The Datagram newsletter

May, 2016 Volume 1, No. 5

From the Chair...

This month, Corey White explained how to detect whether your site is compromised and how compromising software is injected into a system. The detection part was very interesting and not at all trivial. Intrusion occurs directly, through an attack made directly on the server of interest, and indirectly, through some third party with, typically, web ties to the server. This latter approach was taken to breach both Target and Home Depot. White said that after an active penetration is made, the attackers may wait some indefinite time before beginning an active campaign. The wait can be to allow gradual insertion of specially tailored malware on Point of Sale (POS) terminals or for other hacker determined reasons. Well-known program names are used to masquerade objectionable software.

One thing that I found startling is that analysis should begin by looking at successful logins in preference to their unsuccessful brethren. Success is the gateway to penetration.

This month's speaker will address cryptopgraphy. We hear

Continued on page 2

Next meeting:

May 25, 2016

6:00 PM Exec Com Meeting
6:30 - 7:00 PM Networking
7:00 - 8:00 PM Meeting
Dinner: $10 (Pay and RSVP at cssig.eventbrite.com)

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

Presenter: Dr. Alice Silverberg

This Month's Topic

Our May speakers is Dr. Alice Silverberg. Her topic will be "Cryptography: Using Mathematics to Keep a Secret."

People want to store data on the cloud and use the cloud's superior computing power to perform computations on data. What if they don't trust the cloud? Mathematics and crytographers have come together to give surprising solutions to the problem of how to compute on encrypted data.

About the *Speaker*

Alice Silverberg is a Professor of Mathematics and Computer Science at the University of California, Irvine. Her research areas are cryptography and number theory. She received her undergraduate degree summa cum laude from Harvard University, a Masters degree and PhD from Princeton University, and a Master of Advanced Studies degree from the University of Cambridge. Before joining UCI she was a Professor of Mathematics at Ohio State University. Professor Silverberg has been awarded Humboldt, Sloan, IBM, Bunting, and National Science Foundation Fellowships, and she has held visiting positions at industrial labs and international research centers. She consulted for the TV show NUMB3RS, and occa-sionally writes mathematically-inspired Scottish country dances.

Google Releases Security Update

Good news! Google has released a new version of Chrome, V. 50.0.2661.75, to address vulnerabilities for Windows, Mac, and Linux.

To download it, go to http://googlechromereleases.blogspot.com/2016/04/stable-channel-update_13.html

From the Chair, Cont'd.

more and more of Cyber-Attacks: active threats to data and the sometimes successful extraction of data by the attackers. We know it can be done. We know some of the things required to obtain data, and we know some things that can be done to prevent it from being captured. But what we don't often talk about is to how to make the data unreadable; to make data captured useless to the hacker and the hacker's sponsors.

This is the subject of our April presenter, Dr. Alice Silberberg. She will give us a talk on Digital Cryptology, the science of "hiding data." Hiding data doesn't mitigate the threat of loss, and, indeed, once an active attacker is capable of acquiring data, the attacker may also be in a position to do other damage. But cryptology does alter the hacker metric from only acquiring data to acquiring data, cryptographic keys, and the cryptographic algorithm, any one of which may make an attack unproductive.

The issue of hiding data goes back some 4,000 years, somewhat before the digital age, I think. Digital cryptography goes back to about 1977, the NIST publication of DES. An excellent resource on classical encryption is Kahn's *The Codebreakers,* which can be purchased at Amazon and other stores. A very good introduction to digital encryption is the *Handbook of Applied Cryptography* or the less intense *Cryptography: An Introduction.* Download both at cssig. brats.com.

Since cryptographic algorithms are not perfect, this presentation is an excellent time to ask questions on what is good enough, and how nonperfections can be detected; for example, how the DES flaw was detected and are AES and elliptic cryptography, good enough.

On a confusing note, Meetup .com is attempting to extort undeserved dues from us, and as a result, we are actively pursuing rehosting our general registration onto another site. Meetup.com provides a secure location for your individual email addresses. Your addresses are not distributed and so, the SIG has no way of contacting you if Meetup.com terminates our contract. If your concern is continuity of presence and not shielding your email address, email me at slipbits@ yahoo.com. If you do so, I will put your email addresses onto my personal desktop. I use Thunderbird, a Mozilla product, as my emailer. When we re-establish ourselves, your address will be migrated. I am truly sorry for this and any inconvenience.

Art

(reluctant) Chair,
CyberSecurity SIG

SANS Institute Offers Sought-After Course

SANS Institute will hold "SEC 504: Hacker Techniques, Exploits, and Incident Handling" at the Marina del Rey Hotel in Marina del Rey, California June 20-25, 2016.

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques you can directly apply when you get back to work.

Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

The Early bird savings of $400 expires on May 11th. Register today. For details, go https://www.sans.org/community/event/sec504-marina-del-rey-20jun2016-ronald-hamann?utm_medium=Email&utm_source=House+List&utm_campaign=Community&utm_content=MarinaDelReyCA+SEC504

NIST Releases White Paper

NIST announces the final release of a new White Paper titled "Best Practices Guide for Personal Identity Verification (PIV)-enabled Privileged Access." It explains the need for multi-factor PIV-based user authentication. To download, go to http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

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	Christopher Ries Mark Wich
Web Design	Jo3 McCarthy
Audio-Visual	Mark Wich

Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com