GW CSPRI Newsletter

March 19, 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.

Contents

Events 1

Announcements 2

Legislative Lowdown 3

Cyber Security Policy News 4

Events

-Mar. 20 10:00 a.m., **Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions** - The Senate Finance Committee's Subcommittee on Fiscal Responsibility & Economic Growth will hold a hearing. Room 215, Dirksen Senate Office Building. More information.

-Mar. 20, **5th Annual Symantec Government Technology Summit** - This conference will address challenges that government agencies are facing with current and future trends in IT, including widespread adoption of virtualization; increasing borders of where data resides; consumerization of IT and the evolution of the endpoint; transparency of government and handling FOIA requests; and the evolution of the cyber threat landscape. The keynote speaker will be Joel Brenner, author of America the Vulnerable. Brenner, a former top-level National Security Agency insider, will discuss his new book which explores America's next great battleground: digital security. Crystal Gateway Marriott, 1700 Jefferson Davis Highway Arlington, Virginia. More information. .

-Mar. 21, 10:00 a.m., **Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards** - The House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security will hold a hearing, which will also be webcast this event. Room 2141, Rayburn House Office Building. More information.

-Mar. 21, noon - 1:30 p.m., **Data Breach Risks and Protections for Health Lawyers: Do You Know Where Your Information is Today?** - The DC Bar Association will host the event. DC Bar Conference Center, 1101 K St., NW. More information.

-Mar. 21, noon - 2:00 p.m., **Fundamentals of Chinese Information Warfare and Impacts on the Western World** - This event, put on by the Potomac Institute Cyber Center, features guest speaker William T. Hagestad II, author of the new book "21st Century Chinese Cyberwarfare." 901 N. Stuart St., Suite 200, Arlington, Va. The event also will be webcast. More information.

-Mar. 21, 2:00 p.m. - 6:00 p.m, **7th Annual ABA/FCBA Privacy & Data Security Symposium** - The conference is organized by the Federal Communications Bar Association's Privacy and Data Security Committee and the American Bar Association's (ABA) Communications Law Forum. Arnold & Porter, 555 12th St. NW. More information.

-Mar. 22-23, **CyberFutures Conference and Technology Exposition** - This conference brings together Air Force leadership, industry experts, and academia and current cyber security specialists from around the world to discuss the cyber security issues and challenges facing America today. Invited speakers for the 2012 cyber conference include: Secretary of the Air Force Michael B. Donley, General William Shelton, commander, Air Force Space Command, Representative Mike Rogers, Chairman of the U.S. House Intelligence Committee and Secretary Eric Rosenbach, Deputy Under Secretary of Defense for Cyber Policy. Gaylord National Resort & Convention Center, 201 Waterfront St., National Harbor, Md. More information.

-Mar. 23, 12 noon, **Cybersecurity: Will Federal Regulation Help?** - With the Senate poised to consider comprehensive "cybersecurity" legislation this month, a bevy of questions need answers. Although it is difficult to secure computers, networks, and data, are government spending and regulation the answer? Are the cybersecurity threats touted in Washington real or trumped up? Should legal protections for privacy and other values give way in the name of "information sharing" with the Department of Homeland Security? Join us for a discussion with technology policy experts about cybersecurity's challenges and the approaches taken in current legislation. Speakers will include Jim Harper, Director of Information Policy Studies, Cato Institute; Jerry Brito, Senior Research Fellow, Mercatus Center at George Mason University, Ryan Radia, Associate Director of Technology Studies, Competitive Enterprise Institute, moderated by Laura Odato, Manager of Government Affairs, Cato Institute. 2203 Rayburn House Office Building. More information.

Announcements

-On Mar. 21, 12 noon - 2:00 p.m., the CSPRI will continue its 2011-12 Seminar Series with a discussion session titled, "Developing the Cybersecurity Workforce - Different Perspectives." Two noted experts will debate opposing points:

View 1: *We Need Lots of People, Chosen and Developed Properly*: "A holistic approach to developing the cybersecurity workforce is needed, based on careful integration of workforce development strategies into a plan that involves educators, career professionals, employers, and

policymakers. A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we are the weakest." (From "Holistically Building the Cybersecurity Workforce" by Lance J. Hoffman, Diana L. Burley, and Costis Toregas, IEEE Security & Privacy Magazine, March-April 2012.)

View 2: *A Human in the Loop May Not be a Failsafe but a Liability* " … We security professionals make a claim to the salary we draw because of our 'judgment' and 'skill.' I suggest that the demand for that judgment, that skill will soon wither in the face of the second [machine to machine] economy. We see computers doing things right now—Amazon or Netflix recommendations, Zillow estimates—that a decade ago would have required a human to intervene. The networked security militias of the second economy do not wait for humans, and it's possible to argue that for the scale and speed at which a networked security collective operates, a human in the loop is not a failsafe but a liability" (http://geer.tinho.net/geer.suitsandspooks.8ii12.txt).

Debating the first point will be Diana Burley, Associate Professor in the Graduate School of Education and Human Development at The George Washington University (GW). Her research and scholarly activities advance understanding of knowledge management initiatives, IT/cyber security education and workforce development strategies, and the impact of IT- enabled change on individuals, organizations and society (social informatics). Defending the second point will be Daniel Geer, who is currently the chief information security officer for In-Q-Tel, a not-for-profit venture capital firm that invests in technology to support the intelligence community. Visit http://cyberworkforce.eventbrite.com/ to RSVP for this event.

Legislative Lowdown

-Open government organizations last week sent a letter to Sen. John McCain, opposing specific provisions in a cybersecurity bill he introduced. The SECURE IT Act would create a new Freedom of Information Act (FOIA) exemptions for "cyber threat information" as well as for all information shared with a cybersecurity center. FOIA exemptions limit public access to government information. The organizations stated, "Unnecessarily wide-ranging exemptions of this type have the potential to harm public safety and the national defense more than they enhance those interests." In a statement for a hearing on the FOIA and critical infrastructure information, the Electronic Privacy Information Center (EPIC) also warned (PDF) against new FOIA exemptions, warning that the National Security Agency has become a "black hole" for public information about cybersecurity.

Meanwhile, The Hill's Brendan Sasso delves into some of the rhetoric being used to try to convince lawmakers on Capitol Hill into passing comprehensive cybersecurity legislation. Sasso writes that lawmakers and administration officials have warned of potentially catastrophic consequences if Congress doesn't pass cybersecurity legislation this year, but some observers question whether the rhetoric is overblown.

Cyber Security Policy News

-A House oversight committee has awarded the federal government an overall grade of C-minus for agency performance in responding to FOIA requests. When President Obama signed the Open Government Initiative on January 21, 2009, he said "the Freedom of Information Act is perhaps the most powerful instrument we have for making our government honest and transparent, and of holding it accountable. And I expect members of my administration not simply to live up to the letter but also the spirit of this law." But an evaluation released last week by the House Oversight and Government Reform Committee found that many federal agencies failed or struggled to transparently demonstrate an ability to track basic information about the processing of Freedom of Information Act (FOIA) requests.

-Cybersecurity experts have long warned that China has consistently been the source of sophisticated cyber attacks aimed at stealing intellectual property and trade secrets from firms, but few firms have been willing to come forward to talk about the extent of the damage. That changed last week, with the cover story in Bloomberg magazine about several U.S. companies that have suffered billions of dollars in losses after discovering incidents linked to such activity.

-The Department of Health and Human Services last week announced a settlement with Blue Cross Blue Shield after the company's inadequate security measures allowed 57 unencrypted hard drives containing private health information to be stolen from a facility in Tennessee, Computerworld writes. The agency cannot issue a fine greater than $1.5 million, but it could have filed criminal charges or required Blue Cross to mitigate future patient harms.

-In the race to develop ever more security code, it seems the software developers writing code for U.S. government systems are losing the race to their private sector counterparts. That's according to data to be presented at the Black Hat Europe security conference next week by security researcher and chief technology officer of bug-hunting firm Veracode. Forbes reports that Chris Wysopal plans to give a talk breaking down the company's analysis of 9,910 software applications over the second half of 2010 and 2011, automatically scanning them for errors that a hacker can use to compromise a website or a user's PC. And one result of that analysis is that government software developers are allowing significantly more hackable security flaws to find their way into their code than their private industry counterparts.

-The U.S. Army is reminding servicemen and women that many of today's digital devices that people use to post data to social networking sites like Facebook and Twitter can give away precise geolocation data that -- in the hands of a cyber-savvy enemy -- could lead to unnecessary deaths. Reporting for MSNBC, Athima Chansanchai writes: "Soldiers who upload photos to Facebook "could broadcast the exact location of their unit," wrote Rodewig, citing Steve Warren, an administrative officer in the intelligence office of the Army's Maneuver Center of Excellence (MCoE). Warren gave Rodewig a chilling example of the consequences of geo-tagging from 2007: 'When a new fleet of helicopters arrived with an aviation unit at a base in Iraq, some soldiers took pictures on the flightline,' he said. From the photos that were uploaded to the Internet, the enemy was able to determine the exact location of the helicopters inside the compound and conduct a mortar attack, destroying four of the AH-64 Apaches.'"

-The FBI is seeking a court order to force Google to help it crack the pattern lock on a suspect's Android phone. Wired.com writes that the bureau claims in federal court documents that forensics experts performed "multiple attempts" to access the contents of a Samsung Exhibit II handset, but failed to unlock the phone. An Android device requires the handset's Google e-mail address and its accompanying password to unlock the handset once too many wrong swipes are made. The bureau is seeking that information via a court-approved warrant to Google in order to unlock a suspected San Diego-area prostitution pimp's mobile phone.

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.