GW CSPRI Newsletter

September 8, 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 will once again serve as the academic co-sponsor for the Washington Post's annual Cybersecurity Summit on October 1, 2014. Speakers include: Congressman Mike Rogers, Arati Prabhaker, Alejandro Mayorkas, John P. Carlin, Christopher Painter, Jane Holl Lute, Tiffany Rad, Andy Bochman, and Eric Friedberg. The event is free to the public, but registration is required. Click here for the registration portal and more details.

Events

-Sept. 9-10, **Cybersecurity Simulation and Exercise for Banks and Credit Unions** – Over a two day period this fall, hundreds of security risk and IT professionals will experience a highly realistic set of scenarios in a safe environment in order to practice and improve their response to cyber incidents. The teams are encouraged to involve multiple parts of their organizations, from IT and security to payments experts to communications teams to line of business leaders and executive teams. Registration and more information (PDF).

-Sept. 10, 2:00 p.m., **Operationalizing Cyber for the Military Services** – The House Committee on Armed Services' Subcommittee on Intelligence, Emerging Threats and Capabilities will hold a hearing. Rayburn House Office Bldg., Room 2212. More information.

-Sept. 10, 3:00 p.m. – 4:30 p.m., **Data Breach Prevention, Response and Management: The Road to Reasonable Security** – Panelists on this Webinar will offer an overview of "reasonable security" with an emphasis on consumer protection, business continuity and litigation considerations. More information.

-Sept. 10, 3:00 p.m. – 8:00 p.m., **ISACA CM Meetup: Building an Effective Periodic User Access Review Process** – During this session, the speaker will discuss Identity Access Governance Theory, common pitfalls the access review process will face, what an actual review process looks like, and then conduct a real world walk through. Chiapparelli's Restaurant, 237 S. High St., Baltimore, MD 21202. More information.

-Sept. 16, 8:00 a.m. – 5:30 p.m., **5th Annual Billington Cybersecurity Summit** – This conference will feature talks from well-known cybersecurity speakers including Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service. This leading summit also will feature Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, The White House; David DeWalt, Chairman and Chief Executive Officer, FireEye; Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity, NPPD. Capital Hilton, 1001 16th St. NW. More information.

-Sept. 17, 6:00 p.m. – 9:00 p.m., **NovaInfosec Meetup West** – If you are in the IT security business, like the idea of meeting to discuss the foibles of the industry, demo your recent discovery and conquest, or just drink a beer with like minded folks, then this meeting is for you. Lost Rhino Brewing Company, 21730 Red Rum Drive #142, Ashburn, VA, 20147. More information.

-Sept. 18, 5:30 p.m. – 8:30 p.m., **ISSA NoVa Meetup: Secure Computing with AWS** – In this presentation, accompanied by live demonstrations, the speaker will make the case that the automation and scale of true utility-style cloud computing enables customers to build more secure systems than they can typically build on-premises at any reasonable

cost. Avaya Government Solutions, 12730 Fair Lakes Circle, Fairfax, VA, 22033. More information.

-Sept. 23-24, **Safeguarding Health Information: Building Assurance Through HIPPA Security** - NIST and the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) will host a conference to explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This event will highlight the present state of health information security, and practical strategies, tips and techniques for implementing the HIPAA Security Rule. The Security Rule sets federal standards to protect the confidentiality, integrity and availability of electronic protected health information by requiring HIPAA covered entities and their business associates to implement and maintain administrative, physical and technical safeguards. Grand Hyatt, 1000 H Street NW. More information.

-Sept. 24-26, **2014 Trusted Cyber Collaboration Workshop** - An opportunity for professional information sharing, and a vendor exhibition. The event is focused on secure collaboration among industry partners and their supply chain members, mitigating the risks of information security breaches, and accelerating secure information sharing while reducing overall program costs. Hyatt Regency Crystal City, 2799 Jefferson Davis Hwy, Arlington, VA 22202. More information.

Legislative Lowdown

-Sen. Dianne Feinstein wants Silicon Valley leaders to call their congressional representatives to express their support for her cyber-security bill, which is facing opposition from privacy advocates, CBS News writes. Speaking at last week's Silicon Valley Leadership Group, the Senate Intelligence Committee chair called her Cyber Security Information Sharing Act a first step in protecting the country from cyber attacks. The legislation passed in July, but has faced significant hurdles getting to the Senate floor.

Some of that resistance has come in the form of protests and campaigns against the bill launched by civil liberty and privacy advocates would rather see Congress move on a measure to rein in the surveillance programs of the National Security Agency. "More than 40 groups wrote a letter to Senate leaders on Thursday praising the 'important first step' that would be taken if Sen. Patrick Leahy's (D-Vt.) USA Freedom Act were passed in coming months, even while noting that 'further reform will still be needed," The Hill's Julian Hattem writes. "The bill, which Leahy released earlier this summer after months of negotiations with lawmakers and the Obama administration, would end the NSA's bulk collection of Americans' phone records — the most controversial program revealed by Edward Snowden last year."

Cyber Security Policy News

-The Justice Department last week released two decade-old memos that offer perhaps the fullest public airing to date of the Bush administration's legal justification for the warrantless wiretapping of Americans' phone calls and e-mails — a program that began in secret after the 2001 terrorist attacks, The Washington Post reports. "The broad outlines of the argument — that the president has inherent constitutional power to monitor Americans' communications without a warrant in a time of war — were known, but the sweep of the reasoning becomes even clearer in the memos written by then-Assistant Attorney General Jack Goldsmith, who was head of President George W. Bush's Office of Legal Counsel," The Post's Ellen Nakashima writes.

-GOP lawmakers are calling for hearings in the wake of news that hackers managed to install malware on the Healthcare.gov Obamacare insurance panel. Politico reports that even though the government claims no personal, financial or health data were compromised in the attack, "which may not even have been aimed specifically at HealthCare.gov, the hacker implanted a bug that appears to have gone undetected for six weeks. Republicans in Congress had long warned of security breaches of the site, as had cybersecurity experts familiar with its workings."

-NATO country leaders meeting in Wales last week agreed that a cyber-attack on one member nation could be treated as a cyber-attack on all members, meaning the alliance could respond by launching military or cyber attacks against an adversary, GovInfoSecurity reports. "Today, we declare that cyber-defense is part of NATO's core task of collective defense," NATO Secretary-General Anders Fogh Rasmussen said. Leaders still need to define what exactly they mean when they say cyber attack, and what kind of cyber attack might trigger a response by NATO allies.

The news came as Europol launched a cybercrime task to combat online crime in the European Union and elsewhere. According to PC World, the "Joint Cybercrime Action Taskforce" or (J-CAT) will be piloted for six months, and "will coordinate international investigations to take action against key online threats and top targets, such as underground forums and malware, including banking Trojans, botnets and online fraud."

-Verizon agreed to pay $7.4 million to settle charges that it used subscribers' personal information to target advertising toward them without their knowledge or consent. CNN writes that the telephone giant paid the fine by the Federal Communications Commission (FCC), which charged that Verizon had used personal data about approximately 2 million customers' billing or location information to sell services to them without first informing them of their rights or telling them how to keep their information private.

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.