Securing the Domain Name System

Daniel Massey
Colorado State University

Dorothy E. Denning
The Naval Postgraduate School

The Domain Name System (DNS) is a critical part of the Internet infrastructure. Virtually every Internet application depends on some form of DNS data, yet access to and the reliability of that data aren't assured. DNS attacks and abuses, meanwhile, are increasingly common and sophisticated. Part of the problem is that security wasn't a major goal of the original DNS design. The DNS community has been aware of security issues for decades, but only now are solutions ready for wide-scale deployment. Motivated by both its importance and recent enhancements to strengthen its security, this issue of *IEEE Security & Privacy* looks at the challenges in securing the DNS.

Security Aspects of Today's DNS

The DNS maps host names such as www.computer.org to IP addresses and provides a wide range of other mapping services, from email to geographic location. In its most basic form, a DNS attack can prevent an application from receiving critical DNS data or redirect the application to a bogus server by providing false data. For example, a Web browser will be unable to load the www.computer.org Web site if DNS fails to respond to a request for the site's IP address. If DNS responds but with the wrong IP address, the browser will contact the wrong server and load phony Web pages. Even if the user recognizes that the loaded pages are fake, he or she generally can't reach the valid site unless DNS provides a legitimate IP address. In this sense, the DNS is truly critical Internet infrastructure, and we must understand its security vulnerabilities and potential solutions.

The article "Protecting the DNS from Routing Attacks: Two Alternative Anycast Implementations," by Ioannis Avramopoulos and Martin Suchara, addresses the challenge of reaching legitimate DNS servers in the first place. To obtain the IP address of www.computer.org, the application must communicate with servers, but by disrupting the routes to them, a DNS attack can deny service or redirect queries to false servers that provide forged DNS data. This article shows how to apply different anycast routing techniques to ensure that critical DNS servers remain available.

Legitimate network administrators work to ensure that DNS data is available for their sites, but spam and phishing campaign organizers also want to guarantee that their sites remain available. The article "Phishing Infrastructure Fluxes All the Way," by D. Kevin McGrath, Andrew Kalafut, and Minaxi Gupta, examines how attackers are abusing the DNS to ensure the availability of fake sites and make it more difficult to shut them down. Using a technique called "fast flux," a DNS name resolves to a large number of IP addresses, which typically have short validities and change frequently, making it difficult to track them down and end the phishing campaign. The article describes the fast-flux behavior in more detail along with variations such as DNS flux and double flux. The authors consider techniques for detecting various flux events and provide both an understanding of the fast-flux problem and a potentially powerful tool for detecting it.

The DNS Security Extensions

Protecting routes to servers improves the DNS's availability, whereas addressing problems such as fast flux limits its misuse. These security enhancements are clearly important, but fundamental problems remain. An attacker with sufficient capabilities can provide false DNS data that denies legitimate service or redirects traffic to false sites. This basic vulnerability has been well known since the early '90s, when Steve Bellovin circulated a paper—"Using the Domain Name System for System Break-Ins"—and several years later presented it at the Fifth Usenix Security Symposium.[1] Concerns over the ability to spoof DNS responses and poison DNS caches remain today. A little more than a year ago, Dan Kaminsky identified an exploit that lets attackers effectively poison DNS caches with false results and demonstrated this attack's devastating impact at Black Hat 2008. Patches were released for most DNS software to help mitigate the vulnerability, but the race between attack strategies and defenses continues.

To address the vulnerabilities Bellovin and others have discovered, the DNS community developed DNS Security Extensions (DNSSEC), which adds data origin authentication and data integrity to the DNS. Roughly speaking, DNSSEC uses digital signatures to provide cryptographic assurance that IP addresses reported for a name such as www.computer.org were entered by the owner of the computer.org zone. With DNSSEC deployed, attackers can't provide DNS data for the site unless they've gained access to a private key belonging to the zone or its ancestors in the DNS hierarchy. After many years of development, DNSSEC was published in March 2005 as RFCs 4033, 4034, and 4035.[2–4] The focus has since shifted from DNSSEC design to deployment.

As of today, DNSSEC deployment is still in its infancy, with only a tiny fraction of zones having deployed it, but it has reached important milestones. Several DNS server and resolver implementations support DNSSEC, and there are both open source tools for administering it in most any size zone and commercial appliances that automate its deployment. Several country code top-level domains, including se (Sweden) and bg (Bulgaria), have deployed DNSSEC for a few years now. The US government has mandated deployment in the gov domain—the gov zone itself is already signed, and a growing set of *.gov zones are deploying DNSSEC. The generic top-level domain org has deployed DNSSEC, and the deployment list is growing. You can find operational guidelines, best practices, and updated information on current deployment at sites such as the DNSSEC Deployment Initiative (www.dnssec-deployment.org), the DNSSEC Industry Coalition (http://dnsseccoalition.org/website/), the SecSpider DNSSEC Monitoring Site (http://secspider.cs.ucla.edu), and the NLnet Labs DNSSEC page (www.nlnetlabs.nl/projects/dnssec/).

This issue provides three articles that cover different aspects of DNSSEC. The combined result discusses how zone administrators can deploy it at authoritative servers, how DNS resolvers can use DNSSEC signatures to authenticate data, and open issues on managing public keys.

"Open Issues in Secure DNS Deployment," by Ramaswamy Chandramouli and Scott Rose, considers DNSSEC from a zone administrator's standpoint. The authors provide a solid overview of both the basic DNSSEC design and DNSSEC deployment issues. With DNSSEC, a zone operator will generate a public-private key pair and use the private key to sign zone data. This article discusses deployment challenges ranging from the selection of appropriate key sizes and rolling over keys to managing authentication chains that let resolvers learn the public keys. It's essential reading for anyone who wants to understand how zone operators should deploy and manage DNSSEC.

Wouter C.A. Wijngaards and Benno J. Overeinder also consider DNSSEC in their article, "Securing DNS: Extending DNS Servers with a DNSSEC Validator," but from the perspective of a DNS resolver trying to validate the DNSSEC signatures zone operators provide. The authors have carefully considered the trade-offs in building a resolver that offers both security and performance and present a publicly available resolver that meets their design objectives. They further analyze their resolver's performance, providing insights on both the advantages and costs in deploying a DNS validator.

Having discussed how authoritative servers sign DNS data and how resolvers validate it, we finally turn to a challenging problem that faces any system that relies on public-key cryptography: How do we learn and manage public keys? A zone owner can create public keys, and resolvers that have learned them can validate data from the zones, but it would be impractical to distribute public keys from all secure zones to all validating resolvers. In an ideal world, DNSSEC would be fully deployed, we could configure resolvers with a single public key of the root zone, and each zone would coordinate with its secure parent so resolvers could follow an authentication chain from the root public key to the desired DNS record. For example, a resolver could use the root public key to authenticate the org public key, which could authenticate the computer.org public key, which in turn could authenticate the IP address (or, more precisely, the DNS type A record set) for www.computer.org. In reality, security extensions are incrementally deployed, and full deployment at every DNS zone might never occur. The article "Interadministrative Challenges in Managing DNSKEYs," by Eric Osterweil and Lixia Zhang, considers the problem of managing these public keys both when an authentication chain can be formed with a secure parent and when no secure parent exists.

We believe this special issue provides an interesting and important look at the DNS, a system that almost everyone relies on but is often overlooked when assessing overall security. The article on protecting routes to the DNS servers illustrates some of the complexities and interactions between Internet infrastructure components, whereas the one on fast flux and phishing demonstrates how attackers can misuse the seemingly simple DNS system in complex ways. Enhancing security in these areas is complementary to the DNSSEC objective of adding origin authentication and data integrity, which the remaining articles examine. We hope this issue helps readers understand the security challenges facing the DNS and the efforts under way to enhance DNS security. □

Acknowledgments

We thank all those who submitted articles for this special issue. We also thank the external reviewers who helped select the articles from a very impressive set of submissions and provided valuable feedback to the authors. Finally, we also thank the *IEEE Security & Privacy* staff and volunteer editors for all their work in producing this issue.

References

1. S.M. Bellovin, "Using the Domain Name System for System Break-Ins," *Proc. 5th Usenix UNIX Security Symp.*, Usenix Assoc., June 1995.
2. R. Arends et al., *DNS Security Introduction and Requirements*, IETF RFC 4033, Mar. 2005; www.ietf.org/rfc/rfc4033.txt.
3. R. Arends et al., *Records for the DNS Security Extensions*, IETF RFC 4034, Mar. 2005; www.ietf.org/rfc/rfc4034.txt.
4. R. Arends et al., *Protocol Modifications for the DNS Security Extensions*, IETF RFC 4035, Mar. 2005; www.ietf.org/rfc/rfc4035.txt.

Daniel Massey *is an associate professor at Colorado State University. His research interests include security for large-scale critical infrastructure such as the DNS and Internet routing. Massey has a PhD in computer science from the University of California, Los Angeles. He is a coeditor of the DNS Security Extensions. Contact him at massey@cs.colostate.edu.*

Dorothy E. Denning *is distinguished professor in the Department of Defense Analysis at the Naval Postgraduate School. Her research interests include cybersecurity and cyberconflict. Denning has a PhD in computer science from Purdue University. She's the author of* Information Warfare and Security *(Addison-Wesley, 1999). Contact her at dedennin@nps.edu.*