The Datagram newsletter

February 2017 Volume 2, No. 2

From the Chair...

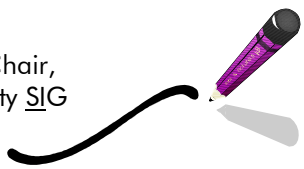
Our Web Site is expected to expand. We are planning on adding a forum, a place where we can meet, talk, and discuss various topics and exchange ideas. The forum will be established around various topics of interest, and here your input is helpful. What are the topics of interest? If you want to discuss something and don't want to be distracted by things that are not relevant, how do you want us to describe it? Are the generic characterizatons of CyberSecuriity, Cryptography and Software specific enough?

We have put some articles onto the Web Site of at least peculiar interest. Look at Resources->Other and tell me that the "CIA Intelligence Officer's Handbook" doesn't strike a resonant chord. We made available the Microsoft Security Posture to allow you to see how Microsoft views CyberSecurity and what steps they are taking to address the issues. And for a little curious reading, we have included a reference to the 'Unclassified Russian Hacking Paper" from the intelligence agencies.

We are growing. Please grow with us.

Art

(reluctant) Chair,
CyberSecurity SIG



Next meeting:

February 22, 2017

6:30 PM Dinner and Networking
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM Meet & Mingle

Dinner: FREE

ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106 (Room number subject to change)

Speaker: Carlos A. Villegas

This Month's Topic: Protecting Passwords in a Post-Quantum Computing Era with Military-Grade Crypto

This month's presentation is about how to create and store passwords in a secure way using military-grade cryptography so that even in the hands of your worst enemies, they can't be cracked. It will look at will passwords from a digital forensics point-of-view to show what needs to be done on the back-end to secure them properly. At least four live password attack vectors will be demonstrated live along with a way on how to properly defend against those attacks. ■

Check Out Our Website

Visit the CyberSecurity SIG's website for links to great books and articles, other orgniazations associated with cyber security, software, online classes in cyber security, and more!

About the Speaker

Carlos A. Villegas is a cybersecurity engineer at Northrop Grumman Aerospace Systems, where he has been employed for the past 20 years. He started programming at the age of 13 and has been doing so professionally for 25 years. He is CompTIA Security+ certified.

His Open Source contributions include Linux Logs for Digital Forensics, Secure Messaging with Steganography, and he serves as Cyber Advisor to KMEX Channel 34 in Los Angeles and has mentored high-school students for the U.S. CyberPatriot National Youth Cyber Defense Competition since 2014.

At the U.S. Cyber Challenge in 2015 in Cedar City, Utah, he ranked 10th place by scoring 100% in the entry quiz. He placed 37th in the National Cyber League in 2014.

He received a Master of Science degree in Cyber Security at New York University in January of 2016 and a Master of Science in Computer Science, Artificial Intelligence, from USC. ■

Contact Information

Website: sites.ieee.org/ocs-cssig

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

January Meeting Report:

Defending Against DDoS Attacks On the Cloud

by Carol J. Amato

Our January speaker, Huy Huynh, a solution architect with Amazon Web Services, discussed DDoS (Distributed Denial of Service) attacks, which he stated can come from anywhere. Attacks occur in three layers: 1) network; 2) transport; and 3) applications.

DDoS attacks can look like real traffic. The main issue is "amplification," which means that the attacker can use a small number of resources but get back large amounts of data. The attacker makes the request of the DNS or NTP server. The Reply address is to the victim, and the victim's computer gets overwhelmed. The reflectors don't even have to be compromised.

He explained the concept of a "Rudy" ("Are you dead yet?"). This is a very large payload that is sent slowly over a long duration. A Rudy blocks real traffic to the server.

There are challenges in mitigating DDoS attacks. Another DNS server may have to be added. Application re-architecture may be conducted. Traffic may have to be rerouted manually via a distant scrubbing location.

Amazon Web Services protects against these common attacks and incorporates some DDoS infrastructure into their systems, and Huynh discussed AWS's service offerings in detail. Huynh also stated that most companies use more than one DNS provider to prevent a system-wide attack. ■

Hacker Shuts Down Thousands of Sites on the Dark Web

At the beginning of February, a hacker attacked the Dark Web, taking down a server on the Tor network (not on the Dark Web) that hosts around 10,000 websites.

The Tor network is designed to hide the identity of its users, who, for the most part, are involved in illegal activities.

According to Tech News World, this was the first hack the attacker carried out, and he/she stole 74 GB in files and a 2.3 GB database of 381,000 email addresses with .gov extensions. Whether the addresses are legitimate is not known at this time.

For a detailed report, go to http://www.technewsworld.com/story/84285.html ■

Queen Elizabeth to Open Britain's National Cyber Security Centre

On February 14th, Queen Elizabeth, along with Prince Philip and several government ministers, including finance minister Phillip Hammond, will open Britain's new National Cyber Security Centre (NCSC) in London.

According to Hammond, Britain is experiencing increasing cyber attacks. The NCSC has responded to 188 attacks in the first three months of its existence. Staff is also gearing up for a "Category 1" attack, which they expect "sooner or later," says Ciarin Marting, CEO.

See the detailed article at https://www.yahoo.com/tech/queen-unveil-britains-cyber-security-centre-000939689.html ■

Please Provide Feedback on Our Website

We want your feedback on our new website. (See the announcement on page 1.) If you like what you see, tell us and tell others. If you have any changes to suggest, please let us know. We are open to any suggestions and would appreciate your comments. Let us know what you think! ■

Place Your Ads in The Datagram

Do you have information about an academic program, seminar, workshop, symposium, presentation, or job listing related to cybersecurity? Consider placing an ad in The Datagram.

Ads are currently FREE and will be published for three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at sites.ieee.org/ocs-cssig.com for maximum exposure.

Submit a camera-ready, business-card-sized (3.5" x 2") JPG file to Carol Amato at stargazer@stargazerpub.com. ■

Have suggestions for what you would like to see in the newsletter?

Send them to Carol J. Amato at stargazer@stargazerpub.com.■

Request for Articles

This newsletter is open for article or information submission by all members of the CyberSecurity SIG. If you have something to say or leads on information that would be of benefit to the SIG, the members would love to read it.

Articles must be a maximum of 500 words and concern some aspect of cybersecurity. Submit them double-spaced via a .doc, .docx, or .rtf file to Carol J. Amato, Newsletter Editor, at stargazer@stargazerpub.com. ■

Speakers Requested

If you know of an expert in cybersecurity who is willing to speak to our CyberSecurity SIG, please contact our program chair, Irvin Lemus, at ilemus3@coastline.edu. ■

2016 CyberSecurity SIG Executive Committee

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Irvin Lemus
Newsletter	Carol J. Amato
Web Design	Jo3 McCarthy
Audio-Visual	Open

TEKsystems

Thank you!

Our sincerest thanks to Ashley Groothuis of TEKsystems for sponsoring our food and beverages for the rest of the year. This means dinner will be free to everyone. Thanks again so much to Ashley Groothuis and TEKsystems! ■