The Datagram newsletter

September, 2017 Volume 2, No. 9

From the Chair...

We are electing volunteers for the next 2 years. The volunteers are responsible for SIG operations and direction. We look forward to the new Executive Committee (ExCom) officers providing additional insight and direction and to lead the SIG into a new direction. We, the old ExCom, are committed (or should be) but need new blood.

The election procedure is a two-stage affair. During the preliminary stage, you self-nominate. You, the volunteers, select the positions that you would like to hold. You then become a candidate. As a candidate, you can provide a brief bio and sales pitch to tell the SIG members about your qualifications, what direction you would like to take the SIG, and why you should be elected. This is an awesome task which only you can do.

The second stage is the election. The members cast ballots for the candidates. The candidate receiving the most votes receives the post. If there is no clear majority, then the Ex-Com selects their replacements.

Continued on page 2

Next meeting:

September 27, 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: Paul Myer

This Month's Topic: The Differences Between HDN and SDN and Network Security Impacts

There are many misconceptions about Software Defined Networks (SDN) today, and it begins with the acronym itself. This session will explore key differences in the technology and approaches of Hardware Defined Networks (HDN) vs. SDN. With SDN, there are new impacts to security Supervisory Control And Data Acquisition (SCADA) networks that take into account "Operational Realism" to simplify industrial network and security. It will also explore new capabilities of industrial SDN that raise interesting questions for the future of industrial networking. ■

About the Speaker

Paul Myer is an accomplished technology leader with over 25 years in executive management, operations, consulting, sales, marketing, and strategic alliances and partnership roles. Paul has been focused in the network security and big data software market, including M86 Security (Web and Email Security), and Public Engines (Cloud-based crime data visualization and predictive analytics). In his current position as CEO of Veracity Industrial Networks, Paul is building an industrial network security platform based on Software Defined Networking (SDN) for critical infrastructure networks. ■

2017 CyberSecurity SIG

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

From the Chair, *Cont'd.*

selects their replacements.

And after all is said and done, you become a member of the new ExCom officers.

The general time frame is that you will receive a request for nominations to the ExCom in September, an election ballot in October, and officer installations in January. At this point, the old ExCom officers offer support and training for 6 months or so (and, of course, longer as needs be).

You can find out more about officer responsibilities on our web site (Home->Charter), but because of some IEEE issues, the document is poorly formatted at the time of this writing. So it's all there, but it doesn't look nice.

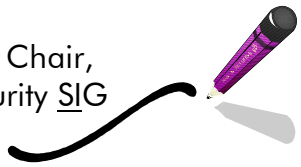
No volunteers. No SIG.

A little history and whatnot. We started in October, 2015, with 6 members. We are now at (about) 250 and with our current growth will probably be between 350 and 400 by January, 2019. We have members in Virginia, Texas, San Diego, and Northern California, as well as in our home base of Orange County. Our web site has grown to over 700 items, and we are currently adding about one new topic a month. We have become a "'go-to" place.

This month, we will be adding a rather small section on airplane cyber security. By some strange circumstance, articles and references died out in 2016, so most of the material is pre-2016. As time becomes available, we will be making a concerted effort to expand this area.

Art

(reluctant) Chair,
CyberSecurity SIG



Equifax Hack Affects 143,000,000 Americans

by Carol J. Amato

On September 7th, Equifax revealed that from mid-May through July of this year, it had been hacked and the data for approximately 143,000,000 Americans compromised. This information includes names, Social Security numbers, birthdates, addresses, and some driver's license numbers. Credit card information for around 209,000 consumers and some dispute documents for approximately 182,000 consumers were also accessed.

While Equifax worked immediately to stop the intrusion and its investigation is expected to be completed in the next several weeks, the big question is why the company waited until September to reveal this breach to consumers.

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to allow consumers to check if their information was involved.

The problem is that the response given to the check is "Your information may have been hacked." There is no definite yes or no. Equifax then advises the consumer to sign up for its complimentary identity theft protection and credit file monitoring service. Some people have suggested that this is a ruse with a view to eventually charging consumers to continue this service, but there is nothing on the website to indicate this.

Experts suggest that another good line of defense is for consumers to freeze their credit if they feel they could have been part of this security breach. According to the Federal Trade Commission, a credit freeze prevents creditors from accessing a consumer's credit report. While the consumer can still see it and get an annual report, and existing creditors, debt collectors, and government agencies can, too, anyone else trying to use the stolen information to obtain credit will be prevented from doing so. A freeze will have to be scheduled with each of the three credit reporting agencies.

The consumer must temporarily lift the ban in order to obtain credit again. It would have to be lifted only with the credit reporting agency that the company granting the loan uses.

Experts claim that this breach occurred due to Equifax's refusal to spend money on avail-

able cyber security patches, instead using the money to buy back stock from its own executives. This deliberate negligence could result in the demise of the company.

For further information, go to https://www.equifaxsecurity 2017. com/potential-impact/ and https://www.usatoday.com/story/money/2017/09/13/how-freeze-your-credit-protect-your-identity/657304001/■

Harvard University Offers Online Cyber Security Course

Harvard University's Harvard Kennedy School, is offering a new 8-week online course in cyber security. Taught by course convener Eric Rosenbach, attendees will come away with the following:

- The ability to draft, strategize, and develop a cyber risk mitigation strategy, including the appropriate legal and compliance steps that need to be taken when responding to cyber attacks and reporting cyber attacks to law enforcement.

- An in-depth understanding of the different types of cyberattacks, the business systems that are most at risk, and the importance of an organization-wide approach to cybersecurity.

- A premier certificate from Harvard University's Office of the Vice Provost for Advances in Learning, in association with HarvardX, as validation of your new-found cyber security knowledge and skills, as well as access to a global network of likeminded cybersecurity professionals.

Rosenbach is theCo-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School. In addition, he is the Director of the Defending Digital Democracy Project, and Co-Director of the Belfer Center for Science and International Affairs at Harvard Kennedy School. He previously served as the Chief of Staff to US Secretary of Defense Ash Carter, and held the position of Assistant Secretary of Defense. He was the Chief Security Officer for Tiscali, the largest pan-European internet service provider, and is a former US Army Intelligence Officer. (2017, https://gs.harvardx.harvard.edu/harvard-cybersecurity-online-short-course-hm/?utm_source=PPC& utm_medium=adwords_ppc&utm_campaign=HAR_CYB_aw_usa_mo&AdID=217859486778&CID=914493353&AgID=46118795176&KW=%2Bcyber%20%2Bsecurity&gclid=Cj0KCQjwruPNBRCKARIsAEYNXIiee4uQnebKBLkdNWAJVEYRscbHqvPlHONZq6_iiCSaS3U0BAekvk4aAmJ8EALw_wcB)■

Global Cyber Attack on Energy Sector

The hacker group "Dragonfly" conducted recent cyberattacks on the energy sectors of Europe and North America, Symantec reported.

Contact Information

Website: sites.ieee.org/ocs-cssig

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

The attacks could provide the group with the means to severely disrupt energy operations on both continents. Dragonfly launched a similar campaign from 2011 to 2014, but it entered a quiet period in 2014 after its activities were exposed. For details, go to http://www.technewsworld.com/perl/■

Request for Articles

This newsletter is open for article or information submission by all members of the Cyber-Security 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. For articles over 500 words, please provide a double-spaced abstract for publication in *The Datagram*, and the full article, single-spaced, as a .doc, .docx, or .rtf file to Carol J. Amato, Newsletter Editor, at stargazer@ stargazerpub .com. ■

Please Provide Feedback on Our Website

We want your feedback on our new website. If you like what you see or have any changes to suggest, tell us and others. If you have any changes in mind, please let us know. We are open to any suggestions and would appreciate your comments.■