservers

Top 5 Domains
- arizona.edu
- ucla.edu
- uoregon.edu
- nyu.edu
- berkeley.edu
Valuable Nameservers

- Many nameservers in the .EDU domain appear in dependency graphs.

- Operators have no fiduciary responsibility to name owners.

- Name owners as well as operators most likely do not realize the dependencies.
  - Potential security risks and legal liabilities!
Conclusions

- Domain names have subtle dependencies
  - Due to name-based delegations inherent to DNS

- High risk of domain hijacks
  - Conventional wisdom is wrong, name owners should delegate carefully

- DNS is overdue for a redesign, for security
  - More data available at:
    http://www.cs.cornell.edu/people/egs/beehive/