THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

June 27, 2011

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Upcoming Events

-June 28, 2:00 p.m., **Cyber Security in 2011: New Solutions for Data Isolation Separation** - This webinar will address the immediate steps that federal agencies can take to tackle the growing cybersecurity challenge. Speakers include Tim Hartman, publisher of Government Executive Media Group; and Ryan Durante, chief of the cross domain solutions and innovation section, Air Force Research Labs. More information.

-June 29, 8 a.m. - 3:00 p.m., **Responsible Information Sharing** - This conference digs deep into how agencies such as DoD, DHS and DNI are collaborating in specific areas to make information sharing a reality given the various outcomes of what happens with

Wikileaks in the post-insider threat environment of today. Hilton Alexandria Mark Center, 5000 Seminary Rd., Alexandria, Va. More information.

-June 29, 10:00 a.m., **Privacy and Data Security: Protecting Consumers in the Modern World** - The Senate Commerce Committee will hold a hearing to examine how entities collect, maintain, secure, and use personal information in today's economy and whether consumers are adequately protected under current law. The committee will hear from representatives from relevant government agencies as well as business and consumer advocate stakeholders. Russell Senate Office Building, Room 253. The hearing will be webcast live at this link. More information.

-June 29-30, **Smart Grid Virtual Summit 2011** - This conference will highlight the perspectives of leading utilities, technology companies, systems integrators, and regulators in making the smart grid a reality. Stream 7 on the second day of this summit includes a track with four sessions on smart grid security, including: Securing the Emerging Smart Grid; An Initiative to Enhance Cyber Security on the Electric Grid; Increasing Reliability Through Incident Response; and NERC Regulatory Requirements: Managing the Necessary Controls for Addressing Security Intrusions. More information.

Announcements

-This past week, the Department of Emergency Medicine of the George Washington University held an intensive week long conference entitled "Innovations in Telemedicine" led by **Dr. Neal Sikka**, CSPRI Advisory Board member. The program culminated with a practical exercise requiring conference participants (primarily graduate students from several colleges and departments) to work in teams to create new health focused applications for mobile devices. One of the important dimensions of the exercise was the security and privacy consideration. Assistant Director of CSPRI, **Costis Toregas**, acted as one of the judges, who were all impressed by the creativity of the students and the capacity of smart phones and other consumer devices to provide new secure applications in the medical field.

-There is a new monthly seminar series at the National Science Foundation: the Washington Area Trustworthy Computing Hour (WATCH). The series will meet at NSF at noon on the first Thursday of each month, starting June 2, 2011. These talks will be held in Stafford I, Room 110, (4201 Wilson Boulevard, Arlington, VA) and the public is invited; no badges required.

The inaugural speaker was **Prof. Fred B. Schneider** of Cornell, who spoke on "Cybersecurity Doctrine: Towards Public Cybersecurity." Abstract: With increasing dependence on networked computing systems comes increasing vulnerability. The vulnerabilities are mostly technical in origin, but their remediation is not. Only by coupling technical insights with public policy do we stand a good chance to create a safer and more secure cyberspace. This talk surveyed the landscape, discussed why past doctrines have failed, and proposed a new doctrine of Public Cybersecurity. This is joint

work with **Deirdre Mulligan**, a professor of law at the UC Berkeley School of Information and a Faculty Director of the Berkeley Center for Law and Technology.

The next talk in the series will be held on July 7, 2011. Paul L. Harris of Harvard University Graduate School of Education will be speaking on “Selective Credulity.”

Legislative Lowdown

-Internet Service Providers would likely be among the private-sector firms that would be subject to federal oversight under the White House's proposed cybersecurity legislation, The Hill reports. At a hearing in front of the Senate Judiciary Subcommittee on Crime and Terrorism, DHS Acting Deputy Under Secretary Greg Schaffer acknowledged that under the White House's plan, ISPs would likely be among the private firms deemed critical infrastructure and therefore subject to federal security standards. Schaffer emphasized that the administration's legislative proposal doesn't explicitly lay out which industries would be deemed critical and core critical infrastructure.

-House Speaker **John Boehner** announced Friday the formation of a Republican-only House Cybersecurity Task Force that will examine and make recommendations on cybersecurity authorities, public-private information sharing, critical infrastructure and domestic legal frameworks, as well as evaluating the Obama administration's cybersecurity proposal, according to GovInfoSecurity's Eric Chabrow. The task force is expected to report back to GOP leaders in October.

Cyber Security Policy News

-The United States is building a virtual version of the Internet, this one designed as a testbed to help the nation hone its defense against cyberattacks, Reuters reports. The Defense Advanced Research Projects Agency, is building a virtual firing range in cyberspace -- a replica of the Internet on which scientists can test how successfully they can thwart feared foreign, or domestic, launched attempts to disrupt U.S. information networks. Called the National Cyber Range, it will also help the U.S. government train cyberwarriors and hone advanced technologies to guard information systems. The range is expected to be fully up and running by mid-2012, four years after the Pentagon approached contractors to build it. It cost an estimated $130 million.

-The European Union may soon force companies to admit publicly when they've had data breaches that expose personal and financial information. H-Online reports. Speaking in London, **Viviane Reding**, the EU justice commissioner and vice president of the European Commission, said data protection rules in the EU date back to 1995 and need to be updated because the regulations for data protection vary greatly between different EU member nations. Reding said the proposals for revising the EU data protection laws will be finalized over "the coming months."

-From Al Jazeera this week comes a fascinating look at a program in North Korea that is recruiting young hackers at grade school level to fill slots in new cyberwarfare units designed to battle international IT powerhouses. The piece begins: “As South Korea blames North Korea for a recent slew of cyberattacks, two defectors share their experiences with Al Jazeera, shedding some light into the inner workings of the cyberwarfare programme in the communist country.” The piece describes North Korea's cyber warrior ambitions through the eyes of Kim Heung-kwang, a trainer of “cyberwarriors,” and hacker Jang Se-yul also warns of the regime's concentrated efforts to bolster its cyberwarfare capabilities.

-Authorities seized computers and servers in the United States and seven other countries this week as part of an ongoing investigation of a hacking gang that stole $72 million by tricking people into buying fake anti-virus products. In a statement released last week, the U.S. Justice Department said it had seized 22 computers and servers in the United States that were involved in the scareware scheme. The Justice Department said 25 additional computers and servers located abroad were taken down as part of the operation, in cooperation with authorities in the Netherlands, Latvia, Germany, France, Lithuania, Sweden and the United Kingdom.

-Federal authorities have declared victory over the Coreflood botnet and shut down the replacement server that the FBI used to issue commands to infected PCs. The FBI has scrubbed some 19,000 PCs that were infected with the Coreflood bot malware, the agency told a federal court last week. The effort is part of an ongoing and unprecedented legal campaign to destroy one of the longest-running and most menacing online crime machines ever built. In April, the Justice Department and the FBI were granted authority to seize control over Coreflood, a criminal botnet that enslaved millions of computers. On April 11, 2011, the U.S. Attorney’s Office for the District of Connecticut was granted authority to seize 29 domain names used to control the daily operations of the botnet, and to redirect traffic destined for the control servers to a substitute server that the FBI controlled. More significantly, the FBI was awarded a temporary restraining order allowing it to send individual PCs infected with Coreflood a command telling the machines to stop the bot software from running.

-An anarchic hacker group that claimed responsibility for attacks against the CIA, FBI, the Senate, the Arizona Department of Public Safety, Sony, Fox, PBS and a number of other high-profile targets says it is calling it quits after a 50-day hacking spree. The group known as "Lulzsec" said it was time to say "bon voyage," in what it said was its last news release, posted Saturday on the PasteBin website. Meanwhile, TechCrunch's **Paul Carr** takes the media to the woodshed for its coverage of the Lulzsec hacks, which he called "cowardly and pathetic."

-Failure to address cybersecurity in government systems could erode public trust and confidence in open government initiatives, writes **Dan Chenok**, a senior fellow in the IBM Center for The Business of Government. Chenok argues that it is vital that federal agency open government teams, and the contractors and business partners who support them, reach out to their colleagues in the security world to understand how they can build

in data and systems protections up front. "This will catch and correct most incidents before they become significant enough to cause a backlash that leads to restrictions on government information. Spending a little time on security in advance can save a lot of time spent responding to a major incident down the road, and can also allow the vast majority of open information to remain so over time."

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.