GW CSPRI Newsletter

August 20, 2012

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.

Events

-August 21, 6:30 p.m., **ISSA National Capital Chapter August Meeting** - The Information Systems Security Association will host Curtis Levinson, selected by NATO (the North Atlantic Treaty Organization) to represent the United States as an advisory subject matter expert on cyber defense for the Industrial Resources and Communications Services Group, which falls under NATO's Civil-Military Planning and Support Section. Government Printing Office, Room A138, 732 N. Capitol St. More information.

-August 22, 9:30 a.m. - 1:00 p.m., **Multistakeholder Meetings To Develop Consumer Data Privacy Code of Conduct Concerning Mobile Application Transparency** - The National Telecommunications and Information Administration will hold one in a series of meetings regarding consumer data privacy in the context of mobile applications. NTIA, 1401 Constitution Avenue NW., Room 4725. More information.

-August 22, 2:00 p.m., **Big Data: Exploring Cybersecurity and Scientific Use Cases** - A national town hall teleconference series with a panel government experts from CIA, NIST, and NITRD, and industry experts from Intel and Oracle explore Big Data in use cases, including continuous monitoring for security, malware detection, fraud prevention, anti-terrorism and scientific research and discovery. More information.

-August 30, 6:00 p.m. - Monthly Cybersecurity Workshop - The Women's Society of Cyberjutsu will hold a free workshop to highlight 10-15 popular tools used in IT security for information gathering, scanning, vulnerability assessments and Web application testing. Participants will have the chance to run commands against live hosts to see how the tools work. The workshop also will be available for remote participation via Teamviewer. 1616 Anderson Rd., Rm E, McLean, VA. More information.

Announcements

GW's CSPRI recently won several research grants. What follows is a brief synopsis of each grant awarded:

Secure and Trustworthy Cyberspace Principal Investigator Meeting Program Development

This project is developing the program for a significant invitational meeting of the Principal Investigators of the National Science Foundation’s Secure and Trustworthy Cyberspace (SaTC) program. This effort will further effective collaborations among computer scientists, electrical engineers, economists, psychologists, sociologists, and others working on cybersecurity. The project will identify and recruit a stimulating program of speakers and activities for the meeting which will take place in late November. The meeting will broaden the perspectives of researchers from all of the fields involved, help them begin to form new partnerships and collaborations, and help them to better understand how their discoveries and advances may be transitioned into practice. It will also help put researchers with diverse backgrounds from diverse institutions on a common footing. The Principal Investigator is Prof. Lance Hoffman and the project lead is Dr. Carl Landwehr.

Enlarging the Pipeline of Cybersecurity Students and Mentoring CyberCorps institutions

This project organizes and runs a workshop that focuses on enlarging the pipeline of institutions providing participants in the CyberCorps program. It also provides related mentoring for principal investigators at existing and new CyberCorps institutions. The Principal Investigator is Prof. Lance Hoffman. Dr. Costis Toregas also plays a key role on the project.

Workshop on Integrating Social Sciences into the Design of Cybersecurity Systems

This project organizes and runs a workshop that brings together computer scientists, social scientists, and other stakeholders in an attempt to integrate social sciences into design of future cyber security mechanisms and systems. The workshop fosters the development of new models of and paradigms for cyber security, and will lead to the development of communities of researchers who today do not interact, but whose cooperative work is necessary for the development of cyber security mechanisms and systems. It will also produce a research agenda in economics and other social sciences related to cyber security that addresses user, economic, and sociopolitical realities. The principal investigator is Prof. Lance Hoffman.

Legislative Lowdown

-After investigations revealed a startling number of law enforcement requests for private cellphone data in recent years, Rep. Edward Markey (D-Mass.) on Thursday released a discussion draft of legislation that would limit such digital searches and seizures, The Hill reports. As co-chairman of the Congressional Bipartisan Privacy Caucus, Markey's inquiry with nine major wireless carriers revealed that law enforcement officials at all levels of government made 1.3 million requests for user data from the companies in 2011. The responses also showed that the number of requests by law enforcement is increasing each year, in some cases by as much as 16 percent. In response, the Wireless Surveillance Act of 2012 would require law enforcement to provide regular disclosure of information on the requests and to obtain search warrants prior to conducting geolocation tracking. It would also mandate Federal Communications Commission regulations limiting how long wireless carriers keep consumers' personal information.

Cyber Security Policy News

-Kaspersky Lab last week appealed for help from top-notch cryptographers to help it break the encryption of a still-mysterious warhead delivered by the Gauss cyber-surveillance malware. "We are asking anyone interested in cryptology and mathematics to join us in solving the mystery and extracting the hidden payload," said the Moscow-based security company in a blog post Tuesday. "Despite our best efforts, we were unable to break the encryption." Computerworld writes that the payload is one of the unknowns of Gauss, a sophisticated spying tool uncovered by Kaspersky last week. According to researchers, Gauss monitors financial transactions with Middle Eastern banks and was built by or backed by one or more governments.

-A federal appeals court ruled on Tuesday that police do not need a warrant to track the location of a suspect's phone. According to Ars Technica, in a 2-1 ruling, the US Circuit Court of Appeals for the Sixth Circuit has ruled that law enforcement has the right to obtain location data from a cellphone in order to track a suspect without a warrant. The case involves a man named Melvin Skinner, a newly convicted drug trafficker, who was part of a cross-country, large-scale drug operation organized by another man, James Michael West. In the court's majority opinion, Judge Rogers specifically referred to the Jones v. United States case, which was decided by the United States Supreme Court in January 2012. In that unanimous decision, the Supreme Court found that law enforcement does not have the authority to warrantlessly place a GPS tracking device on a suspect's vehicle. But at least in this case, the Sixth Circuit Court of Appeals found that "no such physical intrusion occurred."

-The FBI last week warned Americans about an increasingly common "ransomware" email scam campaign that spoofs the agency and tries to frighten people into paying fines to avoid prosecution for supposedly downloading child pornography and pirated content. In an alert published last week, the FBI said that The Internet Crime Complaint Center — a partnership between the FBI and the National White Collar Crime Center — was "getting inundated with complaints" from consumers targeted or victimized by the scam, which uses drive-by downloads to hijack host machines. The downloaded malware displays a threatening message and blocks the user from doing anything else unless he pays the fine or finds a way to remove the program. KrebsOnSecurity.com has a more in-depth look at the mechanics and earnings of one ransomware operation.

-The Dept. of Energy (DoE) has issued a call for to electric-power companies that encourages them to make cybersecurity a top priority by setting up a "cybersecurity governance board" to oversee an internal cybersecurity program for protection and share information with the DoE, Network World reports. In exchange for information about sensitive information, such as identifying network vulnerabilities or attacks, the government will share this "benchmarking data" that's given to it anonymously with any other utility that participates in the information-sharing.

-The Defense Department is asking researchers to help it build a system that can replay cyber attacks. Federal News Radio writes that the goal is to enhance training and cyber situational awareness, and that DoD wants the end product to work for both the government and commercial sector. It'll begin accepting proposals on Aug. 27. More information on the department's requirements are here.

Meanwhile, the National Institute of Standards and Technology is seeking vulnerability analysis and security scanning for the Pentagon's Android software applications, according to a solicitation posted Thursday. NextGov writes that the tools will be used to audit intelligence and imagery applications used by ground troops on tablets and handheld devices in Iraq and Afghanistan. The solicitation, which closes Aug. 24, did not disclose whether there was an incumbent contractor performing this task and whether it would be invited to rebid.

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.