The Datagram

newsletter

March, 2017 Volume 2, No. 3

From the Chair...

The Web Site changed and expanded. We now have an online listing of all IEEE OC Cyber-Security SIG officers with their email addresses. This allows direct contact with us about concerns, complaints, direction, and a few compliments. We are always available to support you and will respond to your requests as quickly as we can.

The Web Site has changed and expanded. INFOSec->Cryptography has now morphed into INFOSec->Cryptology. Under this title, we now have Cryptography, containing both classical and digital cryptography—basically, the old "Cryptography" now buried one level. We also have a section on Cryptanalysis and History.

The Cryptanalysis section is divided into Digital and Classical with some material by William F. Friedman, our Cryptanalyst Extraordinaire, who developed the World War II training manuals on classical cryptanalysis. Classical methods are an ideal exercises for beginning computer courses.

Continued on page 2

Next meeting:

March 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: Mahmoud Hammad

This Month's Topic:

DELDroid: An Automated System for Determination and Enforcement of Least Privilege Architecture

Modern mobile platforms rely on a permission model to guard the system's resources and apps. In Android, since the permissions are granted at the granularity of apps and all components belonging to an app inherit those permissions, an app's components are typically over-privileged; i.e., components are granted more privileges than they need to complete their tasks.

Systematic violation of the least-privilege principle in Android has shown to be the root cause of many security vulnerabilities.

Continued on page 2

About the Speaker

Mahmoud Hammad is a Software Engineering PhD student in the Informatics Department within the School of Information and Computer Science at the University of California, Irvine. He is also a member of the Institute for Software Research and a researcher at the Software Engineering and Analysis Laboratory (SEAL) led by his advisor, Dr. Sam Malek.

Mahmoud's general research interests are in the field of software engineerlng, and his main focus is in the area of software architecture and Android mobile security.

After he finished his B.S. in Computer Science (2005), he worked as an Oracle database application developer for six years followed by two years as a mobile software developer. Mahmoud received his M.S. degree in Software Engineering with an outstanding achievement award from George Mason University (2013). ■

From the Chair, *Cont'd.*

We now have a History section with material from the 17th Century to the present. The material shows not only the techniques used in cryptography/cryptanalysis but the evolution of our current security agencies. This is an interesting read for both technical and non-technical people. It spells our who we are and why.

Art

(reluctant) Chair,
CyberSecurity SIG

DELDroid , *Cont'd.*

To mitigate this issue, we have developed DELDROID, an automated system for determination of least-privilege architecture in Android and its enforcement at run-time.

A key contribution of our approach is the ability to limit the privileges granted to apps without the need to modify them. DELDROID utilizes static program analysis techniques to extract the exact privileges each component needs for providing its functionality.

A Multiple-Domain Matrix representation of the system's architecture is then used to automatically analyze the security posture of the system and derive its least-privilege architecture. Our experiments on hundreds of real-world apps corroborate DELDROID's ability in effectively establishing the least-privilege architecture and its benefits in alleviating the security threats. ■

February Meeting Report:

Protecting Passwords in a Post-Quantum Computing Era with Military-Grade Crypto

by Carol J. Amato

Carlos A. Vargas gave us a very informative talk on protecting passwords and data. He stated that hardware and software need each other, and that requires the need to be creative with how solutions are developed. This means making systems cyber-resilient so they can still function and do job even if they are hacked. Most antivirus programs can be hacked, however.

Vargas pointed out that the real cyber security problem is a global one. Medical equipment is the most recently targeted area, and this includes x-ray printers, MRI scanners, blood gas analyzers, and PACS (picture archiving and communication systems). This is serious because the damage costs could reach $6 trillion by 2021.

There is a new era of quantum-computing dawning. It uses qubits instead of classic binary digits. This is the quantum state between zero and one and allows an infinite number of states between those digits. As a result, this is a threat to encryption. Secrets run the risk of being recorded today and decrypted by quantum computing by 2030. Two thousand qubits are available today. Three thousand will be the number to make brute force attacks on AES encrypted plain text feasible and isn't far off.

To maintain as much security as possible, Vargas advises using long passwords that don't exist in the dictionary. They should also be composed of four words and at least 12 characters (upper, lower, number, and symbol).

For a list of unsafe and recommended algorithms for quantum computing, please see the slides from this talk posted on the SIG website at sites.ieee.org/ocs-cssig. ■

Contact Information

Website: sites.ieee.org/ocs-cssig

Meetup.com/CyberSecuritySIG

Newsletter Editor:
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. ■

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 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. 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. ■

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. ■

2017 CyberSecurity SIG Executive Committee

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Irvin Lemus
Newsletter	Carol J. Amato
Web Design	Ginson Samuel
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! ■

Your ad here

Your ad here

Your ad here

Your ad here