GW CSPRI Newsletter

February 14, 2011

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

Upcoming Events

-Feb. 15, 7:30 a.m. - 4:45 p.m., **ISACA National Capital Area Chapter Conference for DoD Community** - This all-day conference will focus on topics of interest to the Department of Defense community and to those who provide support to the DoD. This event, however, is not restricted to those with a current DoD affiliation as there are opportunities to learn about how to engage with DoD, obtain a clearance sponsored by a DoD organization, as well as many lessons to learn about the cyber threats impacting the nation's infrastructures and applying practical applications, cyber defense mechanisms and counter measures. Holiday Inn Rosslyn @ Key Bridge, 1900 North Fort Myer Drive, Arlington. More information.

-Feb. 16, noon, "Managing the Security of Knowledge Assets in the Age of Intelligent Everythings", talk by **GWU Prof. Julie Ryan**, chair of the Department of Engineering Management and Systems Engineering. Infrastructure elements, systems, and enterprises rely not only on data and information, but also on the implicit and explicit knowledge represented by their associated human resources. As the information society continues to

benefit from innovation, the underlying knowledge becomes a valuable and coveted property. Yet since it resided in human brains, the challenges to information security professionals and enterprise executives becomes more complex than simply protecting a piece of paper or a file in a computer. Tensions arise between intellectual property rights and human rights, which must be addressed. This situation is exacerbated by the fact that more and more elements of our surroundings are enabled by local data processing contextualized in an information rich environment.

This talk addresses the engineering and technical management aspects that emerge from this complicated mess. Lunch will be provided for the discussion session from 1pm-2pm following the talk. Please email cspriaa@gwu.edu if you want us to reserve a lunch for you. Room 302, Marvin Center at 800 21st St. NW. PDF Abstract.

-Feb. 16, 6:30 - 8:30 p.m., **Cyber-Security and Cyber-Deterrence - Dr. Martin Libicki**, senior management strategist at The Rand Corporation, discusses the increasing connectivity of systems and passing of information, vulnerabilities to information systems, and whether it is possible to have cyber deterrence versus playing the constant measure-countermeasure game. Marriott Residence Inn, Pentagon City, 550 Army-Navy Dr., Arlington. More information.

-Feb. 16-17, **FISMA Continuous Monitoring: Build Your IT Security Continuous Monitoring Program** - This Digital Government Institute seminar is designed for information security professionals who need to understand and implement an effective "continuous monitoring program" for all government and contractor run IT systems. UVA/Virginia Tech Northern Virginia Center, 7054 Haycock Road, Falls Church, Va. More information.

Feb. 17, **Cloud/Gov 2011** - The 5th annual industry conference addressing the government's movement towards cloud computing. 1400 M Street NW. More information.

-Feb. 22-24, **AFCEA Homeland Security Conference** - Topics of discussion include identity management, interagency collaboration, and DHS/state and local secure information-sharing. Speakers include **Gen. Keith Alexander**, director of the National Security Agency and commander of the U.S. Cyber Command. Ronald Reagan International Trade Center. More information.

-Feb. 24, 8:00 a.m. - 12 noon, **FedScoop's 2nd Annual CyberSecurity Summit** - The summit will host discussions on topics such as "Securing the Cloud," and "Law Enforcement's Perspective on Cyber Crime," and feature talks from U.S. Defense Command and Control Infrastructure Admiral (Ret.) Betsy Hight; Justice Dept. CIO Vance Hitch; Dept. of Defense Deputy CIO Robert Carey; and Symantec Vice President GiGi Schumm, among others. Newseum, 555 Pennsylvania Ave, NW. More information.

Announcements

CSPRI's **Professor Lance Hoffman** is on the program committee of the Tenth Workshop on Economics of Information Security (WEIS 2011) that will take place at George Mason University in Fairfax, Virginia on June 14–15, 2011. Submissions by economists, computer scientists, business school researchers, legal scholars, security and privacy specialists, as well as industry experts are encouraged; the deadline is February 28, 2011. The call for participation is here. Suggested topics include (but are not limited to) empirical and theoretical studies of:

Optimal investment in information security
Online crime (including botnets, phishing and spam)
Models and analysis of online crime
Risk management and cyberinsurance
Security standards and regulation
Cybersecurity policy
Privacy, confidentiality and anonymity
Behavioral security and privacy
Security models and metrics
Psychology of risk and security
Vulnerability discovery, disclosure, and patching
Cyberwar strategy and game theory
Incentives for information sharing and cooperation

Especially encouraged at this year's workshop are submissions of significant and novel research that consider the design and evaluation of policy solutions for improving information security and also those with empirical components. A selection of papers accepted to this workshop will appear in an edited volume designed to help policy makers, managers, researchers and practitioners better understand the information security landscape.

SECuR-IT Summer Internships in California

The Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) is a ten-week paid internship (June 13-August 19, 2011) with academic seminars, sponsored by TRUST partners UC Berkeley, Stanford University and San Jose State University with internships located in Silicon Valley and the San Francisco Bay Area.

SECuR-IT participation is open to graduate students (M.S. & Ph.D). Participation is limited to 30 people selected from a nationwide pool of applicants, who have demonstrated, outstanding academic talent. Women and historically underrepresented ethnic minority groups will be given strong consideration although everyone is encouraged to apply.

This is an excellent opportunity for students, having an emphasis in computer security, to gain invaluable research experience working with Silicon Valley technology companies. Students will attend computer security seminars at UC Berkeley, Stanford University, San Jose State University and at Silicon Valley industry locations.

The application deadline is February 18, 2011. Additional information can be found here.

New Report

The new paper by CSPRI researcher Prof. Diana Burley of GW, "Recruiting, Educating, and Retaining Cyber Security Professionals in the Federal Workforce: Lessons Learned but not yet Applied", is now on the CSPRI website.

Legislative Lowdown

-Utah Republican **Senator Orrin Hatch** said he plans to reintroduce cybersecurity legislation designed to boost international cooperation to confront digital threats. According to NextGov, the senator said the bill would be "basically" the same as the measure he offered in the last Congress with **Sen. Kirsten Gillibrand** (D-N.Y.). That bill, the "International Cybercrime Reporting and Cooperation Act," would have required, among other things, an annual cyber security report from the president; increased goals and benchmarks for combating foreign cyber attacks; increased foreign assistance for countries fighting cyber crime; and more State Department employees focused on cyber security.

-Congressman Bill Keating plans to introduce legislation putting limits on U.S. companies selling net monitoring equipment to repressive regimes, after news that a Boeing subsidiary sold powerful net inspection technology to Egypt's state telecom, Wired.com writes.

"The Iranian and Egyptian protests have taught us that social media can be as powerful as any gun," said Rep. Keating (D-Massachusetts). "Companies that are selling technology to countries that are using it to perpetuate human rights abuses must work with Congress to make this right. We should have the same safeguards – such as end user monitoring agreements – that we do when we sell weapons abroad."

-Rep. Jane Harman (D-CA), a nine-term House veteran and member of the subcommittee on Communications, Technology and the Internet, announced Tuesday she would resign her post later this month to head the Woodrow Wilson Center for Scholars, a think tank in Washington, D.C., writes Broadbandbreakfast.com.

Cyber Security Policy News

-At least five multinational oil and gas companies suffered computer network intrusions from a persistent group of computer hackers based in China, according to a report released Wednesday night by computer security firm McAfee. The New York Times reports that the attacks are thought to be similar to but less sophisticated than a series of computer break-ins discovered in late 2009 by Google, appeared to be aimed at corporate

espionage. Operating from what was a base apparently in Beijing, the intruders established control servers in the United States and Netherlands to break into computers in Kazakhstan, Taiwan, Greece, and the United States, according to a report, "Global Energy Cyberattacks: Night Dragon."

Not everyone is so convinced this attack is new or even that notable. **Marc Maiffret**, chief technology officer at security firm eEye Digital Security, said these on-off disclosures of hacker break-ins by Chinese cyberspies are distracting and designed to help companies drum up business and frighten consumers. Maiffret said if China is the aggressor that it appears to be in cyberspace, then it is time to elevate this conversation and debate to one of substantial action, instead of wielding it as another weapon of fear for security industry sales and budget increase requests.

"As the security industry gathers in San Francisco for RSA next week, let's hope we can for once shift the conversation beyond the latest scary threat and the new silver bullet technology to solve the problem," he wrote in an editorial on the company's blog responding to McAfee's disclosure. "We should engage in a serious conversation about what it will take at a policy level to make lasting improvements that impact the future security of our technology-engrained way of life."

-**CIA Director Leon Panetta** called cybersecurity the "battleground of hte future." Addressing the House Intelligence Committee last week, Panetta echoed concerns of **FBI Director Robert Mueller**, who said cybersecurity was an increasing concern. "Other countries are developing a significant capacity in this area, whether it's Russia or China or Iran," Panetta told the panel. "We're now the subject of literally hundreds of thousands of attacks that come in, in an effort to try to get information."

-The United States still is not well equipped to respond to cyberwarfare attacks and is not taking the threat seriously enough, according to two key congressmen charged with overseeing the Defense Department's efforts to protect U.S. computer systems. Stars and Stripes notes that the bleak assessment is likely to undergird cybersecurity discussions on Capitol Hill the rest of the year. "In Congress, the legislative calendar is under way picking up last year's unfinished business of determining who in the federal government is in charge of the various cyberwarfare responsibilities," writes S&S reporter **Kevin Baron**.

-Attackers behind the Stuxnet computer worm focused on targeting five organizations in Iran that they believed would get them to their final target in that country, according to a new report from security researchers, according to new research released by Symantec. "The five organizations, believed to be the first that were infected with the worm, were targeted in five separate attacks over a number of months in 2009 and 2010, before Stuxnet was discovered in June 2010 and publicly exposed," writes Wired.com's Kim Zetter. "Stuxnet spread from these organizations into other organizations on its way to its final target, which is believed to have been a nuclear enrichment facility or facilities in Iran."

-Hacktivists allied with the Internet troublemaking group known as **Anonymous** are escalating their attacks in their ongoing effort to humiliate and annoy businesses that withheld services from **Wikileaks** or tried to help governments censor the whistleblower outfit. Anonymous has been conducting simple denial-of-service attacks against Visa, Paypal, and other U.S. organizations that refused to provide services for Wikileaks, but last week the group took aim at a security services company that does classified computer security work for the U.S. government and has been helping the government identify Anonymous hacktivists. Anonymous hacked into the e-mail accounts for HBGary's CEO and several other executives, placing entire archives of the messages up on public file-trading networks.

-One-third of Internet users in the European Union experienced malware infections, according to statistics gathered by the EU. Reuters reports that the countries with the highest rates of infection were Bulgaria, where 58 percent of users reported infections, and Malta, Slovakia, Hungary, and Italy, where about half of all users reported infections. Those with the lowest rates were Ireland and Austria, with about a 15 percent infection rate. The statistics were compiled by users reporting infections, so the actual rate of infection is likely to be even higher. Eighty-four percent of the more than 200,000 people surveyed said they have some sort of anti-malware technology in place.

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.