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

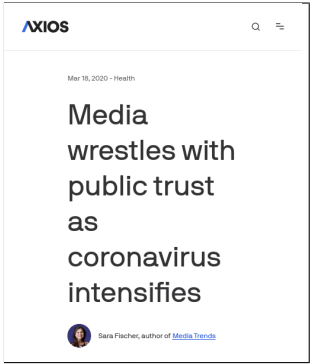
Pouyan Fotouhi Tehrani[1], Eric Osterweil[2], Jochen Schiller[3], Thomas C. Schmidt[4], Matthias Wählisch[3]

[1]Weizenbaum Institut / Fraunhofer FOKUS [2]George Mason University [3]Freie Universität Berlin [4]Hamburg University of Applied Sciences

NANOG 82 Virtual, June 14-16, 2021.

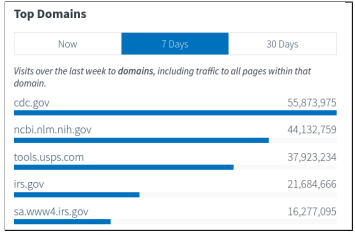
Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.



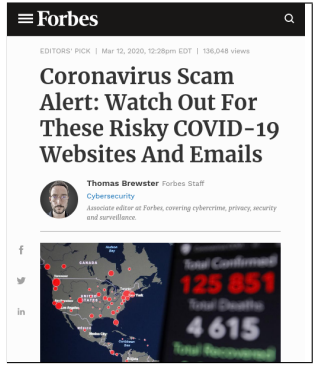
Alerting Authorities are crucial during crises.

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



Alerting Authorities are crucial during crises.

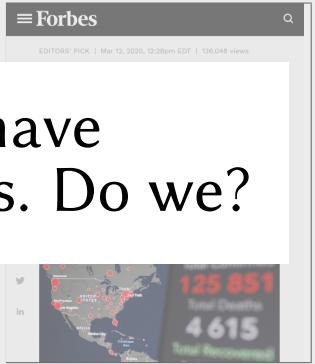
- People rely on **trustworthy sources**.
- Authorities provide services **via web**.
- Evaluating **trustworthiness** is a challenge.



Alerting Authorities are crucial during crises.

- Pe
- Au
- Ev

But wait, we do have protection mechanisms. Do we?



Scammers Attack a German Paycheck Protection Plan. True Story.

https://nrw-corona-soforthilfe.de

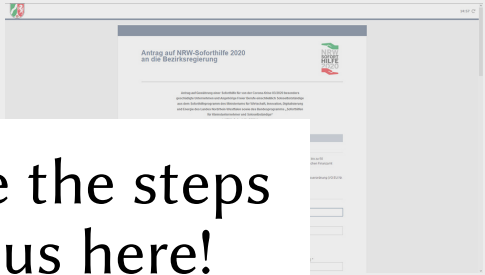
- ✓ Sound domain name under `.de`
- ✓ HTTPS enabled
- ✓ DNSSEC enabled

?

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!

`https://nrw-` … `orona.nrw.de`

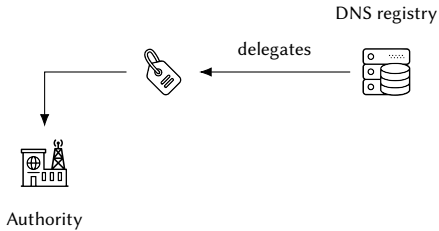
- ✓ Sound domain name under `.de`
- ✓ HTTPS enabled
- ✓ DNSSEC enabled

- ✓ Sound domain name under `.de`
- ✓ HTTPS enabled
- ✘ DNSSEC not enabled

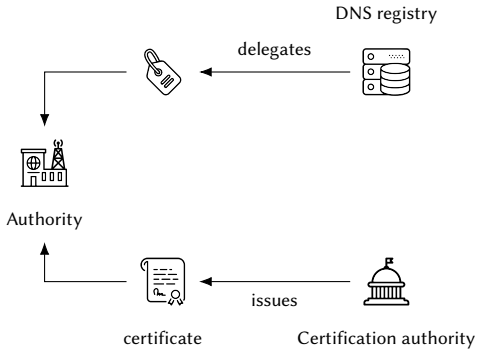
Secure Web-based Communication. A Complex System.

Authority

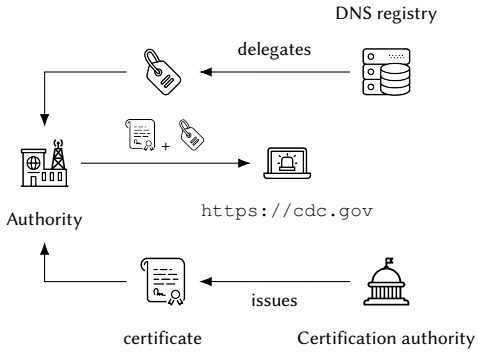
Secure Web-based Communication. A Complex System.



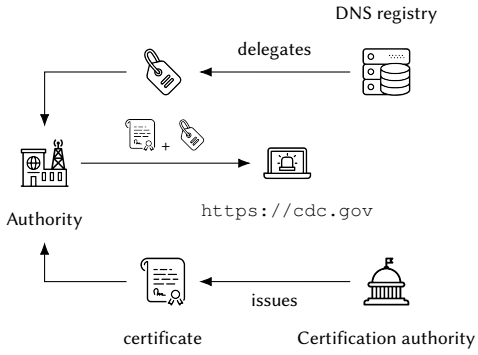
Secure Web-based Communication. A Complex System.

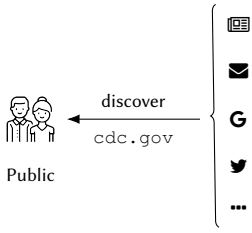


Secure Web-based Communication. A Complex System.

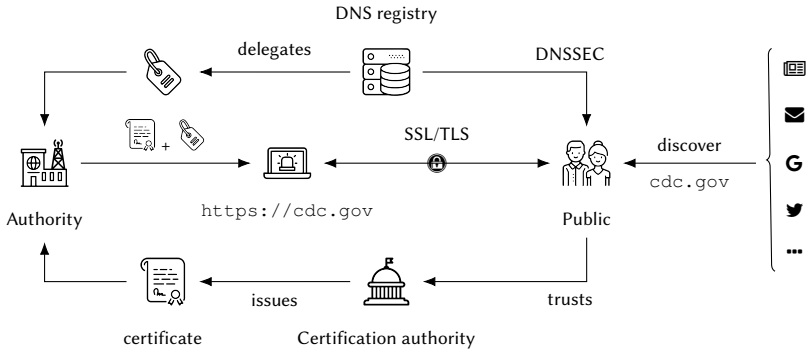


Secure Web-based Communication. A Complex System.

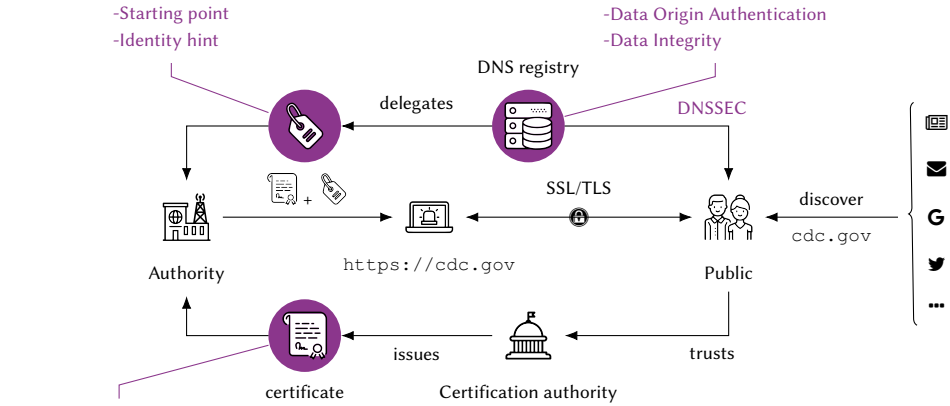




Secure Web-based Communication. A Complex System.



Secure Web-based Communication. A Complex System.



Secure Web-based Communication. A Complex System.

-Starting point
-Identity hint

-Data Origin Authentication
-Data Integrity

DNS registry

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.

certificate

Certification authority

-Proof of domain ownership
-Proof of Identity

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.

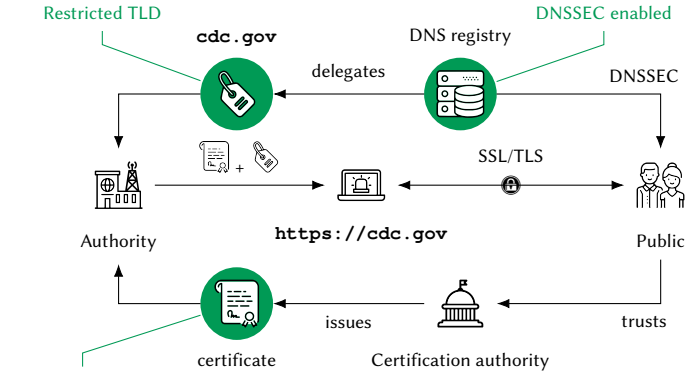
Threat Model. Three Dimensions.

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

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

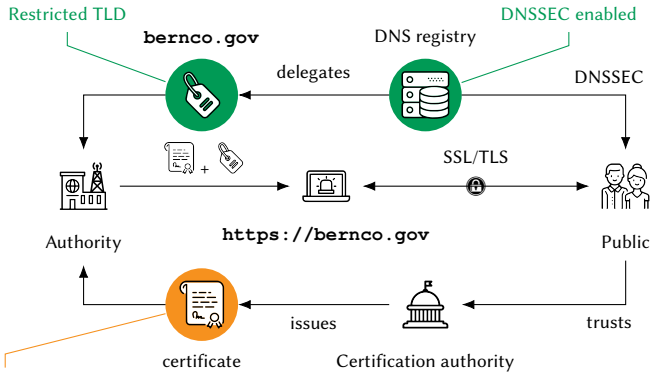
the session.

Secure Web-based Communication. Assurance Profiles.



- Strong Assurance:
  - Identification
  - Resolution
  - Transaction

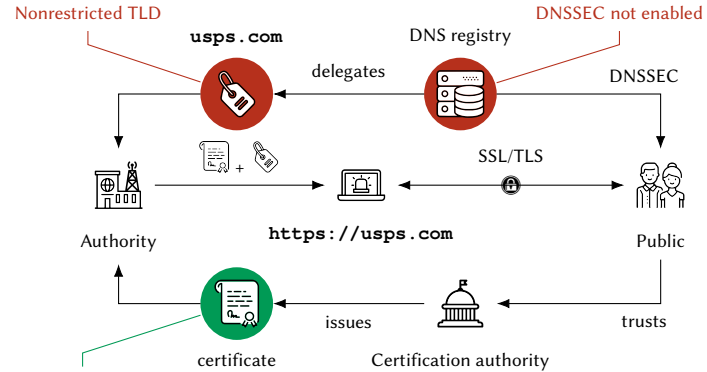
Secure Web-based Communication. Assurance Profiles.



◐ Weak Assurance:

- ⚠ Identification
- 👍 Resolution
- 👍 Transaction

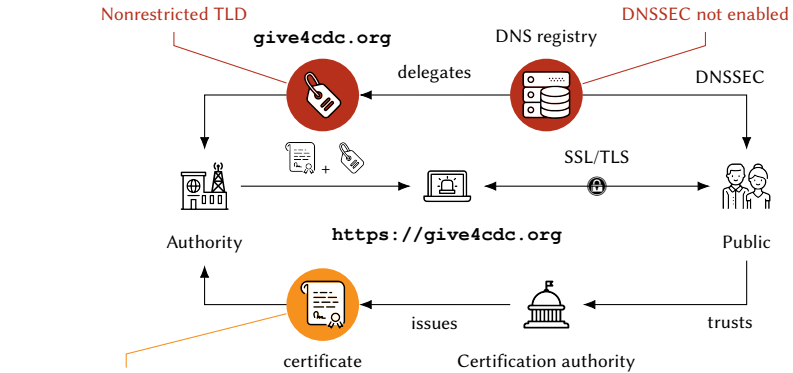
Secure Web-based Communication. Assurance Profiles.



◐ Weak Assurance:

- Identification
- Resolution
- Transaction

Secure Web-based Communication. Assurance Profiles.



- Inadequate Assurance:
  - Identification
  - Resolution
  - Transaction

Threat Model in context. Assurance profiles.

#	DNS		Web PKI		Security Implications			Weakness	Assurance Profile
	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction		
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✘	⚠	👍	👍	Ambiguous identification	◐
03	✘	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✘	–	✓	⚠	👎	👍	DNS hijacking	◐
05	✘	✘	–	✓	⚠	👎	👍	Name spoofing, DNS hijacking	◐
06	✓	✘	✓	✘	⚠	👎	👍	DNS hijacking and ambiguous identification	○
07	✘	✘	✓	✘	👎	👎	👍	Impersonation and DNS hijacking	○
08	✘	✓	✓	✘	👎	👍	👍	Impersonation	○
09	✓	✓	✘	✘	👎	👎	👎	Content poisoning	○
10	✓	✘	✘	✘	👎	👎	👎	DNS hijacking, content poisoning	○
11	✘	✓	✘	✘	👎	👍	👎	Impersonation, content poisoning	○
12	✘	✘	✘	✘	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

Threat Model in context. Assurance profiles.

#	DNS		Web PKI		Security Implications			Weakness	Assurance Profile
	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction		
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✘	⚠	👍	👍	Ambiguous identification	◐
03	✘	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✘	–	✓	⚠	👎	👍	DNS hijacking	◐
05	✘	✘	–	✓	⚠	👎	👍	Name spoofing, DNS hijacking	◐
06	✓	✘	✓	✘	⚠	👎	👍	DNS hijacking and ambiguous identification	○
07	✘	✘	✓	✘	👎	👎	👍	Impersonation and DNS hijacking	○
08	✘	✓	✓	✘	👎	👍	👍	Impersonation	○
09	✓	✓	✘	✘	👎	👎	👎	Content poisoning	○
10	✓	✘	✘	✘	👎	👎	👎	DNS hijacking, content poisoning	○
11	✘	✓	✘	✘	👎	👍	👎	Impersonation, content poisoning	○
12	✘	✘	✘	✘	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

Threat Model in context. Assurance profiles.

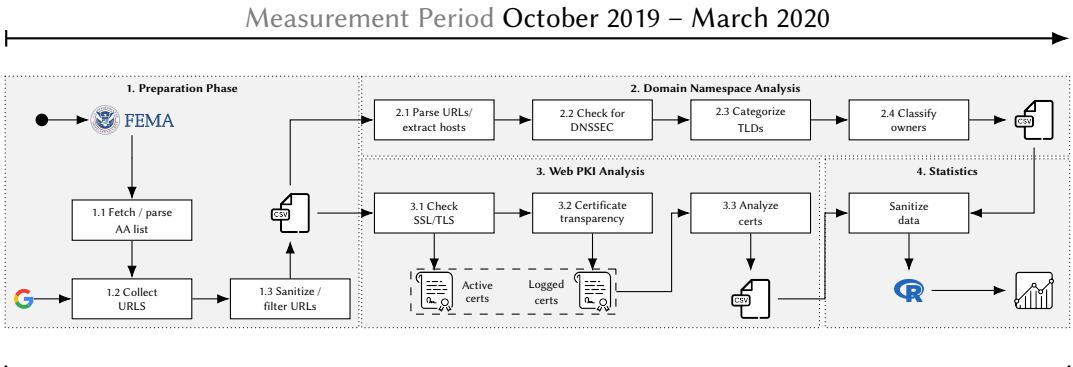
#	DNS		Web PKI		Security Implications			Weakness	Assurance Profile
	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction		
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✘	⚠	👍	👍	Ambiguous identification	◐
03	✘	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✘	–	✓	⚠	👎	👍	DNS hijacking	◐
05	✘	✘	–	✓	⚠	👎	👍	Name spoofing, DNS hijacking	◐
06	✓	✘	✓	✘	⚠	👎	👍	DNS hijacking and ambiguous identification	○
07	✘	✘	✓	✘	👎	👎	👍	Impersonation and DNS hijacking	○
08	✘	✓	✓	✘	👎	👍	👍	Impersonation	○
09	✓	✓	✘	✘	👎	👎	👎	Content poisoning	○
10	✓	✘	✘	✘	👎	👎	👎	DNS hijacking, content poisoning	○
11	✘	✓	✘	✘	👎	👍	👎	Impersonation, content poisoning	○
12	✘	✘	✘	✘	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

Threat Model in context. Assurance profiles.

#	DNS		Web PKI		Security Implications			Weakness	Assurance Profile
	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction		
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✘	⚠	👍	👍	Ambiguous identification	◐
03	✘	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✘	–	✓	⚠	👎	👍	DNS hijacking	◐
05	✘	✘	–	✓	⚠	👎	👍	Name spoofing, DNS hijacking	◐
06	✓	✘	✓	✘	⚠	👎	👍	DNS hijacking and ambiguous identification	○
07	✘	✘	✓	✘	👎	👎	👍	Impersonation and DNS hijacking	○
08	✘	✓	✓	✘	👎	👍	👍	Impersonation	○
09	✓	✓	✘	✘	👎	👎	👎	Content poisoning	○
10	✓	✘	✘	✘	👎	👎	👎	DNS hijacking, content poisoning	○
11	✘	✓	✘	✘	👎	👍	👎	Impersonation, content poisoning	○
12	✘	✘	✘	✘	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

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

Methodology, Toolchain, and Data Set



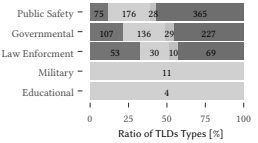
1388 Alerting Authorities in the US → 1365 URLs → 1327 unique hosts

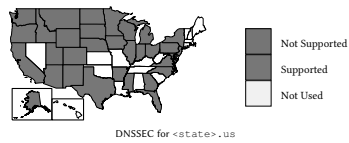
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

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?**

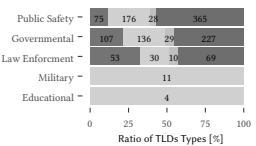




Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

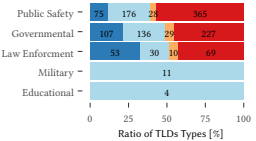
- **Does each AA have its own dedicated domain name?**
  About 49% of Alerting Authorities do not have dedicated names,
  e.g., `https://www.vercounty.org/ema.htm`
  → unnecessary dependencies, *e.g.,* for X.509 certificates.

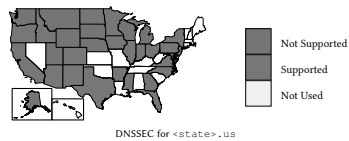


Results: Namespace and DNS(SEC) Analysis

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
  $\rightarrow$ poor recognizability and inferior security.

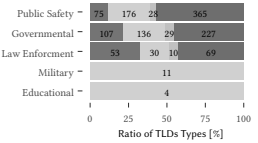


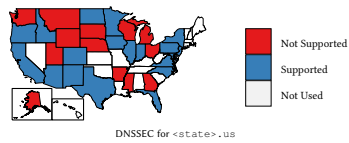


Results: Namespace and DNS(SEC) Analysis

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
  $\rightarrow$ high susceptibility to DNS hijacking

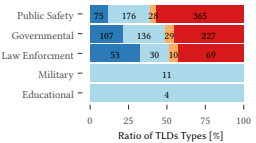


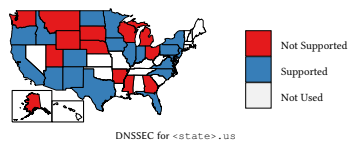


Results: Namespace and DNS(SEC) Analysis

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



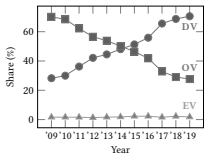


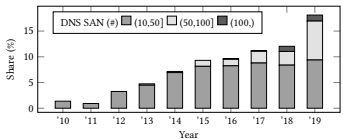
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

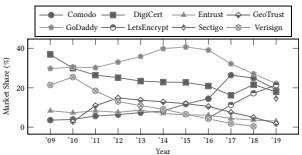
Results: Web PKI Analysis

1327 Unique Hosts

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



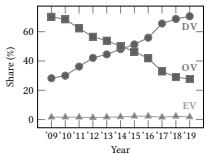


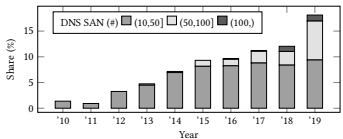


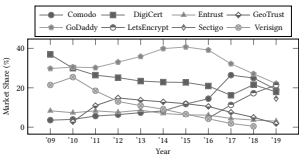
Results: Web PKI Analysis

1327 Unique Hosts

- **To what extent do AAs adapt web PKI?**
  About 15% provide none or invalid certificates (OpenSSL validation)
  $\rightarrow$ secure identification and transaction impossible



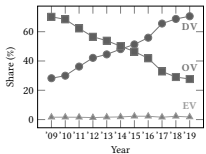


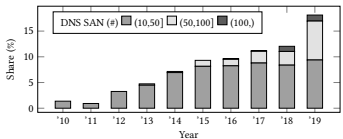


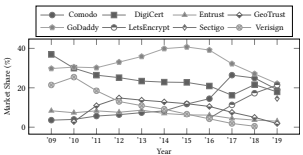
Results: Web PKI Analysis

1327 Unique Hosts

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



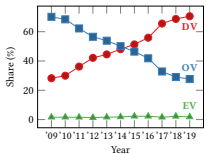


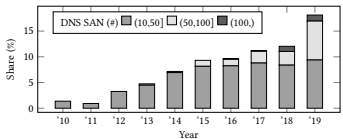


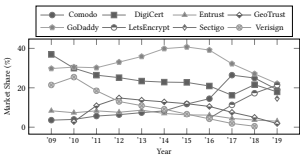
Results: Web PKI Analysis

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



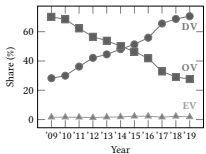


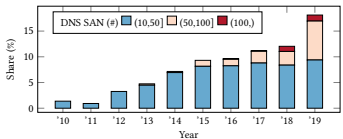


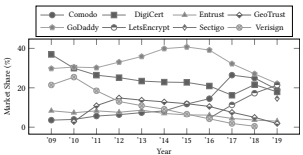
Results: Web PKI Analysis

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



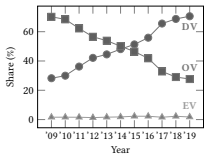


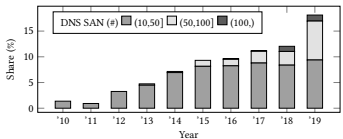


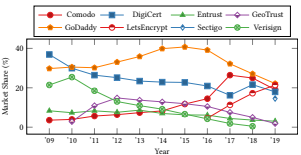
Results: Web PKI Analysis

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



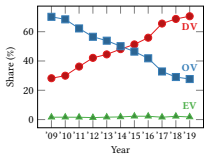


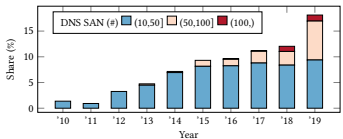


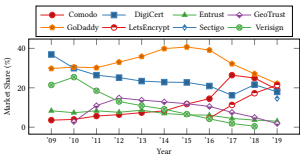
Results: Web PKI Analysis

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.

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	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.

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	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).

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	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).

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[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.

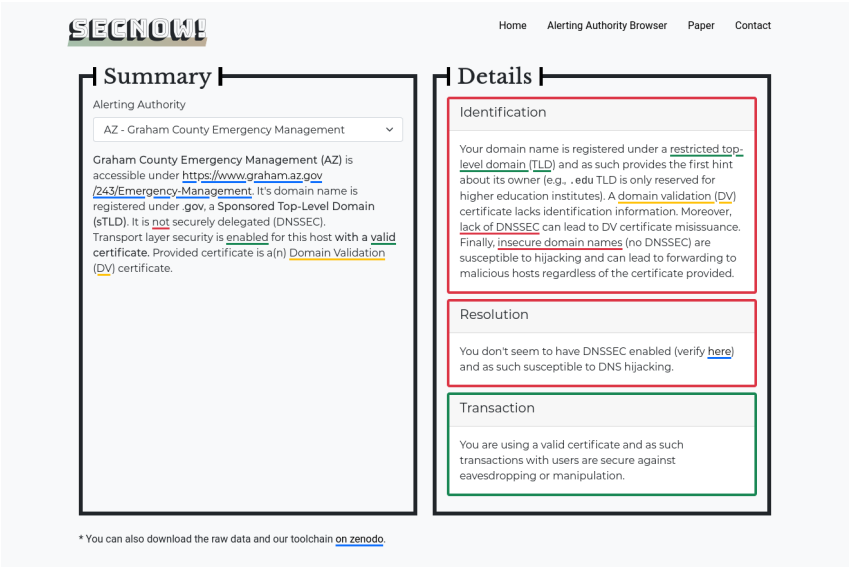
The Road Ahead. Suggested Improvements for Alerting Authorities.

- 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.

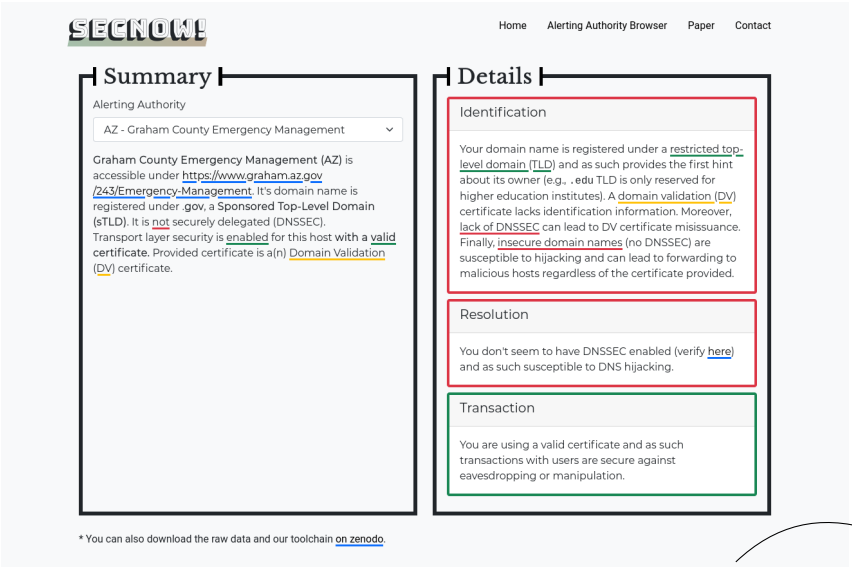
The Road Ahead. Suggested Improvements for Alerting Authorities.

- 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**!



Data? More Details? Check out **https://aa.secnow.net**!



Question, critique, cooperation? pft@acm.org

Backup Slides

Select Results

DNS and Web PKI alongside assurance profiles

#	DNS		Certificate		Assurance profile[1]	# Names
	Restricted delegation	Supports DNSSEC	DV	O/EV		
1	✓	✓	–	✓	●	29 (≈ 2%)
2	✓	✓	✓	✘	◐	11
3	✘	✓	–	✓	◐	2
4	✓	✘	–	✓	◐	132
5	✘	✘	–	✓	◐	117
					Total:	262 (≈ 20%)
6	✓	✘	✓	✘	○	354
7	✘	✘	✓	✘	○	482
8	✘	✓	✓	✘	○	3
9	✓	✓	✘	✘	○	2
10	✓	✘	✘	✘	○	67
11	✘	✓	✘	✘	○	2
12	✘	✘	✘	✘	○	126
					Total:	1036 (≈ 78%)
					Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Select Results

DNS and Web PKI alongside assurance profiles

#	DNS		Certificate		Assurance profile[1]	# Names
	Restricted delegation	Supports DNSSEC	DV	O/EV		
1	✓	✓	–	✓	●	29 (≈ 2%)
2	✓	✓	✓	✘	◐	11
3	✘	✓	–	✓	◐	2
4	✓	✘	–	✓	◐	132
5	✘	✘	–	✓	◐	117
					Total:	262 (≈ 20%)
6	✓	✘	✓	✘	○	354
7	✘	✘	✓	✘	○	482
8	✘	✓	✓	✘	○	3
9	✓	✓	✘	✘	○	2
10	✓	✘	✘	✘	○	67
11	✘	✓	✘	✘	○	2
12	✘	✘	✘	✘	○	126
					Total:	1036 (≈ 78%)
					Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Select Results

DNS and Web PKI alongside assurance profiles

#	DNS: Restricted delegation	DNS: Supports DNSSEC	Certificate: DV	Certificate: O/EV	Assurance profile[1]	# Names
1	✓	✓	–	✓	●	29 (≈ 2%)
2	✓	✓	✓	✘	◐	11
3	✘	✓	–	✓	◐	2
4	✓	✘	–	✓	◐	132
5	✘	✘	–	✓	◐	117
					Total:	262 (≈ 20%)
6	✓	✘	✓	✘	○	354
7	✘	✘	✓	✘	○	482
8	✘	✓	✓	✘	○	3
9	✓	✓	✘	✘	○	2
10	✓	✘	✘	✘	○	67
11	✘	✓	✘	✘	○	2
12	✘	✘	✘	✘	○	126
					Total:	1036 (≈ 78%)
					Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Select Results

DNS and Web PKI alongside assurance profiles

#	DNS		Certificate		Assurance profile[1]	# Names
	Restricted delegation	Supports DNSSEC	DV	O/EV		
1	✓	✓	–	✓	●	29 (≈ 2%)
2	✓	✓	✓	✘	◐	11
3	✘	✓	–	✓	◐	2
4	✓	✘	–	✓	◐	132
5	✘	✘	–	✓	◐	117
					Total:	262 (≈ 20%)
6	✓	✘	✓	✘	○	354
7	✘	✘	✓	✘	○	482
8	✘	✓	✓	✘	○	3
9	✓	✓	✘	✘	○	2
10	✓	✘	✘	✘	○	67
11	✘	✓	✘	✘	○	2
12	✘	✘	✘	✘	○	126
					Total:	1036 (≈ 78%)
					Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Select Results

Validation types and assurance profiles per sector

	Certificate				Assurance profile[1]		
Type	N/A	DV	OV	EV	●	◐	○
Public Safety	102	415	119	8	10	120	514
Governmental	73	318	102	6	7	104	388
Law Enforcement	21	110	31	0	5	28	129
Military	1	4	5	1	6	3	2
Educational	0	0	4	0	0	4	0
Other	0	3	3	1	1	3	3
Total	197	850	264	16	29	262	1036

[1] ● strong, ◐ weak, ○ inadequate