



The Datagram

newsletter

February, 2016

Volume 1, No. 2

From the Chair...

We are off to a good start. Our January 27th meeting had an ExCom session followed by a presentation from Mark Wich on CyberThreats on Home Computers (see page 2 for a full report).

ExCom made several decisions. We will accept advertisements for seminars, symposia, workshops, presentations and job listings. The advertisements will be dual posted on our Web Site (cssig.brats.com) to achieve maximum exposure. Until our policy changes, the ads will cost nothing and are renewable every three months. We are particularly eager to get opportunity announcements for our membership. This allows member career growth in the CyberSecurity space.

Our Web Site hosts as many resources as we can find. We just uploaded 15 books that all come from free download sites. The range of issues covered goes from executive (20,000 ft. looking down) to implementer (somewhat below 0 ft. trying to get up). You are welcome to them and you don't have to say "thanks."

Mark's presentation was a gentle introduction to home security—the things that get you into trouble and why. The content was for a general audience, not specifically software-oriented, and presented a means to work and play safely on the Net. Popcorn was not served, but dinner was. Those present were able to listen, enjoy, comment and eat.

Continued on page 2

Next meeting:

February 24, 2016

6:00 PM Exec Com Meeting
6:30 - 7:00 PM Networking
7:00 - 8:00 PM Meeting
Dinner: \$5

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

Presenter: Dr. Ron Pike

President Launches National CyberSecurity Plan

President Obama has announced a new national Cybersecurity National Action Plan (CNAP) to help Americans safeguard their identities online. He has earmarked \$19 billion for this program, a 35% increase over the cybersecurity budget from last year. Three billion of that will go to upgrading the government's outdated computer systems.

The plan will also:

- bring top strategic, business, and technology thinkers together to make recommendations
- transform how the government will manage cybersecurity
- empower Americans to secure their online accounts by using additional security tools like multi-factor authentication.

Source: <https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know>

A b o u t t h e

Speaker

Ron Pike, Ph.D., is an assistant professor in the Department of Computer Information Systems at Cal Poly, Pomona. He co-leads the Center for Information Assurance (<http://www.thecenteratcpp.com/>), which is the focal point for Information Assurance and Cyber Defense Activities at Cal Poly. His work focuses on networking and network security.

From 1990 - 2012, Dr. Pike was a lecturer in the Department of Management Information at California State University, Chico. His business experience includes being a project manager at Apple Computer, McClellan Air Force Base, and Hughes Aircraft Company and assistant project manager at TransAmerica.

Dr. Pike holds a B.S. and M.B.A from California State University, Chico, and a Ph.D. from Washington State University, Pullman.

For more information about Dr. Pike, go to his website at <http://www.dr-pike.com/>.

Speakers Requested

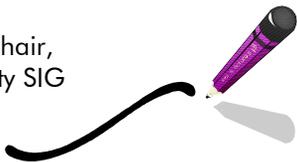
If you know of an expert in cybersecurity who is willing to speak to our CyberSecurity SIG, please contact our program chair, Angela Young, at angela.y@email.com.

From the Chair, Cont'd.

We now have an additional sponsor, Cylance. Chris, our Outreach Chair, was able to secure funding for the CyberSecurity SIG. We are grateful and relieved.

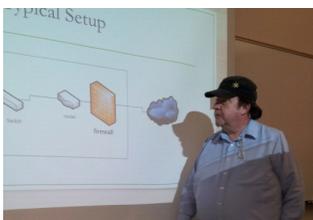
Art

(reluctant) Chair,
CyberSecurity SIG



January Meeting Report

by Carol J. Amato



On January 27, 2016, the IEEE CyberSecurity SIG held its first general meeting in Tustin, California. Mark Wich, a senior-level systems/software engineer with more than 30 years of experience in systems and network engineering and member of the SIG, presented "Protecting Your Home Environment from Hackers and Identity Thieves." His talk covered several areas: wi-fi, anti-viruses, operating system security, email, web surfing, cookies, and password security. Here are the highlights.

Wi-Fi

Wich advised changing the default wi-fi router SSID and passwords and adding MAC filtering, which lets specific devices only talk to your home network. Since the latter is difficult to set up, contact your provider for instructions.

Anti-virus Protection

Wich emphasized installing only one virus protection program. He suggested Avast, which is free, and that you scan weekly.

Operating System Security

Every computer should ask for a password when powered up. Change passwords every so often.

Email Do's and Don'ts

1. Inform your email provider of any phishing scams you receive. Keep your anti-virus program running.
2. Don't open attachments from people you don't know.
3. Don't click on links inside emails even if you think you know where you're going. If it appears like a legitimate link from your bank, for instance, hover your mouse over it to see who the sender is. Banks (and government institutions) do not ask for personal information via email, so if you have any doubt that it could be the bank, click out and go to the bank website via your browser or call their customer service.

Surfing 101

Don't click on ads or any pop-ups. Just displaying them can infect your computer, so Wich advises installing ad-blocking software and webmail ad-blocking software. Make sure your browser's pop-up blocker is enabled.

Beware of any pop-up that says your computer is infected. Don't click on it to make it go away as that will launch the virus. Instead, unplug the computer from the wall right away.

Ransomware is a specific type of virus. When you click on the popup to get rid of it, it immediately hijacks your computer and encrypts your data. You will have to pay a ransom to get your data back. Again, don't click on the popup. Unplug your computer instead.

"Don't let websites, even ones such as Paypal and Amazon, store your personal information, as you are dependent upon their level of security," says Wich. "If you don't give it to them, they can't lose it. And never use your phone for online banking, as it, too, is easily hacked."

He also warned against using cloud services because of the hacking danger.

Cookies

Cookies are bits of data that websites store on your computer. Turn off cookies in your browser.

Password Security

Wich's most detailed suggestions concern instant password security. Here are the steps:

1. Get a notebook.
2. Pick a phrase to use as your password (e.g., tomato4soup).
3. In your notebook, write three things:
 - a. Site name
 - b. Username
 - c. Password nickname (e.g., tword)
4. Repeat Step 3 for all your sites/ usernames/passwords, but use different versions for each one.
 - Here's an example:
 - Citibank - milominderbender, tword4
 - Yahoo - milominder2, Tword7
 - Gmail - milo123, Tword35
5. Take a picture of your notebook on your phone.

These may seem like many tasks to perform, but take Wich's suggestions one-by-one to reduce overwhelm and keep your computer safe from hackers.

Have suggestions for what you would like to see in the newsletter?

Send them to Carol J. Amato at stargazer@stargazerpub.com.



FREE Books on IT Security

Download these FREE .pdf books via your browser from the URLs indicated.

BIOS Disassembly Ninjutsu Uncovered
by Darmawan Salihun
www.e-booksdirectory.com

Identity Management on a Shoestring: Architectural Lessons from a Real-World Implementation
by Ganesh Prasad and Umesh Rajbhandan
www.onlineprogrammingbooks.com

Beginner's Guide to Digital SSL Certificates
by Symantec
https://www.symantec.com/content/en/us/enterprise/white_papers/beginners-guide-to-ssl-certificates_WP.pdf

HackerProof: Your Guide to PC Security
by Matt Smith
www.makeuseof.com/tag/hacker-proof-your-guide-to-pc-security/

Forensic Discovery
by Dan Farmer and Wietse Venema
www.fish2.com/security/wf-book.pdf

Rethinking Public Key Infrastructures and Digital Certificates
by Dr. Stefan Brands
www.credentica.com/the_mit_press_book.html

The Hacker Crackdown
pdf.textfiles.com/books/hackcrac.pdf
Firewalls and Internet Security
by William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin
www.ebookdb.org/item/1515/

Intrusion Detection with SNORT
by Rafeeq Ur Rehman
ptgmedia.pearsoncmg.com/imprint_downloads/.../0131407333.pdf

Security Engineering
by Ross Anderson
<http://www.cl.cam.ac.uk/~rja14/book.html>

Handbook of Applied Cryptography
by Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone
citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838...pdf

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier
by Suelette Dreyfus
pdf.textfiles.com/books/Underground.pdf

Keep Cyber Threats From Destroying Your Clients' Business
by LabTech
<http://www.labtechsoftware.com/Landing/security-eBook-ppc/>

More Cool Links

IEEE Computer Society Technical Committee on Security and Privacy (<http://www.computer.org/web/tandc/tcsp>) and (<http://www.ieee-security.org/index.html>)

<http://www.dhs.gov/topic/cybersecurity>

<http://www.huffingtonpost.com/news/cybersecurity/>

<http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm>

<http://www.microsoft.com/security/cybersecurity/#!Overview>

<https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

<http://www.govinfosecurity.com/cybersecurity-c-223>

http://info.surfwatchlabs.com/cyber-risk-business-resilience?utm_source=bing&utm_medium=cpc&utm_term=keyword&utm_campaign=SWCCS

<http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security.html>

<https://www.silentcircle.com/products-and-solutions/technology/zrpf/>

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

Brown University Offers Master's Degree in Cyber Security

Brown University's Executive Master in Cybersecurity explores the question of what true cybersecurity leadership means. This 16-month program takes a global perspective on this burgeoning field.

The world-class international faculty includes experts from government, academia, and industry who seek to foster executives to develop the ability to devise and execute integrated and comprehensive cybersecurity strategies.

The program covers technologies, social trends, human factors, economic tradeoffs and risk management, policy and privacy, and effective leadership.

Source: <http://www.brown.edu/academics/professional/cybersecurity/>

Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

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 a period of three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at cssig.brats.com for maximum exposure.

Submit your camera-ready, business-card-sized (3.5" x 2") .jpg file to tCarol 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, please submit it to Carol J. Amato, Newsletter Editor, at stargazer@stargazerpub.com.

Oracle Scraps Java Browser Plug-in

During the last week of January of this year, Oracle announced its decision to scrap its Java browser plug-in. A frequent target of hackers, this plug-in will not be a part of the next version of JDK 9, which is expected to ship in September, 2016. The company stated that developers of applications that depend on it need to consider other alternatives.

Source: <http://www.technewsworld.com/perl/section/cyber-security/>

Your ad here

Your ad here