Monthly ECC Information Security Briefing
January 30, 2018

ECC Internal News

Where does the intelligence information come from that I rely on to make info security decisions? Since this question has been asked so many times, I thought I would give you a glimpse inside my toolbox! (Note: This is not an exhaustive list.)

- Online/print trade journals:
  - We Live Security
  - Dark Reading Room
  - Information Security Buzz
  - SC Magazine
  - Tech Republic Security

- Membership organizations (some requiring background checks/clearance credentials):
  - FBI Infragard
  - Information Systems Security Assoc.
  - Information Systems Audit and Control Association
  - CIA Spy Briefing (Jason Hanson)
  - Special Operations Forces Report (SOFREP)

- Cybersecurity intelligence feeds:
  - FBI/DHS Alerts
  - DISA (Defense Intelligence Security Agency) Alerts
  - NIST Computer Security Division
  - CCC Tech/Security Center
  - ThreatConnect Threat Intelligence Feed
• FireEye Cyber Threat Map
• AlienVault OTX (Open Threat Exchange)
• Forcepoint ThreatSeeker Intelligence Feed
• Fellow ITS employees
• Radio/TV news stories

External News

URGENT - Meltdown & Spectre CPU Vulnerability
• Who’s affected? Mac’s, PC’s, iOS devices, cloud-computing platforms
• https://meltdownattack.com/

Surprise: Android apps are riddled with trackers
• In case you’re wondering, yes, there’s a good chance at least some of your Android apps have tracked you more than you expect. That’s the conclusion of a joint project between Yale University’s Privacy Lab and French non-profit Exodus Privacy. This month they’ve documented snoopware features in apps from Uber, Tinder, Skype, Twitter, Spotify, and Snapchat, the university said. The 25 trackers were discovered by scanning Google Play apps looking for signatures it developed to identify tracking code. Yale said the trackers are mostly used “for targeted advertising, behavioral analytics, and location tracking”, all of which may be legitimate applications, but often operated without users’ knowledge. Lack of transparency about the collection, transmission, and processing of data via these trackers raises serious privacy concerns and may have grave security implications for mobile software downloaded and actively used by billions of people worldwide. Of 300 apps Exodus has analyzed, Yale says, 75 percent contain trackers. Users might be less pleased that apps are sending their name, phone number, e-mail address, login, IP address and device ID to OutBrain, and other trackers like Ad4Screen. Trackers are pervasive across a huge number of publishers and platforms. Don’t feel...
smug if you're an iPhone user, the Privacy Lab post said the tracker companies advertised iOS versions of their software, but auditing iOS apps is difficult.

- The full Exodus list is here: https://reports.exodus-privacy.eu.org/trackers/

**Data Breach Watch**

**U.S. Higher Education Breaches for November/December 2017:**

- Academy of Art University – San Francisco, CA
- Chapman University – Orange, CA
- Louisiana State University
- Oklahoma State University Center for Health
- Rutgers University
- Stanford University (internal glitch)
- University of Chicago Hospital
- University of Iowa (internal hack)

**Tip of the Month**

**Wireless Keyboards**

- The problem?
  - Most wireless keyboard work on an unencrypted radio frequency
  - There are tools available that can easily intercept these radio signals
  - Radio frequencies are also not traceable – meaning if someone did intercept your keyboard commands, you would never even know it!

- The solution?
  - Wireless Bluetooth-enabled keyboards that use encrypted communications
  - Bluetooth-enabled keyboards can protect anything you type: secure login info, banking info, personal emails, etc.

- Here are 3 Bluetooth keyboards worth looking into:
  - Kanex EasySync iPad Keyboard with Stand Cover
  - Logitech K380 Multidevice Bluetooth Keyboard
  - Apple Magic Keyboard
Cyber Security Trivia:

This month I’m starting a new section called Cyber Security Trivia. Each month I will post a trivia question. Each person emailing me the CORRECT answer will have their name included in a special drawing to take place in December, 2018. The winner will receive a really cool prize swag bag!

- The trivia question for this month is: Who or what was the Bluetooth wireless technology named after?
- Email your answer to pyoder@elcamino.edu

Write in with your IT security questions:

If you have any questions about cyber security, please send them to: pyoder@elcamino.edu

All current and previous issues of the Monthly E.C.C. Information Security Briefing are posted online at:
- http://www.elcamino.edu/about/depts/its/techservices/infosec.aspx

Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District
pyoder@elcamino.edu