Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

Pouyan Fotouhi Tehrani\textsuperscript{1}, Eric Osterweil\textsuperscript{2}, Jochen Schiller\textsuperscript{3}, Thomas C. Schmidt\textsuperscript{4}, Matthias Wählisch\textsuperscript{3}

\textsuperscript{1}Weizenbaum Institut / Fraunhofer FOKUS \textsuperscript{2}George Mason University \textsuperscript{3}Freie Universität Berlin \textsuperscript{4}Hamburg University of Applied Sciences

NANOG 82 Virtual, June 14-16, 2021.
Alerting Authorities are crucial during crises.

- People rely on trustworthy sources.
Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.
- Authorities provide services **via web**.

### Top Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Now</th>
<th>7 Days</th>
<th>30 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdc.gov</td>
<td>55,873,975</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ncbi.nlm.nih.gov</td>
<td>44,132,759</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tools.usps.com</td>
<td>37,923,234</td>
<td></td>
<td></td>
</tr>
<tr>
<td>irs.gov</td>
<td></td>
<td>21,684,666</td>
<td></td>
</tr>
<tr>
<td>so.www4.irs.gov</td>
<td></td>
<td></td>
<td>16,277,095</td>
</tr>
</tbody>
</table>
Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.
- Authorities provide services **via web**.
- Evaluating **trustworthiness** is a challenge.
Alerting Authorities are crucial during crises.

But wait, we do have protection mechanisms. Do we?
Scammers Attack a German Paycheck Protection Plan. True Story.

https://nrw-corona-soforthilfe.de

- Sound domain name under .de
- HTTPS enabled
- DNSSEC enabled

https://soforthilfe-corona.nrw.de

- Sound domain name under .de
- HTTPS enabled
- DNSSEC not enabled
Scammers Attack a German Paycheck Protection Plan. True Story.

Let’s retrace the steps that took us here!

- Sound domain name under .de
- HTTPS enabled
- DNSSEC enabled

- Sound domain name under .de
- HTTPS enabled
- DNSSEC not enabled

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD

→ Proof of identity
- DNSSEC enabled

\[\text{Strong Assurance:}\]
- Restricted TLD
- DV certificate
- Proof of domain ownership
- DNSSEC enabled

\[\text{Weak Assurance:}\]
- Nonrestricted TLD
- OV/EV certificate
- Proof of identity
- DNSSEC not enabled

\[\text{Inadequate Assurance:}\]
- DNS Namespace Analysis
- Web PKI Analysis
- https://cdc.gov

Public

\[\text{Authority} + \text{Certification authority}\]

\[\text{certificate} + \text{issues}\]

\[\text{DNS registry} + \text{delegates}\]

\[\text{DNSSEC} + \text{trusts}\]

\[\SSL/TLS\]

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD
- OV/EV certificate → Proof of identity
- DNSSEC enabled
- Resolution
- Identification
- Transaction

Strong Assurance:
- Restricted TLD
- DV certificate → Proof of domain ownership
- DNSSEC enabled
- Resolution
- Identification
- Transaction

G #

Weak Assurance:
- Nonrestricted TLD
- OV/EV certificate → Proof of identity
- DNSSEC not enabled
- Resolution
- Identification
- Transaction

Inadequate Assurance:
- DNS Namespace Analysis
- Web PKI Analysis
- https://cdc.gov
- Authority
+ Certification authority certificate issues
- DNS registry
- delegates
- DNS registry

SSL/TLS

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD
  - OV/EV certificate → Proof of identity
  - DNSSEC enabled
  - Resolution
  - Identification
  - Transaction
  - Strong Assurance:
  - Restricted TLD
    - DV certificate → Proof of domain ownership
    - DNSSEC enabled
    - Resolution
    - Identification
    - Transaction
  - Weak Assurance:
    - Nonrestricted TLD
      - OV/EV certificate → Proof of identity
      - DNSSEC not enabled
      - Resolution
      - Identification
      - Transaction
    - Inadequate Assurance:
      - DNS Namespace Analysis
      - Web PKI Analysis
      - Authority
      - Certification authority
      - https://cdc.gov

DNS registry

Authority

certificates

Certificate authority

Public

discovers

cdc.gov

https://cdc.gov

Strong Assurance:

Restricted TLD

OV/EV certificate

→ Proof of identity

DNSSEC enabled

Resolution

Identification

Transaction

Weak Assurance:

Nonrestricted TLD

DV certificate

→ Proof of domain ownership

DNSSEC not enabled

Inadequate Assurance:

DNS Namespace Analysis

Web PKI Analysis

Public authority issues certificate

Certification authority delegates to DNS registry

- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD
- OV/EV certificate
  → Proof of identity
- DNSSEC enabled
  /thumbs_up_alt Resolution
  /thumbs_up_alt Identification
  /thumbs_up_alt Transaction
- Strong Assurance:
  Restricted TLD
  DV certificate
  → Proof of domain ownership
  DNSSEC enabled
  /thumbs_up_alt Resolution
  /thumbs_up_alt Identification
  /thumbs_up_alt Transaction
- Weak Assurance:
  Nonrestricted TLD
  OV/EV certificate
  → Proof of identity
  DNSSEC not enabled
  /_335 Resolution
  /warning_sign Identification
  /thumbs_up_alt Transaction
- Weak Assurance:
  Nonrestricted TLD
  DV certificate
  → Proof of domain ownership
  DNSSEC not enabled
  /thumbs_down_alt Resolution
  /thumbs_down_alt Identification
  /thumbs_up_alt Transaction
- Inadequate Assurance:
  DNS Namespace Analysis
  Web PKI Analysis

https://cdc.gov

Authority

Public

Certificate authority

Certificate

- Starting point
- Identity hint

- Proof of domain ownership
- Proof of Identity

DNS registry

delegates

DNSSEC

Authority

Certificate authority

Certificate

issues

Trusts

Public

SSL/TLS

https://cdc.gov

discover

cdc.gov

- Data Origin Authentication
- Data Integrity

Restricted TLD

OV/EV certificate

→

Proof of identity

DNSSEC enabled

Resolution

Identification

Transaction

Strong Assurance:

Restricted TLD

DV certificate

→

Proof of domain ownership

DNSSEC enabled

Resolution

Identification

Transaction

G

Weak Assurance:

Nonrestricted TLD

OV/EV certificate

→

Proof of identity

DNSSEC not enabled

Resolution

Identification

Transaction

#

Inadequate Assurance:

DNS Namespace Analysis

Web PKI Analysis

https://cdc.gov

Public

Authority

Certification authority

Certificate

issues

Trusts

- Proof of domain ownership
- Proof of Identity

We contribute:

(1) A threat model for Web-based communication.
(2) A method to discover and analyze Alerting Authorites.
(3) Web security profiles of Alerting Authorities in the US.
Threat Model. Three Dimensions.

Identification Securely authenticating the person, etc. behind the service name.
Threat Model. Three Dimensions.

**Identification**  Securely authenticating the person, etc. behind the service name.

**Resolution**  Securely verifying that users have not been misdirected and are transacting with the service name they have identified.
Threat Model. Three Dimensions.

Identification  Securely authenticating the person, etc. behind the service name.

Resolution  Securely verifying that users have not been misdirected and are transacting with the service name they have identified.

Transaction  Ensuring that the content was not altered, leaks privacy etc. during the session.
Threat Model. Three Dimensions.

Identification: Securely authenticating the person, etc. behind the service name.

Resolution: Securely verifying that users have not been misdirected and are transacting with the service name they have identified.

Transaction: Ensuring that the content was not altered, leaks privacy, etc. during the session.

How DNS(SEC) and WebPKI amount to secure communication?

- **Starting point**
  - Identity hint
  - Proof of domain ownership
  - Proof of identity

- **Data Origin Authentication**
- **Data Integrity**

**Restricted TLD**
- **DV certificate**
  - Proof of domain ownership
  - DNSSEC enabled
  - **Strong Assurance:**
    - Identification
    - Resolution
    - Transaction

**Nonrestricted TLD**
- **OV/EV certificate**
  - Proof of identity
  - DNSSEC not enabled
  - **Weak Assurance:**
    - Identification
    - Transaction

**Inadequate Assurance:**
- **DNS Namespace Analysis**
- **Web PKI Analysis**

---

**https://cdc.gov**

**Authority**

- Certification authority
  - issues

**Public**

- trusts

**Certificate**

- OV/EV certificate
  - Proof of identity

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD
- OV/EV certificate
- → Proof of identity
- DNSSEC enabled
- /thumbs_up_alt
- Resolution
- /thumbs_up_alt
- Identification
- /thumbs_up_alt
- Transaction

Strong Assurance:

- Restricted TLD
- bernco.gov
- DNS registry
- delegates
- DNSSEC
- DNSSEC enabled
- SSL/TLS
- https://bernco.gov
- Authority
- Public
- Certificate authority
- issues
- trusts
- DV certificate
- → Proof of domain ownership

Weak Assurance:

- Nonrestricted TLD
- OV/EV certificate
- → Proof of identity
- DNSSEC not enabled
- /thumbs_down_alt
- Resolution
- /thumbs_down_alt
- Identification
- /thumbs_up_alt
- Transaction

Inadequate Assurance:

- DNS Namespace Analysis
- Web PKI Analysis
- https://bernco.gov
- Public

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity
- Restricted TLD
- OV/EV certificate
- → Proof of identity
- DNSSEC enabled
- /thumbs_up_alt Resolution
- /thumbs_up_alt Identification
- /thumbs_up_alt Transaction
- Strong Assurance:
- Restricted TLD
- DV certificate
- → Proof of domain ownership
- DNSSEC enabled
- /thumbs_up_alt Resolution
- /thumbs_up_alt Identification
- /thumbs_up_alt Transaction
- Weak Assurance:
- Nonrestricted TLD
- OV/EV certificate
- → Proof of identity
- DNSSEC not enabled
- /warning_sign Resolution
- /thumbs_up_alt Identification
- /thumbs_up_alt Transaction
- Inadequate Assurance:
- DNS Namespace Analysis
- Web PKI Analysis

https://usps.com

Authority
Certificate authority
issues
trusts
Public

data.png

- Starting point
- Identity hint
- Proof of domain ownership
- Proof of Identity
- Data Origin Authentication
- Data Integrity

Restricted TLD

→ Proof of identity

DNSSEC enabled

Resolution

Identification

Transaction

Strong Assurance:
Nonrestricted TLD
give4cdc.org

DV certificate
→ Proof of domain ownership

DNS registry

Certificate authority

trusts

issues

certificate

Authority

Public

https://give4cdc.org

Weak Assurance:
Nonrestricted TLD

DNSSEC not enabled

DNS Namespace Analysis
Web PKI Analysis

Inadequate Assurance:
### Threat Model in context. Assurance profiles.

<table>
<thead>
<tr>
<th>#</th>
<th>DNS</th>
<th>Web PKI</th>
<th>Security Implications</th>
<th>Weakness</th>
<th>Assurance Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restricted TLD</td>
<td>DNSSEC</td>
<td>DV</td>
<td>OV/EV</td>
<td>Identification</td>
</tr>
<tr>
<td>01</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✅</td>
</tr>
<tr>
<td>02</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>🔴</td>
</tr>
<tr>
<td>03</td>
<td>✗</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>🔴</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>✗</td>
<td>–</td>
<td>✓</td>
<td>🔴</td>
</tr>
<tr>
<td>05</td>
<td>✗</td>
<td>✗</td>
<td>–</td>
<td>✓</td>
<td>🔴</td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>🔴</td>
</tr>
<tr>
<td>07</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>08</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>09</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✅</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>11</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>12</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✅</td>
</tr>
</tbody>
</table>
## Threat Model in context. Assurance profiles.

<table>
<thead>
<tr>
<th>#</th>
<th>DNS</th>
<th>Web PKI</th>
<th>Security Implications</th>
<th>Weakness</th>
<th>Assurance Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restricted TLD</td>
<td>DNSSEC</td>
<td>DV</td>
<td>OV/EV</td>
<td>Identification</td>
</tr>
<tr>
<td>01</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>02</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>03</td>
<td>✗</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>✗</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>05</td>
<td>✗</td>
<td>✗</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>07</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>08</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>09</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>11</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>12</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
## Threat Model in context. Assurance profiles.

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted TLD</th>
<th>DNSSEC</th>
<th>DNS</th>
<th>Web PKI</th>
<th>Security Implications</th>
<th>Weakness</th>
<th>Assurance Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>N/A</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>02</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>03</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>05</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>07</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>08</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>09</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>11</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>12</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>©</td>
<td>✓</td>
<td>○</td>
</tr>
</tbody>
</table>

- DV: Domain Validation
- OV/EV: Optional Validation
- Identification: Ambiguous identification
- Resolution: Possible impersonation through name spoofing
- Transaction: DNS hijacking
- Weakness: Name spoofing, DNS hijacking
- Assuredness: DNS hijacking and ambiguous identification
- Assuredness: Impersonation and DNS hijacking
- Assuredness: Impersonation
- Assuredness: Content poisoning
- Assuredness: DNS hijacking, content poisoning
- Assuredness: Impersonation, content poisoning
- Assuredness: DNS hijacking, impersonation, content poisoning
## Threat Model in context. Assurance profiles.

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted TLD</th>
<th>DNSSEC</th>
<th>DV</th>
<th>OV/EV</th>
<th>Security Implications</th>
<th>Weakness</th>
<th>Assurance Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>🔄 🔄 🔄</td>
<td>N/A</td>
<td>●</td>
</tr>
<tr>
<td>02</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>Ambiguous identification</td>
<td>○</td>
</tr>
<tr>
<td>03</td>
<td>✗</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>🔄 🔄 🔄</td>
<td>Possible impersonation through name spoofing</td>
<td>○</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>🔄 🔄 🔄</td>
<td>DNS hijacking</td>
<td>○</td>
</tr>
<tr>
<td>05</td>
<td>✗</td>
<td>✗</td>
<td>–</td>
<td>✓</td>
<td>🔄 🔄 🔄</td>
<td>Name spoofing, DNS hijacking</td>
<td>○</td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>DNS hijacking and ambiguous identification</td>
<td>○</td>
</tr>
<tr>
<td>07</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>Impersonation and DNS hijacking</td>
<td>○</td>
</tr>
<tr>
<td>08</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>Impersonation</td>
<td>○</td>
</tr>
<tr>
<td>09</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>Content poisoning</td>
<td>○</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>DNS hijacking, content poisoning</td>
<td>○</td>
</tr>
<tr>
<td>11</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>Impersonation, content poisoning</td>
<td>○</td>
</tr>
<tr>
<td>12</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>🔄 🔄 🔄</td>
<td>DNS hijacking, impersonation, content poisoning</td>
<td>○</td>
</tr>
</tbody>
</table>
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI
Methodology, Toolchain, and Data Set

Measurement Period October 2019 – March 2020

1. Preparation Phase
   1.1 Fetch / parse AA list
   1.2 Collect URLs
   1.3 Sanitize / filter URLs

2. Domain Namespace Analysis
   2.1 Parse URLs/ extract hosts
   2.2 Check for DNSSEC
   2.3 Categorize TLDs
   2.4 Classify owners

3. Web PKI Analysis
   3.1 Check SSL/TLS
   3.2 Certificate transparency
   3.3 Analyze certs

4. Statistics
   Sanitize data

1388 Alerting Authorities in the US → 1365 URLs → 1327 unique hosts
Security of Alerting Authorities in the WWW: Measuring *Namespaces*, *DNSSEC*, and Web PKI
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- Does each AA have its own dedicated domain name?
- How do AAs integrate in the global DNS namespace?
- Do AAs secure their names using DNSSEC?
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- Does each AA have its own dedicated domain name?
  About 49% of Alerting Authorities do not have dedicated names, e.g., https://www.vercounty.org/ema.htm → unnecessary dependencies, e.g., for X.509 certificates.

![Dedicated domain names (%)](image)

Educational: 29%, Military: 10%, Law Enforcement: 28%, Governmental: 75%, Public Safety: 53%

![Ratio of TLDs Types (%)](image)

DNSSEC for <state>.us

- Not Supported
- Supported
- Not Used
1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- **How do AAs integrate in the global DNS namespace?**
  More than 50% of unique names are under non-restricted TLDs → poor recognizability and inferior security.
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- More than 50% of unique names are under non-restricted TLDs
- **Do AAs secure their names using DNSSEC?**
  96% of unique hosts do not support DNSSEC
  → high susceptibility to DNS hijacking
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- More than 50% of unique names are under non-restricted TLDs
- 96% of unique hosts do not support DNSSEC
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI
Results: Web PKI Analysis

1327 Unique Hosts

- To what extent do AAs adapt web PKI?
- How is the historic landscape of X.509 certificates shaped among AAs?
Results: Web PKI Analysis

1327 Unique Hosts

- To what extent do AAs adapt web PKI?
  About 15% provide none or invalid certificates (OpenSSL validation)
  → secure identification and transaction impossible
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- How is the historic landscape of X.509 certificates shaped among AAs?

![Graphs showing trends in certificate types, DNS SAN, and market share over years.](image-url)
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- How is the historic landscape of X.509 certificates shaped among AAs?
  - Which validation types have been popular?
  - OV/EV certificates are losing popularity

![Graph showing the market share of different certificate issuers over the years](image1)

![Graph showing the share of different validation types over the years](image2)

![Graph showing the DNS SAN distribution over the years](image3)
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 certificates shaped among AAs?**
  - OV/EV certificates are losing popularity
  - **Has certificate usage been exclusive?**
    Certificate sharing is on the rise
    → fate-sharing is increasing
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 certificates shaped among AAs?**
  - OV/EV certificates are losing popularity
  - Certificate sharing is on the rise
- **How has the CA market been changed?**
  - CA giants are losing to free and automated DV certificate issuers
  - → AAs care more about encryption than identification
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- OV/EV certificates are losing popularity
- Certificate sharing is on the rise
- CA giants are losing to free and automated DV certificate issuers
Security of Alerting Authorities in the WWW:
Measuring Namespaces, DNSSEC, and Web PKI
Putting the Pieces Together

Only about 22% exhibit strong or weak assurance profiles.

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile¹</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>29 (≈ 2%)</td>
</tr>
<tr>
<td>✓</td>
<td></td>
<td>✓</td>
<td>11</td>
</tr>
<tr>
<td>x</td>
<td>✓</td>
<td>–</td>
<td>2</td>
</tr>
<tr>
<td>✓</td>
<td></td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>–</td>
<td>117</td>
</tr>
<tr>
<td>✓</td>
<td>x</td>
<td>–</td>
<td>262 (≈ 20%)</td>
</tr>
</tbody>
</table>

1. strong, ◯ weak, ○ inadequate
## Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted delegation</td>
<td>Supports DNSSEC</td>
<td>DV</td>
<td>O/EV</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>X</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Grand Total:** | | | | **1327** |

1. ● strong, ○ weak, ○ inadequate
Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.
- About 15% of all fail to provide valid certificates (inadequate assurance profile).

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted delegation</td>
<td>Supports DNSSEC</td>
<td>DV</td>
<td>O/EV</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>❌</td>
</tr>
<tr>
<td>❌</td>
<td>✓</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>❌</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>Total:</td>
<td></td>
<td></td>
<td>262 (≈ 20%)</td>
</tr>
</tbody>
</table>

- Total: 262 (≈ 20%)

- Total: 354
- Total: 482
- Total: 3
- Total: 2
- Total: 67
- Total: 2
- Total: 126
- Total: 1036 (≈ 78%)
- Grand Total: 1327

1. ● strong, ○ weak, ○ inadequate
Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.
- About 15% of all fail to provide valid certificates (inadequate assurance profile).

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted delegation</td>
<td>Supports DNSSEC</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Total:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th># Names</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>354</td>
<td>482</td>
<td>3</td>
<td>2</td>
<td>67</td>
<td>2</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>Total: 1036 (≈ 78%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grand Total: 1327</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ ● strong, ○ weak, ○ inadequate
The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates. Makes affiliations recognizable and proofs identity.
The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates. Makes affiliations recognizable and proofs identity.
- Enable DNSSEC. Secures name resolution and avoids possible DV misissuance.
The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates. Makes affiliations recognizable and proofs identity.
- Enable DNSSEC. Secures name resolution and avoids possible DV misissuance.
- Consider TLSA domain issued certificates (DANE EE) Provides alternative to DV certificates.
The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates.
  Makes affiliations recognizable and proofs identity.
- Enable DNSSEC.
  Secures name resolution and avoids possible DV misissuance.
- Consider TLSA domain issued certificates (DANE EE)
  Provides alternative to DV certificates.
- Use dedicated domain names and certificates.
  Avoids fate-sharing.
Data? More Details? Check out [https://aa.secnow.net](https://aa.secnow.net)!

Summary

**Alerting Authority**

AZ - Graham County Emergency Management

Graham County Emergency Management (AZ) is accessible under [https://www.graham.az.gov/243/Emergency-Management](https://www.graham.az.gov/243/Emergency-Management). Its domain name is registered under .gov, a Sponsored Top-Level Domain (sTLD). It is not securely delegated (DNSSEC). Transport layer security is **enabled** for this host with a valid certificate. Provided certificate is a(n) Domain Validation (DV) certificate.

Details

**Identification**

Your domain name is registered under a restricted top-level domain (TLD) and as such provides the first hint about its owner (e.g., .edu TLD is only reserved for higher education institutes). A domain validation (DV) certificate lacks identification information. Moreover, lack of DNSSEC can lead to DV certificate misissuance. Finally, insecure domain names (no DNSSEC) are susceptible to hijacking and can lead to forwarding to malicious hosts regardless of the certificate provided.

**Resolution**

You don't seem to have DNSSEC enabled (verify [here](https://example.com)) and as such susceptible to DNS hijacking.

**Transaction**

You are using a valid certificate and as such transactions with users are secure against eavesdropping or manipulation.

* You can also download the raw data and our toolchain on [zenodo](https://zenodo.org).

Question, critique, cooperation? pft@acm.org
Backup Slides
Select Results
DNS and Web PKI alongside assurance profiles

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted delegation</th>
<th>Supports DNSSEC</th>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile¹</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>x</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>x</td>
<td>x</td>
<td></td>
<td>✓</td>
<td></td>
<td>132</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>x</td>
<td>x</td>
<td></td>
<td>✓</td>
<td></td>
<td>482</td>
</tr>
<tr>
<td>8</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>67</td>
</tr>
<tr>
<td>11</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>126</td>
</tr>
</tbody>
</table>

Total: 262 (≈ 20%)

Grand Total: 1327

¹ • strong, ○ weak, o inadequate
## Select Results

**DNS and Web PKI alongside assurance profiles**

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted delegation</th>
<th>Supports DNSSEC</th>
<th>DNS</th>
<th>Certificate</th>
<th>Assurance profile¹</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>⚫</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>⚫</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>✓</td>
<td>✗</td>
<td>⚫</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>⚫</td>
<td>132</td>
</tr>
<tr>
<td>5</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>⚫</td>
<td>117</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>○</td>
<td>354</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>✓</td>
<td>✗</td>
<td>○</td>
<td>482</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>✓</td>
<td>✗</td>
<td>○</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>○</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>○</td>
<td>67</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>○</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>○</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1327</td>
</tr>
</tbody>
</table>

---

¹ ⚫ strong, ⚫ weak, ○ inadequate
Select Results

DNS and Web PKI alongside assurance profiles

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted delegation</th>
<th>Supports DNSSEC</th>
<th>Certificate</th>
<th>DV</th>
<th>O/EV</th>
<th>Assurance profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
<td>29 (≈ 2%)</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>×</td>
<td>–</td>
<td>✓</td>
<td></td>
<td></td>
<td>132</td>
</tr>
<tr>
<td>5</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>✓</td>
<td></td>
<td></td>
<td>117</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td>354</td>
</tr>
<tr>
<td>7</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td>482</td>
</tr>
<tr>
<td>8</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
<td>67</td>
</tr>
<tr>
<td>11</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>×</td>
<td></td>
<td></td>
<td>126</td>
</tr>
</tbody>
</table>

Total: 262 (≈ 20%)

Total: 1036 (≈ 78%)

Grand Total: 1327

1 ● strong, ◦ weak, ○ inadequate
## Select Results

DNS and Web PKI alongside assurance profiles

<table>
<thead>
<tr>
<th>#</th>
<th>Restricted delegation</th>
<th>DNSSEC</th>
<th>Certificate</th>
<th>Assuranc profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>29</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>117</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>354</td>
</tr>
<tr>
<td>7</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>482</td>
</tr>
<tr>
<td>8</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>67</td>
</tr>
<tr>
<td>11</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>126</td>
</tr>
</tbody>
</table>

Grand Total: 1327

1. ● strong, ○ weak, ○ inadequate
## Select Results

Validation types and assurance profiles per sector

<table>
<thead>
<tr>
<th>Type</th>
<th>Certificate</th>
<th>Assurance profile&lt;sup&gt;1&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N/A</td>
<td>DV</td>
</tr>
<tr>
<td>Public Safety</td>
<td>102</td>
<td>415</td>
</tr>
<tr>
<td>Governmental</td>
<td>73</td>
<td>318</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>21</td>
<td>110</td>
</tr>
<tr>
<td>Military</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Educational</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>197</td>
<td>850</td>
</tr>
</tbody>
</table>

<sup>1</sup> • strong, • weak, ○ inadequate