GW CSPRI Newsletter

May 5, 2014

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

Announcements

CSPRI researchers Prof. Gabriel Parmer (principal investigator) and Prof. Rahul Simha (co-PI) have just received a grant from the Office of Naval Research for $603,000 for a three-year study on Foundations for Component-Based Operating Systems. This project examines recovery from attacks in operating systems, and explores how to build non-monolithic operating systems with components so that recovery can take place during an attack.

Events

-May 5, 6:00 p.m. - 8:15 p.m., **NSA Telephonic and Electronic Surveillance** - This seminar will examine judicial review of constitutionality of the NSA metadata collection program, and possible outcomes of the appeal process, pending Obama Administration/congressional reforms, and the likely short term and longer term scenarios for reform due to these various pressures on existing surveillance programs. It will also examine how private industry, including carriers and ISPs, privacy advocates and the national security community have been responding to these

potential reforms. Drinker Biddle & Reath LLP, 1500 K Street, NW, Conference Room 2B. More information.

-May 6, 4:00 p.m. - 5:30 p.m., **Technical Tuesday: Malware Reverse Engineering** - Cybergamut Technical Tuesday is for cyber professionals to exchange innovative ideas and discuss technical issues of mutual interest. 6841 Benjamin Franklin Drive, Columbia, MD 21046. More information.

-May 6-8, **High Confidence Software and Systems Conference** - The High Confidence Software and Systems (HCSS) Conference, now in its second decade, was created to support the interchange of ideas among researchers, practitioners, and research managers from Government, research labs, and industry practice. HCSS provides a forum for dialogue centered upon the development of scientific foundations together with innovative and enabling software and hardware technologies for the assured engineering of complex computing systems. These systems, which include networked and cyber-physical systems, must be capable of interacting correctly, safely, and securely with humans and the physical world even while they operate in changing and possibly malicious environments with unforeseen conditions. In many cases, they must be certifiably dependable. Governor Calvert House, 58 State Circle, Annapolis, Maryland 21401-1906 More information.

-May 7, 1:00 p.m. - 2:30 p.m., **Privacy and Social Media** - The American Bar Association will host a Webinar to review recent case law and current and proposed privacy legislation; discuss privacy and potential constitutional issues; and best practice tips for crafting social media policies. More information.

-May 7, 2:00 p.m., **DHS Hearing: Investing in Cybersecurity** - The Senate Appropriations Committee will hold a hearing. The witness list will include Phyllis Schneck, Deputy Undersecretary – Cyber, National Protection and Programs Directorate, U.S. Department of Homeland Security; Peter Edge, executive associate director, homeland security investigations, Immigration and Customs Enforcement, U.S. Department of Homeland Security; William Noonan, deputy special agent in charge, Criminal Investigative Division - Cyber Operations, U.S. Secret Service, U.S. Department of Homeland Security; Jonathan Katz, director, Maryland Cybersecurity Center, University of Maryland; Dave Mahon, vice president and chief security officer, CenturyLink; Scott R. Bowers, vice president of government relations, Indiana Statewide Association of Rural Electric Cooperatives; and Christopher Peters, vice president, NERC/critical infrastructure protection compliance, Entergy Corporation. Dirksen Senate Office Bldg., Room SD-192. More information.

-May 8, 9:30 a.m. - 3:00 p.m., **3rd Annual F5 Government Technology Symposium** - This conference will feature tracks covering the latest topics in IT, from cybersecurity, mobility, cloud, and application delivery. The Newseum Knight Conference Center, 555 Pennsylvania Ave., N.W. More information.

-May 8, 10:00 a.m., **Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland** - This is a joint hearing by the House Homeland Security Committee's Subcommittee on Counterterrorism and Intelligence, and the Subcommittee on Cybersecurity, Infrastructure

Protections, and Security Technologies. The witness list TBA. This hearing will be Webcast. 311 Cannon House Office Bldg., Room 311. More information.

-May 8, 2:00 p.m., **Electromagnetic Pulse (EMP): Threat to Critical Infrastructure** - The Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies hearing. Cannon House Office Bldg., Room 311. More information.

-May 12, 12:00 p.m. (noon), **Google Glass and the Future of Photography** - The speaker will be Marc Levoy, the VMware Founders Professor of Computer Science at Stanford University, with a joint appointment in the Department of Electrical Engineering. National Press Club, 529 14th St NW, 13th Floor. More information.

-May 13-14, **Cyber Security for National Defense Symposium** - This conference is designed as an educational and training "Town Hall" forum, where thought leaders and key policy-makers across military and civilian organizations can come together for actionable discussions and debate. The symposium will focus on increasing the security and resiliency of the Nation's critical networks, operating freely in the Cyber Domain, and the protection of infrastructure in support of national defense and homeland Security. Defense Strategies Institute, 20 F. St. NW. More information.

Legislative Lowdown

-Leaders of the Senate Intelligence Committee are putting together legislation that would enable companies to share cyber threat information with federal agencies without fear of getting sued, The Washington Post writes. "The new, 39-page draft bill, written by Sen. Dianne Feinstein (D-Calif.), chairman of the intelligence committee, and Sen. Saxby Chambliss (Ga.), the ranking Republican, states that no lawsuit may be brought against a company for sharing threat data with 'any other entity or the federal government' to prevent, investigate or mitigate a cyberattack," reports Ellen Nakashima. "Protection from lawsuits has been a key demand from industry officials and a point of contention for privacy advocates, who have argued that such an exemption could expose consumers' data to potential government abuse or even encourage firms that have been hacked to go on the offensive." Prospects for the bill's passage are unclear. As The Post notes, the House of Representatives twice passed such legislation, but the Senate has never been able to muster the votes to pass it.

Meanwhile, the White House last week released a sweeping review of "big data" practices that calls for an update to privacy laws, The Hill writes. "Officials who conducted the review recommended that Congress enact legislation based on the "Consumer Privacy Bill of Rights" that President Obama first introduced in 2012," The Hill's Kate Tummarello writes. "The report also calls for a law to create notification requirements for companies that suffer data breaches and urges an update to a decades-old statute that allows warrantless access to emails."

Cyber Security Policy News

-In a rare insight, The Obama administration last week published a series of questions it asked in deciding when and whether to make public the discovery of major computer security flaws -- or whether to keep them secret so that American intelligence agencies can use them for offensive and surveillance capabilities, The New York Times reports. "Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks," wrote Michael Daniel, the White House cybersecurity coordinator, describing the review that has taken place at the White House in the past few months. "Mr. Daniel wrote that the administration has now 'established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure'. He did not say who would participate, or whether the hardest questions would be bounced to the president, much as he sometimes reviews the details of drone strikes or other covert operations that could have diplomatic implications. Mr. Daniel did not say who runs that process, but administration officials say it is largely directed by the National Security Council, and often by Mr. Daniel himself."

-Last week, President Obama denied reports that the United States has brokered a "no-spy agreement" with some of its allies. "It's not quite accurate to say that the U.S. government offered a no-spy agreement and then withdrew it," National Journal writes, quoting Obama at a news conference where he appeared with German Chancellor Angela Merkel. "What is accurate to say is that we do not have a blanket no-spy agreement with any country, with any of our closest partners,' including Germany. Obama continued: 'What we do have are series of partnerships and procedures and processes that are built up between the various intelligence agencies, and what we're doing with the Germans—as we do with the French or British or Canadians or anybody—is to work through what exactly the rules are governing the relationship between each country, and make sure that there are no misunderstandings.' As National Journal notes, the press conference "arrived just a day after a New York Times report that efforts between the two countries to reach a sweeping accord on their relationship had fallen apart."

The FBI warned healthcare providers that attacks against medical devices and information systems across the industry are likely to increase in the coming months and years. "The FBI has warned healthcare providers their cybersecurity systems are lax compared to other sectors, making them vulnerable to attacks by hackers searching for Americans' personal medical records and health insurance data," Reuters reports. The FBI warning comes amid a flurry of reports of tax fraud targeting physicians and employees of healthcare organizations. According to KrebsOnSecurity.com, an organized cybercrime gang appears to have targeted a large number of healthcare and senior living organizations that were all using the same third-party payroll and HR services provider.

Indeed, Wired.com reported last week about medical equipment at a chain of healthcare organizations in the midwest whose drug infusion pumps -- devices for delivering morphine drips, chemotherapy and antibiotics -- could be remotely manipulated to change the dosage doled out to patients. The Wired piece follows the work of Scott Erven, a security researcher who was

given free rein to roam through all of the medical equipment used at a large healthcare chain. What did they find? "Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care. Erven's team also found that, in some cases, they could blue-screen devices and restart or reboot them to wipe out the configuration settings, allowing an attacker to take critical equipment down during emergencies or crash all of the testing equipment in a lab and reset the configuration to factory settings."

-The U.S. Supreme Court will weigh in this week on a pair of appeals over whether police must obtain a warrant to search data on the cell phone of a person under arrest. CNN reports that the cases involve criminal suspects in Massachusetts and California were convicted, in part, after phone numbers, text messages, photos and addresses obtained from personal electronic devices linked them to criminal drug and gang activity. Recent conflicting decisions in the lower courts have left judges nationwide divided over how to apply a 40-year-old high court precedent, which allows searches of items a suspect possesses after arrest.

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.