

THINGS YOU SHOULD KNOW ABOUT... DNSSEC

Scenario

When Laura returns to campus after the holiday break, she is shocked to hear that she has been de-registered from classes due to nonpayment of tuition. She calls her parents, who confirm that they paid her bill online in early December. They tell her that when they went to the bursar's website, the page looked a bit different and asked for information they had previously entered, but the browser displayed the padlock icon indicating a secure connection, so they paid the bill as usual. They assure her that the funds have already been transferred from their bank account.

Laura heads over to the bursar's office, only to find a crowd of students in the same boat. As they talk about their predicament, they discover that they all paid their tuition online and that they all use the same regional ISP. Further investigation by the university's IT staff confirms that the students fell victim to DNS cache poisoning—a kind of computer attack in which hackers insert bad data into an ISP's name server cache, which, as a result, directs Internet traffic from an intended site (in this case, the bursar's website) to another location. The hackers even purchased an SSL certificate so that the bogus site would have the padlock icon. The university has to let several hundred students re-register without having yet paid tuition, and the students and their families spend months getting their banks to refund the money that was fraudulently transferred from their accounts.

In the future, as administrators of domains and websites implement DNSSEC, such attacks will be prevented. DNSSEC adds a set of security provisions to the way Internet traffic is routed through name servers, protecting users from the kind of attack Laura suffered. When DNSSEC is implemented, if a user's computer is redirected to a bogus version of a website, software that manages web traffic will encounter security keys that should match but do not, indicating a problem. In this way, DNSSEC will plug a fundamental weakness of the Internet.

1 What is it?

Internet-connected devices are identified by IP addresses, though users typically only know web addresses—people can remember “example.edu,” for instance, more easily than “192.168.7.13.” The Domain Name System (DNS) uses a distributed network of name servers to translate text-based web addresses into IP addresses, directing Internet traffic to proper servers. Though invisible to end users, DNS is a basic element of how the Internet functions.

DNS was built without security, however, leaving Internet traffic exposed to forged DNS data, which, among other things, allows the spoofing of addresses to redirect traffic to malicious websites. DNS Security Extensions (DNSSEC) adds security provisions to DNS so that computers can verify that they have been directed to proper servers. DNSSEC authenticates lookups of DNS data (including the mapping of website names to IP addresses) for DNSSEC-enabled domains so that outgoing Internet traffic (including e-mail) is always sent to the correct servers, without the risk of being misdirected to fraudulent sites.

2 Who's doing it?

VeriSign administers the “root,” which supports all top-level domains (TLDs) (.com, .net, .info, and so forth), and is expected to implement DNSSEC for the root (“sign the root”) in 2010. Once that happens, DNSSEC traffic can be validated at its highest level—the root. Several nations—including Sweden (.se domain), Brazil (.br), Bulgaria (.bg), and the Czech Republic (.cz)—have implemented the technology for their country-code domains, and the Public Interest Registry has enabled DNSSEC validation for the .org domain. As part of its compliance with the Federal Information Security Management Act of 2002, which requires increased security for the nation's cyberinfrastructure, the U.S. federal government has implemented DNSSEC for the .gov domain. Until the root is signed, these domains will use a surrogate authority to validate their DNSSEC-enabled web traffic, but all TLDs will eventually use DNSSEC. EDUCAUSE is working with VeriSign to implement DNSSEC for the .edu domain, also in 2010, and this effort is expected to provide guidance about best practices to smooth the transitions of the much-larger .com and .net domains in 2010 and 2011.

3 How does it work?

As data packets travel over the Internet, DNS provides the “maps” that correlate web addresses with IP addresses and route traffic to proper destinations. Because DNS does not provide a mechanism to authenticate the data in name servers, forged or

[more >>](#)

corrupt data in a name server can direct traffic to the wrong server—a weakness that malicious parties use to their advantage. DNSSEC adds digital signatures that ensure the accuracy of lookup data, guaranteeing that computers can connect to legitimate servers.

With DNSSEC, a series of encryption keys are handed off and authenticated—the second-level domain (SLD) key (from example.edu) is authenticated by the TLD (.edu), and the TLD key is authenticated by the root. In this way, when an SLD, its parent TLD, and the root are all signed, a chain of trust is created. (Holders of SLDs can implement DNSSEC before their TLD or the root is signed, creating so-called “islands of trust” that rely on intermediate measures to validate their encryption keys.) If the encryption keys don’t match, DNSSEC will fail, but because the system is backwards-compatible, the transaction will simply follow standard DNS protocols.

The value of the system will come when the root, the TLDs, and SLDs are signed, allowing DNSSEC to be used for all Internet traffic. At that point, when DNSSEC fails, users will not be routed to bogus servers, and they might also be notified that nonmatching DNSSEC keys prevented their transaction from going through.

4 Why is it significant?

Hackers continue to exploit the security weakness of DNS to their advantage. By caching address information, name servers don’t have to look up the IP address every time a frequently visited site is accessed, and this speeds up the experience for end users. If hackers are able to insert a bogus IP address into a cache, however, all users of that name server will be directed to the wrong site (until the cache expires and is refreshed). Corrupting the operation of DNS in this way can lead to many kinds of fraud and other malicious activity. By plugging some of the largest security holes in the Internet, DNSSEC has the potential to significantly expand the trustworthiness—and thus the usefulness—of the Internet as a whole.

5 What are the downsides?

Fully implementing DNSSEC will require an enormous amount of work across every quarter of the Internet—signing the root and the TLDs is simply the tip of the iceberg. Participation is voluntary at this time, and the benefit that DNSSEC ultimately provides will be a reflection of the willingness of domain holders to do that work—that is, the value of DNSSEC will be in direct proportion to the number of sites that implement it. Even after the root and the TLDs are signed, the advantage of DNSSEC will be qualified by uneven rates of adoption.

Adding encryption keys to Internet lookups introduces complex logistical problems of managing those keys, such as how to periodically update keys without breaking the way name servers (and their caches) work, and how to accommodate the differing keys and protocols of different TLDs. Name server software is still evolving to support DNSSEC; many organizations will need to

update their DNS software, and, in some cases, hardware upgrades will also be required. In addition, DNSSEC might degrade the speed of Internet lookups, resulting in a slower experience for end users. On top of the technical and resource-based challenges are policy issues that will need to be resolved at an international level. The effort to implement DNSSEC for the root has renewed a longstanding debate about where “control of the Internet” resides.

6 Where is it going?

Having the root and TLDs signed will provide some incentive for domain holders to implement DNSSEC because the chain of trust can be established, but until a critical mass of domains incorporate the technology, the benefits might not seem to justify the effort. Administrators of most TLDs are expected to develop resources to help ease the implementation of DNSSEC for domain holders, but many of the thorniest technical issues—about not only the transition to but also the maintenance of DNSSEC in practice—still need to be sorted out. Presumably, as domains begin implementing DNSSEC in large numbers, momentum will grow and sustain the transition, but it remains to be seen how long the process might take or at what point a mandate to implement DNSSEC will be required for full adoption.

7 What are the implications for higher education?

The risks posed by DNS and the benefits of implementing DNSSEC have special significance for higher education. Colleges and universities are expected to be “good Internet citizens” and to lead by example in efforts to improve the public good. Because users tend to trust certain domains, including the .edu domain, more than others, expectations for the reliability of college and university websites are high. To the extent that institutions of higher education depend on their reputations, DNSSEC is an avenue to avoid some of the kinds of incidents that can damage a university’s stature.

In more tangible terms, higher education institutions store enormous amounts of sensitive information (including personal and financial information for students and others, medical information, and research data), and they maintain valuable online assets to which access must be effectively restricted. DNS attacks result in stolen passwords, disrupted e-mail (which often is the channel for official communications), exposure to malware, and other problems. DNSSEC can be an important part of a broad-based cybersecurity strategy.

EDUCAUSE

EDUCAUSE is a nonprofit membership association created to support those who lead, manage, and use information technology to benefit higher education. A comprehensive range of resources and activities is available to all EDUCAUSE members. The association’s strategic directions include focus in four areas: Teaching and Learning; Managing the Enterprise; E-Research and E-Scholarship; and the Evolving Role of IT and Leadership. For more information, visit educause.edu.