The Blame Starts with Computer Science Curricula

BeaCon 2015
Ming Chow (@0xmchow)
Roy Wattanasin (@wr0)

Why Are We Here?

- We are both in the higher education business and we have a close relationship with the Security community
- From what we have seen, there is a lot not to like; some things are not working out
- Lots of gap between the academia world and the professional world. It has been that way for a long time but it is particularly bad in Security
- This is a conversation to "clear-the-air" and your comments are invaluable
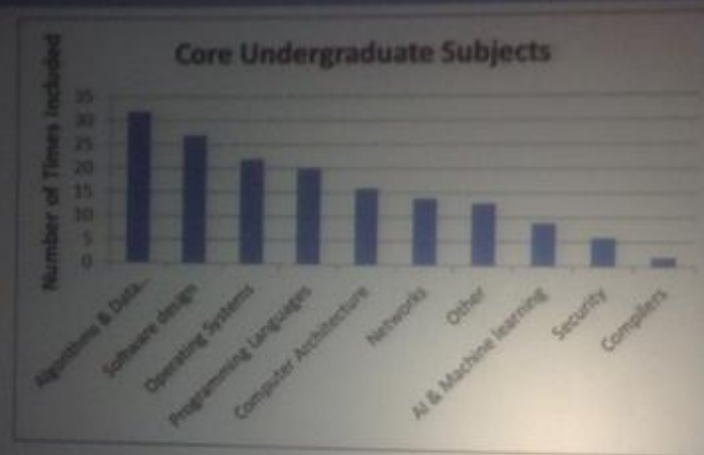
- From: "How to Prevent Security Afterthought Syndrome" by Sarah Zatko at HOPEX 2014
  https://www.youtube.com/watch?v=iLiQqii0c9E
- @sambowne: Security's importance as rated by CS Dept. Chairs #HOPEX

Wesley McGrew
@McGrewSecurity
Follow

Dunno how to teach someone all the fundamentals needed to be a good hacker other than putting them through a 4 year CS program or equivalent

RETWEETS
9

FAVORITES
10

7:21 AM - 3 Apr 2015

Tottenkoph
@tottenkoph
Follow

@McGrewSecurity I can see how a CS degree can be a good foundation, but there are some big gaps in trad CS progs if you want to be a hacker

RETWEET
1

FAVORITES
4

8:06 AM - 3 Apr 2015

InfoSec Taylor Swift
@SwiftOnSecurity
Follow

IMPORTANT: Multiple people who are graduating college have asked how they can get into InfoSec. What is your advice for people with degrees?

RETWEETS
25

FAVORITES
61

4:24 PM - 26 Apr 2015

Tottenkoph
@tottenkoph
Follow

@jth @McGrewSecurity I was surprised a group of freshmen of CS students hadn't even thought of sec as something to "get into" (job/hobby)

8:28 AM - 3 Apr 2015

What We Are Facing

- Perhaps that's why we are still battling the same major security issues known for over a decade.
- Perhaps that's why there is a skills gap in information security.

So Where Do People Learn Security?

- *"Criminal hackers don't go to college to learn it. The good guys need to learn it too." --Sam Bowne*
- *"The bad guys and girls share information so readily and we as the good guys need to share information as well."*

A CS Curriculum's Responsibility and Obligation

- Most Computer Science curricula go through national accreditation (e.g., Accreditation Board for Engineering and Technology)
- Why is accreditation important? To assess the quality of curriculum; to ensure curriculum has basic foundations according to specific accreditation.
- One of the important outcomes of a Computer Science curriculum via ABET: **"An understanding of professional, ethical, legal, security and social issues and responsibilities"**

For Your Eyes Only

From 11/6/2011 during evaluation of Tufts' Computer Science curriculum, preliminary findings of the ABET evaluator: *"There are several gaps in coverage that I have already pointed out to you and are obvious to anyone looking at a map of our coverage: > e. An understanding of professional, ethical, legal, security and social issues and responsibilities --We have part of this with EM54 (an Ethics course), but there is little or no coverage of legal and security issues in the required curriculum."*

Not So Feasible Ideas

- Require all students to take a course on Security; not everyone would want to take the course
- Can't over-prescribe requirements to students

The Need

- Make students think #whatcouldpossiblygowrong; violate invariants, preconditions
- "Thinking like an attacker" is hard, a very different way of thinking and mindset
- Encourage students to think about security at the beginning of any project/assignment rather than being bolted on at the end
- Hands-on practice is required
- Inform them of opportunities in Security

Example 1: Data Structures

- The second course in most Computer Science curricula
- Discussion: the hash function for hash tables: collisions are bad but will be inevitable for simple hash functions. In the real world, hash functions are critical for security, use to verify integrity, and collisions are extremely bad (e.g., MD5)

Example 2: Realistic assignments

- Assignments
  - information security policy, risk assessments to determine critical issues, risk management, interviews (to be used right-away)
  - Research paper on security topics that students care about.
- Many Resources: Verizon DBIR, EFF, Conference videos, industry surveys, CIS, HIMSS, AHIMA, NHISAC, FDA, MDISS

Example 3: Web Programming

- The full-stack: HTTP, HTML5, CSS, JavaScript, server-side, data persistence using database(s)
- Build client and server, then break. In fall 2014 and fall 2015, students had to create "Marauder's Map"
- Issues taught: input validation, XSS, injection attacks
- Assignment: Students are paired to perform a security audit another student's client and server.
- Example (from spring 2013): https://tuftsdev.github.io/WebProgramming/assignments/security-gjoseph/report.html

Example 4: Lessons taught in a Healthcare information security course at Brandeis

- HIPAA Security, HIPAA Privacy
- HITECH, PCI, Red Flags Identity Theft
- MA Privacy Law 201 CMR 17 (Your local state laws/regs.)
- Ethics and Privacy
- NIST, ISO standards, HITRUST
- Compliance
- Risk/risk management, vulnerabilities, 0-days, PTES
- Protected Health Information (PHI)
- Personal Identifiable Information (PII)
- Healthcare industry landscape, HIE, EHR/EMR, CSF, VMM
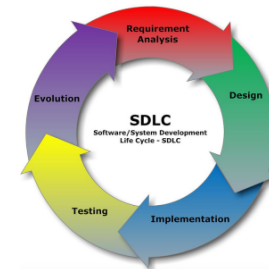
Example 5: Intro to Security at Tufts

- Syllabus runs the broad spectrum: network security, web security, incident handling, privacy, forensics
- Real assignments: analyze packets captured from DefCon, build an intrusion detection system (using Ruby and PacketFu)
- There is a CTF game; students play in teams
- World class guest speakers. Special thanks to Steve Christey Coley, Chris Wysopal, Peter Ballerini and his team at Putnam Investments, Kade Crockford, Gary McGraw, Vik Solem, Silicosis, Josh Abraham for their contributions over the years.

Example 6: Applications of Information Security in Healthcare at Brandeis

- Application security in SDLC
  - o "Before any project not bolted on . . ."
- Testing/monitoring applications
- Evaluate information security tools to help perform tests to protect against threats facing healthcare organizations
- Medical device security / IoT
- Incident handling, preparation and DFIR tools
- OWASP Top 10
- Submission assistance to academic conferences: USENIX

Example 7: Intro to Security at Tufts

- Syllabus runs the broad spectrum: network security, web security, incident handling, privacy, forensics
- Real assignments: analyze packets captured from DefCon, build an intrusion detection system (using Ruby and PacketFu)
- There is a CTF game; students play in teams
- World class guest speakers. Special thanks to Steve Christey Coley, Chris Wysopal, Peter Ballerini and his team at Putnam Investments, Kade Crockford, Gary McGraw, Vik Solem, Silicosis, Josh Abraham for their contributions over the years.

Example 8: Emerging Information Security Issues in Healthcare at Brandeis

- Discussions of current events on a weekly basis
- Implantable Medical Devices
- Portable healthcare records (PHR)
- IoT technologies, mobile devices security/applications
- remote access and third-party risks from vendors
- business associate agreements (BAA)
- Threat vectors/FBI warnings and healthcare breaches
- Resources
  - Conferences, local meetups, webinars, networking opportunities, news and social media

Example 9: Mobile Medical Devices and Apps at Tufts

- Issues taught: security and privacy of medical devices (https://mchow01.github.io/talks/SecurityMedicalDevices.pdf)
- Activities: think of security issues in the design phase
- Project 1: Build a temperature sensing device using an Arduino (hardware); iOS app to display readings
- Project 2: Build a patient monitoring device
- Guest speakers: former President of St. Elizabeth Hospital in Brighton, MA, Chief Medical Information Officer at University of California, San Francisco
- Article about our work: http://now.tufts.edu/articles/engineering-reality

Example 10: Ways to Shine at Brandeis

- Case Studies
- Research Papers on various and interested security topics
- Students review other students' research papers
- Feedback from students throughout semester
- Invited speakers throughout semester using webinars
- Analyze videos
- Opportunities to do additional security research
- Opportunities to present and improve other skills
- Opportunities to help teach future classes
- Opportunities to be mentored

Example 11: Web Engineering

● Issues taught: SQL injection, incident handling

Example 12: Other Additional Skills

- Not just theory
- Thinking "outside the box"
- Communication
- Presentation
- Team
- Volunteering Opportunities
- Free Training
- Defender and Attacker Mindsets

Example 13: Game Development

- Issues taught: cheating in games, virtual economies, and abusing online games (https://tuftsdev.github.io/GameDevelopment/lecture_notes/ethics_security.html)
- Assignment: Read four accepted articles from IEEE Security & Privacy Securing Online Games issue (May/June 2009), answer five questions https://tuftsdev.github.io/GameDevelopment/assignments/a4.html

Example 14: Course Development

- Ways to meet at local meetings and conferences
- Scheduled time to meet online face to face
- Video and audio presentation narrations
- Continuous feedback from students and other faculty throughout semester
- Out of office hours
- Email, online discussions/postings, private messages, Twitter, encrypted emails

Success Stories

Thanks   Academic   x

Mar 9

to Ming

Hey Ming,

Just wanted to reach out an say thank you for your generous guidance and enthusiasm as a professor while I was at Tufts. Barstool Sports (my employer) recently relaunched our entire infrastructure and I was charged with the development of the mobile app and API that powers it.

The lessons learned in your courses were major influences not only in my ability to land the job, but to help build a scalable a reliable product. We just mitigated a XSS attack this morning, and I am confident that without the information I learned in your courses that the exploit would have gone unnoticed.

Thanks again Ming,

Hope all is well!

P.S. Tough year to be Arsenal or United fans. :(
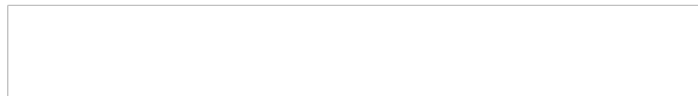
Success Stories (continued)

Still active XSS!
https://www.boston.com/yourtown/news/medford/2009/08/tufts_president_among_those_li.html

Boston Globe Article   Academic   x   ⬆ 🖨 ⬀

| | 5/5/10 ☆ | ↩ | ▼ |

http://www.boston.com/yourtown/news/medford/2009/08/tufts_president_among_those_li.html

So apparently I'm such a leet haxor I can hack sites without even
being aware of it. Comp20 A4 taught me well?

-Mike
(pretty darn baffled - a friend found this for me today)

Success Stories (continued)

Never trusting user input   📁   Academic   x   ⬇ 🖨 ↗

| 👤 | [   ] | Hi Ming, Wanted to let you know that I put my Comp20 knowledge to very good u... | 10:42 AM (5 hours ago) ☆ |

🎱 **Ming Chow**   Ironically, they are some of the worst developers with regards to handling so...   12:17 PM (3 hours ago) ☆

| 👤 | [   ] | d be happy to have the example in the talk, as long as you remove the speci... | 1:35 PM (2 hours ago) ☆ |

| 👤 | [   ] via cs.tufts.edu | | 1:42 PM (2 hours ago) ☆   ↩ ▾ |

to Ming ▾

The following would be good:

Today at my internship, I was looking at some code that sent post requests to the server and realized the input wasn't
sanitized! I showed my supervisor some cross site scripting on his development server and he's now pretty frantically running
around trying to determine the scope of the security holes. Hilarious that a government contractor with a cyber security
department in the same building made a thing so insecure, but at least they've got a Comp20 grad to come to the rescue. I
have a feeling that security might become a focus of my internship. Anyways, just wanted to say thanks for the preparation for
this job, I've been using literally every part of Comp20 every day here and it's been easy so far.

...

Success Stories (continued)

" I had the opportunity to take an Information Assurance Management class taught by Prof. Wattanasin at Brandeis last spring.

I found the course content extremely useful and enjoyed the 10 weeks thoroughly. What made the learning process most effective was Roy's teaching style- He kept his students engaged and probed us all further to think in the right direction and reach the appropriate conclusions.

Due to his vast experience in the healthcare field, I have turned to him for advice time and again. He has always been available to share his expertise and was able to help me make some important career decisions.

I highly recommend Mr. Wattanasin as a professor, coach and mentor. **less** "

Success Stories (continued)

" I had the opportunity to take an Healthcare Information Security class taught by Prof. Wattanasin at Brandeis University last fall.

I found the course content extremely useful and enjoyed the 10 weeks thoroughly. This is an online class however Roy made this class so engaging that I feel that I was in a real classroom. Roy has very special teaching skills that kept his students engaged and probed us all further to think in the right direction and reach the appropriate conclusions. He also designed the program in a very good way : ordered, good coverage from entry level to mid-advanced level, and brought everyone's experience out to benefit with each other.

Due to his vast experience in the healthcare field, I have turned to him for advice. He has always been available to share his expertise and was able to help me make some important career decisions.

I am really happy that I had opportunity to learn and know from Roy. I highly recommend him. **less** "

Success Stories (continued)

" I met Roy a few years ago as a student of his class "Information Security in the Healthcare Industry." The dates that mandated healthcare organizations to commit to the Health Insurance Portability and Accountability Act (HIPAA) compliance requirements were closing in, so this was a class I intended to get a lot out of. Roy did not disappoint me. Roy's knowledge of the industry and its compliance regulations were impressive, but that was second to his patience and willingness to help individual students when they really needed it. I was very happy to have him as a teacher, and you will be happy to have him on your team of instructors. **less** "

So What is a Formal Degree in Computer Science Good For?

- Knowledge of the fundamentals
- Learn how to deal with and manage busywork
- Some introduction to software development
- Making friends, connections

The Bottom Line

- The idea of security is hardly being conveyed in Computer Science curricula
- There is no excuse to not integrate security into Computer Science courses, especially systems and application-based courses
- Learning how to take tests isn't helping

What Do You Think? What's Next?

- *This is an area where we really need help*
- Opportunities
  - Inform students of the security and privacy problems and opportunities; ask students to be good citizens
  - Encourage and challenge students to develop the curiosity and mindset of the attacker and defender
  - Do not use only traditional teaching and learning techniques for courses
  - Provide mentorship and networking opportunities
  - Integration with other organizations

Resources and References

- "How to Prevent Security Afterthought Syndrome" by Sarah Zatko at HOPEX 2014 https://www.youtube.com/watch?v=iLiQqii0c9E
- http://www.irongeek.com/i.php?page=videos/teaching-hacking-at-college-sam-bowne (slides https://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-bowne.pdf)
- http://www.slideshare.net/cchardin/bsides-las-vegas-caroline-d-hardin-on-hacking-education
- https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-jon_kibler-mike_cooper-hack_the_textbook.pdf
- Security Requirements of Biomedical Devices in 2013 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=https%3A%2F%2Fwww.issa.org%2Fresource%2Fresmgr%2F2013_december_web_conference_slides%2F2013_dec_5_web_conference.pptx&ei=V6MHVYe7Mq-PsQS0rYGYAQ&usg=AFQjCNH6hEhEXuU-T9asfmPmD7uGlPxSjw&sig2=S8x1IQ2SEQS8ylwnKLjjRg&bvm=bv.88198703,d.cWc
  - Recording at http://www.issa.org/event/id/374666/login.aspx but needs ISSA login now
- http://www.irongeek.com/i.php?page=videos/bsidesri2013/2-4-feeling-sick-healthcare-information-security-roy-wattanasin
- http://www.boston-spin.org/talks.html#yr2012
- https://twitter.com/tottenkoph/status/584009115887775744
- https://twitter.com/SwiftOnSecurity/status/592469306069266435