Internet Infrastructure Workshop Report

Organizer: VeriSign, Inc.

Panelists:

- Brian Cute, Vice President, VeriSign Inc.
- Christina Arida, Advisor, ICT Initiative, National Telecom Regulatory Authority, Government of Egypt
- Lars-Johan Liman, Senior System Specialis, Autonomica AB
- Izumi Aizu, Institute for HyperNetwork Society, Kumon Center, Tama University
- Henrik Kaspersen, Chairman of the Cybercrime Convention Committee; professor at the Computer Law Institute in Amsterdam, the Netherlands

Discussion

The workshop focused on several Internet infrastructure security issues, including perspectives of two operators of Internet root severs on the attacks to the Internet root servers and methods for protecting against attacks; the importance to governments of infrastructure investment that facilitates access and enhances security; the value of international cooperation to respond to Internet-related crimes; and the need for increased awareness and participation of individual users in Internet security.

Brian Cute of VeriSign gave a brief overview of the hierarchy of the Internet infrastructure and discussed the exponential rise in attacks affecting the Internet root system in relation to the normal traffic flow that has itself grown at a significant rate. He described how VeriSign, as the operator of two of the 13 Internet root servers, has taken a multi-faceted approach to ensure that its operations continue with 100 percent up-time. In particular, Mr. Cute discussed VeriSign's Regional Internet Root Server project that will replicate its platform in servers throughout the world. He summarized the importance of the Internet infrastructure security as encompassing five factors: capacity, redundancy, diversity, disaster recovery, and human resources. Lars-Johan Liman addressed Autonomica's use of anycasting to enhance security of its operation of one of the 13 root servers. He noted that the anycast technology enables Autonomica to handle a higher load of traffic, thereby providing better service to local communities, rather than out of one location in Stockholm; and to defend against attacks. He noted that there are strategic challenges related to governance—he said root server operators are in agreement with the current arrangement in which VeriSign handles changes to the root zone file and propagates them to the other root servers; having multiple publishers, he argued, would be problematic. He also stated that operating a root server costs real money. Direct threats, he noted, include distributed denial of service attacks; the transmission of "packets of death" that kill software; social engineering threats; the input of bad data to the root if more any change is made; and false root servers.

Christina Arida of Egypt's National Telecom Regulatory Authority discussed the increased use of the Internet to provide governmental services to the citizens of Egypt, and how a secure infrastructure is essential to the provision of these services, as well as to the access of all citizens to the Internet. She announced the installation of a Regional Internet Resolution Server by VeriSign in Cairo. She noted that the server will be housed in a newly established data center, and that the server will, in addition to enhancing overall security for the Internet, also provide faster DNS responses, and better server access to Internet users in Egypt and throughout the surrounding region.

Dr. Henrik Kaspersen opened his presentation citing statistics of a recent study which found that Internet users are no longer able to protect their systems, with 67 percent of Internet users not aware of risks, and 62 percent being victim to Internet crime in the last year. He argued that we should have means to follow up and address the wrong doers and the Council of Europe Cybercrime Convention of 2001 is a promising means in that regard. In particular, he said, the convention seeks to: harmonize substantive law proficient in this field; harmonize procedural powers to investigate cyber crimes; and provide instruments for international cooperation between law enforcement bodies. He described the convention as a framework for further deliberation and extension, and said that the more countries participating, the more the system will work.

Izumi Aizu's presentation addressed the need for "Netizens" participation in Internet security. He argued that Internet users are not passive, and they are aware and skillful, and provide innovation at the edges of the Internet. He argued that the existing international cooperation frameworks, such as Cybercrime Convention, are either not global or not sufficient, and that few of the government organizations responsible for cyber protection have a multi-stakeholder approach or citizen participation. Their budgets are also not transparent. In the future, he said that a "Ubiquitous Network Society" requires a new form of governance that does more than rely on trust. He said that netizens need to be brought to the table in a meaningful way, and that a balance needs to be struck between security and other values—such as economic, human rights.

Inventory of events and actors related to the issue under discussion

Attacks on the Internet infrastructure; deployment of Regional Internet Root Servers; Anycasting; Council of Europe Cybercrime Convention; involvement of Internet users in security activities.

Internet infrastructure operators; Governments; International and intergovernmental organizations; and "Netizens"

Possible follow-up

Copies of presentations can be obtained by emailing: damari@verisign.com

Useful links

VeriSign DNS Assurance Resources & iDefense Security Intelligence
http://www.verisign.com/Resources/DNS_Assurance_Services_Resources/index.html
http://www.verisign.com/security-intelligence-service

Council of Europe—Cybercrime
http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp

ITU Cybersecurity Gateway
http://www.itu.int/cybersecurity/index.html