The Datagram newsletter

August, 2016 Volume 1, No. 8

From the Chair...

The workshop went extremely well. The insights gained allow even the least knowledgeable to become a first-class hacker, to discover that which would otherwise be well-hidden. And towards this, I have to thank the attendees. You all accepted the many challenges and valiantly (and I hope successfully) got into the "Winner's Circle."

Some high-school (and one 7th-grader) kids were there to hear, learn, and participate. The 7th grader told me that he was successful on the first four challenges; hence, was able to infiltrate our "server" with illicit code and enter the famed "Winner's Circle" but didn't have the computing knowledge to do the fifth and beyond. That's the 7th grade. The 8th grade should be much, much better. And where were you? This was a great workshop.

There is a note of more than casual interest. We would like to support publication of small articles in The Datagram, and for this, let me direct you to NIST (http://csrc.nist.gov/) and DARPA (http://www.darpa.mil/our-research?tFilter=15&oFilter=&sort=undefined) for some articles to review. One or two of them are on our web site. Take a look. If you read the articles maybe you can summarize the conclusions and write an article about it. My interest is in Lightweight Cryptography, and I intend to read, learn and report.

To keep you abreast of ongoing activity, we are in the process of moving

Continued on page 2

Next meeting:

August 24, 2016

6:30 PM Networking and dinner
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM More networking

Dinner: FREE

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

Presenter: Aaron Sramek, enSilo

This Month's Topic:

Aaron Sramek of enSilo will present "We Lost The Battle Against Intrusion — Are We Left to Raise Our Hands in Defeat?"

Enterprises are pouring billions of dollars into preventing threat actors from infiltrating the organization. Yet, the rising level of breaches shows that dedicated threat actors will penetrate the organization. Perhaps then the problem is not a technological one, but is rather one of strategy in dealing with cyber-threats?

In this session, he willl propose a new defense approach. This strategy assumes that the environment is already compromised and focuses on preventing the real risk to the enterprise: the actual exfiltration and hijacking of data. We'll show how adopting such a strategy enables organizations to streamline security and align with the business operations as they investigate and remediate a threat.

This session will discuss:

Continued in Column 3

About the Speaker

Aaron Sramek, Security Engineering Manager at enSilo, has over 15 years experience in network, systems, and application security. Aaron has worked to architect and secure networks and applications for naval defense systems, emergency notification systems, and large international distributed data center environments. At enSilo, Aaron focuses on the evolution of malware and advanced threat containment systems.

This Month's Topic, Cont'd.

- The current landscape of advanced threats and the current approaches to stop the consequences
- New and effective strategies to combat today's advanced threats
- Removing the OpEx associated with security solutions
- Real-life cases of successful enterprises challenging their security status quo ■

Contact Information

Web site: cssig.brats.com

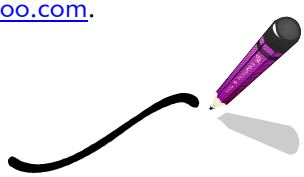
Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

From the Chair, Cont'd.

our web site to an IEEE host. The new location will be at http://sites.ieee.org/ocs-cssig. We're not there yet, but if you take a look, comment. This is your site and you deserve to let us know how we're doing. Some things we can change, some not. but we don't need to change anything without your input. And, you can check on our progress. Hopefully you'll complain if it's too slow. This is a public site, not an IEEE only site. Just saying.

We have also moved all non-meetup announcements to an IEEE Listserver. This provides an (almost) single source for our official announcements. For those receiving notification through Meetup.com, you will remain supported. We would like you to transition over to the new Listserver at your leisure. Send an email to slipbits@yahoo.com.



Art

(reluctant) Chair,
CyberSecurity SIG

July Meeting Report: Web Application Security: Command Injection Workshop

by Carol J. Amato

This month, Dr. Sam Bowne from the City College of San Francisco conducted our first hands-on workshop to a standing-room-only crowd. According to him, the most important cybersecurity problem in the world is code injection, which is responsible for over 95% of all stolen data.

Armed with our computers, we used the code he provided to hack into a server he set up for student practice. He issued several challenges:

- Ping form
- Buffer overflow
- ImageMagick exploitation
- SQL injection

Why learn to hack?

Dr. Bowne stated that his students don't understand how to defend against attacks as well if they don't also appreciate how attacks are accomplished in the first place. The point of hacking is to find the vulnerabilities. If the student can learn to attack a system first, he/she can then grasp what to defend against.

Attendees altered the provided code so that their names would appear in his server logs. The SQL test used the same process that hackers employed to infiltrate the Sony and Target servers. What was most surprising was just how easy it was to gain access; it required only one small line of code. Dr. Bowne explained that despite repeated efforts to warn companies of these security dangers, many don't seem interested in preventing them.

To try these tests yourself, go to www.samsclass.info. If the CyberSecurity SIG workshop is not listed on the main page, go to "Old Classes" in the links at the top. It will be listed there.

This workshop was definitely an interesting and enjoyable experience, and we look forward to scheduling more in the future.

Free Cybersecurity Book!

For a free book on cybersecurity, go to http://www.labtechsoftware.com/it/landing/MMsecurity-eBook-ppc/index.php?source=LTMM-PdSch-Google-Cybersecurity-US-16Q3&utm_source=google&utm_medium=pdsch&utm_term=information%20cyber%20security&utm_campaign=securitymm&loc=us&sc_camp=0B8006299BFB4AFCA4FA6722EFBD3A42&gclid=CKekqujzss4CFQxrfgodBPsL5A

Malicious Email Mitigation Strategies

In July, 2016, the Australian Cyber Security Centre (ACSC) published guidelines for malicious email mitigation strategies. These strategies cover the cyber intrusions that have targeted organizations. The Centre warns that not all of the strategies will apply to every organization. For top security effectiveness, do the following:

1. Convert attachments to another file format, such as a PDF.
2. Whitelist file formats based on file extension rather than blacklisting them as it is more proactive.
3. Block password-protected archives and unidentifiable or encrypted attachments.
4. Perform automated dynamic analysis of attachments run in a sandbox to detect suspicious behavior such as network traffic, new or modified files, or changes to the Windows registry. Don't rely on the use of signatures.
5. Sanitize attachments to remove active or potentially harmful content such as macros in MS Office files and JavaScript and embedded content such as an executable in MS Word documents and Flash content inside MS Excel spreadsheets.
6. Disable or control macros in MS Office files.

To read the full document, go to http://www.asd.gov.au/publications/index.htm#tabs-1

Thank you, TEKSystems!

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 through December. Thanks again so much to Ashley Groothuis and TEKsystems!

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 cssig.brats .com for maximum exposure.

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

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, Angela Young, at angela.y@email.com.

2016 CyberSecurity SIG Executive Committee

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Angela Young
Newsletter	Carol J. Amato
Outreach	Mark Wich
Web Design	Jo3 McCarthy
Audio-Visual	Open

Vulnerabilities in Qualcomm Chip Sets

Four vulnerabilities relating to Qualcomm chipsets used by an estimated 900 million Android smartphones and tablets could each be exploited to seize control of devices and steal any data they store, warns Israeli cybersecurity firm Check Point. For complete details, go to http://www.databreachtoday.com/four-android-flaws-leave-900m-devices-at-risk-a-9329.