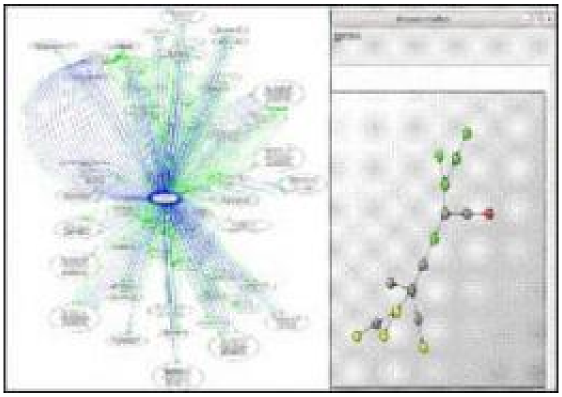
What's in a name? Homeland Security develops Domain Name System Security Systems Extensions

December 7 2011



The DHS Science and Technology Directorate (S&T) is working to restore trust in the system and make websites more secure and reliable by improving the Internet's Domain Name System (DNS). Credit: DHS S&T

At the advent of the Internet thirty years ago, the brand new Domain Name System (DNS) (which translated website names like science.com into a network address like 1.2.3.4) was trusted by everyone. Today, hackers take advantage of our long-standing trust in DNS and work to trick the system by stealing information and redirecting data every day.

The DHS Science and Technology Directorate (S&T) is working to restore trust in the system and make websites more secure and reliable by improving the DNS. Last October, during National Cybersecurity

Awareness Month, Internet safety was discussed as a shared responsibility.

DHS's role in this effort is S&Ts Domain Name System Security Extensions (DNSSEC) project, which received the National Cybersecurity Innovation Award at the Sans Institute's Second Annual National Cybersecurity Innovation Conference for innovation in promoting research that "pays off" by focusing on work that can result in real products and real risk reduction.

Most websites are not self-contained, but are rather a patchwork of information drawn from scores of sources. DNSSEC authenticates the existence, ownership, and integrity of data while systematically validating sources—including hundreds of servers, or nodes.

"The value of DNSSEC reaches far beyond preventing hackers from obtaining login information," said Edward Rhyne, DNSSEC program manager in S&T's Cyber Security Division. "DNSSEC is the foundation for a new trust model for all communications on the Internet, essentially protecting this vital infrastructure."

As governments, banks, Internet service providers, businesses, and other stakeholders become more aware of DNS-related threats, DNSSEC adoption is gaining momentum. "Users are starting to understand," said Rhyne. "A hacker may insert a malicious server between a user and their bank, enabling collection of login credentials and account information-allowing the hacker to steal an identity and transfer money as the authorized user."

Since 2004, S&T and its partners, including the National Institute of Standards and Technology and the DNSSEC Deployment Initiative, have worked to build support for DNSSEC, which has resulted in support and compliance by registrars from all over the world. Registars for more than

20 country codes, including .us and .uk, are involved in this effort. In addition, DNSSEC was deployed in the .edu, .gov,.org, .net, and .com zones, while top-level domains of the U.S. military's .mil are slated to be DNSSEC-signed in December 2011. Adoption by these most commonly utilized domains paves the way for adption by lower-level domains, and will ultimately create a complete end-to-end chain.

By authenticating and protecting data, DHS is continuously working to build a safer, more secure, and more resilient cyberspace.

Provided by US Department of Homeland Security

Citation: What's in a name? Homeland Security develops Domain Name System Security Systems Extensions (2011, December 7) retrieved 10 April 2024 from https://phys.org/news/2011-12-homeland-domain-extensions.html