

Lessons Not Learned in the Last Ten Years

Ming Chow

mchow@cs.tufts.edu

Twitter: @0xmchow

Tactical Edge Virtual Summit 2021

June 23, 2021

The Significance of This Presentation

- Tenth anniversary of my Introduction to Security course at Tufts
- Tenth anniversary of my first talk at DEF CON and a few other big conference talks
- One can see many patterns in ten years time

Motivation

- A list of bright shiny objects seen in security products and startups (or buzzword hell)
 - APTs
 - Machine Learning
 - Comprehensive cybersecurity
 - Real-time monitoring
 - Behavioral analysis
 - Next-gen <FILL IN THE BLANKS> (thanks Russell Butturini)
 - Xgen
 - Cloud-enabled


Motivation (continued)


- ͇͇(ツ)͇͇
 - ["Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes"](#)
 - ["Here are the 61 passwords that powered the Mirai IoT botnet"](#)
 - ["One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids"](#)
 - ["Yahoo Says Hackers Stole Data on 500 Million Users in 2014"](#)

Motivation (continued)


Source:

<https://twitter.com/jeremiahg/status/866783974311444480>




Jeremiah Grossman  @jeremiahg

\$81,000,000,000 later: "survey found 35% of companies suffered 2 or more breaches in the last 12mo. 3 in 5 expect to be breached in 2017..."

Help Net Security  @helpnetsecurity · May 18, 2017
3 in 5 companies expect to be breached in 2017 - bit.ly/2rhuwLD

71% aren't sure how to manage and protect unstructured data




6:32 PM · May 22, 2017 · TweetDeck

7 Retweets 3 Quote Tweets 9 Likes

The Gist

- Those motivating slides were from a presentation I gave in 2017
- I could give the same exact talk from 2017 now, without any changes, and get away with it
- In 2013, Veracode gave a presentation “We See the Future and it’s Not Pretty”. The predictions were accurate.
- While a lot of things have changed, a lot have stayed the same...



Key Findings:

- 70% of applications failed to comply with enterprise security policies on first submission.
- SQL injection prevalence has plateaued, affecting approximately 32% of web applications.
- Eradicating SQL injection in web applications remains a challenge as organizations make tradeoffs around what to remediate first.
- Cryptographic issues affect a sizeable portion of Android (64%) and iOS (58%) applications.

Predictions:

- Average CISO Tenure Continues to Decline.
- The Rise of the Everyday Hacker
- Decreased Job Satisfaction/ Higher Turn-over for Security Professionals.
- Default Encryption, Not “Opt-in,” Will Become the Norm.

Let's Start With Education...

- Colleges and universities now offering Cyber Security programs
- Plethora of free Cyber Security programs offered online

...however (with regards to education)

- The Cyber Security programs offered at colleges and universities are mostly graduate-level programs
- By end of undergraduate computing science or engineering program, most graduating still have no knowledge of Security
- Most students don't know about the opportunities online to learn
- Few K-12 opportunities or requirements

Application Architecture

- Boils down to one word: cloud (a.k.a., someone else's computer)

...however (with regards to application architecture)

- Same mistakes from decades ago still being made
 - Open FTP servers => open AWS S3 buckets, open ElasticSearch instances
 - Open [insert favorite service here]

Data Privacy

- Alphabet soup of U.S. data privacy laws, federal and state level
- At the international level, there is now the General Data Protection Regulation (GDPR)

...however (with regards to data privacy)

- But what's the point when companies and institutions collect so much data --and then they all get broken into? (too many companies and institutions to name)
- Plethora of vulnerable voter databases via SQL injection
- Open databases and buckets there for the taking (see previous slide on application architecture)
- Leaky application programming interfaces (APIs)
- Data sold on forums for cheap

Are We Still Facing These Problems?

- Phishing and social engineering
- Password reuse
- Weak passwords
- Distributed Denial of Service (DDoS)

Geopolitical Changes

- Full-blown international crisis
- Infrastructure now being attacked: hospitals, schools, utilities
- Almost impossible to read an article about an incident without a country being named

Options We Now Have

1. (really easy) no changes, business as usual
2. (really hard and really expensive) draconian changes including requiring Cyber Security education at K-12 level
 - a. Example: Cybersecurity Maturity Model Certification (CMMC)

Solutions

- Immediate: password managers, multi-factor authentication, input sanitization
- Intermediate term: “Don’t call it a comeback” --invest in old-school, no/non-tech, and radical (thanks Matt)
 - Example: the U.S. Navy is resurrecting celestial navigation
- Long term: invest in Cyber Security education early
- Continuing:
 - Connecting and communicating with non-technical folks and the policymakers (policy)
 - Simplicity
- Last resort: the heavy hand of legislation

But For Now and For the Future

- Crime will continue to pay --and pay well
- We will still be talking about a Cyber Security skills shortage
 - I've been monitoring how long we've been playing this game for <https://gist.github.com/mchow01/9569350f3b975ce84dad68f0d95c4579>
- There will be another Executive Order on Improving the Nation's (United States) Cybersecurity
- In five years, someone will still be giving a presentation on what SQL injection is, what DDoS is
- In five years, I can give this presentation again without any changes, and get away with it

References

1. https://comp116.org/readings/predicting_the_future_veracode.pdf
2. <https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html>
3. <https://threatpost.com/sql-injection-attack-is-tied-to-election-commission-breach/122571/>
4. <https://abc7chicago.com/politics/how-the-russians-penetrated-illinois-election-computers/3778816/>
5. <https://www.popularmechanics.com/military/research/a36078957/celestial-navigation/>