The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

YEAR:
2012

STATUS:
Laureate

Organization:
Verisign

Organization URL:
http://verisigninc.com/en_US/index.xhtml

Project Name:
Verisign's Domain Name System Security Extension (DNSSEC) program

What social/humanitarian issue was the project designed to address? What specific metrics did you use to measure the project's success?

The Domain Name System (DNS) translates domain names into IP addresses to ease end-user navigation of the Internet. DNS was developed as a scalable, distributed navigation system across the global network with an expectation of trusted responses, but it has a vulnerability that could be exploited to redirect traffic on the Internet without the Internet user's awareness. The vulnerability is known as "cache poisoning" attacks and occurs when fraudulent DNS data is returned to an Internet user with the intention of redirecting the user to an illegitimate address. Verisign's Domain Name System Security Extension (DNSSEC) program protects the Internet community from forged DNS data by using public key cryptography to digitally sign authoritative zone data. DNSSEC validation assures that the data originated from verified DNS data was not modified in transit, thereby adding integrity and authentication to the DNS. Effective deployment requires the involvement of the entire Internet community. Verisign recognized that the best way to secure DNS was to deploy DNSSEC for the zones that it managed and to involve and enable key Internet stakeholders in the process. Adoption of DNSSEC will enable Internet users to navigate the Internet in a more secure and trusted manner. Verisign collaborated with Nominet, DENIC and technologists from Telematica, Internet Systems Consortium (ISC), Colorado State University (CSU) and the National Institute of Standards and Technology (NIST), as well as the wider Internet engineering community, to develop the current working standards for DNSSEC. The standards are the technical backbone for introducing DNS Security extensions to the core of the Internet, which are being used by registries around the world to secure the zones that they

manage. In addition, Verisign took a leadership role in defining the processes and practices of handling the secure keys for DNSSEC.

Please describe the technologies used and how those technologies were deployed in an innovative way. Also, please include any technical or other challenges that were overcome for the successful implementation of the project.

Verisign's DNSSEC program focused on increasing the Internet community's technical readiness for DNSSEC and providing tools to support its implementation and adoption. Verisign, in conjunction with IANA (Internet Assigned Numbers Authority) and under agreements with the U.S. Department of Commerce, helped manage the authoritative database for the root DNS infrastructure, which is the top of the DNS hierarchical tree and contains authoritative information for all worldwide TLDs. Verisign is the registry operator for the .com and .net TLDs (more than 100 million names). The ubiquitous nature of the root zone, coupled with the near real-time response rate and load of servicing billions of queries for the.net/.com domains, created both operational and business challenges. The following challenges were addressed: Technology Challenge: Introducing a more rigid, complex, and compute-intensive technology to the core of the Internet without disruption or degradation in performance or availability of the .net/.com registries. Operational Challenge: Communicating fundamental changes to the DNS to the registrar community and providing tools, support, and solutions to encourage adoption among all key Internet stakeholders. Business Challenge: Raising awareness among the Internet stakeholders so that they could make necessary changes within their infrastructure components. The DNSSEC program has become a best practice for introducing a significant infrastructural change to the core of a system that is as pervasive as the Internet. The Internet's ubiquitous nature and the extensive transactions and load on the system require a careful, methodical approach to implementation with the constituents having the ability to test their systems before adoption of the technology. Verisign with IANA developed the innovative Deliberately Unvalidatible Zone rollout methodology to create a "staged deployment" to incrementally introduce changes to the DNS root zone system and assess their impact, which become a best practice used by other TLD operators.

Please list the specific humanitarian benefits the project has yielded so far.

Verisign's DNSSEC program benefits society by protecting the Internet community from forged DNS data. Verisign's methodology for deploying DNSSEC involves minimal disruption to the Internet infrastructure and also underscores the importance of engaging industry stakeholders as a whole to find the safest and most suitable methods for securing the DNS. In addition to the goal of increasing the Internet community's technical readiness for DNSSEC, Verisign's DNSSEC program also provided the tools to support DNSSEC implementation and adoption. Most of all, it offered a technology to allow Internet users to navigate the Internet in a more secure and trusted manner by receiving authenticated DNS responses.

Please provide the best example of how the project has benefited a specific individual, enterprise or organization. Feel free to include personal quotes from individuals who have directly benefited from the work.

Deploying DNSSEC in the root zone paved the way for DNSSEC to be enabled throughout the Internet infrastructure, introducing a single trust anchor for all TLD operators to submit DNSSEC records and adding integrity and authentication properties to global DNS system. Example: "One of the Commerce Department's most important accomplishments went into effect when DNSSEC was deployed at the root of the Domain Name System. This action essentially gives a tamper-proof seal to the address book of the Internet, a seal that gives Internet users confidence in their online experience," said Gary Locke, U.S. Secretary of Commerce. Verisign's Operational Testing

& Evaluation environment is a functional reproduction of the production platforms that are available to registrars to test their systems prior to deploying modifications, updates or upgrades. Example: Verisign and EDUCAUSE hosted a test-bed environment, which enabled EDUCAUSE and select registrants to test their implementation outside the production environment to ensure that devices operate properly when DNSSEC is enabled. "EDUCAUSE has appreciated the opportunity to work with Verisign to advance the security and integrity of the Internet through early testing and deployment of DNSSEC," said EDUCAUSE President and CEO Diana Oblinger. The Verisign DNSSEC Interoperability Lab aims to ensure that systems and solution providers proactively evaluate their products and services in order to verify that their equipment is ready for a DNSSEC-enabled Internet. Example: "We're pleased that Verisign took the steps to ensure that solution providers can evaluate system interoperability," said Nicko van Someren, Chief Security Architect at Juniper Networks. "We recognize the importance of conducting DNSSEC testing as soon as possible, and VeriSign DNSSEC Interoperability Lab has made this easy for us." The program provides educational awareness and information to the broader community to support the adoption of DNSSEC by driving down the cost and complexity for the registrar community.