the WHITE HOUSE

A Major Milestone for Internet Security

JULY 22, 2010 AT 2:03 PM ET BY ANDREW MCLAUGHLIN

Summary: Last week marked a significant advance in the security of the Internet. After years of intensive design, testing, and implementation work, the Internet's domain name system now has a new security upgrade that allows Internet service providers and end users alike to protect against an important online vulnerability: the clandestine redirecting of online communications to unwanted destinations.

Last week marked a significant advance in the security of the Internet. After years of intensive design, testing, and implementation work, the Internet's domain name system now has a new security upgrade that allows Internet service providers and end users alike to protect against an important online vulnerability: the clandestine redirecting of online communications to unwanted destinations.

The Internet's domain name system (DNS) functions like a phone book, translating easy-to-remember domain names such as www.whitehouse.gov into numerical addresses, such as 92.122.212.144, that identify each server connected to the Internet. The new upgrade is a set of standards known collectively as the Domain Name System Security Extensions (DNSSEC) protocol, and it helps ensure that when computers want to communicate with one another they don't get tricked into talking to digital imposters instead.

What does this mean for you as you use the Internet at home or at work? Importantly, the look and feel of the Internet and the ways you use it will not change. You'll still type URLs, click links, and send emails exactly as before. What will change is the reliability of your Internet interactions. Sticking with the phone book analogy, your computer will be able to determine automatically when you're being given the true phone number for your bank, and when you're being given a false number intended to trick you into giving your account information to criminals.

For the nerdier among you, here's a more technical explanation of what happened, and why it matters:

As users access Web pages or send emails, they depend on the DNS to accurately convert each website URL or email address (names with dots) into a routable Internet Protocol address (numbers with dots). For years, however, there have been concerns about DNS vulnerabilities that permit spoofing and "man-in-the-middle" attacks. For example, bad actors can use a technique known as DNS cache poisoning to reroute traffic from legitimate websites and email servers to IP addresses that they control, all without the users knowing that they had been redirected to a malicious site. Though the DNS community has managed, for the most part, to stay ahead of these techniques, they have continued to be a serious concern.

DNSSEC ensures that the IP addresses generated by the DNS have not been intercepted or spoofed. Using public-key cryptography to digitally sign each IP address sent out by the DNS at each stage of the hierarchical name-to-number resolution process, DNSSEC allows Internet-connected systems to verify that the responses are authoritative and have not been altered.

Last Thursday, the Internet Corporation for Assigned Names and Numbers (ICANN) published the “root zone trust anchor” for DNSSEC and VeriSign distributed a DNSSEC-signed root zone file. The trust anchor provides a pre-configured public key that allows the thirteen root nameservers to verify each others’ digital signatures and exchange valid certificates, enabling them to identify each other securely. The signed root zone file creates an authentication and verification capability right from the top of the DNS hierarchy.

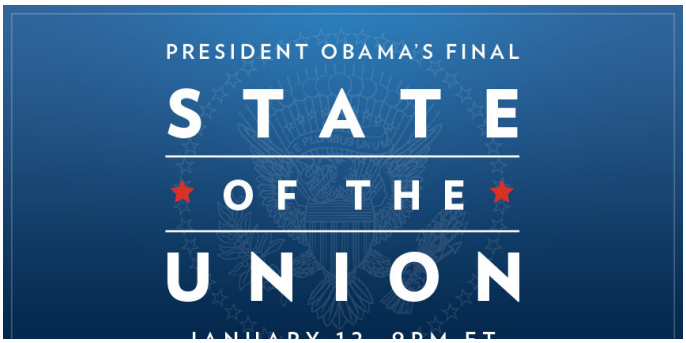
The release of the root zone trust anchor, distribution of a signed root, and subsequent deployment of DNSSEC across the global Internet together comprise the strongest defense so far against known vulnerabilities like DNS cache poisoning. There is still a lot more to do to achieve global implementation of DNSSEC and to secure the Internet's core infrastructures and practices against other known vulnerabilities. But last week's developments represent a notable step forward.

Huge thanks are owed to the members of the Internet technical community who made DNSSEC possible. Special recognition goes to those who led the development of the Internet Engineering Task Force's suite of DNSSEC specifications, and to the teams at the Department of Commerce, ICANN, and VeriSign that executed last week's successful trust anchor and signed root zone deployment.

Their hard work has created an Internet security upgrade that is important not only for its practical, day-to-day value in blocking a class of online threats, but also for

demonstrating that the cooperative, private-sector-led, standards-based model of Internet architecture remains vital and effective.

Andrew McLaughlin is Deputy Chief Technology Officer for Internet Policy



THE FINAL STATE OF THE UNION

Watch President Obama's final State of the Union address.

THE SUPREME COURT

Read what the President is looking for in his next Supreme Court nominee.

FIND YOUR PARK

Take a look at America's three newest national monuments.