ImpersoNATION: The adoption of anti spoofing DNS records in U.S. Government domains

By Alex Gebhard

Overview

1. Introduction and Motivation
2. Introduction to CAA, SPF, and DMARC
3. Current Results
4. Future Plans

Introduction

- DNS is most commonly used to map from a domain name to an IP address
  - There are also other security specific uses too:
    - DNS Security (DNSSEC)
    - Domain Keys Identified Mail (DKIM)
    - Sender Policy Framework (SPF)
    - Certification Authority Authorization (CAA)
    - Domain-based Message Authentication, Reporting & Conformance (DMARC)
- These security related records help provide authenticity to prevent forgery or impersonation.
- The goal of this research is to determine the adoption and validity of CAA, SPF, and DMARC records in U.S. Government domains across all government types.

Motivation

- According to the United States Census Bureau, there are over 90,075 governments in the United States
  - Includes governments such as townships, cities, counties, and school districts.
- These governments provide crucial services like voting information, taxes, utilities, and public notices.
- Cybersecurity is paramount to state and local governments effort to maintain the trust of their citizens.

Certification Authority Authorization (CAA)

- Certification Authority Authorization (CAA) records is a DNS record indicated which Certification Authority (CA) can issue a certificate for a given domain. Specified in RFC 6844
  - Prevents all CAs from issuing certificates on the domain's behalf
- Direct result of CAs mis-issuing certificates
- All CAs must check to ensure it's on the domains list before it gives a certificate

Ex: “issue "letsencrypt.org"”
Ex: “issuewild "sectigo.com"”

Sender Policy Framework (SPF)

- Sender Policy Framework (SPF) allows website operators to specify which mail servers can send email on their behalf. Specified in RFC 7208
  - A whitelist for mail servers
- SPF records are published as a TXT record on the base of the domain.

Ex: “`v=spf1 ip4:134.48.6.21 include:mu.edu -all`”

Domain-based Message Authentication, Reporting & Conformance (DMARC)

- Domain-based Message Authentication, Reporting and Conformance (DMARC) informs receiving mail servers actions if the email message does not pass SPF. Specified in RFC 7489
- Published as a TXT record under the `_dmarc` subdomain (ex. `_dmarc.example.com`)

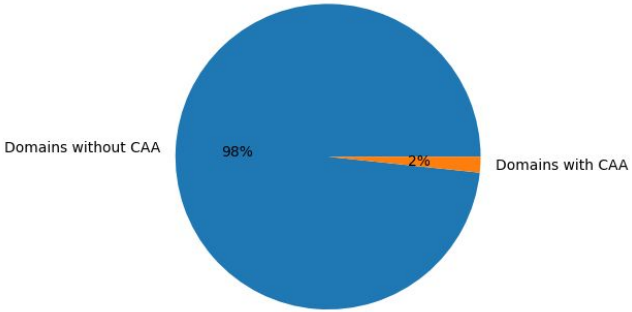
Ex: “`v=DMARC1 p="reject" ruf="mailto:admin@mu.edu”`”

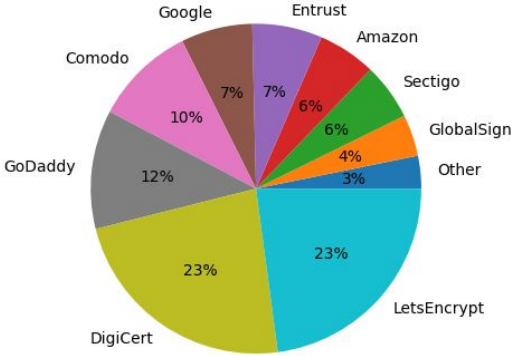
Experiment

- I’ve used the union between the DotGov data set (published by CISA) and the Govt-URL dataset (published by GSA).
  - In total this gives us 17,763 domains across all government types in the U.S.
- Created a scanner and parser to validate each record in accordance to its RFC
- Conducted the first scan across all domains using Google’s Public DNS on January 28th
  - Took a little over 24 hours to complete

Results (CAA)

- Only 2% of scanned government domains have an CAA record





Results (SPF)

- 78% of scanned government domains have an CAA record

Government Type	Adoption Rate
Local	75.70%
County	76.23%
State	45.87%
Federal	70.48%
Native Sovereign Nations	72.88%

Government Type	Error Rate
Local	8.97%
County	8.39%
State	9.25%
Federal	2.44%
Native Sovereign Nations	10.14%

Results (SPF)

Error	Number of domains
More than 10 DNS lookups	508
Use of deprecated PTR mechanism	249
Unresolvable domain in record	239
Unknown mechanism	170
Mechanism after `all`	104

Results (DMARC)

- 23% of scanned government domains implement DMARC.
- *More to come…*

Future Work

- **Three weeks from now**: Run February monthly scan, remove domains that no longer exist, create visualization for CAA, SPF, and DMARC adoption by state.
- **Six weeks from now**: Run March monthly scan, create graphs to determine adoption trends over the previous three months, begin writing paper, and look into possibly notifying domain owners.
- **Eight weeks from now**: Run April monthly scan, finish writing paper.