Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

CyberCorps program still accepting applications

The GW CyberCorps Program is accepting applications for the upcoming 2016 - 2017 academic year.

The scholarship includes fully funded tuition and fees, a living stipend, book allowance, and a professional development fund.

Completed scholarship packages are due byJanuary 31, 2016.

Click **here** for more information.

January 19, 2016

Six (6) events scheduled in the Greater Washington Area in the next few weeks.

ShmooCon Recap

GW Interdisciplinary Student Team Discusses New Research at ShmooCon Conference

On Sunday, January 17, Trey Herr, a doctoral candidate in political science and a senior research associate at CSPRI, and Eric Armbrust, a junior in computer science, spoke about their work differentiating state and non-state authored malicious software at ShmooCon, a major East Coast hacker conference. They discussed the challenges of combining work in political and computer science and their findings, a rudimentary means to differentiate the architecture and behavior of state code (milware) from non-state code (malware). For more, see **their paper** and look for the entire talk to be posted in the next few weeks.

Legislative Lowdown

-The Senate Judiciary Committee is expected to meeton Thursday to vote on the Judicial Redress Act, which gives some Europeans the rights to sue U.S. agencies if their personal data is misused. According to Morning Consult, the bill is

Events

January 20
Novalnfosec Meetup, West

January 20 - 21
Moving Forward: Collaborative Approaches to Medical Device Cybersecurity

January 21
How Germany and the United States are Racing to Build the Factory of the Future with the Internet of Things

January 21
ISSA NoVA Meetup: Encryption and Federal Law Enforcement

January 21
ISACA NCA Meetup" Young Professionals Event: Effective Vulnerability Scanning and PowerShell Scripting

January 21
Charmsec

Click here for detailed descriptions

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

"vital to European officials as they negotiate a new data sharing agreement with the United States. The EU and U.S. have until Jan. 31 to decide on a new pact that would allow American companies in Europe to transfer Europeans' personal information to servers in the U.S. If they fail to finish the deal, any data transfers made by American companies could result in legal action." Read more here.

Cyber Security Policy News

Mexican criminal taken down by Blackberry messages
-Joaquín "El Chapo" Guzmán, once Mexico's most-wanted criminal, was busted after his BlackBerry messages were obtained by the Mexican government, reports NextGov. His BlackBerry conversations with Mexican actress Kate de Castillo, who helped organize an interview with U.S. actor Sean Penn, were one of the many elements that led to his arrest (link in Spanish,) Mexico's Secretario of the Interior Miguel Angel Osorio Chong told Radio Fórmula,"writes Ana Campoy for Quartz. "It's unclear how Mexican authorities got the BlackBerry communications published by Milenio." While Blackberry has a reputation for security (President Obama uses one) that reputation is eroding. "Dutch police have learned how to crack encrypted BlackBerry messages," Campoy writes. "In response, BlackBerry said in a statement that there are no "backdoors" to its devices."

Automakers increasing efforts to enhance safety and defend against cyber-attacks
-The U.S. Transportation Department and 17 automakers have reached agreement on efforts to enhance safety, including sharing information to thwart cyber-attacks on their increasingly wired vehicles, according to Bloomberg. "Automakers including General Motors Co., Ford Motor Co. and Toyota Motor Corp. also agreed to reform the way they report fatalities, injuries and warranty claims to the government," Jeff Plugis writes. "The companies agreed to keep meeting regularly to exchange information and identify emerging safety issues."

Casino suing Trustwave
-A U.S. casino is suing the cybersecurity firm it hired to help handle a data breach in a case that experts say is likely the first of many. The Hill reports that the lawsuit, filed in late December, appears to be one of the first of its kind, in which a company challenges a cybersecurity contractor on how it manages the fallout from a hack. "Affinity Gaming hired Trustwave, a Chicago-based cybersecurity firm, to investigate and remedy a 2014 breach that compromised credit card information for around 300,000 customers,"writes Katie Bo Williams. "Affinity now alleges that it discovered a second hack that occurred during the investigation process - after

Trustwave assured it that its systems were secure."

Texan manufacturing firm suing its cyber insurance provider
-A Texas manufacturing firm is suing its cyber insurance provider for refusing to cover a $480,000 loss following an email scam that impersonated the firm's chief executive. At issue is a cyber insurance policy issued to Houston-based Ameriforge Group Inc. (doing business as "AFGlobal Corp.") by Federal Insurance Co., a division of insurance giant Chubb Group. AFGlobal maintains that the policy it held provided coverage for both computer fraud and funds transfer fraud, but that the insurer nevertheless denied a claim filed in May 2014 after scammers impersonating AFGlobal's CEO convinced the company's accountant to wire $480,000 to a bank in China. KrebsOnSecurity.comhas the rest of the scoop on this story.

Presidential debate highlights technical issues
-The Democratic presidential debate last week demonstrated a lot of things, but it also showcased where the candidates were weak. According to GovInfoSecurity, the Dems don't have a strong handle on the continuing dispute among some in the government such as FBI Director James Comey and cryptography experts on whether technology companies should provide law enforcement with a backdoor to decrypt secret messages. "Should we expect the candidates to have a strong understanding of a critical security and privacy issue that is highly technical? No, we don't need a president who is a technologist," writes Eric Chabrow. "But the next commander in chief should be someone who can tap the brightest minds to advise them on technical and scientific matters that are critical to our nation's well-being."

Nations with nuclear power plants lack protection against cyberattacks
-Twenty nations with significant atomic stockpiles or nuclear power plants have no government regulations requiring minimal protection of those facilities against cyberattacks, The New York Times reports. The data - from a report released by the Nuclear Threat Initiative -- build on growing concerns that a cyberattack could be the easiest and most effective way to take over a nuclear power plant and sabotage it, or to disable defenses that are used to protect nuclear material from theft, the Times writes. The countries on the list include Argentina, China, Egypt, Israel, Mexico and North Korea.

US nuclear cybersecurity update
But that hardly means the United States is in a much better position. A report released last week by the Nuclear Regulatory Commission found that the nation's unclassified nuclear computer systems are vulnerable to successful cyber attacks because "generic" security contracts don't make it clear who's

responsible for keeping an eye on them. Read more at NBC News.

About this Newsletter

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. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613, **cspri@gwu.edu**
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052