Improving Critical Infrastructure Cybersecurity

[Response to NIST Docket Number 130208119311901]

April 5, 2013

Security and Stability of Internet Critical Infrastructure

VeriSign, Inc. operates several of the world's largest and most important DNS Registries (`.com`, `.net`, `.gov`, and more). Because of this operational role that we fulfill, we continually strive to foster and ensure the security and stability of the global Internet [10]. In this vein, we applaud the National Institute of Standards and Technology's (NIST's) request for information: NIST Docket Number 130208119-3119-01 [9]. The nature of many of the cyber threats that we frequently observe is that they often orchestrate compromises by exercising previously unseen (or undocumented) vulnerabilities. By contrast, compliance checks, such as those mandated by [5, 6, 1, 4, 8, 7, 2, 3], are necessarily focused on previously observed threats and practices that are derived from analyses of these threats. While these compliance checks are very important, they consume the majority of time and expenditures of many Information Security (INFOSEC) teams. As new (and previously unseen) threats emerge, detecting and quantifying them is increasingly done through intelligence gathering and information sharing [15, 13, 14, 11]. Moreover, a recent report [10] outlined that even the seemingly straightforward alteration of adding new global Top Level Domains (gTLDs) to the DNS can prompt a great many systemic interdependencies that may require more "interdisciplinary" attention. As adversaries and attackers evolve their tactics, there is a growing gap created between Intelligence Driven Security (IDS) [12, 16, 15, 13] and Compliance Driven Security (CDS) [5, 6, 1, 4, 8, 7, 2, 3] models.

We believe that CDS is an important component of the overall security posture needed for cyber infrastructure, but we also feel that it should not be mistaken for a solution to the cybersecurity threats of today, and many of new cyber threats that may be emerging. As stated in [9], the nation's security and economic stability is affected by the security of its critical infrastructure, and the overall infrastructure has an increasingly prevalent dependence on its cyber critical infrastructure. As a result, we feel it behooves critical infrastructure providers to understand any gaps that may exist between their CDS postures and the current "threatscape." A critical inspection of such gaps, perhaps, could identify would-be requirements that might be imposed on critical infrastructure and providers. The process, however, to designate the specific Internet elements and providers as "critical infrastructure" is not widely known. Further, the ramifications arising from such a designation have not been identified. For example, if a private corporate entity is classified as critical infrastructure, is it required to implement additional security controls? What impact might that have on it? In addition, such a classification makes the issue of transitivity unclear. For example, if a system is classified as critical infrastructure, does that mean that all systems that it depends upon are also deemed to be critical? If so, what are the pros and cons of this approach? Further, it is not clear if the list of those entities that are classified as critical infrastructure will be made public, or if not, within what specific non-public groups would such a list be shared.

As a large service provider, we (again) applaud NIST's efforts to understand the issues outlined in [9]. With the size of the gap between IDS and CDS being as unclear as it currently is, and the size of this gap being a function of the evolving threatscape, we feel that creating a framework to track and describe emerging threats would be a very useful first-step. It is our belief that a structured vehicle that could facilitate providers' abilities to continually quantify the gaps between CDS and IDS, and which could inform information sharing efforts, would be invaluable in shaping future security frameworks and practices. Such a vehicle might take the form of a threat taxonomy, information sharing primitives, or other semantics that help enable the heterogeneous needs of IDS models.

References

[1] Federal Information Security Management Act (FISMA). http://csrc.nist.gov/groups/SMA/fisma/index.html.

[2] ISO27001 Certification. http://17799.standardsdirect.org/iso27001.htm.

[3] PCI Compliance. https://www.pcisecuritystandards.org/.

[4] Sarbanes-Oxley (SOX). http://www.sec.gov/about/laws/soa2002.pdf.

[5] Service Organization Controls (SOC 2) Type II. http://www.ssae-16.com/.

[6] Service Organization Controls (SOC 3). http://www.ssae-16.com/.

[7] TRUSTe Privacy Program. http://www.truste.com/.

[8] US-EU/Swiss Safe Harbor Privacy Frameworks. http://export.gov/safeharbor/.

[9] Developing a Framework To Improve Critical Infrastructure Cybersecurity. Request for Information (RFI) Docket Number 130208119-3119-01, National Institute of Standards and Technology (NIST), March 2013.

[10] New gTLD Security and Stability Considerations. Technical Report #1130007 Version 2.2, Verisign Labs, March 2013.

[11] Carolyn G. DuChene. Information Security: Distributed Denial of Service Attacks and Customer Account Fraud, December 2012. http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html.

[12] Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137, National Institute of Standards and Technology (NIST), September 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

[13] Christopher Ling and Bill Wansley. Intelligence-Driven Security Minimize Risk by Mastering the Motives, Strategies, and Tactics of Your Cyber Adversaries. http://www.boozallen.com/media/file/Intelligence_Driven_Defense_Folio.pdf.

[14] The White House - Office of the Press Secretary. Executive Order on Improving Critical Infrastructure Cybersecurity, February 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

[15] Verisign. iDefense Security Intelligence Services. http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/.

[16] David Waltermire, Stephen Quinn, and Karen Scarfone. The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1. NIST Special Publication 800-126, National Institute of Standards and Technology (NIST), February 2011. http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf.