CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Why Organizations Need a Secure Domain Name System

Key Message: Use of Domain Name System security extensions can help prevent website hijacking attacks.

Executive Summary

Domain Name System (DNS) hijacking attacks attempt to redirect a website request to another site for malicious or unintended purposes. The Internet Engineering Task Force developed security extensions for the Domain Name System that use verification of digital signatures to avert these attacks.

In this podcast, Alex Nicoll, a member of CERT's Enterprise Threat and Vulnerability Analysis team, discusses why Domain Name System security extensions are critical for protecting digital information, networks, and computers.

PART 1: DNS AS INTERNET PHONE BOOK

Using Names Instead of Numbers

In the Internet routing scheme, Internet addresses are long strings of numbers such as "32.36.38.27." In much the same way as a phone book maps telephone numbers to names and addresses, the Domain Name System maps those strings of numbers to names that people can remember more easily, such as "cert.org."

Each device on the Internet (computer, server, mobile device, etc.) has a unique number. DNS takes the name provided by the user and translates this into the unique number for the desired destination device.

Internet Routing System

The Internet is comprised of a large number of subnetworks (subnets). In concert with DNS, the Internet Routing System serves as the map for all Internet subnets, associating names and device numbers.

The routing system and DNS, in effect, associate a specific phone number with a specific physical address.

Subnets can be thought of as regional phonebooks. Only the owner of each subnet can change its phonebook, i.e., the association of names and numbers.

PART 2: HOW SECURITY EXTENSIONS TO DNS MITIGATE HIJACKING

Hijacking Attacks

DNS hijacking attacks occur when a user, without their knowledge, is redirected to a web site that they did not intend. For example, they think they are browsing at CNN.org but are actually browsing an attacker's version of that site.

In the mid 1990s, this problem was recognized but the risk was not considered significant. After about the year 2000, as computers got faster and more powerful, as the kind of computing power needed for hijacking attacks became available to the average person, and as there was money to be made, this security vulnerability began to be exploited.

In response, the Internet Engineering Task Force started developing a backwards-compatible add-on to the DNS that was intended to help mitigate the risks associated with these attacks.

Levels of Verification

The main idea behind the security extensions is based on what we call a “chain of trust:”

- The DNSSEC system allows a name server to assert that the address it’s giving is the right one and to sign its assertion with a digital signature. These signatures form the core of the chain of trust.
- Each signature gets verified at the next level up in the Internet, the parent domain. So with cert.org, for example, DNSSEC checks at .org whether the signature that cert.org issued is valid. If it is, .org signs off on it. DNSSEC can actually go up and ask the root of the Internet itself whether .org gave the right answer.
- Since the Internet is hierarchical, the more dots there are in the site name, the more layers of the naming system you have to go through, so it actually gives more opportunities for verification.

PART 3: CHALLENGES TO IMPLEMENTING DNSSEC; FIRST STEPS TO TAKE

Performance and Resource Impacts

This process does add some overhead:

- The signature that a domain name server provides to the client takes up more space. So it takes longer to transmit on the Internet. It requires more traffic for every transaction.
- If you have a very busy website that can result in a lot of additional needed bandwidth, which can translate into additional cost.
- In terms of processing, the cryptographic algorithms are run only on the client system. The servers have static answers, so little additional processing is required on the server end. But on the client end, processing is required to verify the signature, which takes additional time.

Inplementation Challenges

DNSSEC uses public-key cryptography for the signing of the verification that the domain name is what it claims to be. Public-key cryptography requires you to have a private key that only you know and that you keep secret from everyone else, and a public key that you give to everyone else so they can verify that you were the one who signed with the private key. They’re essentially two halves of a whole.

So to implement DNSSEC effectively, organizations need someone who understands public-key cryptography and someone who understands key management. Training someone for the proper handling of keys is nontrivial.

Early Adopters

Many organizations are starting to adopt DNSSEC:

- The big hosting companies online, those who run DNS servers for others, are adopting. They are high-value targets.
- Google is another early adopter.
- The Office of Management and Budget of the U.S. government issued a memorandum requiring all government agencies to use the DNSSEC extensions.
- The governments of the Netherlands and Sweden have mandated that those countries go entirely DNSSEC to provide a more secure and stable environment for their citizens.

Evaluating Your Readiness to Adopt DNSSEC

- First, figure out what your exposure is. A lot of companies, it turns out, don’t actually have a good handle on where or what domains they actually have registered to them and where those domains are being hosted from.

And ask the following questions:

- Are you running your own DNS servers? Are you paying somebody else to run your DNS servers?
- What is the footprint you have on the Internet, and how much is it going to take to protect it? Do you already have the infrastructure in place to do this? A lot of the most recent domain name server software, like Microsoft Server 2008, comes with a DNS server built into it that already implements DNSSEC.
- Do you have people in your organization who understand public and private key management and implementation? If not, what training will be needed?

Resources

Internet Engineering Task Force

DNS Security Extensions (DNSSEC) Briefing, U.S. National Institute of Standards and Technology, June 3, 2009.

DNSSEC.NET