ISSA ROCHESTER CHAPTER

June/July 2013 Newsletter
www.RocISSA.org

Topic: Privacy

Bruce Schneier – Excerpts from *Schneier on Security* Blogs

"*The Eternal Value of Privacy*"

Two proverbs say it best: *Quis custodiet custodes ipsos?* ("Who watches the watchers?") and "Absolute power corrupts absolutely."

Cardinal Richelieu understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged." Watch someone long enough, and you'll find something to arrest -- or just blackmail -- with. Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political enemies -- whoever they happen to be at the time.

To read this full essay visit
https://www.schneier.com/essay-114.html

"*Government Secrets and the Need for Whistle-blowers*"

We don't know how big the U.S. surveillance apparatus is today, either in terms of money and people or in terms of how many people are monitored or how much data is collected. Modern technology makes it possible to monitor vastly more people -- yesterday's NSA revelations demonstrate that they could easily surveil everyone -- than could ever be done manually.

Whistle-blowing is the moral response to immoral activity by those in power. What's important here are government programs and methods, not data about individuals. I understand I am asking for people to engage in illegal and dangerous behavior. Do it carefully and do it safely, but -- and I am talking directly to you, person working on one of these secret and probably illegal programs -- do it.

If you see something, say something. There are many people in the U.S. that will appreciate and admire you.

For the rest of us, we can help by protesting this war on whistle-blowers. We need to force our politicians not to punish them -- to investigate the abuses and not the messengers -- and to ensure that those unjustly persecuted can obtain redress.

Our government is putting its own self-interest ahead of the interests of the country. That needs to change.

To read this full essay visit
http://www.schneier.com/blog/archives/2013/06/government_secr.html

“*NSA Secrecy and Personal Privacy*”

There are a lot of articles about Edward Snowden cooperating with the Chinese government. I have no idea if this is true -- Snowden denies it -- or if it's part of an American smear campaign designed to change the debate from the NSA surveillance programs to the whistleblower's actions. (It worked against Assange.) In anticipation of the inevitable questions, I want to change a previous assessment statement: I consider Snowden a hero for whistleblowing on the existence and details of the NSA surveillance programs, but not for revealing specific operational secrets to the Chinese government. Charles Pierce wishes Snowden would stop talking. I agree; the more this story is about him the less it is about the NSA. Stop giving interviews and let the documents do the talking.

To read this full essay visit https://www.schneier.com/blog/archives/2013/nsa_secrecy_and.html

A Government Perspective:
Department of Homeland Security

From the website at
http://www.dhs.gov/cybersecurity-and-privacy

Cybersecurity and Privacy

The Department of Homeland Security (DHS) integrates privacy protections into our cybersecurity operations through the DHS Privacy Office and the Component privacy offices. The National Protection and Programs Directorate (NPPD) manages our risk-reduction mission, which includes the protection of physical and cyber infrastructure.

This factsheet summarizes the nexus between privacy and cybersecurity at DHS. (*PDF, 2 pages - 119 KB)*

In 2008, DHS issued a policy declaring the eight Fair Information Practice Principles (FIPPs) (*PDF, 4 pages - 101 KB*) as the foundation and guiding principles of the Department’s privacy program:

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

The FIPPs were formed from the foundations of the Privacy Act of 1974, and memorialized in the National Strategy for Trusted Identities in Cyberspace. On February 12, 2013, the President signed an Executive Order on Improving Critical Infrastructure Cybersecurity (Executive Order) (learn more about the White House’s ongoing cybersecurity policies). Section 5 of the Executive Order directs the DHS Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties to issue an annual report using the FIPPs to assess the Department’s cyber operations under the Executive Order. As Deputy Attorney General James M. Cole explained during the public presentation of the Executive Order, the FIPPs are “time-tested and universally recognized principles that form the basis of the Privacy Act of 1974 and dozens of other federal privacy and information protection statutes.”

The Executive Order also directs the senior agency privacy and civil liberties officials of other agencies engaged in activities under the order to conduct their own assessments for inclusion in the DHS public report. In 2010, DHS issued a White Paper on Computer Network Security & Privacy Protection (*PDF, 11 pages - 114 KB*) to provide an overview of the Department's cybersecurity responsibilities, the role of the EINSTEIN system in implementing those responsibilities, and the integrated privacy protections.

In case you missed it…

Review of
June Chapter Meeting
Larry Kovnat, speaker

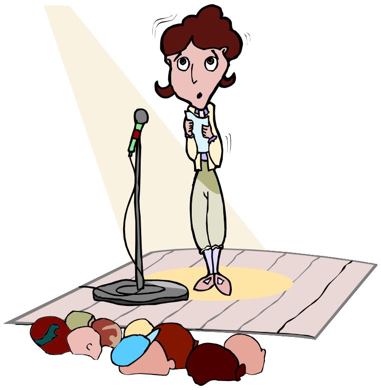
On June 20th at 5:30 PM, the Rochester ISSA held its quarterly chapter meeting at Nixon Peabody with light refreshments being served. After calling the meeting to order, Larry Kovnat, formerly a Senior Product Security Manager at Xerox, spoke about embedded systems security and his efforts to build security into the embedded controllers of advanced hardcopy multifunction devices.

Larry's presentation highlighted the fact that while management and developers are quick to grasp the advantages of embedded control and connectivity, they often underestimate the vulnerabilities that are unintentionally introduced during the development process. As a result, Larry and his team focused on educating both management and developers on the use of a security development lifecycle (SDLC). By linking security to quality, they were able to build trust within the organization by showing how such an approach results in a better product with lower acquisition costs.

The discussion afterwards was lively, with questions ranging from how to develop security metrics to growing a security practice within organizations to "cultural engineering". A special shout-out to Matthew A. Arian who drove 4.5 hours from Ohio to hear Larry speak.

Interested in Membership?
Visit www.RocISSA.org for more information.

Call for Speakers – Continues!!!



We've received a number of presentations to date. Topics cover 'mobile', 'cloud', 'security awareness', 'static code analysis', 'encryption', and 'ethical hacking'. There are still openings for all speaker tracks.

Guidelines for speaker presentations are posted to our webpage at www.rochestersecurity.org under the 'Speakers' menu.

Proposals may be submitted to
present2013@rochestersecurity.org

If you believe you have a significant research or technical presentation that the security community would value and enjoy hearing, we invite you to submit your presentation topic for consideration.

All four tracks will consist of presentations in 50-minute blocks, including Q&A. Presentations may be allowed to span two blocks to accommodate topic exploration to different depths if the committee sees the merit in the longer time allotment.

Open Invitations: Track openings are still available, additional presentations may be submitted. *These presentations may be on any topic of interest to the security community.*

- Submit proposals by August 16
- Acceptances sent by Aug 30
- Draft copy of the slides due Sept 6
- Final Abstracts are due Sept 13
- Final submissions are due Sept 27

Continuing Education Units (CEU)

There are many opportunities to get CEU for security certifications like CISSP or CISA.

- Attend an ISSA chapter meeting
- Speak at RSS or chapter meeting
- Volunteer for a committee
- Write a journal article

Rochester Security Summit 2013

Tuesday and Wednesday, October 22 - 23
www.rochestersecurity.org

Hyatt Regency
www.rochester.hyatt.com

Register now for Two Day Super Saver
$125 until July 30

Enter and win!
iPad or Android Tablet

2013 Rochester Security Summit Sponsors

Diamond

paloalto NETWORKS
the network security company™

Platinum

Carousel INDUSTRIES®

Juniper® NETWORKS

Silver

IMPERVA®
Protecting the Data That Drives Business®

Bronze

SMP

fishnet™ SECURITY

Trust earned. FreedMaxick CPAs, P.C.

Guidance® SOFTWARE

Thank You to our 2013 Rochester Security Summit In-Kind Sponsors

DCI
Durkee Consulting, Inc

IANS

2013 Rochester Chapter Officers

President – Ralph Durkee
Vice President – Rich Savacool
Secretary – Jackie Stewart
Communication Officer – Holly Turner
Treasurer – Phil LaGraff
Membership Director – Joel Cort
Web Administrator – Susan Casserino
Accountant – Jim Pierce

About our Chapter

The Information Systems Security Association (ISSA) is a not for profit business association comprised of information security professionals and practitioners. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government. The Rochester Chapter was the 101st official chapter of the International Information Systems Security Association.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

In 2006 Rochester ISSA members hosted the first annual Rochester Security Summit. The Summit is a community focal point for education and awareness in collaboration with higher education and business and industry partners, held during National Cyber Security Awareness Month. Speakers and panels provide education opportunities for executives, CFOs, CIOs/CSOs, business managers, IT managers, security professionals, technical specialists and developers.

Links:

www.issa.org

https://www.owasp.org/index.php/Rochester

http://www.rit.edu/programs/information-security-and-forensics
https://www.facebook.com/RITInfosec

http://www.isacawny.org/

http://www.infragard.net/chapters/rochester/index.php

ISC2 Central NY Chapter – Utica, NY
https://www.isc2.org/

http://digitalrochester.com/