GW CSPRI Newsletter

August 13, 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.

Events

-August 13, 5:30 p.m. - 8:30 p.m., **NoVA Hackers Association Meetup** - This Northern Virginia area DC area infosec group will host a dinner meetup at QinetiQ, 11091 Sunset Hills Road, Reston, VA. More information.

-August 14-16, **TechNet Land Forces East: Cyber** - The operational theme, "Cyberspace Operations - Prevent, Shape, and Win" will highlight the operational security focus of DoD and Industry Networks, and Cyber Operations with Joint and Coalition partners, to prevent, shape, and win future cyber conflicts. Government, industry, and academia leaders will address a broad range of topics and focus on the opportunities for Cyber Superiority. Baltimore Convention Center, 1 West Pratt Street, Baltimore, Md. More information.

-August 21, 6:30 p.m., **ISSA National Capital Chapter August Meeting** - The Information Systems Security Association will host Curtis Levinson, selected by NATO (the North Atlantic Treaty Organization) to represent the United States as an advisory subject matter expert on cyber defense for the Industrial Resources and Communications Services Group, which falls under NATO's Civil-Military Planning and Support Section. Government Printing Office, Room A138, 732 N. Capitol St. More information.

-August 22, 2:00 p.m., **Big Data: Exploring Cybersecurity and Scientific Use Cases** - A national townhall teleconference series with a panel of government experts from CIA, NIST, and

NITRD, and industry experts from Intel and Oracle explore Big Data in use cases, including continuous monitoring for security, malware detection, fraud prevention, anti-terrorism and scientific research and discovery. More information.

Announcements

-The new GW Magazine cover story, “Of Mice and Menace”, interviews graduates from four different GW Schools (Engineering and Applied Science, Columbian College of Arts and Sciences, Elliott School of International Affairs, and Business) who have studied cybersecurity and gone on to work for the federal government as part of the GW's CyberCorps. Professors Lance Hoffman (CSPRI Director) and Shelly Heller, the co-principal investigators, and Mischel Kwon, who has taught many of our graduates, are also interviewed. A preview of the new GW-wide cybersecurity initiative also appears at the end of the article.

Legislative Lowdown

-Two Democratic congressmen are proposing sweeping changes to a U.S. privacy law that for the first time would require the government to obtain a probable-cause warrant to access data stored in the cloud, writes Wired.com. The law that the measure would amend is the Electronic Communications Privacy Act, which has seen few updates following President Ronald Reagan’s 1986 signature on the measure. But technology has evolved, and e-mail often remains stored on cloud servers indefinitely, in gigabytes upon gigabytes — meaning the authorities may access it without warrants if it’s older than six months. The same rule also applies to content stored in the cloud. That includes files saved in Dropbox, communications in Facebook, and Google’s cloud-storage accounts. Such personal storage capabilities were nearly inconceivable when President Reagan signed the bill.

Cyber Security Policy News

-A reporter for Wired last week suffered a series of embarrassing and devastating attacks on his data, thanks to a combination of security weaknesses at tech giants Amazon and Apple. "In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages," Honan wrote in a chilling account of the episodes. "And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook." Honan took some responsibility for the attack, noting that he should have taken more care to protect each individual account, instead of daisy-chaining various accounts together in a security chain that was only as strong as the weakest link.

In response to the high-profile incident, Amazon issued a policy change that fixes the security hole exploited to ruin Honan's data, by no longer allowing people to call Amazon and change account settings like credit cards and email addresses. Previously, Amazon's phone policy essentially allowed hackers to use social engineering tricks on support representatives to learn sensitive information about targets like Honan. But as Ars Technica notes, Apple has yet to change its policies, noting that "in this particular case, the customer's data was compromised by a person who had acquired personal information about the customer. In addition, we found that our own internal policies were not followed completely. We are reviewing all of our processes for resetting account passwords to ensure our customers' data is protected."

-A newly uncovered espionage tool, apparently designed by the same people behind the state-sponsored Flame malware that infiltrated machines in Iran, has been found infecting systems in other countries in the Middle East, according to researchers at Kaspersky Lab. The malware, named "Gauss" after its main module, which steals system information but also has a mysterious payload that could be destructive against critical infrastructure, has been found infecting at least 2,500 machines, most of them in Lebanon. Wired writes that the discovery appears to add to the steadily growing arsenal of malware created by the U.S. and Israeli governments. That list includes the groundbreaking Stuxnet cyberweapon that is believed to have infiltrated and caused physical damage to Iran's uranium enrichment program, as well as the spyware tools known as Flame and DuQu. But Gauss marks the first time that apparently nation-state-created malware has been found stealing banking credentials, something that is commonly seen in malware distributed by criminal hacking groups.

News of the emergence of yet another apparently nation-state-backed malware family surfaced as security experts announced findings that a commercial spyware tool marketed to governments worldwide has previously undisclosed global reach, with computers on at least five continents showing signs of being command centers that run the intrusion tool. Bloomberg News charts the carnage in a story about the global adoption of FinFisher, which can secretly monitor computers -- intercepting Skype calls, turning on Web cameras and recording every keystroke.

-The Pentagon has proposed that military cyber-specialists be given permission to take action outside its computer networks to defend critical U.S. computer systems — a move that officials say would set a significant precedent. According to The Washington Post, the proposal is part of a pending revision of the military's standing rules of engagement. The secretary of defense has not decided whether to approve the proposal, but officials said adopting the new rules would be within his authority.

-Dozens of hospitals across the country lost access to crucial electronic medical records for about five hours during a major computer outage last week, raising fresh concerns about whether poorly designed technology can compromise patient care, the Los Angeles Times reports. Cerner Corp., a leading supplier of electronic health records to hospitals and doctors, said "human error" caused the outage July 23 that it said affected an unspecified number of hospitals that rely on the Kansas City, Mo., company to remotely store their medical information.

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.