The Datagram newsletter

July, 2016 Volume 1, No. 7

From the Chair...

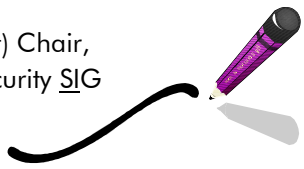
We must apologize. Our speaker for June, Michael Lipsey, was detained on a pressing business matter and could not make the meeting. In his stead, our October speaker, John McCarthy (Jo3) gave a presentation of Cyber-Security issues and resources. The presentation focused on detection of threats and resources available for threat recovery. Mr. McCarthy is a long-time CyberSecurity specialist and ably presents the issues. If you missed him, then you missed a live one.

Our July presentation is a 2- hour workshop instead of a speaker. See "This Month's Topic" in the next column for details. Unlike normal presentations, the workshop begins at 6:00 PM and not 7:00 PM. Bring your laptop.

Take a look at some current threats and Government and Corporate responses to them at cssig.brats.com->INFOSec->Articles. The SIG attempts to keep the articles relevant to the times, current events as well as historical precedents.

Art

(reluctant) Chair,
CyberSecurity SIG



Next meeting:

July 27, 2016

6:00 - 8 PM Hands-on Workshop
Bring your laptop

Dinner: $10 (cash only)

ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106

Presenter: Sam Browne, City College of San Francisco

This Month's Topic

Sam Browne from the City College of San Francisco will be our July speaker. He will be conducting a 2-hour workshop on web application security. The most important cyber-security problem in the world is Code Injection, responsible for over 95% of all stolen data.

In this workshop, participants will exploit command injection vulnerabilities in a CTF-style series of challenges:

- Ping form
- Buffer overflow into shell command
- ImageMagick exploitation
- SQL injection

No previous coding experience is required. For the basic challenges, all you need is a computer with a Web browser. For the more advanced challenges, you need a Kali Linux machine (real or virtual). This should be an educational experience for all of us.

About the Speaker

Sam Browne has been teaching computer networking and security classes at City College of San Francisco (CCSF) since 2000. He has given talks and hands-on trainings at DEFCON, HOPE, B-Sides SF, B-Sides LV, Bay Threat, Layer One, and Toorcon, and taught classes at many other schools and teaching conferences.

He has a B.S. in Physics from Edinboro University of Pennsylvania and a Ph.D. in Physics from University of Illinois, Urbana-Champaign.

Bring Your Laptop

Just anither reminder that this month's meeting is not our usual speaker format. It's a hands-on workshop, so bring your laptop so you can take full advantage of this

Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

FYI

Here are some interesting developments of which you should be aware:

1. New device can allegedly clone 15 contactless bank cards a second
The *Daily Star* newspaper is reporting that a new device has surfaced online which has the ability to clone 15 contactless bank cards a second.

Source: http://www.scmagazine.com/new-device-can-allegedly-clone-15-contactless-bank-cards-a-second/article/502599/

2. Netgear removes crypto keys hard-coded in routers
Qualys security researcher Mandar Jadhav has discovered two serious vulnerabilities in Netgear D6000 and D3600 modem routers, which can be exploited to gain access to the devices and to intercept traffic passing through them. The vulnerabilities reside in the devices' firmware, versions 1.0.0.47 and 1.0.0.49.

Source: https://plus.google.com/+Webimprints/posts/XCjV5g3Qyvk

3. Scammers have already started trying to exploit Orlando shooting for bitcoins
The vultures have already begun to descend on the tragedy in Orlando, Florida. A fake Twitter account claiming to represent the nightclub where the largest mass shooting in modern U.S. history took place in the early hours of June 12 was calling for donations to assist victims—by sending bitcoins to buy bottled water and Oreo cookies. The account was suspended on Monday afternoon.

Source: http://arstechnica.com/security/2016/06/scammers-have-already-started-trying-to-exploit-orlando-shooting-for-bitcoins/

4. Forget Game of Thrones as Android Ransomware Infects TVs
Researchers at Trend Micro have spotted a new variant of ransomware code that can be used to lock down Android-powered smartphones and telephones.
The FLocker (short for the Frantic Locker) malware has been in circulation since at least April 2015 and has concentrated on locking down smartphone handsets running the latest builds of Android. But the writer keeps on adding new features and has now extended the code to give smart TV owners problems, too.

Source: https://news.google.com.my/news/more?ncl=dBMTApbQcSQk59MQA48uoFQpHlZHM&authuser=0&ned=en_my

5. Average Bug Bounty Payouts Are Increasing
During the past year, the Bugcrowd bug bounty platform has seen a tremendous growth when it comes bug bounty payouts, but also in terms of the enterprises that signed up for its service.

The company has recently published its annual State of the Bug Bounty report, and according to statistics gathered since the service started back in 2013, the company ran 286 total bug bounty programs, received 54,114 bug submissions, and paid researchers $2,054,721 for 6,803 accepted reports.

Source: https://bugcrowd.com/resources/state-of-bug-bounty-press-release-2016

6. Hackers find a way to send massive messages on Telegram
Security researchers have devised a method to send massive messages on Telegram. The experts have found a flaw that allows them so send messages of any size.

The Iranian researcher Sad Ghaf, who discovered the issue, explained that it is the result of a coding error. The expert also added that over 20 million Iranians use the popular Telegram instant messaging app.

For futher details, go to *http://securityaffairs.co/wordpress/48371/hacking/send-massive-messages-telegram.html*

FYI for Anyone Running Microsoft Products

According to the Traffic Light Protocol (TLP): White, the following are analyses of several Microsoft security bulletins based on information Microsoft provided.

(MS16-063) - Cumulative Security Update for Internet Explorer

Severity: Critical
Primary Attack Vector: Specially crafted web page.

Vulnerability: Multiple, the most severe of which could allow for remote code execution.
Publicly Disclosed: No
Assumptions: No
Recommendations: Patch immediately after appropriate testing
Advisory Candidate: Yes

(MS16-070) - Security Update for Microsoft Office

Severity: Critical
Primary Attack Vector: Specially crafted document.

Vulnerability: Multiple, the most severe of which could allow remote code execution.
Publicly Disclosed: No
Assumptions: No
Recommendations: Patch immediately after appropriate testing
Advisory Candidate: Yes

(MS16-071) - Security Update for Microsoft Windows DNS Server

Severity: Critical
Primary Attack Vector: Specially crafted DNS request.

Vulnerability: Remote code execution.
Publicly Disclosed: No
Assumptions: No
Recommendations: Patch immediately after appropriate testing
Advisory Candidate: Yes

For a complete list, go to http://www.us-cert.gov/tlp/

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	Mark Wich

Whitepaper Discusses Trends for 2016

Tableu.com has posted a whitepaper discussin