A Cybersecurity Terminarch: Use It Before We Lose It

Eric Osterweil | George Mason University

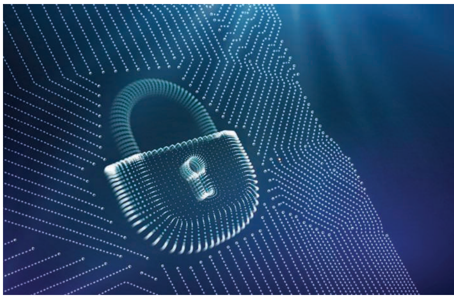
term · in · arch
/ʹ tərmə, närk/
noun
an individual that is the last of its species or subspecies. Once the terminarch dies, the species becomes extinct.

Why can't we send encrypted email (secure, private correspondence that even our mail providers can't read)? Why do our health-care providers require us to use secure portals to correspond with us instead of directly emailing us? Why are messaging apps the only way to send encrypted messages directly to friends, and why can't we send private messages without agreeing to using a single platform (WhatsApp, Signal, and so on)? Our cybersecurity tools have not evolved to offer these services, but why?

Cybersecurity and cryptographically enhanced tools in the Internet have faced an uphill battle for many years, due in no small part to the fact that we do not have a global architecture for deploying interorganizational (platform-agnostic) verifiability, authentication, and encryption. This deficiency stems largely from the absence of a single/unambiguous global-root cryptographic key for verification [i.e., a public key that is usable as a global Trust Anchor (TA)]. A global TA could be used to foundationally enhance protections for security tools, protocols, and more, but attempts to deploy one in the Internet have a long history of failure.

To date, there has only been one success story, and, fortunately, it is still operating. Today, almost everything we do online begins with a query to a single-rooted hierarchical global database, whose namespace is collision-free, and which we have relied on for more than 30 years: the Domain Name System (DNS). Moreover, although the DNS protocol did not initially have verification protections, it does now: the DNS Security Extensions (DNSSEC). DNSSEC's protections stem from the DNS tree's root TA [often called the *Root Zone's Key Signing Key* (*Root KSK*)].

Since its deployment, the management, maintenance, and policies surrounding the Root KSK have been overseen by an international multistakeholder community, the Internet Corporation for Assigned Names and Numbers (ICANN) community.[1] This model ensures that there is no single entity that has unilateral jurisdiction over the Root KSK. Today, DNSSEC's protocol, policies, and infrastructure are operationally mature and widely distributed. However, these protections lie at the low level of the Internet's foundation and are not often noticed at the application (or other



user-facing) layer(s). This has left the potential to extend DNSSEC's verification protections largely untapped. Moreover, the model we are using exposes systemic vulnerabilities.

Since the late 1990s, the verification and authentication used by essentially all our security protocols have made do with a collision-prone hierarchical verification model called the *Web public-key infrastructure* (*Web PKI*). Interfaces like secure sockets use the Web PKI so that applications can benefit from protections from this model without needing to delve into its complexity. Under these covers, the Web PKI's verification substrate uses multiple roots (i.e., multirooted verification). It is a loosely organized list of certification authorities (CAs) that our software uses to verify essentially all our interorganizational data and transactions (TLS tunnels, HTTPS, secure SMTP, file encryption, etc.). The Web PKI provides verification

Digital Object Identifier 10.1109/MSEC.2020.2989703
Date of current version: 9 July 2020

and also asserts trust, but these are separable protections.

Although the Web PKI has raised the bar on miscreants, it has also left important security doors unguarded. Without a definitive starting point for verification, multirooted verification hierarchies suffer from architectural vulnerabilities. For instance, when a multirooted verification hierarchy like the Web PKI is used to authenticate HTTPS web transactions, relying party software packages (like web browsers) have no way to know which CA is authorized to vouch for a website. This is a problem because it can lead to attestation collisions; whereby browsers have no choice but to trust any certificate that is verified by any CA.

One of the earliest high-profile exploits of this attack vector was on a CA named *DigiNotar* in 2011.[2] That event served as a large-scale existence proof of the vulnerability of this model. In multirooted hierarchies, RPs generally don't even have a way to know who all the roots are supposed to be. Knowing all the CA roots in the Web PKI is an open challenge. Browsers attempt to stay current with each other's trust stores, and there is an organization called the *CA/Browser* (CAB Forum) to coordinate this, but other systems that have tried to use TLS (HTTPS's underlying secure connection protocol) have found this intractable. Uses in software like mail servers have essentially become nonstarters for that reason.

Single-rooted verification hierarchies (like traditional PKIs) address the aforementioned problems at an architectural level. With a single root, there is no ambiguity about which signing authority is allowed to vouch for whom (the single root clearly disambiguates this), and there is only one single (well-known) root for RPs to bootstrap and maintain.

There have been several community attempts to create single-rooted verification hierarchies for Internet services, but single-rooted verification has proven to be a difficult species to breed. In 1989, there was an attempt to create a single global root for Privacy-Enhanced Mail in RFC-1114, but the question of who would operate that root was never answered. Later the Web PKI began deployment but not as a multirooted hierarchy. In 1995, VeriSign, Inc. had its CA certificate configured in the then-dominant Netscape Navigator web browser.[3]

At that time, secure web connections verified all websites' cryptographic keys by tracing secure delegation paths from that single root. However, the Web PKI did not have protections that mandated a single root, and as browser software continued to diversify and the World Wide Web continued to grow, the list of root CAs also grew. Today, there are hundreds of root CAs in the Web PKI that are configured in browsers, and they are often maintained (i.e., rolled over, revoked, or otherwise changed) in nontransparent/nonstandard ways.

More recently, the Internet Engineering Task Force (IETF) has standardized protocols for verifying the proper holders of Internet Protocol (IP) addresses and autonomous system numbers using an architecture called the *Resource Public-Key Infrastructure* (*RPKI*) in RFC-6480. After years of trying to align Internet stakeholders, and even after unambiguous advice from the Internet Architecture Board in 2010, the RPKI has not been able to agree on a single root and now plans to operate in perpetuity as a multirooted hierarchy. Just as with the Web PKI, the RPKI now has attestation collisions. Missed attempts like these underscore the singular opportunity that DNSSEC represents. It has even succeeded at an operational scale that other large (private) single-rooted PKIs have failed. As the first and only example of a deployed Internet-scale single-rooted verification hierarchy species, one could worry that we will not be able to create and operationalize another.

New standards, like the DNS-based Authentication of Named Entities (DANE) suite (RFC-6698, RFC-8162, and RFC-7929)[4] have emerged that have the immediate potential to be used to unambiguously secure our protocols and data by using DNSSEC. At a time when recent global events have caused a dramatic increase in teleworking, distance learning, and reliance on online communications and when our Internet privacy has become top-of-mind to many, why shouldn't we be able to apply end-to-end encryption and object-security to our online lives?

Looking forward, this should also include email, medical records, cybersecurity information sharing, and much more. Indeed, now is the right time for us to reassess the foundations that we have built our protections on, and also consider if we may be undermining our strongest (and largely untapped) foundational component.

Problems on the Horizon

Recent DNSSEC-based protocols, like DANE, enable rich protections and are within our grasp; that is, if we don't lose them before we use them. Several recent proposals for DNS over HTTPS, DNS over TLS, and even DNS over QUIC aim to add security and privacy protections in ways that would actually create verification loops and thereby fundamentally (albeit inadvertently) jeopardize the security, stability, and resiliency (SSR) of the DNSSEC.

These proposals focus on using transport-layer security protections, derived from verification performed by the Web PKI, to access DNSSEC. This would be a disastrous weakness because it would fundamentally undercut DNSSEC's verification substrate. Our single-rooted verification hierarchy would (effectively) become a subtree under the multirooted Web PKI. DNSSEC's protections would be subordinated and thereby have an architectural dependency. Although the proposal to protect the transport of DNS is well intended, the approach must not come at the greater cost of our architectural correctness. If we aren't conscientious in our designs, we may never get another global single root, making DNSSEC a terminarch (i.e., the last of its kind).

Other proposals for alternate (i.e., competing) DNS roots (such as the Yeti DNS project) threaten potential disaster, alternate naming schemes (like those of Namecoin, Ethereum Name Service, or the GNU Name System) could portend extinction, and alternate verification schemes like certificate transparency, which essentially enshrine a global default trusted source (the way the Web PKI started), herald the same. In its current state, the DNS has been an extensible resource for more than 30 years, and we have only just begun to tap its potential as a cybersecurity substrate.

How Secure Is DNSSEC? You Be the Judge!

The operations of the DNSSEC root zone follow the strictest form of security hygiene. The DNSSEC root follows a DNSSEC Practice Statement (which is published and available to anyone to inspect at iana.org); its cryptographic keys are maintained in FIPS 140-2 Level 4 hardware security modules, the process and installations have achieved SOC 3 certification for nine consecutive years, there are multiple geographically distributed disaster recovery sites, and high-value top-level domains (TLDs) (like .com, .net, and so on) are also following the same level of security practices.

Even routine processes like generating zone signing keys require a quorum of trusted community representatives to be physically present and to verify material, transactions, and adherence to the ICANN community processes. The DNSSEC root and TLDs are being meticulously protected and managed to ensure the SSR of the entire DNS hierarchy with the same level of security as CAs.

Even exceptions are treated with the highest level of prudence. In 2017, the Root KSK was scheduled to gracefully transition to a newer key (i.e., rollover) because of proactive operational hygiene. However, before this rollover was executed, measurements indicated a potential problem, which prompted operators to postpone this rollover. This prudence serves as just one of many examples of the diligence and care that exists in the management of DNSSEC's global root key. In short, experts are plugged in and taking every precaution necessary to ensure proper operation and success of this critical resource.

Deploying DNSSEC

Now that DNSSEC is enjoying broad adoption by service providers, there are increasingly easy ways for administrators to deploy it. For those who operate their own DNS infrastructure, almost all modern DNS name server software platforms can enable DNSSEC via trivial configurations. For those who use DNS registrars or other managed DNS (mDNS) providers to operate their DNS infrastructures, many of these providers offer to deploy and manage DNSSEC through configuration pages in their online portals. Often, simply looking at the existing configuration options of either one's own infrastructure or the pages of one's provider can be the one-stop shopping for turning DNSSEC on. The DNSSEC communities want to help, and resources like the Internet Society's Deploy 360[5] pages offer resources for guidance to answer questions and to otherwise help with deploying DNSSEC.

Use It Before We Lose It

Although using the DNS to resolve a domain name to an IP address is a critical starting point for almost all our transactions on the Internet, the DNS was designed to be used to look up essentially arbitrary data. Based on this, DNSSEC has evolved the DNS into a global PKI. DNSSEC is in a position to implement general-purpose object security. This could be used to secure threat intelligence, cybersecurity information sharing, the Internet of Things, email, electronic protected health information (e-PHI), and much more.

By using DNSSEC as the Internet's global single root, we will get interoperability across all those Internet systems that already speak DNS. With DNSSEC, we can secure caches against poisoning attacks and reduce transitive trust attack surfaces.[6] The DNSSEC deployment is now counted in the millions of domains and has been growing and succeeding at exponential rates, and operators are becoming increasingly adept at managing their cryptographic deployments.[7] It is ready to be built on.

Protocols like DANE propose to do exactly that, thereby repairing architectural holes that have hamstrung HTTPS. This will allow us to enable fallow object-security models, like using S/MIME for secure end-to-end email encryption and signing.[4] This would not only plug existing security holes, it would also give us never-before-seen cybersecurity facilities. Even DANE's nascent deployment already numbers in the hundreds of thousands. It has opened new possibilities for Internet cybersecurity companies, start-ups, and more.

This all stems from DNSSEC's global single root, the DNS Root KSK, the multistakeholder policy community, and the state-of-the art operations that support the cryptographic material. Cybersecurity professionals have the opportunity now to embrace this resource and capitalize on it to bring the Internet's cybersecurity to a new high watermark, but we as a community need to continue to carefully protect the Internet's first (and possibly last) global single-root verification terminarch: DNSSEC. ■

References

1. "ICANN's multistakeholder model," ICANN. [Online]. Available: https://www.icann.org/community
2. D. Fisher, "Final report on DigiNotar hack shows total compromise of CA servers," Threatpost, Oct. 31, 2012. [Online]. Available: https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
3. N. Wingfield, "Digital IDs to help secure Internet," *InfoWorld*, Oct. 23, 1995. [Online]. Available: https://tinyurl.com/yaf6cwun
4. "How DANE strengthens security for TLS, S/MIME, and other applications," Verisign, Nov. 19, 2015. [Online]. Available: https://blog.verisign.com/security/how-dane-strengthens-security-for-tls-smime-and-other-applications/
5. Internet Society. Accessed on: May, 9, 2020. [Online]. Available: https://www.internetsociety.org/deploy360/dnssec/
6. E. Osterweil, D. McPherson, and L. Zhang, "The shape and size of threats: Defining a networked system's attack surface," in *Proc. 2014 IEEE 22nd Int. Conf. Network Protocols (ICNP)*, pp. 636–641. doi: 10.1109/ICNP.2014.101. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6980440
7. "Growth and health metrics for the global deployment," 2020. [Online]. Available: http://secspider.net/

Eric Osterweil is the vice-chair of the ICANN Second Security, Stability, and Resiliency Review Team (SSR2 RT). Osterweil received a Ph.D. from the Computer Science Department, George Mason University, Fairfax, Virginia. Contact him at eoster@gmu.edu.

Rejuvenating Binary Executables • Visual Privacy Protection • Communications Jamming
IEEE SECURITY & PRIVACY
Building Dependability, Reliability, and Trust
SOFTWARE EVERYWHERE
January/February 2016 Vol. 14, No. 1
Policing Privacy • Dynamic Cloud Certification • Security for High-Risk Users
IEEE Symposium on Security and Privacy
March/April 2016 Vol. 14, No. 2
Smart TVs • Code Obfuscation • The Future of Trust
ECONOMICS OF CYBERSECURITY PART 2
May/June 2016 Vol. 14, No. 3
IEEE
IEEE computer society
CELEBRATING 70 YEARS
IEEE Reliability Society
S & P

Digital Object Identifier 10.1109/MSEC.2020.3002086