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

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**.
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

/thumbs_up_alt Resolution
/thumbs_up_alt Identification
/thumbs_up_alt Transaction

Strong Assurance:
- Restricted TLD
- DV certificate
- DNSSEC enabled

/thumbs_up_alt Resolution
/thumbs_up_alt Identification
/thumbs_up_alt Transaction

G #

Weak Assurance:
- Nonrestricted TLD
- OV/EV certificate
- DNSSEC not enabled

/thumbs_down_alt Resolution
/thumbs_down_alt Identification
/thumbs_up_alt Transaction

Inadequate Assurance:
- https://cdc.gov
- Public
- Authority

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

→ Proof of identity

DNSSEC enabled

Resolution

Identification

Transaction

Strong Assurance:

- Restricted TLD
- DV certificate

→ Proof of domain ownership

DNSSEC enabled

Weak Assurance:

- Nonrestricted TLD
- OV/EV certificate

→ Proof of identity

DNSSEC not enabled

Inadequate Assurance:

https://cdc.gov

Public

Certificate authority

Certificate issues

Certificate authority

Authority

Certificate

DNS registry delegates

https://cdc.gov

Start point → Identity hint → Proof of domain ownership → Proof of identity → DNSSEC enabled

Resolution → Identification → Transaction

Strong Assurance:
- Restricted TLD
- OV/EV certificate → Proof of identity
- DNSSEC enabled

Weak Assurance:
- Nonrestricted TLD
- DV certificate → Proof of domain ownership
- DNSSEC not enabled

Inadequate Assurance:
- Nonrestricted TLD
- DV certificate → Proof of domain ownership
- DNSSEC not enabled

https://cdc.gov

Authority

Certificate authority

cdc.gov

- 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:
- https://cdc.gov
- Authority + Certificate authority
- certificate issues
- Certificate authority trusts
- Public discover cdc.gov

- Starting point
- Identity hint

- Data Origin Authentication
- Data Integrity

- Proof of domain ownership
- Proof of Identity

Restricted TLD

→ Proof of identity

DNSSEC enabled

Resolution

Identification

Transaction

Strong Assurance:

Restricted TLD

→ Proof of domain ownership

DNSSEC enabled

Weak Assurance:

Nonrestricted TLD

→ Proof of identity

DNSSEC not enabled

Inadequate Assurance:

https://cdc.gov

Certificate authority

Certificate

issues

Authority

Public

trusts

discover

cdc.gov

Authority

Certificate authority

Certificate

issues

https://cdc.gov

DNS registry

delegates

DNSSEC

SSL/TLS

We contribute:

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

Certificate authority

-Proof of domain ownership
-Proof of Identity

DNS registry

-Starting point
-Identity hint

Restricted TLD

OV/EV certificate

→

Proof of identity

DNSSEC enabled

Resolution

/thumbs_up_alt

Identification

/thumbs_up_alt

Transaction

Strong Assurance:

Restricted TLD

DV certificate

→

Proof of domain ownership

DNSSEC enabled

Resolution

/thumbs_up_alt

Identification

/thumbs_up_alt

Transaction

G #

Weak Assurance:

Nonrestricted TLD

OV/EV certificate

→

Proof of identity

DNSSEC not enabled

Resolution

/thumbs_down_alt

Identification

/thumbs_up_alt

Transaction

G #

Weak Assurance:

Nonrestricted TLD

DV certificate

→

Proof of domain ownership

DNSSEC not enabled

Resolution

/thumbs_down_alt

Identification

/thumbs_up_alt

Transaction

Inadequate Assurance:

https://cdc.gov
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?

- **Strong Assurance:**
  - Restricted TLD
  - OV/EV certificate
  - DNSSEC enabled
  - DNSSEC trusts
  - Resolution
  - Identification
  - Transaction

- **Weak Assurance:**
  - Nonrestricted TLD
  - DV certificate
  - DNSSEC not enabled
  - DNSSEC trusts
  - Resolution
  - Identification
  - Transaction

Inadequate Assurance:

- https://cdc.gov
- Authority delegates
- DNS registry
- SSL/TLS
- Certificate authority
- Certificate
- Public
- Trusts

Public authority delegates to DNS registry, which issues an OV/EV certificate that proves identity. SSL/TLS provides strong assurance when DNSSEC is enabled.

- 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

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:

- https://bernco.gov
- Public
- Authority
- Certificate authority
- Certificate
- issues
- trusts

DV certificate
→ Proof of domain ownership

- **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**

**Strong Assurance:**

- **Restricted TLD**
- **DV certificate**
  → **Proof of domain ownership**
- **DNSSEC enabled**

**Weak Assurance:**

- **Nonrestricted TLD**
- **OV/EV certificate**
  → **Proof of identity**
- **DNSSEC not enabled**

**Inadequate Assurance:**

- **Nonrestricted TLD**
- **DV certificate**
  → **Proof of domain ownership**
- **DNSSEC not enabled**

- **https://usps.com**
  - **Public**
  - **Certificate authority**
  - **Certificate issues**
  - **Certificate authority trusts**
  - **SSL/TLS**
  - **Delegates**
  - **DNS registry**
  - **DNSSEC not enabled**

**Weak Assurance:**

- **Identification**
- **Resolution**
- **Transaction**

Nonrestricted TLD

- **give4cdc.org**
  - DNS registry delegates
  - DNSSEC not enabled

Weak Assurance:

- **Nonrestricted TLD**
  - DV certificate
  - Proof of domain ownership
  - DNSSEC not enabled

Inadequate Assurance:

- **https://give4cdc.org**
  - Public
  - Trusts
  - Certificate
  - Issues
  - Certificate authority

Strong Assurance:

- **Restricted TLD**
  - OV/EV certificate
  - Proof of identity
  - DNSSEC enabled

Identity hint

- **Starting point**

Proof of domain ownership

Data Origin Authentication

Data Integrity

Authority

Certificate authority

Certificate

issues

trusts

SSL/TLS

Identification

Resolution

Transaction
<table>
<thead>
<tr>
<th>#</th>
<th>DNS</th>
<th>Web PKI</th>
<th>Security Implications</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restricted TLD</td>
<td>DNSSEC</td>
<td>DV</td>
<td>OV/EV</td>
</tr>
<tr>
<td>01</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>02</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>03</td>
<td>×</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>×</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>05</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>07</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>08</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>09</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>11</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>12</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

Assurance Profile:
## 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>x</td>
<td>✖</td>
</tr>
<tr>
<td>03</td>
<td>x</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✖</td>
</tr>
<tr>
<td>04</td>
<td>✓</td>
<td>x</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>x</td>
<td>x</td>
<td>–</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✖</td>
</tr>
<tr>
<td>08</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>✖</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>12</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Details see paper.
Security of Alerting Authorities in the WWW: *Measuring* Namespaces, DNSSEC, and Web PKI
Methodology, Toolchain, and Data Set

Measurement Period October 2019 – March 2020

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](https://www.vercounty.org/ema.htm) → unnecessary dependencies, *e.g.*, for X.509 certificates.
Results: Namespace and DNS(SEC) Analysis

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

![Diagram showing the ratio of TLD types and dedicated domain names for different categories like Educational, Military, Law Enforcement, Governmental, and Public Safety.](image-url)
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 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
  - → 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 shaped among AAs?
Results: Web PKI Analysis

1327 Unique Hosts

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

[Graphs and charts showing trends over years for different certificate validation types and market share of certificate issuers.]
Results: Web PKI Analysis

1327 Unique Hosts

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

---

![Graph Showing Certificate Usage Trends](image1)

![Graph Showing Market Share Trends](image2)
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 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

- 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>Assured profile</th>
<th># Names</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DV O/EV</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>29 (≈ 2%)</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓ X</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>2</td>
</tr>
<tr>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Total: 262 (≈ 20%)</td>
</tr>
<tr>
<td>✓</td>
<td>X</td>
<td>✓ X</td>
<td>354</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>482</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>✓ X</td>
<td>3</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>X X</td>
<td>2</td>
</tr>
<tr>
<td>✓</td>
<td>X</td>
<td>X X</td>
<td>67</td>
</tr>
<tr>
<td>X</td>
<td>✓</td>
<td>X X</td>
<td>2</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X X</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Total: 1036 (≈ 78%)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Grand Total: 1327</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>
</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></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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.
- 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</td>
<td>Supports</td>
</tr>
<tr>
<td>delegation</td>
<td>DNSSEC</td>
</tr>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Total:</td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Total:</td>
<td></td>
</tr>
<tr>
<td>Grand Total:</td>
<td></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.
- About 15% of all fail to provide valid certificates (inadequate assurance profile).

<table>
<thead>
<tr>
<th>DNS</th>
<th>Certificate</th>
<th>Assuranc e 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></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>×</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></td>
</tr>
<tr>
<td>Grand Total:</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.

Summary

Alerting Authority

AZ - Graham County Emergency Management

Graham County Emergency Management (AZ) is accessible under https://www.graham.az.gov/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) 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.

Question, critique, cooperation? pft@acm.org