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

Pouyan Fotouhi Tehrani
Weizenbaum Institute / Fraunhofer FOKUS
pft@acm.org

Eric Osterweil
George Mason University
eoster@gmu.edu

Jochen H. Schiller
Freie Universität Berlin
jochen.schiller@fu-berlin.de

Thomas C. Schmidt
HAW Hamburg
t.schmidt@haw-hamburg.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

ABSTRACT

During disasters, crisis, and emergencies the public relies on online services provided by official authorities to receive timely alerts, trustworthy information, and access to relief programs. It is therefore crucial for the authorities to reduce risks when accessing their online services. This includes catering to secure identification of service, secure resolution of name to network service, and content security and privacy as a minimum base for trustworthy communication.

In this paper, we take a first look at *Alerting Authorities* (AA) in the US and investigate security measures related to trustworthy and secure communication. We study the domain namespace structure, DNSSEC penetration, and web certificates. We introduce an integrative threat model to better understand whether and how the online presence and services of AAs are harmed. As an illustrative example, we investigate 1,388 Alerting Authorities. We observe partial heightened security relative to the global Internet trends, yet find cause for concern as about 78% of service providers fail to deploy measures of trustworthy service provision. Our analysis shows two major shortcomings. First, how the DNS ecosystem is leveraged: about 50% of organizations do not own their dedicated domain names and are dependent on others, 55% opt for unrestricted-use namespaces, which simplifies phishing, and less than 4% of unique AA domain names are secured by DNSSEC, which can lead to DNS poisoning and possibly to certificate misissuance. Second, how Web PKI certificates are utilized: 15% of all hosts provide none or invalid certificates, thus cannot cater to confidentiality and data integrity, 64% of the hosts provide domain validation certification that lack any identity information, and shared certificates have gained on popularity, which leads to fate-sharing and can be a cause for instability.

CCS CONCEPTS

• **Security and privacy → Web application security**; **Domain-specific security and privacy architectures**;

WWW '21, April 19–23, 2021, Ljubljana, Slovenia

ACM ISBN 978-1-4503-8312-7/21/04.
https://doi.org/10.1145/3442381.3450033

KEYWORDS

DNS, DNSSEC, Web PKI, Emergency Management

ACM Reference Format:
Pouyan Fotouhi Tehrani, Eric Osterweil, Jochen H. Schiller, Thomas C. Schmidt, and Matthias Wählisch. 2021. Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI. In *Proceedings of the Web Conference 2021 (WWW '21), April 19–23, 2021, Ljubljana, Slovenia.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3442381.3450033

1 INTRODUCTION

Online media have been proven to be an effective channel to communicate with the public. An ever growing number of Americans prefer to get their news online [41], social media is being used for public health announcements [87], and authorities provide public disaster education and services via Web portals [33]—just to mention a few examples. Communication of critical information such as emergency response [10, Chapter 3] and provisioning of critical services are no exception to this trend. Research shows that in emergencies the public turns to official and authoritative sources especially when specific, precise, and trustworthy information is requested [20, 24, 29]. At the same time, evaluating the credibility and trustworthines of online service providers during an emergency or crisis poses a real challenge for users [59]. A recent example to illustrate such situations is the novel Coronavirus (SARS-CoV-2) pandemic and its outbreak in the US in early 2020: with government institutions and health authorities being perceived as the most (social media being the least) trustworthy sources of information by the public [36, 73], alone in the first month of the outbreak, nearly half a billion visits were registered on websites of Centers for Diseases Control and Prevention (CDC) and the National Institutes of Health (NIH) [3]. Similarly, the high amount of visits on state unemployment websites brought the operation of many of those sites to a halt [16]. The high demand for COVID-related online services took place in parallel with an explosion of misinformation campaigns and fraudulent services. Despite efforts from top tech companies [82] the overwhelming *infodemic* [91] continued to grow and prevail [15]. This over-abundance of information posed serious challenges both to politics and public health, and the growing number of individuals and business relying on unemployment insurance and governmental relief programs led to a boom in online fraud [84] with many falling prey to such schemes.

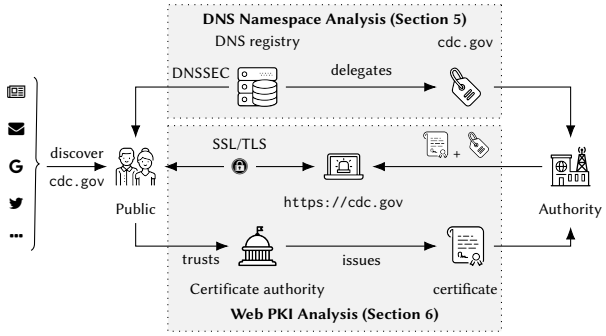


Figure 1: Accessing data from an Alerting Authority

In this paper, we address the research blind spot of trustworthy and secure Web-based emergency services. We systematically investigate the digital representation of emergency and disaster management organizations in the U.S. through the lens of the Domain Name System (DNS), its Security Extensions (DNSSEC) [7–9], *and* the Web PKI (see Figure 1). Based on our threat model, we aim to understand whether and how specific integration of these organizations in the domain namespace and their use of DNSSEC and X.509 certificates can mitigate threats against trustworthy communication. The point of departure for our study is the list of *Alerting Authorities* (AA) provided by FEMA [35], which comprises all entities (the US governmental and non-governmental organizations) on federal, state, territorial, tribal, and local levels authorized to dispatch alerts.

Our key finding shows that only about 22%, *i.e.,* 291 out of a total 1327 unique hosts, provide sufficient measures to ensure trustworthy identification. This decomposes as follow: (*i*) only half the investigated organizations are uniquely identifiable based on dedicated domain names while the rise of multitenancy structures and shared certificates throughout the past decade has complicated identifications in general and has also led to an expansion of attack surfaces [67], (*ii*) the majority of organizations ($\approx$ 64%) do not take advantage of restricted namespaces for better protection against name spoofing and more than 96% of investigated DNS zones are susceptible to DNS attacks due to lack of DNSSEC, and finally (*iii*) about 15% are exposed to content poisoning as a result of invalid or no certificates. In more detail, in this paper we contribute:

(1) **Threat model (Section 3)**. We introduce a threat model that integrates different characteristics of DNS and Web PKI into groups of *Assurances Profiles* that qualifies various degrees of reachable security.
(2) **Method (Section 4)**. Our method identifies common public Alerting Authorities in the US and corresponding websites. The modular and configurable pipeline introduced here for data collection and analysis maintains a certain level of generality which makes it suitable to be extended to non-US regions in future work.
(3) **Analysis of namespace structure and protection (Section 5)**. We map names of Alerting Authorities to fully qualified domain names (FQDN) and identify operational dependencies. Usage of restricted and protected namespaces as well as penetration of DNSSEC among AAs are investigated in this section. We also studied whether there are discrepancies between organizations from various fields of operation (*e.g.,* governmental, military).
(4) **Analysis of Web PKI (Section 6)** We analyze Web PKI certificates used to authenticate and identify Alerting Authorities. On the one hand the historical and actual usage of X.509 are studied, and on the other hand it is investigated how widespread these technologies are, which certificate authorities are leading the market among AAs, and how (automated) domain-validation certificates affect trustworthy communication.

While prior work has investigated the deployment of security protections broadly across different application domains, to the best of our knowledge, this is the first paper that investigates the security profiles of official critical (and critical-to-life) Alerting Authorities. After presenting background and our results, we discuss improving measures and conclude with an outlook.

2 BACKGROUND

Emergency management (EM) can be understood as an ongoing cycle of mitigating, preparing for, responding to, and recovering from incidents that threaten life, property, operations, or the environment [11, 13]. The core objectives of emergency management, ranging from coordination efforts to raising awareness and critical service provision, are carried out by governmental agencies, NGOs, volunteer groups, and international organizations. The structure and organization of these entities differ in each country and even on local and regional levels. In the US, the list of Alerting Authorities regularly published by FEMA [35] provides a non-exhaustive overview of organizations which are (directly or indirectly) involved in the process of emergency management.

In each phase of EM cycle, communication (between and among authorities and the public) plays an integral role not just as a mere necessity but also in amounting to social resilience [58]. Beside using dedicated alerting systems, *e.g.,* FEMA's *Integrated Public Alert & Warning System* [34], social media, or similar channels for information dissemination, many involved organizations have their own dedicated websites not only for informational purposes but also for services such as volunteer registry or disaster aid application (*e.g.,* Homeland Security's `disasterassistance.gov`).

In this paper we investigate the namespace structure, DNSSEC penetration, and deployment of Web PKI certificates among Alerting Authorities to maintain secure communication (as defined in the next section). The global domain name system (DNS), a distributed key-value database with a hierarchical namespace and management scheme, is de facto the entry point to many (if not all) of Internet services. Respectively, for critical service providers, *e.g.,* Alerting Authorities, it is indispensable to be represented within namespaces protected both in organizational and technical terms: top-level domains (TLD) with restricted naming and delegation policies protect domain name owners against name and trademark violations while assuring end users that the domain name owner has undergone some form of vetting; at the same time, DNSSEC [7] compensates the vulnerable client/server paradigm of DNS [12] and caters for authenticated delegation and protect DNS data against tampering. To authenticate the content provider behind a domain name X.509

Table 1: Assurance profiles (● : strong, ◐ : weak, ○ : inadequate) based on the interplay of DNS and X.509 certificate characteristics (✓: deployed, ✘: not deployed) and security implications for users (👍 : fulfilled, ⚠ : dependent protection, 👎 : inadequate). Note if OV or EV certification is deployed, then domain validation is covered and not further assessed (–).

	DNS		Web PKI		Security Implications				Assurance
#	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction	Weakness	Profile
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	○

certificates [26] are used. The semantics of a certificate depends on its certification process: if the real-world entity behind a certificate is vetted by a certification authority (CA) and is respectively awarded with an organization or extended validation certificate (OV/EV), the certificate can used for identification. Otherwise, if the validation is limited to the ownership of a domain name, *i.e.,* domain validation (DV), the certificate is only good for authenticated confidentiality and integrity.

3 A THREAT MODEL FOR WEB-BASED EMERGENCY COMMUNICATION

Emergency communication is dependent on heightened security requirements which are not always as relevant for other Internet services (*e.g.,* video streaming, social media). Three steps constitute our definition of secure online communication: (*i*) securely authenticating the authoritative service ("identification" of the person, organization *etc.* behind the service name), (*ii*) securely verifying that users have not been misdirected and are transacting with the service name they have identified ("resolution" of name to network service), and (*iii*) ensuring that the content was not altered, leaks privacy *etc.* during the session ("transaction" security). Although different methods can be utilized to realize such a secure workflow, here we focus on those technologies that are most accessible to (and deployable by) users and service operators in today's Internet, namely the DNS and the Web PKI ecosystems. Alternative solutions are discussed in Section 8.

An illustrative example. For illustration of the communication workflow and respective security pitfalls, we consider the simple case of inquiring information about COVID-19 guidance as a resident of Jackson County in Missouri. Through a search engine, an online ad, a recommendation from friends, *etc.* the URL is quickly discovered: `https://jacohd.org`. When visiting the website, the presence of a green padlock in the address bar indicates *only* the confidentiality and integrity of data exchange, but does not indicate whether the website belongs to the supposed service (*i.e.,* Health Department of Jackson County in Missouri instead of one of the other 22 Jackson Counties). The generic domain name could haven been registered and operated by anyone. An attacker could have published a forged website implementing the look and feel of the real health department. At no stage is the user given the chance to authenticate the identity (*i.e.,* identification) of the service provider because the provided DV certificate does not include any identification information. In contrast, the health department of Jackson County in Michigan is reachable under `www.co.jackson.mi.us`[1]. Here, the domain name under a restricted TLD indicates that it belongs to Jackson County (`co.jackson`) in Michigan (`mi.us`), and the accompanying EV certificate serves as a definitive proof of identity.

Threaten identification. In a secure setting, it would be possible to identify and authenticate the communication partner *before* initiating the transaction. Yet, the point of departure for Web communication are domain names, which cannot be used for secure identification, while Web PKI certificates (as proofs of identity) are provided only *after* resolution succeeds and transaction is initiated. This implies that targeting authentic names and subsequent secure resolution are necessary (yet insufficient) conditions of identification through a certificate. Respectively, simple name spoofing, *e.g.,* through typosquatting [51], DNS cache poisoning [90], or other DNS hijacking attacks, which can mislead users to malicious services, can act as a precursor for impersonation attacks, especially if subsequently only a DV certificate with no identity information is presented. A viable countermeasure is the use of restricted namespaces so at least the affiliation or identity of the service provider can be inferred directly from its respective name. Governmental organizations in the US, for example, educate visitors that domain names of federal government agencies most commonly end in `.gov` or `.mil`. Subsequently, an OV/EV certificate provides direct elements of proof of identity. When considering using approaches like this, exceptions may serve to help prove the rule: consider that the United States Post Office's (USPO's) official website is `uspo.`**`com`**, *i.e.,* not under `.gov`. This, then, necessitates additional knowledge

[1]The complete URL is `https://www.co.jackson.mi.us/276/Health-Department`.

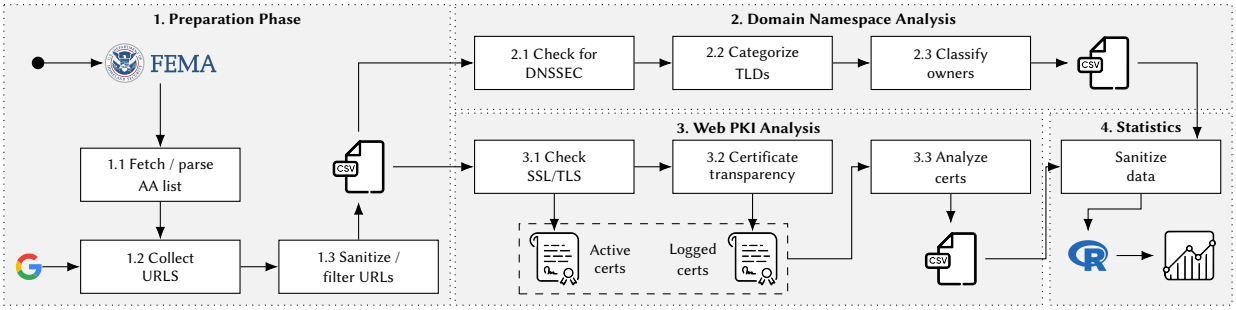


Figure 2: Toolchain to gather and analyze data about Alerting Authorities in the US

or verification before users of *that* government agency can be assured that they are transacting with the official authority online. Proper identification, thus, involves both selection of proper domain names, secure resolution (see below), and identity information from OV/EV certificate.

Threaten resolution. The second attack surface pertains to name resolution. There are two methods to assert that a name has been resolved correctly: either by using DNSSEC or through the X.509 bindings in a certificate's common name (CN) or subject alternative names (SAN). The latter approach, however, provides only an a posteriori assurance, *i.e.,* after transaction initiation with a server, and only if the resolution has already succeeded correctly. Furthermore, especially in case of DV certificates, if resolution is compromised, *e.g.,* through DNS poisoning, and as a result attackers were granted a DV certificate (see Brandt *et al.* [14]), there is no way to verify the integrity of the resolution process. The only effective solution in securing name resolution and deterring collateral damages such as DV certificate misissuances is deployment of DNSSEC.

Threaten transaction. In the final step, after name identification and resolution, it is imperative to secure the transaction using transport security protocols (TLS/SSL) in terms of authenticated confidentiality and integrity. It is worth noting that authentication (using X.509 certificates) is crucial, because encryption and integrity checks alone can also be performed by a malicious actor using monkey-in-the-middle attacks.

Assurance profiles. Based on threats on the three aforementioned dimensions, Table 1 provides the various combinations of DNS and Web PKI options and the security implications of their deployment for users; the *Assurance Profiles* summarizes their combinations.

To achieve *strong assurance*, a service provider should own a domain name that (*i*) indicates its affiliation, (*ii*) is securely delegated, and (*iii*) is bound with a real-world entity through an OV/EV certificate. A prominent example is `coronavirus.gov` which is registered under `.gov` TLD denoting it being a governmental domain name, supports DNSSEC (*i.e.,* cannot be hijacked), and provides a valid OV certificate belonging to the *Executive Office of the President*.

A service provider that only partially covers these aspects and fails to deploy DNSSEC or uses a name under a non-restricted namespace exhibits a *weak Assurance Profile* due to susceptibility to DNS hijacking or simple name spoofing. This is how a campaign in Germany was able to defraud up to 4000 applicants of the corona relief program of a federal state. The scammers spoofed the original domain name `soforthilfe-corona.nrw.de` by registering `nrw-corona-soforthilfe.de` without much burden because the `.de` TLD has no delegation restrictions that cannot be circumvented with minimal effort. Although the authentic name (the former) was bound to a valid OV certificate, the spoofed name was awarded with a DV certificate which gave the impression of authenticity and caused users to fell prey to this phishing campaign. Similarly, the threat of DNS hijacking was highlighted during the pandemic as attackers managed to exploit a vulnerability in home routers and made use of insecure DNS to manipulate name resolution; an attack which could easily be defended through DNSSEC.

In contrast to the previous cases, *inadequate assurance* reflects the case when no certificate or only a DV certificate is provided *regardless* of domain name properties and presence of DNSSEC. Lack of a certificate at the very least defeats the purpose of authenticated encryption and integrity verification[2], while a mere DV certificate can at best only cater to confidentiality and integrity without providing any information about the identity of service provider. An example of weak assurance is the Corona Emergency Response Fund of CDC foundation under `give4cdcf.org` which have raised millions of dollars in fighting the pandemic. The usage of `.org` generic TLD simplifies name spoofing[3], lack of DNSSEC make it a suitable target for hijacking, and finally the provided DV certificate practically doesn't provide any evidence of identity.

4 METHOD AND DATA CORPUS

The subject of study in this paper are the US organizations involved in EM. Due to lack of a central registry, we focus on the list of Alerting Authorities maintained by FEMA. Although this list might not include each and every entity involved in emergency management, it provides a decent, legitimate overview over this field comprising a wide spectrum of organizations ranging from local governments, law enforcement agencies, and military bases to NGOs and universities. Each entry represents an organization by a unique ID, a name, and a territory of operation (including unincorporated territories). Throughout this study, we use the AA list from September 11, 2019 comprising 1,388 entries (excluding a single duplicate entry).

[2]Considering that alternative SSL/TLS authentication methods, *e.g.,* pre-shared keys, are not scalable and suitable for studied cases here.
[3]At the time of writing `give4cdcf.net` remains undelegated.

Table 2: Top-level domains in use by Alerting Authorities

	TLD		Registration		Registry		Statistics		
Type	Label	DNSSEC	Restricted	Fee/year	Name	Country	Share	Count	DNSSEC
gTLD	.com	✓	✘	< 15 $	Verisign	US	19.44 %	258	2
	.org	✓	✘	< 15 $	Public Internet Registry	US	26.15 %	347	5
	.net	✓	✘	< 15 $	Verisign	US	4.37 %	58	0
	.info	✓	✘	< 15 $	Afilias	US	0.15 %	2	0
							50 %	665	7
ccTLD	.cc	✓	✘	< 15 $	eNIC [1]	US	0.07 %	1	0
	.co	✓	✘	< 20 $	.CO Internet S.A.S [2]	US	0.07 %	1	0
	.us	✓	(✓)	< 15 $	Neustar	US	4.89 %	65	0
							5.04 %	67	0
ccSLD	.<code>.us	(✓)	✓	–	Neustar	US	17.71 %	235	2
sTLD	.edu	✓	✓	77 $	Educase [3]	US	0.45 %	6	0
	.gov	✓	✓	400 $	General Services Administration	US	25.92 %	344	30
	.mil	✓	✓	–	Defense Information Systems Agency	US	0.75 %	10	10
							27.12 %	360	40
						Unique domain names		1327	

[1] subsidiary of Verisign, [2] subsidiary of Neustar, [3] operated by Verisign

Our method consists of three phases: (1) preparation phase, (2) domain namespace analysis, and (3) Web PKI analysis. Our measurements were carried out from October 2019 up to March 2020 with each measurement being executed at least twice from various vantage points in Europe and the US to detect any possible vantage point dependent discrepancies, *e.g.,* limited access due to geo-blocking. Figure 2 summarizes our methodology from preparation phase to data gathering and final analysis (see § 5 and § 6).

(1) Preparation. In the preparation phase, we first retrieve and parse the AA list and assign the domain name used for web services for each organization. To identify the primary website of an Alerting Authority, we query and scrape the Google search engine. For each entry in the AA list, the combination of name and territory of operation (*e.g., Fresno Police Department CA*) was used as query string. Each query yielded between 4 and 12 results. Since the results are not necessarily ranked to have the official URL first, we excluded results based on a list of inapt domain names (*e.g.,* social media sites and yellow pages). The topmost remaining URL was then selected for the respective organization. Finally, the list of collected URLs was manually checked to remove any mismatches and falsely associated URLs which were not detected automatically, *e.g.,* same URL for homonymous counties in different states. A total of 23 entries were removed: 11 entries with mismatched names, 11 associated with the wrong territory of operation, and 1 with no matching URL at all; leaving a total of 1,365 URLs for further analysis. The remaining URLs (*e.g.,* `https://www.fresno.gov/police`) were parsed to extract the FQDNs (*e.g.,* `www.fresno.gov`) and path segments (*e.g.,* `/police`).

(2) Domain Namespace Analysis. In the second phase we first separate effective second-level domains (SLD) from TLDs, *e.g.,* for '`www.ci.tracy.ca.us`', '`ca.us`' being the TLD (more specifically the public suffix) and '`tracy`' the effective SLD. We then check DNSSEC status for both the given domain name and its TLD, categorize TLDs (restricted/unrestricted), and finally, based on a list of predefined keywords (see Table A.I in Appendix) map each Alerting Authority to a *field of activity* as either Public safety, Governmental, Law enforcement, Military, or Educational. The results of our analysis on domains names is presented in Section 5.

(3) Web PKI Analysis. Finally, domain names were used to investigate the current and historic adaption of Web PKI certificates by respective hosts. To study the current state, OpenSSL version `1.1.1d` CLI was leveraged to fetch complete certificate chains, perform validation, and verify revocation status using stapled Online Certificate Status Protocol (OCSP) [1], manual OCSP [78], or Certificate Revocation Lists (CRL) [26] (depending on availability). For our historical analysis, we used CT logs [55, 79]. To do this we leveraged the publicly accessible database provided by *Sectigo* under crt.sh, which audits 79 log servers from 12 organizations (at the time of writing). For any given host name, the database was queried for certificates which have the host name or a wildcard covering the host name as their subject name or have it included in the list of subject alternative names (SAN). From a total of 28,370 retrieved unique certificates, 10,826 were pre-certificates and are omitted from further analysis. The remaining 17,544 certificates were then limited to those issued in the past decade (2009-2019), leaving a total number of 17,477 certificates which are analyzed as described in Section 6.

5 DNS NAMESPACE ANALYSIS

By studying the domain names of alerting authorities, we aim to answer the following questions:

(1) Does each AA have its own dedicated domain name?
(2) How do AAs integrate in the global DNS namespace?
(3) Do AAs secure their names using DNSSEC?

The first question is concerned with how Alerting Authorities maintain their online presence, and avoid unnecessary dependencies. Lack of a dedicated name, for example, leads to dependence on someone else for authentication and data security as X.509 certificates are bound to domain names. The second question aims to investigate whether AAs prefer specific TLDs to take advantages of recognizability (*e.g.,* governmental organization under `.gov`) and

security (restricted vs. non-restricted TLDs). Finally, the last question regards measures taken in securing names against threats such as spoofing or DNS hijacking which can also lead to impersonation and phishing. Table 2 summarizes our findings.

5.1 Dedicated Domain Names

We consider an AA to have a dedicated DNS name either if it has its own effective SLD, or has been assigned a sub-domain under the namespace of its parenting organization or any generic service provider, which is not shared. For example, the *Tehama County Sheriff* (`tehamaso.org`) has its own dedicated name whereas *Apache County Sheriffs Office* (`www.co.apache.az.us/sheriff/`) does not.

To measure dedicated domain names we divided the set of AA URLs into two groups depending on whether the URL path segment is empty (674 entries) or not (691 entries); the group with empty path segments was then regarded as having dedicated names. To prevent false positives of non-dedicated names, we manually examined all these websites and verified that the landing page does not relate to the Alerting Authority. We found only 25 false positives (*e.g.,* `http://www.franklincountyema.org/db/` with `/db` path being the start page), which leads to overall ≈ 51% AAs with dedicated names while the rest represents common names of parent organizations or other service providers. We also observed three emergency management agencies with dedicated names which are redirected (using HTTP 301/302 response codes) to web pages under county or state websites. Out of the total 1,365 collected URLs 1,327 unique domain names exist, showing that in some cases multiple entities are subsumed under the same domain, *e.g.,* different agencies all under the domain name of a single state.

The data also shows that all educational entities (total of 4) and over 90% of governmental entities (467 out of 503) such as state and local governments own dedicated names in contrast to only ≈ 25% of public safety entities (164 out of 669), and less than half of military organizations (8 out of 19) which nearly all are represented under `home.army.mil`.

5.2 Namespace Structure

We start with various TLDs and country code second-level domains (ccSLDs) in use by Alerting Authorities, which we group as follows:

gTLD [48]: generic top-level domain, *e.g.,* `.org`
ccTLD [47]: country code top-level domain, *e.g.,* `.us`
ccSLD [49]: country code second-level domain, *e.g.,* `.ny.us`
sTLD [50]: sponsored top-level domain, *e.g.,* `.mil`

Each TLD group features different properties. In general, there are little to no delegation limits and naming conventions for names under gTLDs or ccTLDs except for the `.us` namespace. Under `.us` ccTLD more than 3,000 names are reserved and unavailable for public registration [61] and the namespace has a rigorous structure with domain names at second, third, or fourth levels. This structuring reflects the "political geography" [25] and defines a number of reserved names for designated organizations or purposes, *e.g.,* county or city, and territory of operation [25, 62]. Finally, sponsored TLDs (`.edu`, `.gov`, and `.mil`) impose stricter eligibility requirements and thus have an advantage over gTLD names so that it can be made sure that only eligible registrants are granted the ownership of

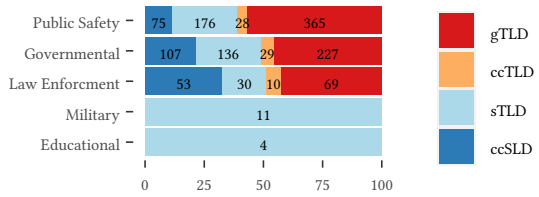


Figure 3: Distribution of TLD types per operation territory

respective domain names [31, 71], given that such policies are adequately enforced by respective registries.

As summarized in Table 2, whereas half of domain names are registered under generic TLDs, the remaining majority (≈ 45%) makes use of sponsored TLDs and names within the `.us` state-code namespace, and the rest 5 percent opts for domains under ccTLDs. It is noteworthy that the `.us` locality namespace exhibits a relatively low penetration among AAs. For example, the usage of canonical forms `[ci,co].<locality>.<state-code>.us` for cities or counties: we observe that for every 5 cities which have the term *city* in their domain names there exists only 1 city which uses the foreseen naming pattern, and for every 4 counties choosing to have the term *county* in its domain name, there is only one county opting for the canonical form.

Finally, we examined if the specific choice of top-level domains for an organization correlates with the organization's field of operation. Figure 3 depicts how widespread various TLD types are in use in different fields of operation. It is noteworthy that educational and military organizations make exclusive use of restricted TLDs (`.edu` and `.mil` respectively), whereas gTLDs remain the more popular choice among the others. This figure also confirms the previous observations that the majority of remaining organizations, regardless of field of operation, opt for generic TLDs instead of taking advantage of special namespaces within the well-organized structured of `.us` namespace.

5.3 DNSSEC Deployment

We used `drill` to chase DNS signatures and verify if a domain has properly activated DNSSEC. All TLDs in use by AAs (see Table 2) support DNSSEC except a number of `.us` ccSLD domains: out of 50 total state ccSLDs under `.us` namespace, 32 have been used by AA organizations with only 18 supporting DNSSEC. Figure 4 depicts the state ccSLDs, which support DNSSEC (blue), which do not support (red), and those which are not used by any of organizations in our data set (white).

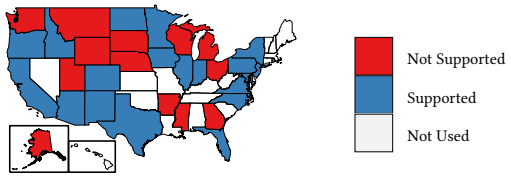


Figure 4: Support for DNSSEC among `.us` ccSLDs in use

Table 3: DNS and Web PKI alongside 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 (see Table 1)

Although ≈ 57% of TLDs in use support DNSSEC, less than 4% of AA domain names have DNSSEC enabled. Compared with the longitudinal DNSSEC study of Chung et al. [22], measuring 0.6% for `.com` and 1.0% for `.org` domains, we observe a higher DNSSEC penetration. However, to our surprise even among `.gov` SLDs which are mandated to implement DNSSEC [66] less than 10% (30) have support for DNSSEC which is considerably less than the ≈ 90% DNSSEC penetration among select governmental organizations (sample set of ca. 1200 `.gov` SLDs) as measured by NIST [63].

6 WEB PKI ANALYSIS

The ecosystem of Web PKI revolves around X.509 certificates. We investigate the deployment and characteristics of certificates in the context of Alerting Authorities to answer the following questions:

(1) To what extent do AAs adapt web PKI?
(2) How is the historic landscape of X.509 shaped among AAs?

6.1 Current Deployment of Certificates

To have a better understanding of the current deployment of web certificates, we gathered a snapshot of SSL/TLS deployment on public servers of Alerting Authorities.

Out of the total 1327 unique names, 1187 hosts (≈ 89%) support SSL/TLS with 1130 hosts (≈ 95%) delivering valid X.509 certificates. Within the remaining 57 hosts, 17 use expired certificates, 9 use self-signed certificates, and 1 has self-signed certificates in its certificate chain. The validity of certificates provided by the remaining 30 hosts could not be verified due to some kind of misconfiguration, *e.g.,* use of invalid certificates or certificates with missing issuer information. Recall that we use OpenSSL trusted root certificates for validation. Compared with other Web PKI studies we see in our focused sample of AA organizations relatively less invalid certificates compared to global average of 65% as observed by Chung et al. [21] over the IPv4 space in 2016, or ≈ 13% as measured by Durumeric et al. [28] for Alexa 1M top domain list in 2013.

Table 4: 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 (see Table 1)

Table 3 combines our findings from this Section and Section 5 to reveal different combinations of DNS and X.509 certificate characteristics, linked to different levels of assurance according to Table 1. In Table 4, we group our results by organization types. Due to low penetration of DNSSEC, popularity of open TLDs, and pervasiveness of DV certificates among AAs (§ 5), only about 22% of AA are considered to be equipped against common threats to trustworthy communication.

6.2 Historic X.509 Certificate Landscape

The historic analysis of X.509 certificates collected from Certificate Transparency logs (see Section 4) helps us to gain a better understanding of security policy changes related to Alerting Authorities and CAs. We span ten years. It should be noted that the total number of organizations with publicly logged certificates changes for each year. We consider this in the following and normalize the results either with respect to the number of organizations or total number of certificates valid per year.

6.2.1 Certificate Authorities. In addition to common regulations, certificate authorities implement and follow their own set of policies. From the perspective of relying parties, *i.e.,* web users, such policies are opaque and as long as a CA is included in a user's trust store, it is considered trustworthy. For the subscribers, however, these policies among other factors such as fees, offered certificate types, and operation costs are decisive in choosing an appropriate CA.

We focus our analysis on the list of top CAs with an average coverage of yearly 20 unique AA subscribers (hosts) in the last decade. We use the term *cover* to differentiate from issuance: if a host, for example, is issued a certificate by a CA valid from 2010 to 2013, we consider this host to be covered by that CA for 2010, 2011, 2012, and 2013. Respectively, if a CA issues multiple short-lived certificates (*e.g.,* 90 days) for a host within a given year, we only count that host as covered once in that year by the issuing CA. This would avoid the data skew in favor of issuers with lower certificate validity windows and higher certification rate per year. It also should be noted that a single host can have certificates issued from different CAs. Figure 5 depicts these findings in terms of relative market share development in the past decade (see Table A.II in Appendix for details). Compared with the CA market share for the Alexa 1M top domain list throughout the last last decade [2, 28, 45] we observe parallels, such as decline of GoDaddy's market share and rapid gains of Let's Encrypt, as well as discrepancies that cannot directly be explained due to dynamic nature of and fluctuations in the Alexa top list.

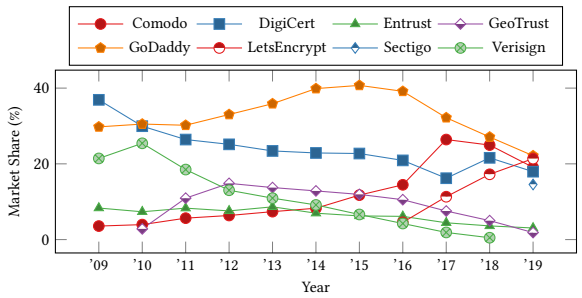
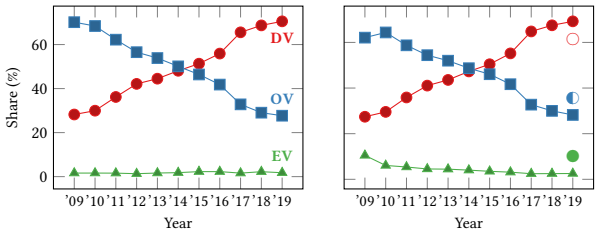


Figure 5: Market share of top CAs in the past decade



(a) Certificate types **(b) Assurance profiles**

Figure 6: Development of certificate types and assurance profiles (§3) in the past decade

Figure 5 also highlights two factors evidently decisive for AAs in their choice of CA: convenience and cost factors. GoDaddy, for example, which has been the market leader among AAs for about two thirds of the past decade, provides web hosting and domain name registration beside certification services in convenient packages; and Let's Encrypt, which has surged to the top in the short period after its public offering, offers automated DV certification at no cost.

6.2.2 Validation types and assurance profiles. In Section 6.1, we showed that currently only about 22% of AAs honor security profiles that are resilient against threats to trustworthy communication (see Tables 3 and 4). Historically, however, as depicted in Figure 6, a higher share of alerting authorities provisioned for such measures. When compared with the share of various certificate validation types (DV, OV, and EV), it becomes evident how the decreasing usage of OV certificates is directly proportional to the reduction of preferred assurance profiles. At the same time the surging popularity of DV certificates has led to an increase in cases of what we consider as inadequately trustworthy (no identification). It should be noted that as our partial historical DNSSEC penetration statistics (collected through SecSpider[4] [67]), covering ≈ 25% of studied hosts, exhibits negligible fluctuation in DNSSEC penetration, we made a simple assumption that historic support for DNSSEC among AAs equals to its current penetration state (see Section 5.3).

6.2.3 Certificate Sharing. Except EV certificates, both DV and OV certificates allow wildcard names as subject alternative names (SAN)

[4] `https://secspider.net`

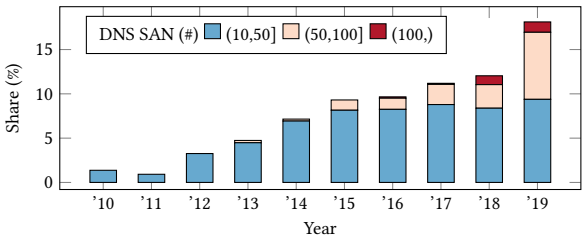


Figure 7: Share of host names represented by certificates with more than 10 unique SAN entries

to avoid enumerating all FQDNs under the control of the certificate holder. In practice, the SAN extension also allows sharing a certificate among different hosts. For example, In 2019 the federal government was issued OV certificates with more than 600 SAN entries each. Certificate sharing expands the attack surface and increases operational costs since if one of the hosts is compromised or the certificate is revoked, every other host also need to configured with a new certificate (sometimes called "fate-sharing").

Multitenancy web hosting and security service providers (both public or government exclusive) are making use of shared certificates as depicted in Figure 7. It is worth noting that Let's Encrypt certificates only allow up to 100 DNS type SANs. In our analysis, we also noticed an increasing number of certificate sharing among hosts which *do not* belong to the same logical entity. Most critically also among OV certificates where a service provider obtains a certificate under its name and lists the host name of its customers as SAN, practically defeating the identification purpose of the certificate. At the time of writing, for example, we observe cases of such certificates listing SANs that obviously belong to separate entities, *e.g.*, `mo.gov`, `asap.farm`, and `incapsula.com` under the same certificate. In this very specific case, records from the *Wayback Machine* archives show that `asap.farm` has previously belonged to Missouri Department of Agriculture [65] but it was never removed from the certificate as the domain name registration was transferred to another entity.

6.2.4 Certificate Validity. A certificate is presumed valid if, among others, it is deployed within its validity period, is issued by a trustworthy CA, carries a valid signature, is bound to the correct subject name, and is not revoked (see RFC 5280 [26]). Checking revocation status often requires network transactions, and is the most expensive operation among aforementioned factors. Thus in many cases it is either performed inadequately or ignored altogether by browsers (partly in favor of proprietary solutions) [57]. Consequently, in the past years both CAs and browser vendors have been negotiating to cap and reduce certificate lifetimes [38–40] as an effort to reduce security risks due to misissued or revoked certificates.

As depicted in Figure 8, the lifetime of certificates utilized by AAs has been constantly decreasing. This trend can partly be attributed to consensus among CAs and browser vendors to reduce certificate lifetimes, but also due to rising popularity of CAs which are specialized on free and automated DV certificates such as Let's Encrypt (fixed lifetime of 90 days). The median validity periods that we observe here are comparable with related works [21, 28], yet

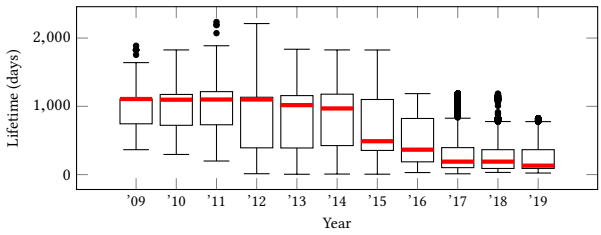


Figure 8: Validity distribution of logged certificates per year

there are no recent studies that can corroborate the sharp decrease in validity periods from 2015 on.

7 RELATED WORK

To the best of our knowledge, this is the first study investigating how Alerting Authorities in the US (as part of broader critical infrastructure) implement measures to cater for trustworthy Web-based communication and service provision. Previous research on trust in online emergency service provision mainly focuses on form and content and its relation to the perception of trustworthiness [17, 29, 46], conception of trustworthy emergency communication and collaboration systems [18, 69] or simply best practices in building trust [10, 58]. Although previous research has already highlighted how knowing who is behind an online emergency service impacts the trustworthiness of their respective services [29, 58, 70], we observe a research gap when it comes to evaluating the measures at one's disposal to reach this goal. More specifically, the interplay of characteristics of domain names and X.509 certificates, *i.e.,* Assurance Profile (Section 3). has not been investigated to our best knowledge. Respectively, we limit ourselves to an overview of related work which studies these technologies on their own.

Domain Namespace and DNSSEC. The influence of a domain name on authenticating or at least recognizing the real-world entity behind that name has been investigated in terms of general trustworthiness associated with TLDs and impersonation of trusted entities through domain name masquerading. Walther, Wang, and Loh [88] examine how choice of TLD can positively impact the credibility of health websites. Seckler *et al.* [81] investigate how a relevant domain name, *e.g.,* a known TLD, can positively enforce familiarity and in turn increase trust. Similarly, a yearly report [37] commissioned by the Public Internet Registry examines the trustworthiness of select TLDs among NGO donors.

A closely related topic is how the domain namespace of malicious websites is structured and operated. Korczynski *et al.* [53] show how low pricing and registration barriers alongside the possibility of bulk registration is an enabler for malicious actors to migrate to new gTLDs. In a longitudinal study of typosquatting, Agten *et al.* [4] reveals how registration fees and registry policies can attract or deter malicious actors; practically determining the credibility of such TLDs (the top three most abused TLDs in the world are new gTLDs [72]). And Antonakakis *et al.* [6] introduce a reputation system for DNS to detect malicious domain names. Different studies show how scammers try to impersonate other entities by partly or fully integrating legitimate domain names in their own domain names [4, 52, 75, 86] or even by using homonymous names using internationalized domain names [85].

With regard to namespace security, studies in the past pinpoint a relatively low DNSSEC penetration due to various factors ranging from lack of support by local resolvers to server misconfigurations [22, 42, 56, 68] despite more than 90% of all TLDs being signed and supporting DNSSEC [74]. The prevalence of DNSSEC among various types of organizations, such as educational, military, commercial, *etc.* has not been subject of study to determine if there is a correlation between field of operation and sensibility for DNS security measures. The only exception is the fine-grained, *i.e.,* including second level domains, regular analysis of DNSSEC deployment among select governmental agencies within the `.gov` namespace, educational institutions, and industry in the US [63, 77].

Web PKI. Throughout the years, various measurements have characterized X.509 certificates in use over the Internet in terms of validity, issuing CAs, key strength, *etc.* [21, 28, 45, 60]. Among these, Mishari *et al.* [60] investigate the difference between certificates of legitimate and fraudulent websites. The study by Holz *et al.* [45] has the advantage of being performed from different vantage points spread over the world. The measurements by Durumeric *et al.* [28] is noteworthy as it goes beyond mere X.509 certificate analysis and investigates the dependencies among root and intermediate CAs, their market share, and the characteristics of respective certificates. And finally, the measurements performed by Chung *et al.* [21] aim to understand why a majority of certificates advertised over IPv4 are invalid. It should be noted that except the last study, the others have been carried out before major changes in the Web PKI occurred, such as various mergers and the public launch of Let's Encrypt [2]. Furthermore, the findings from these studies exhibit different characteristics of sample sets, which are either too limited (*e.g.,* Alexa Top 1M) or too broad (*e.g.,* IPv4 space). Those differences do not allow for statistical inference and comparison with our observations.

In a recent study, which is most closely related to our work, Singanamalla *et al.* [83] measure the adoption of https at government websites. Using primarily an automated, keyword-based matching to collect domain names this approach is prone to false positives and makes comparison to our work infeasible. Also, this work does not relate to Assurance Profiles, which we introduce in our study.

Specifically related to the topic of our work are studies which investigate the trustworthiness of CAs in general and their policies specially in enabling fraud and impersonation. Delignat-Lavaud *et al.* [27], for example, investigate the conformance of CAs to the CA/Browser Forum guidelines, which in turn can influence trustworthiness of a CA. Others have defined various metrics to qualify [19, 30] or quantify trustworthiness of CAs [43] beyond technical measures. In a recent study Schwittmann, Wander and Weis [80], similar to Brandt *et al.* [14], exhibit how various CAs are susceptible to attacks on DV certification processes that can practically lead to domain impersonation. Roberts *et al.* [75] studies which CAs are responsible for issuing DV certificates to malicious target-embedded domains.

8 KEY FINDINGS AND DISCUSSIONS

Our results draw a rather alarming picture of the current online emergency management landscape regarding trustworthy communication. Along the line of our key findings, we discuss the possible reasons for the observed deficiencies and suggest alternatives.

Only about 22% of AAs deploy sufficient identification. Identification, as discussed in Section 3, succeeds over multiple factors, which are only insufficiently attended to by AAs: only about half of AAs have their dedicated names and as such cannot obtain exclusive X.509 certificates as proof of identity (as these are bound to domain names) while a majority of ≈ 78% fail to provide any valid certificate or just DV certificates which lack identification information. The majority of organizations opt for generic TLDs which simplifies name spoofing and phishing as precursors of impersonation. Additionally, the minuscule penetration rate of DNSSEC provides another attack surface by poisoning DNS records and misdirecting users to malicious websites. Alerting Authorities should at best be located under restricted namespaces as an additional factor of recognizably and assurance, have at least their own subdomains instead of being subsumed in the path segment of a URL, secure their namespace using DNSSEC, and provide OV/EV certificates as definitive proof of identity.

Less than 4% of AAs offer secure name resolution. Securing domain names is seemingly a non-priority for investigated organizations as the low penetration rate of DNSSEC suggests. Insecure DNS not only can cause misdirection from authentic websites, but also DV certificate misissuance [14, 80] which impacts both identification and session security. Although DNSSEC suffers low deployment on the global scale in general, it is an indispensable component in securing emergency communication as part of the broader critical infrastructure. Yet, it should be noted that in some cases due to lack of support registrants are forced to abandon DNSSEC in favor of other factors, *e.g.,* registering under a `.us` locality name for which there is, surprisingly, no DNSSEC support (see Figure 4). We also note that although domain names under `.gov` namespaces are mandated to use DNSSEC [66], the low support for DNSSEC has its roots in operational and organizational mismanagement rather than technical issues.

DV certificates dominate transaction security. The popularity of domain validation certificates combined with low penetration of DNSSEC represents an attack surface that can compromise session security through certificate missisuance and monkey-in-the-middle attacks. If DV is indispensable for some, we encourage the stakeholders to reconsider semantically equivalent alternative of TLSA domain issued certificates (DANE EE) as they provide higher resilience against spoofing in contrast to DV certificates [80]. In general, DANE can be used to remove ambiguity regarding public keys and responsible CAs for a domain name [67].

Fate-sharing is on the rise. The lack of dedicated domain names and an increase of certificate sharing in multitenancy settings represents worrisome and de facto unnecessary dependencies, which both can expand the attack surface [67] and can cause instabilities in the future. Regarding shared certificates, we suggest abandoning them completely and also encourage CAs to avoid issuing OV certificates for service providers without ensuring that all the listed subject alternative names belong to the same organization.

Convenience and cost impact security preferences. We observe 15% of AAs providing none or invalid certificates. This can be traced back to carelessness regarding the Web PKI trust model (self-signed certificates) or additional (not only financial) configuration [54] and certification costs. Rapid growth of Let's Encrypt with its fully automated certificate issuance and renewal is an indication of how the aforementioned factors influence the decision for choosing an appropriate CA. Similarly, we measure less than 45% represented under restricted namespaces. In contrast to gTLDs, higher registration fees or bureaucratic hurdles, and longer delegation processing times are among discouraging factors, which call for governmental support and can effectively be addressed by policy-makers through price caps and easier access for eligible organizations which fulfill the strict requirements.

Responsibilities beyond Alerting Authorities. The scope of trustworthy communication goes beyond our investigations and extends to consumers as well as infrastructure operators such as CAs, ISPs, and browser vendors. There is still a gap between CA practices and guidelines [27], some automated DV certification services are susceptible to impersonation attacks [75, 80], and some root CAs do not restrict certification scope for their intermediate CAs [28]. DNS registrars not always offer DNSSEC by default or free of cost [23] and only a minority of ISPs bother to operate DNSSEC-aware recursive resolvers that properly verify signed DNS records [22, 89]. Browser vendors should also provide better security usability by avoiding confusing SSL/TLS warnings [5], improve instead of abandoning visual cues for different certificate types [32, 44, 64], and start offering alternative CA trustworthiness assessment measures beyond the standard binary trust model [19, 30, 43]. Finally, users should be educated in better understanding the semantics of domain names [76] and web PKI certificates and their practical use and ramifications.

9 CONCLUSION AND OUTLOOK

In this paper, we conceptualized a threat model for trustworthy communication in emergency management and analyzed the lack of common technologies, DNS(SEC) and Web PKI, to mitigate threats to identification, resolution, and content manipulation or eavesdropping. We provided an overview of how Alerting Authorities (AA) in the US are structured within the domain namespace, how widespread is DNSSEC in securing their domain names, and how Web PKI is used for authentication and data security. We uncovered deficiencies and discussed alternatives while emphasizing that respective solutions are not necessarily technical but operational as well as political. Protecting critical infrastructure for emergency communication and public safety entails addressing operational and policy challenges on national and international levels and calls for commitment of all stakeholders from service providers to intermediate infrastructure operators and browser vendors alongside policy-makers.

In the future, this work can be extended beyond the US territory while providing a comparison basis for other countries. Furthermore, other technologies can be accommodated in our assurance

profiles. Finally, the role of intermediate infrastructure and further dependency structures can be investigated in depth.

Data Disclosure. We provide a browser that presents the assurance profile of each Alerting Authority and additional accompanying material on `https://aa.secnow.net`. Our toolchain and collected data are published under `doi:10.5281/zenodo.4300946`.

Ethical Considerations. We informed Alerting Authorities about their assurance profiles to raise awareness for improvements.

Acknowledgments. This work was supported in parts by the German Federal Ministry of Education and Research (BMBF) within the project *Deutsches Internet-Institut* (grant no. *16DII111*).

REFERENCES

[1] D. Eastlake 3rd. 2011. *Transport Layer Security (TLS) Extensions: Extension Definitions.* RFC 6066. IETF.

[2] Josh Aas, Eric Rescorla, Seth Schoen, Brad Warren, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J Alex Halderman, Jacob Hoffman-Andrews, and James Kasten. 2019. Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. In *Proc. of the 2019 ACM SIGSAC CCS*. ACM Press, New York, NY, USA, 2473–2487.

[3] U.S. General Services Administration. 2020. Digital Analytics Program. `https://analytics.usa.gov/`

[4] Pieter Agten, Wouter Joosen, Frank Piessens, and Nick Nikiforakis. 2015. Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. In *Proc. of the 2015 NDSS*. Internet Society, Reston, VA, USA, 8–11.

[5] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proc. of 22nd USENIX Security Symposium*. USENIX Association, 257–272.

[6] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. 2010. Building a dynamic reputation system for DNS. In *Proc. of the 19th USENIX Security Symposium*. USENIX Association, 273–289.

[7] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. *DNS Security Introduction and Requirements.* RFC 4033. IETF.

[8] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. *Protocol Modifications for the DNS Security Extensions.* RFC 4035. IETF.

[9] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. *Resource Records for the DNS Security Extensions.* RFC 4034. IETF.

[10] Susana Arroyo Barrantes, Martha Rodriguez, and Ricardo Pérez (Eds.). 2009. *Information Management and Communication in Emergencies and Disasters.* Pan American Health Organization, Washington D.C., USA.

[11] National Fire Protection Association and M.T. Wixted. 2018. *NFPA 1600, Standard on Continuity, Emergency, and Crisis Management, 2019 Edition.* National Fire Protection Association, Quincy, MA, USA.

[12] D. Atkins and R. Austein. 2004. *Threat Analysis of the Domain Name System (DNS).* RFC 3833. IETF.

[13] B. Wayne Blanchard. 2008. Guide To Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation. , 1366 pages.

[14] Markus Brandt, Tianxiang Dai, Amit Klein, Haya Shulman, and Michael Waidner. 2018. Domain Validation++ For MitM-Resilient PKI. In *Proc. of the 2018 ACM SIGSAC*. ACM Press, New York, NY, USA, 2060–2076.

[15] J. Scott Brennen, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. 2020. Types, sources, and claims of COVID-19 misinformation. `https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation`

[16] Minyvonne Burke. 2020. Coronavirus: State unemployment websites crash as applications surge. `https://www.nbcnews.com/news/us-news/coronavirus-state-unemployment-websites-crash-applications-surge-n1162731`

[17] Maria Grazia Busà, Maria Teresa Musacchio, Shane Finan, and Cilian Fennel Stillwater. 2015. Trust-building through social media communications in disaster management. In *Companion Proc. of the 24th ACM WWW*. ACM, New York, NY, USA, 1179–1184.

[18] Monika Büscher, Preben Holst Mogensen, and Margit Kristensen. 2009. When and How (Not) to Trust It? Supporting Virtual Emergency Teamwork. *International Journal of Information Systems for Crisis Response and Management* 1, 2 (apr 2009), 1–15.

[19] David W. Chadwick and Andrew Basden. 2001. Evaluating trust in a public key certification authority. *Computers and Security* 20, 7 (2001), 592–611.

[20] Apoorva Chauhan and Amanda Lee Hughes. 2017. Providing Online Crisis Information. In *Proc. of the 2017 CHI*. ACM Press, New York, NY, USA, 3151–3162.

[21] Taejoong Chung, Yabing Liu, David Choffnes, Dave Levin, Bruce MacDowell Maggs, Alan Mislove, and Christo Wilson. 2016. Measuring and Applying Invalid SSL Certificates: The Silent Majority. In *Proc. of the ACM IMC '16*. ACM Press, New York, NY, USA, 527–541.

[22] Taejoong Chung, Roland Van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A longitudinal, end-to-end view of the DNSSEC ecosystem. In *Proc. of the 26th USENIX Security Symposium*. USENIX Association, 1307–1322.

[23] Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. Understanding the Role of Registrars in DNSSEC Deployment. In *Proc. of the ACM IMC '17*. ACM, New York, NY, USA, 369–383.

[24] Sherri L. Condon and Jason R. Robinson. 2014. Communication media use in emergency response management. In *ISCRAM 2014 Conference Proceedings*. ISCRAM, 687–696.

[25] A. Cooper and J. Postel. 1993. *The US Domain.* RFC 1480. IETF.

[26] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* RFC 5280. IETF.

[27] Antoine Delignat-Lavaud, Martín Abadi, Andrew Birrell, Ilya Mironov, Ted Wobber, and Yinglian Xie. 2014. Web PKI: Closing the Gap between Guidelines and Practices. In *Proc. of the 2014 NDSS*. Internet Society, Reston, VA, USA, 23–26.

[28] Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman. 2013. Analysis of the HTTPS certificate ecosystem. In *Proc. of the ACM IMC '13*. ACM Press, 291–304.

[29] Tristan Endsley, Yu Wu, and James Reep. 2014. The source of the story: Evaluating the credibility of crisis information sources. *ISCRAM 2014 Conference Proceedings* 1, 1 (2014), 160–164.

[30] Tariq Fadai, Sebastian Schrittwieser, Peter Kieseberg, and Martin Mulazzani. 2015. Trust Me, I'm a Root CA! Analyzing SSL Root CAs in Modern Browsers and Operating Systems. In *Proc. of the 2015 10th ARES*. IEEE Press, 174–179.

[31] Federal Networking Council. 1997. *U.S. Government Internet Domain Names.* RFC 2146. IETF.

[32] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo. 2019. Rethinking connection security indicators. In *Proc. of 12th SOUPS*. USENIX Association, 1–14.

[33] FEMA. 2004. Are you ready? An In-depth Guide to Citizen Preparedness.

[34] FEMA. 2020. Integrated Public Alert & Warning System. `https://www.fema.gov/integrated-public-alert-warning-system`

[35] FEMA. 2020. Organizations with Alerting Authority Complete and In Process. `https://www.fema.gov/media-library/assets/documents/117152`

[36] Sara Fischer. 2020. Media wrestles with public trust as coronavirus intensifies. `https://www.axios.com/media-public-trust-coronavirus-da69dd7f-4b8a-4793-ac52-dc1ed2c3e35f.html`

[37] Nonprofit Tech for Good. 2018. 2018 Global Trends in Giving Report. `https://givingreport.ngo/`

[38] CA/Browser Forum. 2017. Ballot 185 – Limiting the Lifetime of Certificates. `https://cabforum.org/2017/02/24/ballot-185-limiting-lifetime-certificates/`

[39] CA/Browser Forum. 2017. Ballot 193 – 825-day Certificate Lifetimes. `https://cabforum.org/2017/03/17/ballot-193-825-day-certificate-lifetimes/`

[40] CA/Browser Forum. 2019. Ballot SC22 – Reduce Certificate Lifetimes (v2). `https://cabforum.org/2019/09/10/ballot-sc22-reduce-certificate-lifetimes-v2/`

[41] Abigail W. Geiger. 2019. Key findings about the online news landscape in America. `https://pewrsr.ch/34CNdu3`

[42] Hao Yang, Eric Osterweil, Dan Massey, Songwu Lu, and Lixia Zhang. 2011. Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing* 8, 5 (sep 2011), 656–669.

[43] Michael P. Heinl, Alexander Giehl, Norbert Wiedermann, Sven Plaga, and Frank Kargl. 2019. MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness. In *Proc. of the 2019 ACM SIGSAC CCSW*. ACM Press, New York, NY, USA, 1–15.

[44] Johann Hofmann. 2019. Intent to Ship: Move Extended Validation Information out of the URL bar. `https://groups.google.com/d/msg/firefox-dev/6wAg_PpnlY4/C_DCyZm9AQAJ`

[45] Ralph Holz, Lothar Braun, Nils Kammenhuber, and Georg Carle. 2011. The SSL landscape – A Thorough Analysis of the X.509 PKI Using Active and Passive Measurement. In *Proc. of the ACM IMC '11*. ACM Press, New York, NY, USA, 427.

[46] Amanda Lee Hughes and Apoorva Chauhan. 2015. Online media as a means to affect public trust in emergency responders. *ISCRAM 2015 Conference Proceedings* (2015), 182–192.

[47] ICANNWiki. 2017. Country code TLD. `https://icannwiki.org/ccTLD`

[48] ICANNWiki. 2017. Generic TLD. `https://icannwiki.org/GTLD`

[49] ICANNWiki. 2017. SLD. `https://icannwiki.org/SLD`

[50] ICANNWiki. 2017. STLD. https://icannwiki.org/STLD

[51] Mohammad Taha Khan, Xiang Huo, Zhou Li, and Chris Kanich. 2015. Every second counts: Quantifying the negative externalities of cybercrime via typosquatting. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 135–150.

[52] Panagiotis Kintis, Najmeh Miramirkhani, Charles Lever, Yizheng Chen, Rosa Romero-Gómez, Nikolaos Pitropakis, Nick Nikiforakis, and Manos Antonakakis. 2017. Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse. In *Proc. of the 2017 ACM SIGSAC CCS*. ACM Press, New York, NY, USA, 569–586.

[53] Maciej Korczynski, Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C. M. Moura, Arman Noroozian, Drew Bagley, and Cristian Hesselman. 2018. Cybercrime After the Sunrise: A Statistical Analysis of DNS Abuse in New GTLDs. In *Proc. of the 2018 ACM ASIACCS*. ACM, New York, NY, USA, 609–623.

[54] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. "I have no idea what I'm doing" – on the usability of deploying HTTPS. In *Proc. of the 26th USENIX Security Symposium*. USENIX Association, 1339–1356.

[55] B. Laurie, A. Langley, and E. Kasper. 2013. *Certificate Transparency*. RFC 6962. IETF.

[56] Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. 2013. Measuring the practical impact of DNSSEC deployment. In *Proc. of the 22nd USENIX Security Symposium*. USENIX Association, 573–587.

[57] Yabing Liu, Will Tome, Liang Zhang, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Aaron Schulman, and Christo Wilson. 2015. An End-to-End Measurement of Certificate Revocation in the Web's PKI. In *Proc. of the ACM IMC '15*. ACM Press, New York, NY, USA, 183–196.

[58] P H Longstaff and Sung-Un Yang. 2008. Communication Management and Trust: Their Role in Building Resilience to "Surprises" Such As Natural Disasters, Pandemic Flu, and Terrorism. *Ecology and Society* 13, 1 (2008), 1–14.

[59] B.S. Manoj and Alexandra Hubenko Baker. 2007. Communication challenges in emergency response. *Commun. ACM* 50, 3 (March 2007), 51–53.

[60] Mishari Al Mishari, Emiliano De Cristofaro, Karim El Defrawy, and Gene Tsudik. 2009. Harvesting SSL Certificate Data to Identify Web-Fraud. *International Journal of Network Security* 14, 6 (September 2009), 324–338.

[61] Neustar. 2020. Frequently Asked Questions about the .US Domain. https://www.about.us/faqs

[62] Neustar, Inc. [n. d.]. .US Compliance Report. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/domain-names/us-locality-compliance-report.pdf

[63] NIST. 2020. Estimating USG IPv6 & DNSSEC External Service Deployment Status. https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov

[64] Devon O'Brien. 2019. Upcoming Change to Chrome's Identity Indicators. https://groups.google.com/a/chromium.org/d/msg/security-dev/h1bTcoTpfeI/jUTk1z7VAAAJ

[65] Missouri Department of Agriculture. 2018. Missouri Agricultural Stewardship Assurance Program. https://web.archive.org/web/20180107233724/https://asap.farm/

[66] Office of E-Government and Information Technology. 2009. Securing the Federal Government's Domain Name System Infrastructure. , 3 pages.

[67] Eric Osterweil, Danny McPherson, and Lixia Zhang. 2014. The shape and size of threats: Defining a networked system's attack surface. In *2014 IEEE 22nd ICNP*. IEEE, 636–641.

[68] Eric Osterweil, Michael Ryan, Dan Massey, and Lixia Zhang. 2008. Quantifying the Operational Status of the DNSSEC Deployment. In *Proc. of the ACM IMC '08*. ACM Press, New York, NY, USA, 231–242.

[69] Leysia Palen, Kenneth M. Anderson, Gloria Mark, James Martin, Douglas Sicker, Martha Palmer, and Dirk Grunwald. 2010. A Vision for Technology-Mediated Support for Public Participation & Assistance in Mass Emergencies & Disasters. In *Proc. of the 2010 ACM-BCS*. BCS Learning & Development Ltd., Swindon, GBR, Article 8, 12 pages.

[70] Douglas Paton. 2007. Preparing for natural hazards: The role of community trust. *Disaster Prevention and Management* 16, 3 (2007), 370–379.

[71] J. Postel and J.K. Reynolds. 1984. *Domain requirements*. RFC 920. IETF.

[72] Spamhaus Project. 2020. The World's Most Abused TLDs. https://www.spamhaus.org/statistics/tlds/

[73] Morning Consult/The Hollywood Reporter. 2020. National Tracking Poll #200342 – Crosstabulation Results. https://morningconsult.com/wp-content/uploads/2020/03/200342_crosstabs_HOLLYWOOD_Adults_v2_JB-1.pdf

[74] ICANN Research. 2020. TLD DNSSEC Report. http://stats.research.icann.org/dns/tld_report/

[75] Richard Roberts, Yaelle Goldschlag, Rachel Walter, Taejoong Chung, Alan Mislove, and Dave Levin. 2019. You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates. In *Proc. of the 2019 ACM SIGSAC CCS*. ACM Press, New York, NY, USA, 2489–2504.

[76] Richard Roberts, Daniela Lulli, Abolee Raut, Kelsey Fulton, and Dave Levin Levin. 2020. Mental Models of Domain Names and URLs. In *Proc. of SOUPS*. USENIX Association, 5.

[77] Scott Rose. 2012. Progress of DNS Security Deployment in the Federal Government. In *Proc. of the 26th LISA*. USENIX Association, 223–228.

[78] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. 2013. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC 6960. IETF.

[79] Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch. 2018. The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem. In *Proc. of the ACM IMC '18*. ACM Press, New York, NY, USA, 343–349.

[80] L. Schwittmann, M. Wander, and T. Weis. 2019. Domain Impersonation is Feasible: A Study of CA Domain Validation Vulnerabilities. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE Press, 544–559.

[81] Mirjam Seckler, Silvia Heinz, Seamus Forde, Alexandre N. Tuch, and Klaus Opwis. 2015. Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior* 45 (2015), 39–50.

[82] Catherine Shu and Jonathan Schieber. 2020. Facebook, Reddit, Google, LinkedIn, Microsoft, Twitter and YouTube issue joint statement on misinformation. https://tcrn.ch/2xJXrg8

[83] Sudheesh Singanamalla, Esther Han Beol Jang, Richard Anderson, Tadayoshi Kohno, and Kurtis Heimerl. 2020. Accept the Risk and Continue: Measuring the Long Tail of Government https Adoption. In *Proc. of the ACM IMC '20*. ACM, New York, NY, USA, 577–597.

[84] Sophos Labs. 2020. Facing down the myriad threats tied to COVID-19. https://news.sophos.com/en-us/2020/04/14/covidmalware/

[85] Hiroaki Suzuki, Daiki Chiba, Yoshiro Yoneya, Tatsuya Mori, and Shigeki Goto. 2019. ShamFinder: An Automated Framework for Detecting IDN Homographs. In *Proc. of the ACM IMC '19*. ACM Press, New York, NY, USA, 449–462.

[86] Ke Tian, Steve T. K. Jan, Hang Hu, Danfeng Yao, and Gang Wang. 2018. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild. In *Proc. of the ACM IMC '18*. ACM Press, New York, NY, USA, 429–442.

[87] Aizhan Tursunbayeva, Massimo Franco, and Claudia Pagliari. 2017. Use of social media for e-Government in the public health sector: A systematic review of published studies. *Government Information Quarterly* 34, 2 (apr 2017), 270–282.

[88] Joseph B. Walther, Zuoming Wang, and Tracy Loh. 2004. The effect of top-level domains and advertisements on health web-site credibility. *Journal of Medical Internet Research* 6, 3 (2004), 1–11.

[89] Matthäus Wander and Torben Weis. 2013. Measuring Occurrence of DNSSEC Validation. In *Passive and Active Measurement*, Matthew Roughan and Rocky Chang (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 125–134.

[90] Zheng Wang. 2015. A revisit of DNS Kaminsky cache poisoning attacks. In *2015 IEEE GLOBECOM*. IEEE, 1–6.

[91] WHO. 2020. Novel Coronavirus (2019-nCoV) Situation Report - 13. https://apps.who.int/iris/handle/10665/330778

APPENDIX

Table A.I: Regular expressions applied on an AA name to categorize its field of operation (in order of application).

Category	Regular expression
Military	`[^[:alnum:]]fort|^fort|army|missile|base|pfpa`
Governmental	`county|counties|city|commission|borough|town|village|parish|authority|council| government|national|aviation|correction`
Educational	`university`
Law Enforcement	`police|sheriff|investigation|patrol|intelligence|'homeland security'|'law enforcement'`
Public Safety	`911|'9-1-1'|emergency|ema|eom|ohsep|fire|safety|communication|dispatch`

Table A.II: Count of unique hosts with at least one publicly logged certificate per issuer for popular CAs. The last row shows the sum of unique host for all observed CAs.

	Year										
CA	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
Comodo†	3	7	15	21	29	38	62	92	238	304	299
DigiCert	31	53	70	83	92	105	120	133	146	263	281
Entrust	7	13	22	25	34	32	33	39	40	44	48
GeoTrust‡	0	5	29	49	54	59	63	67	68	61	29
GoDaddy	25	54	80	109	141	183	215	249	290	330	347
LetsEncrypt††	0	0	0	0	0	0	0	29	102	210	335
Sectigo	0	0	0	0	0	0	0	0	0	0	228
Verisign‡	18	45	49	43	43	42	35	27	17	6	0
All observed CAs	122	244	298	356	398	458	517	630	830	1012	1109

† Rebranded to Sectigo in 2018. ‡ Acquired by DigiCert in 2017. †† Beta in 2015; public in 2016.