GW CSPRI Newsletter

April 9, 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 3

Legislative Lowdown 4

Cyber Security Policy News 4

GW Events

-Apr. 9, 6:00 p.m., **Effective Cybersecurity: Perspectives on a National Solution** - The George Washington University's Business School holds its 13th Annual Robert P. Maxon Lecture, featuring Wes Bush, Chairman, CEO and President of Northrop Grumman Corporation. *See Events below for more information.*

-Apr 11, 6:30 p.m. – 8:00 p.m., **Frank Howard Distinguished Lecture Series: "Why We Won't Solve the Cybersecurity Problem"** Prof. Eugene Spafford, Center for Research and Education in Information Assurance Security, Purdue University, one of the most well-known, noted and cited experts in cybersecurity research and education. *See Events and Announcements below for more information.*

Events

-Apr. 9, 12:00 noon - 1:30 p.m., **Navigating the Landmines of Data Security Breaches: Practical Lessons Learned in Unearthing, Disarming, and Avoiding Cyber Threats and Digital Disasters** - Speakers at this American Bar Association event will include Lucy L.

Thomson, privacy advocate & senior principal engineer, CSC; Kimberly K. Peretti, director, forensics services, PricewaterhouseCoopers, former DOJ prosecutor for major cybercrime prosecutions & investigations; Robin Campbell, counsel, Crowell & Moring LLP. Crowell & Moring, 1001 Pennsylvania Ave., NW. More information (PDF).

-Apr. 9, 6:00 p.m., **Effective Cybersecurity: Perspectives on a National Solution** - The George Washington University's Business School holds its 13th Annual Robert P. Maxon Lecture, featuring Wes Bush, Chairman, CEO and President of Northrop Grumman Corporation. Mr. Bush will discuss the pathway to improving the effectiveness of our national cybersecurity effort, through crafting effective and comprehensive public-private partnerships. GWU School of Media and Public Affairs, Jack Morton Auditorium, 805 21st St. NW. More information.

-Apr. 11, 7:30 a.m. - 5:00 p.m., **Understanding FedRAMP: Creating a Cloud Security Roadmap** - This is a one-day in-depth educational program for government executives, managers, program managers and staff & industry partners. This course provides practical information for the government and industry on cloud security, the federal government's FedRAMP program and what agency leaders should be doing now. The Tower Club, 8000 Towers Crescent Drive #1700, Vienna, Va. More information.

-Apr. 11, 8:00 a.m. - 2:00 p.m., **McAfee Public Sector Summit** - The Ritz-Carlton, Pentagon City, 1250 South Hayes Street, Arlington, Virginia. More information.

-Apr. 11, 12:30 p.m. - 1:45 p.m., **Global Security Forum 2012: Fighting a Cyber War** - This panel will address how cyber could be used in an offensive capacity, including how to conceptualize command and control, targeting, damage assessment, proportionality, and deterrence in a cyber environment either alone or alongside kinetic operations. Speakers include Gen. James E. Cartwright (ret.), former Vice Chairman of the Joint Chiefs of Staff; Harold Brown Chair in Defense Policy Studies, CSIS; James Lewis, director and Senior Fellow, technology and public policy program, CSIS; William Lynn III, former U.S. Deputy Secretary of Defense. Center for Strategic and International Studies 1800 K Street, NW. More information.

-Apr 11, 6:30 p.m. – 8:00 p.m., **Frank Howard Distinguished Lecture Series: "Why We Won't Solve the Cybersecurity Problem"** Prof. Eugene Spafford, Center for Research and Education in Information Assurance Security, Purdue University, one of the most well-known, noted and cited experts in cybersecurity research and education. Lecture with reception to follow. Prof. Spafford will discuss problems of technology, economics, policy and simple human will. He will also discuss some of the factors that we can change, and thus improve the overall security of our systems in the future. George Washington University; Media & Public Affairs Building, Room B07; 805 21st Street NW; Washington, D.C. More details below in Announcements.

-Apr. 12, 10:00 a.m. - 11:30 a.m., **The Cloud as a Shroud: Fraud in a Digital Age** - This Webcast panel discussion will look at the new face of fraud in a digital age, provide insights in how to prevent, detect and investigate fraud in the cloud and identify options to combat fraud in the cloud computing world. Panelist include Mark Herman, executive vice president, Booz Allen Hamilton, Bill Fox, JD, MA, senior director healthcare, LexisNexis Risk Solutions; Timothy A.

Gallagher, section chief, Financial Crimes Section, Criminal Investigative Division, Federal Bureau of Investigation; Richard Ingraham, senior principal healthcare industry consultant, SAS Institute; William J. Mahon, president, The MAHON Consulting Group. More information.

-Apr. 13, 7:00 p.m., **Privacy and Surveillance in America: Its Ramifications And Proliferations; Their Impact On You And Everyone, Every Day** - An objective overview and detailing of the WHO, WHAT, WHEN, WHERE and WHY of surveillance in the United States. Dr. William F. Eyre, a privacy expert and longtime member of the intelligence community, will identify WHOM are being watched, WHO is doing the surveillance, WHAT equipment is used, WHEN surveillance occurs, WHERE it occurs and WHY. Nolan Center at Georgetown Visitation Preparatory School in Georgetown, 1524 Thirty-Fifth Street, NW. More information.

-Apr. 13, **Secure Cyber Operations Start Here: Who are You and How Can I Be Sure?** - At this virtual event, seasoned IT and program implementation experts will address how they are proceeding to support secure, scalable identity protection and management systems for government enterprises. More information.

Announcements

-Dr. Carl Landwehr has joined CSPRI as a Lead Research Scientist. Following a 23-year career leading cybersecurity research at the U.S. Naval Research Laboratory, he spent the past twelve years funding, managing, and guiding cybersecurity research programs for the National Science Foundation (NSF), the Intelligence Advanced Research Projects Activity (IARPA) and its predecessor organizations, and the Defense Advanced Research Projects Agency (DARPA). Dr. Landwehr has also served as Editor-in-Chief of IEEE Security & Privacy Magazine, as a member of several studies for the National Academy of Sciences, and of DARPA's Information Science and Technology (ISAT) Study Group. He has received numerous awards for research and service to the professional community. Welcome, Carl!

-Join us on April 11, 2012, 6:30 p.m. for the next discussion in the Frank Howard Distinguished Lecture Series: "Why We Won't Solve the Cybersecurity Problem." Lecture with reception to follow. Don’t miss Prof. Eugene Spafford, one of the most well-known, noted and cited experts in cybersecurity research and education. He has an ongoing record of accomplishment as a senior advisor and consultant on issues of security and intelligence, education, cybercrime and computing policy to a number of major companies, law enforcement organizations, and academic and government agencies, including Microsoft, Intel, Unisys, U.S. Air Force, National Security Agency, GAO, FBI, National Science Foundation, U.S. Department of Justice, U.S. Department of Energy, and two U.S. Presidents. With over three decades of experience as a researcher and professor, “Spaf” has worked on various aspects of cyber security including software engineering, reliable distributed computing, host and network security, digital forensics, computing policy, and computing curriculum design. He is currently the chair of the ACM's US Public Policy Council.

We have been developing computing ("cyber") resources for over 60 years as an area of both research and practice. In that time we have made computing affordable, dependable, and

ubiquitous. Today, there isn't a sector of society — government, commerce, research, entertainment — that doesn't depend on some underlying computational resource. Why, Prof. Spafford asks, despite decades of experience and research, are our cyber resources still so vulnerable? What are the factors that keep us from really addressing our cyber vulnerabilities? In this talk, he will summarize some of the biggest obstacles to protecting our cyber enterprises. These include problems of technology, economics, policy and simple human will. He will also discuss some of the factors that we can change, and thus improve the overall security of our systems in the future. George Washington University; Media & Public Affairs Building, Room B07; 805 21st Street NW; Washington, D.C.

Legislative Lowdown

The House and Senate will be in recess for the Easter break through April 13.

-Online activists who helped sink the Stop Online Piracy Act (SOPA) earlier this year have now turned their sights to a House cybersecurity bill, the Cyber Intelligence Sharing and Protection Act (CISPA), writes The Hill's Brendan Sasso. CISPA, which is authored by Reps. Mike Rogers (R-Mich.) and Dutch Ruppersberger (D-Md.) and has more than 100 co-sponsors, is expected to come to the House floor for a vote during the week of April 23.

But the bill's sponsors say it has little to do with stopping piracy: The goal of legislation is to help companies beef up their defenses against hackers who steal business secrets, rob customer financial information and wreak havoc on computer systems. The bill would tear down legal barriers that discourage companies from sharing information about cyber attacks. Some companies are worried that antitrust laws bar them from cooperating with each other to address cyber threats, and some fear they could be held liable if they reveal information after an attack. Privacy groups worry that broad language in CISPA could lead to companies handing over people's personal information to the government.

In addition to CISPA, privacy groups have misgivings about other pending provisions, according to PC World, including the Secure IT Act, a bill sponsored by eight Republican senators, including Senator John McCain of Arizona that requires some federal IT contractors to share broad cybersecurity information with the government; and the Precise Act, an information-sharing bill sponsored by Representative Dan Lungren, a California Republican, and the Cybersecurity Act, sponsored by Senator Joe Lieberman, a Connecticut Independent.

Cyber Security Policy News

-Policymakers in the European Parliament approved legislation last week that will levy mandatory two-year sentences against any crimes involving cyber attacks, or possessing or distributing hacking software and tools. Proponents say the proposal was intended to establish harmonized penal sanctions against perpetrators of cyber attacks against an information system - for instance a network, database or website, and that illegal access, interference or interception of data should be treated as a criminal offense. Critics of the measure point out it could criminalize

many of the tools used by security professionals to test the stability and reliability of networks and computers. The bill still must be agreed upon by both the European Parliament and the Council of the European Union.

-The Congressional Research Service issued an exhaustive review (PDF) of the legal underpinnings for cybersecurity. Congress is debating whether to regulate private sector cyber practices, especially for critical infrastructure. But according to Federal News Radio, the CRS found the government is in the cyber regulation business already, citing the Chemical Facility Anti-Terrorism Standards from Homeland Security and the Maritime Transportation Security Act, which gives the Coast Guard regulatory authority, as examples.

-In less than a week, nearly 55,000 people have signed a petition urging the Justice Department to investigate whether employers who ask for their workers' Facebook passwords are breaking the law, ZDNet reports. Progressive Change Campaign Committee (PCCC) has launched a petition backing two U.S. senators who have called for an investigation into the practice of employers asking for Facebook passwords. Late last month, New York Senator Charles Schumer and Connecticut Senator Richard Blumenthal, both Democrats, called for an investigation to determine whether employers are violating federal law when they demand access to Facebook accounts. More recently, the liberal Progressive Change Campaign Committee (PCCC) launched a petition to support the cause: Employers Shouldn't Get Employees' Social Networking Passwords.

-Mac users got a rude awakening on security last week. Security experts in Russia and Finland released data showing that a malicious botnet of more than 600,000 Mac OS X systems had been created by exploiting a widespread vulnerability in Java. In other Mac malware developments, security vendor AlienVault said it found evidence that weaponized Word files targeting Macs have been used in attacks from the same Chinese group that has been targeting the Tibetan government and nongovernmental organizations. The Word files seem to exploit an existing vulnerability and target Microsoft Office for Mac.

-In the wake of a Supreme Court ruling that law enforcement should acquire probable-cause warrants from judges before affixing GPS devices to vehicles, prosecutors are shifting their attention to obtaining warrantless cell-tower location tracking of suspects, reports Wired.com. The change of strategy comes in the case the Justices decided in January, when it reversed the life sentence of a District of Columbia area drug dealer, Antoine Jones, who was the subject of 28 days of warrantless GPS surveillance via a device the FBI secretly attached to his vehicle. In the wake of Jones' decision, the FBI has pulled the plug on 3,000 GPS-tracking devices.

Meanwhile, a "disturbing" number of law enforcement agencies track cell phones without a warrant, the American Civil Liberties warned last week, citing documents gathered from across the United States. NextGov writes that civil liberties advocates have said they believe law enforcement concerns have prevented Congress from updating privacy laws to reduce warrantless tracking and searches. Of the more than 200 law enforcement agencies that responded to the ACLU's requests, 10 reported that they had never used cell phones to track anyone. Most police organizations sought the data from phone companies, although some cities, like Gilbert, Ariz., have purchased their own tracking technology, the ACLU reported.

Facing calls by the FTC and Congress for improved mobile privacy protections, mobile advertising companies are actively working on privacy initiatives. Last week, a group of companies in the mobile advertising industry announced that they are working to create an industry standard for anonymous mobile device identification, according to the InsidePrivacy blog. The companies include Velti PLC, Jumptap, RadiumOne, mdotm, StrikeAd, Smaato, Adfonic and SAY Media. This standard would replace the need to use unique device ID numbers.

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.