Cybersecurity: What You Need to Know and Why
Tufts Faculty Webinar – Unanswered Q&A

Q: Why was the US government late to countering state based cyber threats?

A: (1) There's a lot we don't know, (2) cyber security is generally reactive, (3) skills + talent shortage doesn't help (e.g., "NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization" https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html), (4) government can't compete with industry salary levels

Q: What are your thoughts on AI?

A: Personally speaking: currently, overused buzzword for marketing purposes. AI does not mean comparing two files for differences (and yes, there are security products that dub that method as AI --it's shameful).

Q: A film company was left to its own when attacked by N. Korea, but the US did not respond. How would you recommend we assist our parents with these issues when they were not born with computers in their hands like we did?

A: Keep it simple. I'm also dealing with this, elder care. If your parents need a computer, then locked down environments such as Chromebooks and iPad are very good. They are not perfect but both Chromebooks and iPads have generally very good *usable* security baked in already and they are simpler than full blown PCs https://www.cnet.com/news/how-google-chromebooks-became-the-go-to-laptop-for-security-experts/. Simplicity, not complexity.

Q: With over 10,000 hacks per year I do not hear of any criminal charges. Does our government put any effort into catching the criminals?

A: As I said in my talk loosely speaking, crime does pay (cybercrime). This is from 2008 and still relevant, only grown: "FBI: Cybercrime racks up more profits" https://www.securityfocus.com/brief/716. Remember, that was a time before ransomware too! Attribution is an extremely difficult problem in cyber security. Technologies such as Tor, VPNs are a double-edge sword.

Q: What password manager services can you recommend? Are they (password managers) worth the cost?

A: 1Password and LastPass

Q: Where can we find models of policies to implement in our company?

A: Start with the SANS Institute as I'm an alum there. World class trainings and resources: https://www.sans.org/security-resources/policies. Remember, there is no one-size fit all model.

Q: If you develop within a specific platform, using its own set of API's, how much of the security risks are on you as a developer and how much of the risk is "assumed" by the platform? In my case, it is a popular, cloud-based ERP software system (Oracle).

A: Both. You depending on an API or third-party system => dependency problem. You just don't know how or what is under-the-hood with APIs and third-parties. "Using Components with Known Vulnerabilities" is now in the OWASP Top 10 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. You as developer also have responsibility to deal with user inputs, which are never to be trusted.

Q: Based upon your comments about keeping stuff off the internet - do you NOT use cloud storage or backups... It seems like from Google to Apple, all mobile devices are focusing on using the cloud for backups... Do you think we shouldn't use the cloud for backups?

A: It depends on the stuff. I trust Gmail --Google will do a better job in email *security* (not privacy) than most people and I'm not going to run my own email server. Also, I view email to a postcard. I have a collection of memes and readings (PDFs) on iCloud. I recently turned off iCloud Backup for my phone because backups are not encrypted (see https://fixitalready.eff.org/#/). For virtual machines, I use Dropbox. For source code and projects, I use GitHub. Financial documents, they're not on the cloud.

Q: What is Tufts doing to encourage women to join the field and foster them post-graduation?

A: (1) Tufts was a sponsor of the Day of Security Conference that was held in Boston back on Friday, February 22nd https://www.dayofshecurity.com/, (2) have good role models like Kathleen Fisher, Susan Landau, et al, (3) talks and workshops at hackathons.

Q: How do you recover if a 2FA hardware key is lost or stolen?

A: (1) Have backup codes, (2) have a second hardware key. The latter is a requirement to be a part of Google's Advanced Protection Program https://landing.google.com/advancedprotection/

Q: Do you use social media? why or why not?

A: Yes, Twitter, @0xmchow. The reasons: (1) most of the InfoSec/cyber security community on there, (2) news, (3) everything that you post on Twitter is public record *and* can be searchable via search engine like Google (unlike Facebook). I still use LinkedIn despite thinking of deleting my account because (1) share news, (2) engaging with alumni, and (3) verification purposes -- that is, to help prevent impersonation (see https://www.schneier.com/blog/archives/2017/08/more_on_my_link.html).

Contact Information

Ming Chow

Twitter: @0xmchow

GitHub: https://github.com/mchow01
Website: http://www.cs.tufts.edu/~mchow/
LinkedIn: http://www.linkedin.com/in/mchow01