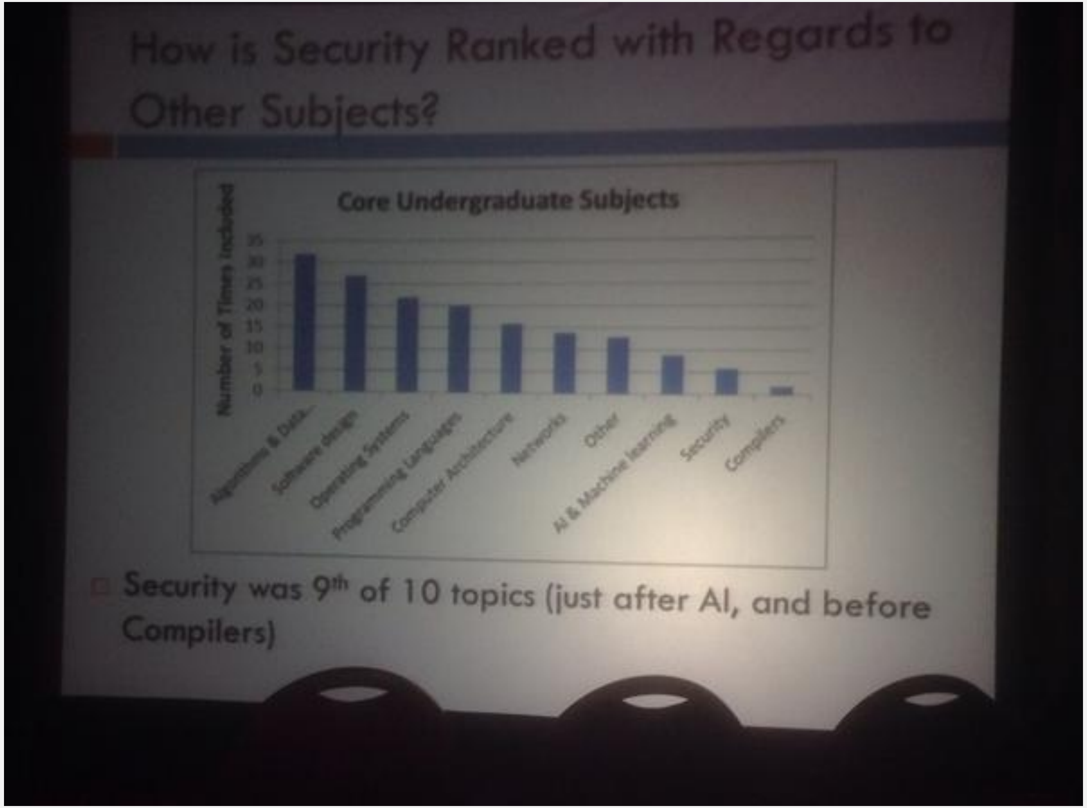
COMPUTER SCIENCE'S CURRICULA FAILURE: WHAT TO DO NOW?

ACSC Cyber Tuesday, November 15, 2016

Ming Chow (Email: mchow@cs.tufts.edu, Twitter: @0xmchow)

SPECIAL ACKNOWLEDGEMENT

- To my friend and colleague Roy Wattanasin whom I've given this talk with this year at a number of venues this year including: New England Security Day Spring 2016, SOURCE Boston 2016, OWASP Boston June 2016, The Eleventh HOPE Conference in New York City in July 2016, BU Security Day 2016, ISSA International 2016 (declined).



How is Security Ranked with Regards to Other Subjects?

- Security was 9th of 10 topics (just after AI, and before Compilers)

The picture that started it all for us: from HOPE X (July 2014): Sarah Zatko’s How to Prevent Security Afterthought Syndrome; image from https://twitter.com/sambowne/status/490316922844872704

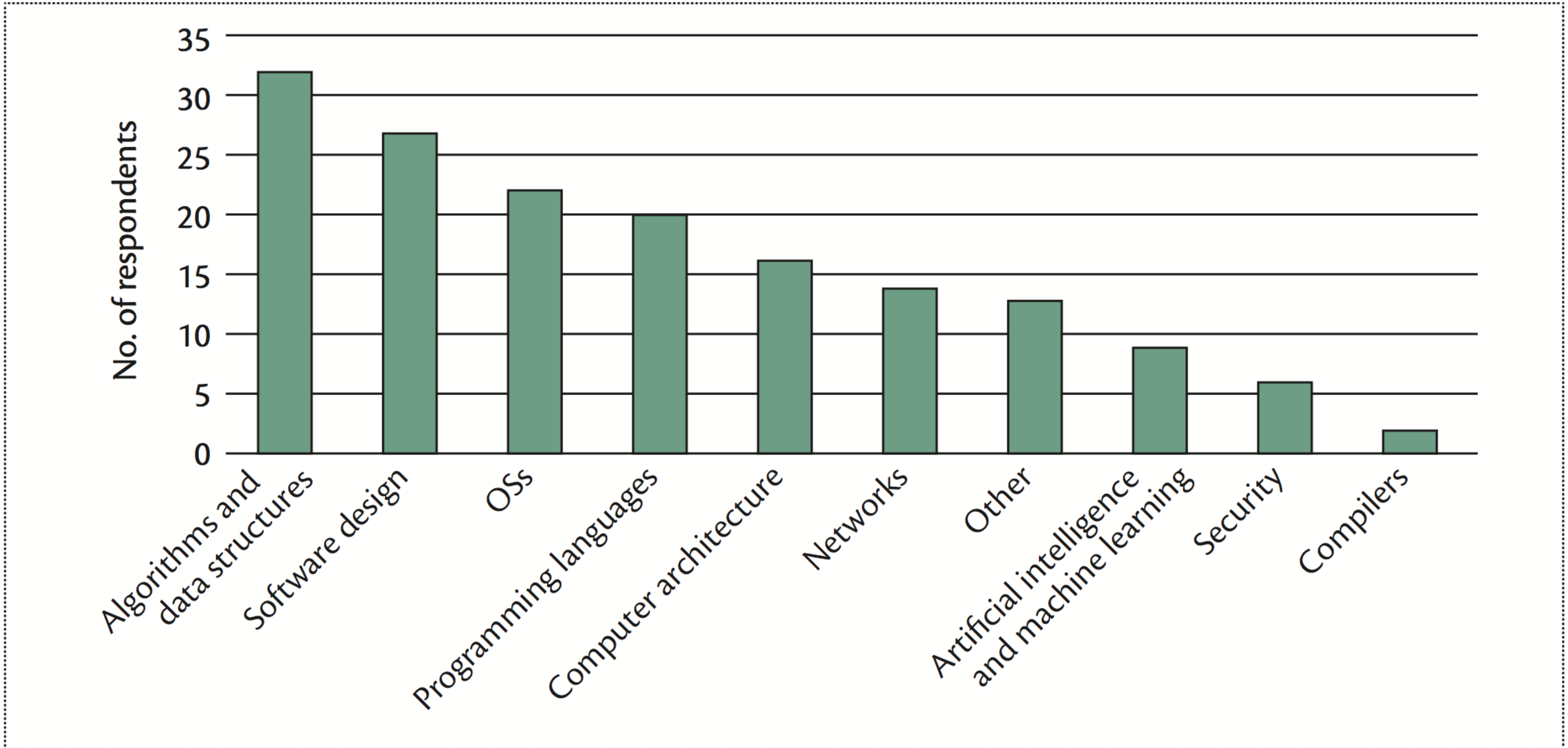


Figure 1. After reviewing a list of 10 computer science subjects, department heads chose which five were most important to include in an undergraduate core curriculum. Only six respondents included security.

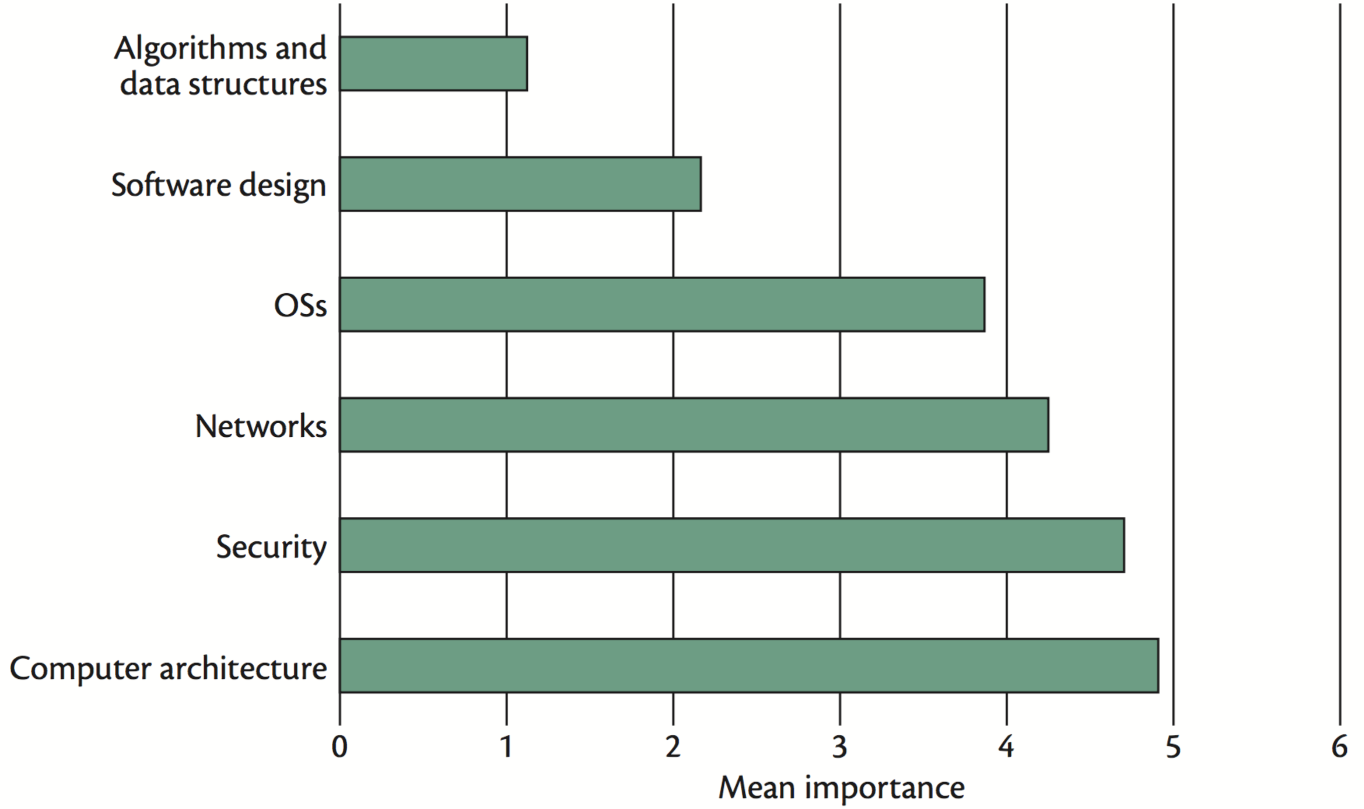


Figure 2. Ranking of the importance of six computer science subjects (1 = most important, and 6 = least important). Security ranked fifth.

CONTINUING SARAH’S TALK

WHAT ARE THE POINTS OF THIS TALK?

1. To understand why cyber security is facing a talent shortage (or why it is difficult to find talent in cyber security)
2. To understand why we are still battling the same vulnerabilities for decades
3. To understand just how big the cyber security education gap is *–or how big is the iceberg (i.e., what else is missing)*
4. To discuss what ***we*** can do to address the problems (***we*** meaning many different contexts)

THE KEY: INTEGRATION INTO (MOST) COMPUTER SCIENCE COURSES

- 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 (sadly, many do not know)

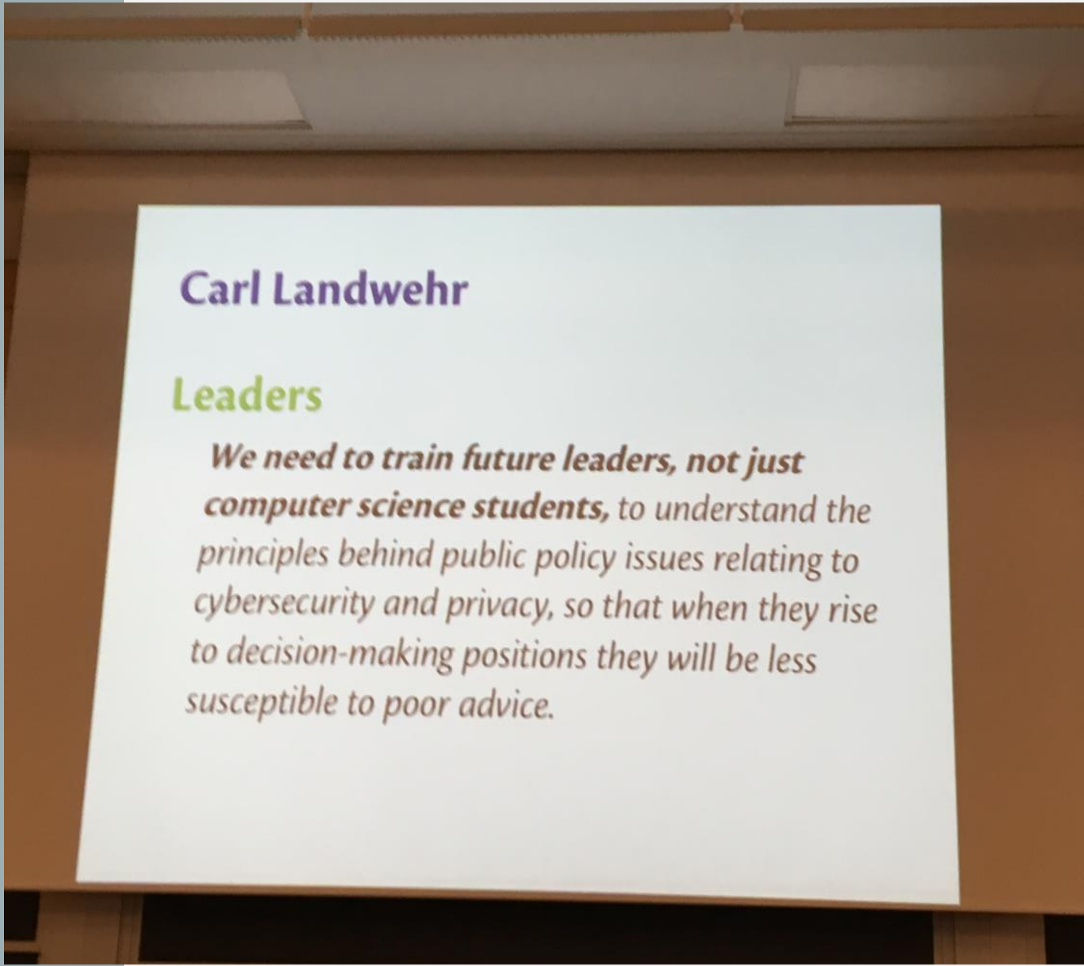
NO EXCUSE

- There is no excuse to not integrate security into Computer Science courses, especially systems and application-based courses.
- 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 an attacker

WOULD BE NICE

- Do not use only traditional teaching and learning techniques for courses. Learning how to take tests isn't helping.
- Provide mentorship, menteeship, and networking opportunities.
- Provide guidelines of lessons learned through presentations like this.
- Work with all and the younger generation through classes, workshops, presentations and conferences.

From New England Security Day Spring 2016, April 28th, Security Education Panel

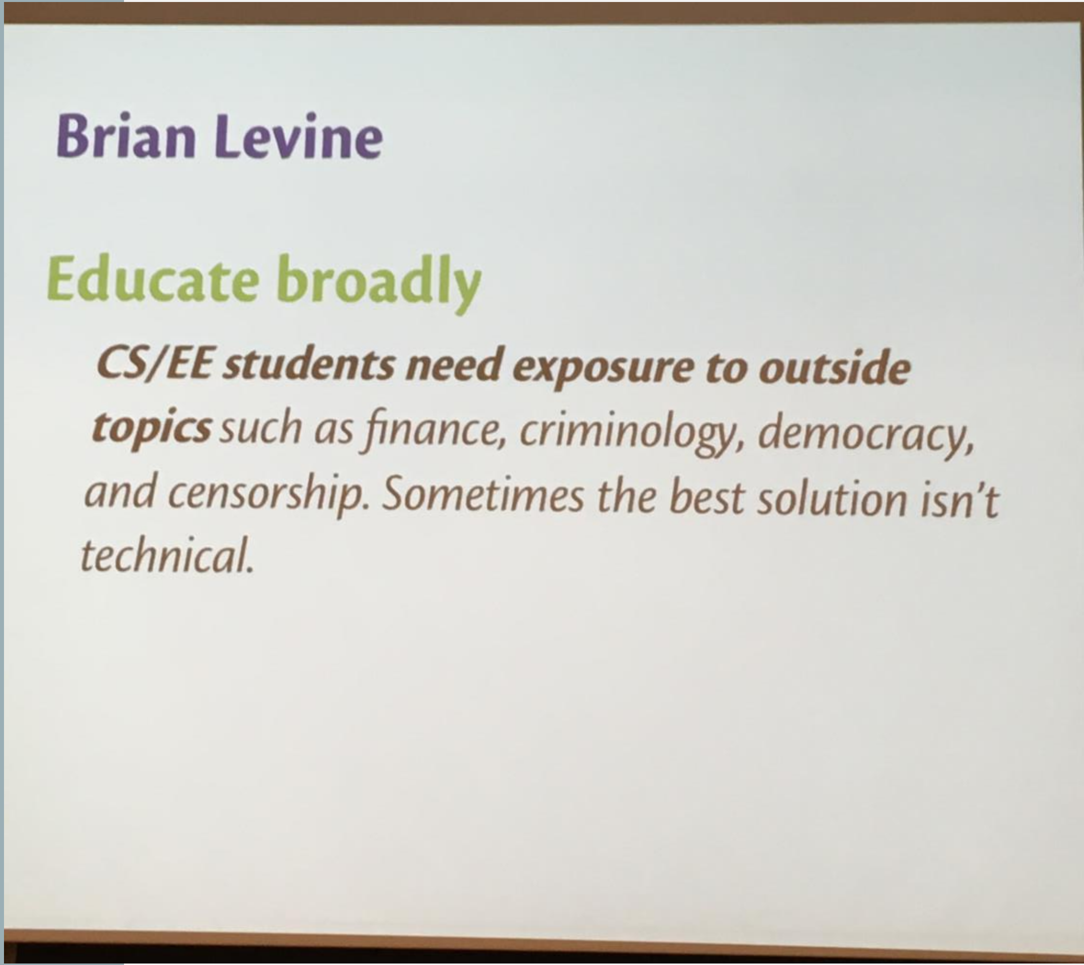


Carl Landwehr

Leaders

We need to train future leaders, not just computer science students, *to understand the principles behind public policy issues relating to cybersecurity and privacy, so that when they rise to decision-making positions they will be less susceptible to poor advice.*

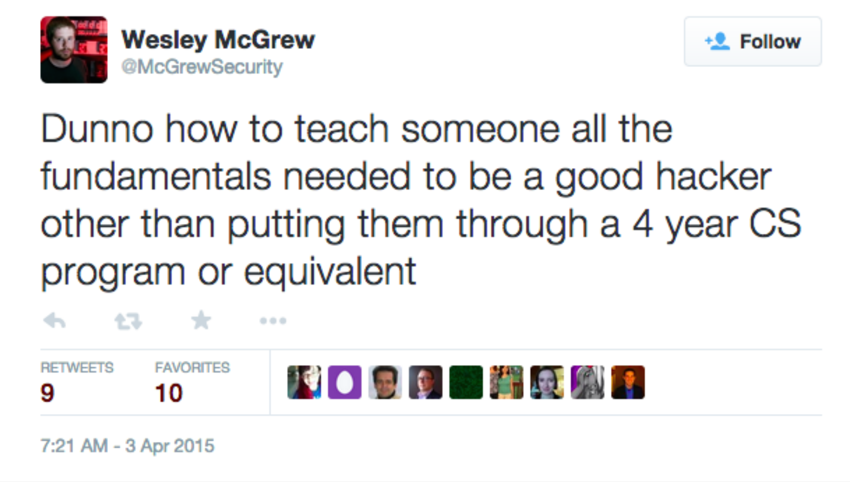
From New England Security Day Spring 2016, April 28th, Security Education Panel



Brian Levine

Educate broadly

CS/EE students need exposure to outside topics *such as finance, criminology, democracy, and censorship. Sometimes the best solution isn't technical.*

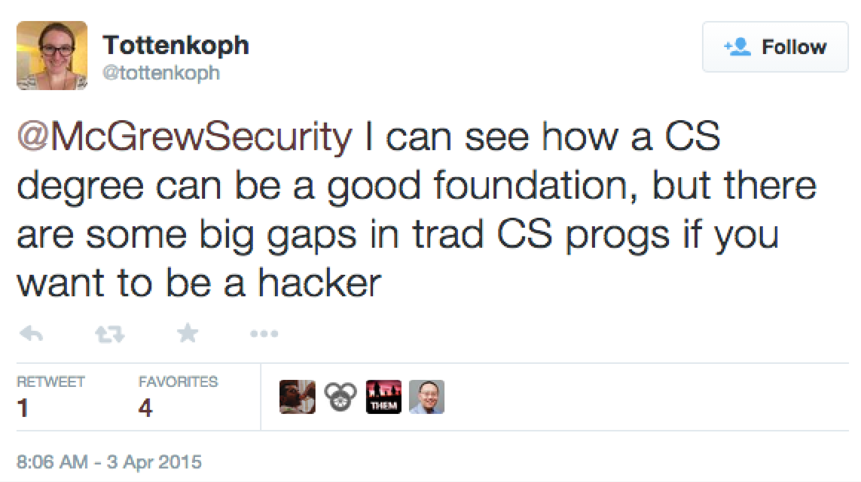


Wesley McGrew
@McGrewSecurity

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

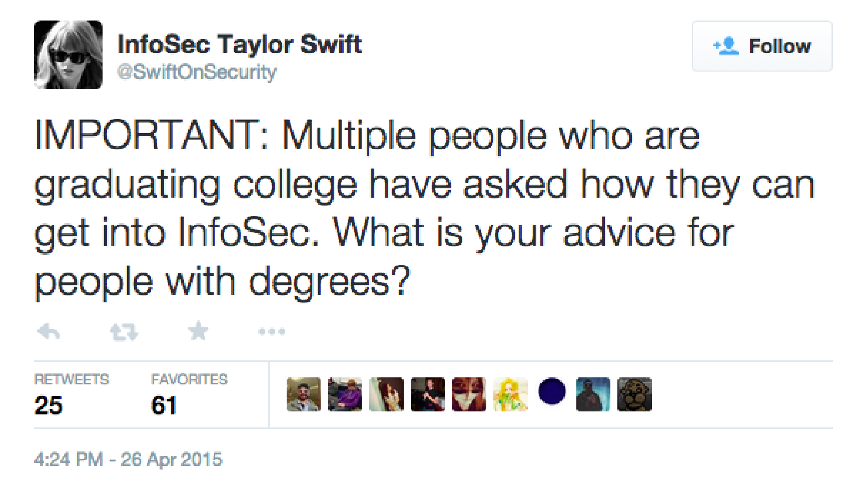


Tottenkoph
@tottenkoph

@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

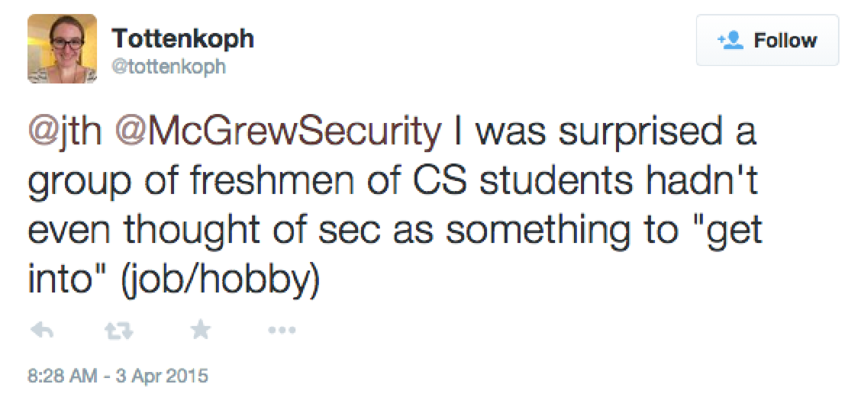


InfoSec Taylor Swift
@SwiftOnSecurity

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

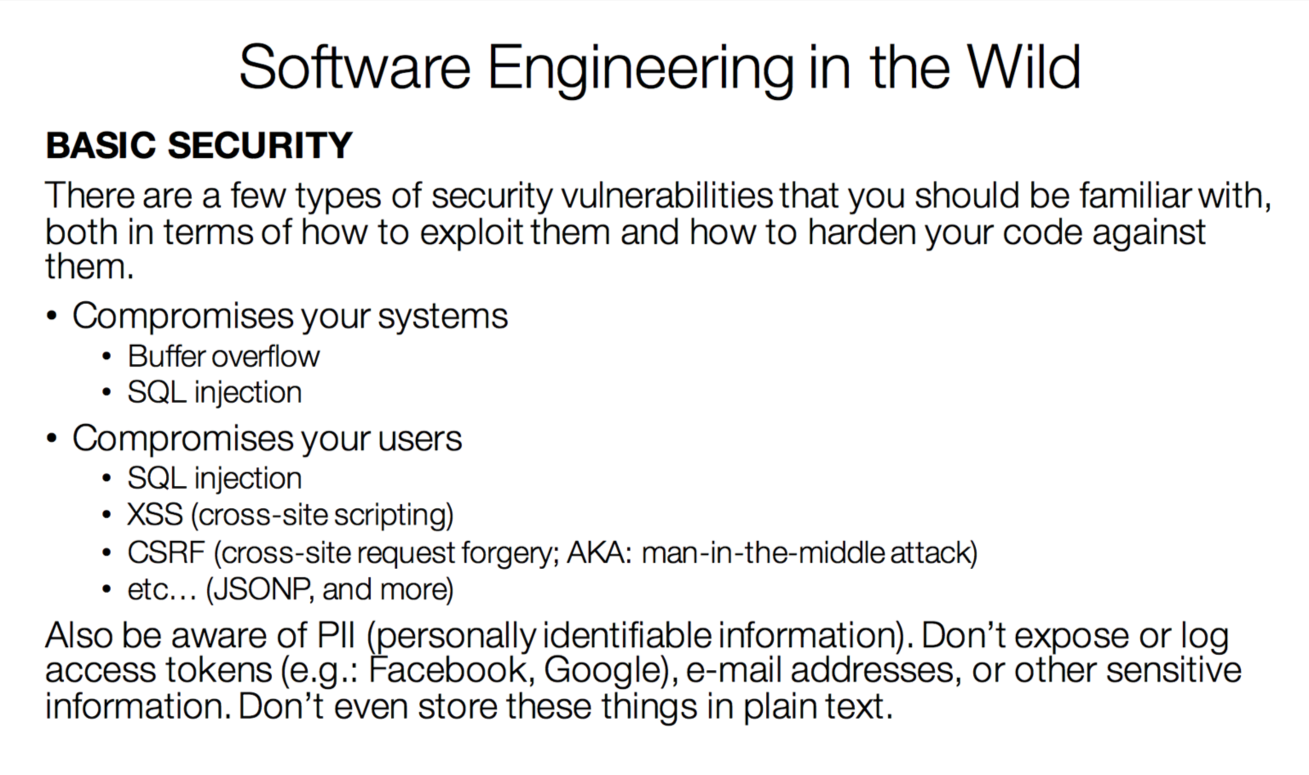
4:24 PM - 26 Apr 2015



Tottenkoph
@tottenkoph

@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



Software Engineering in the Wild

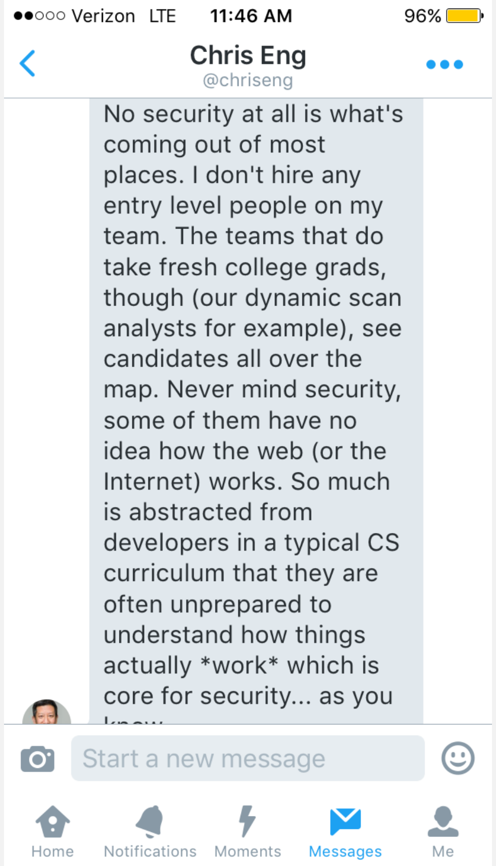
BASIC SECURITY

There are a few types of security vulnerabilities that you should be familiar with, both in terms of how to exploit them and how to harden your code against them.

- Compromises your systems
  - Buffer overflow
  - SQL injection
- Compromises your users
  - SQL injection
  - XSS (cross-site scripting)
  - CSRF (cross-site request forgery; AKA: man-in-the-middle attack)
  - etc… (JSONP, and more)

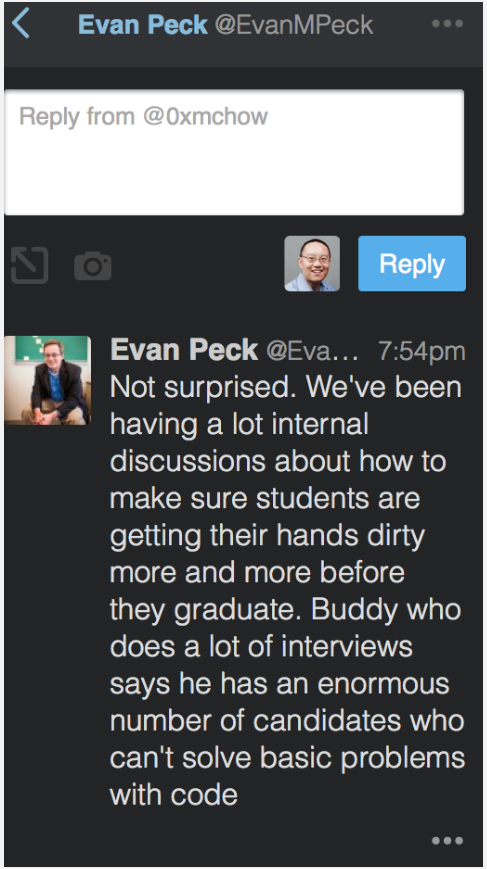
Also be aware of PII (personally identifiable information). Don't expose or log access tokens (e.g.: Facebook, Google), e-mail addresses, or other sensitive information. Don't even store these things in plain text.

From Bill Langenberg, Technical Manager, Software Engineering at TripAdvisor (guest lecture to Web Programming class at Tufts in spring 2016 and in fall 2016)



No security at all is what's coming out of most places. I don't hire any entry level people on my team. The teams that do take fresh college grads, though (our dynamic scan analysts for example), see candidates all over the map. Never mind security, some of them have no idea how the web (or the Internet) works. So much is abstracted from developers in a typical CS curriculum that they are often unprepared to understand how things actually *work* which is core for security... as you know

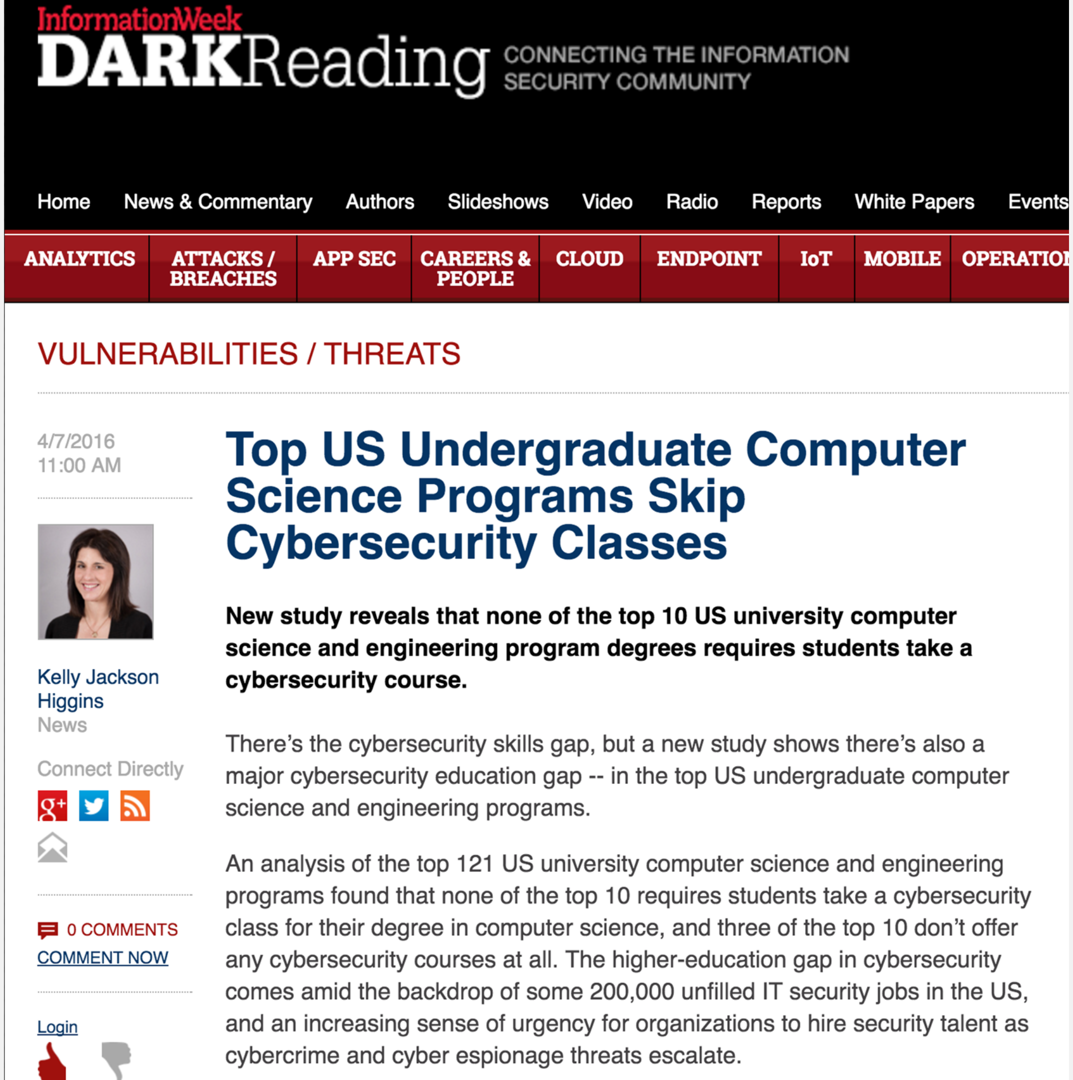
For your eyes only, a private message from Chris Eng, Vice President of Research at Veracode



Evan Peck @Eva… 7:54pm

Not surprised. We've been having a lot internal discussions about how to make sure students are getting their hands dirty more and more before they graduate. Buddy who does a lot of interviews says he has an enormous number of candidates who can't solve basic problems with code

A comment regarding previous image...



VULNERABILITIES / THREATS

4/7/2016
11:00 AM

Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes

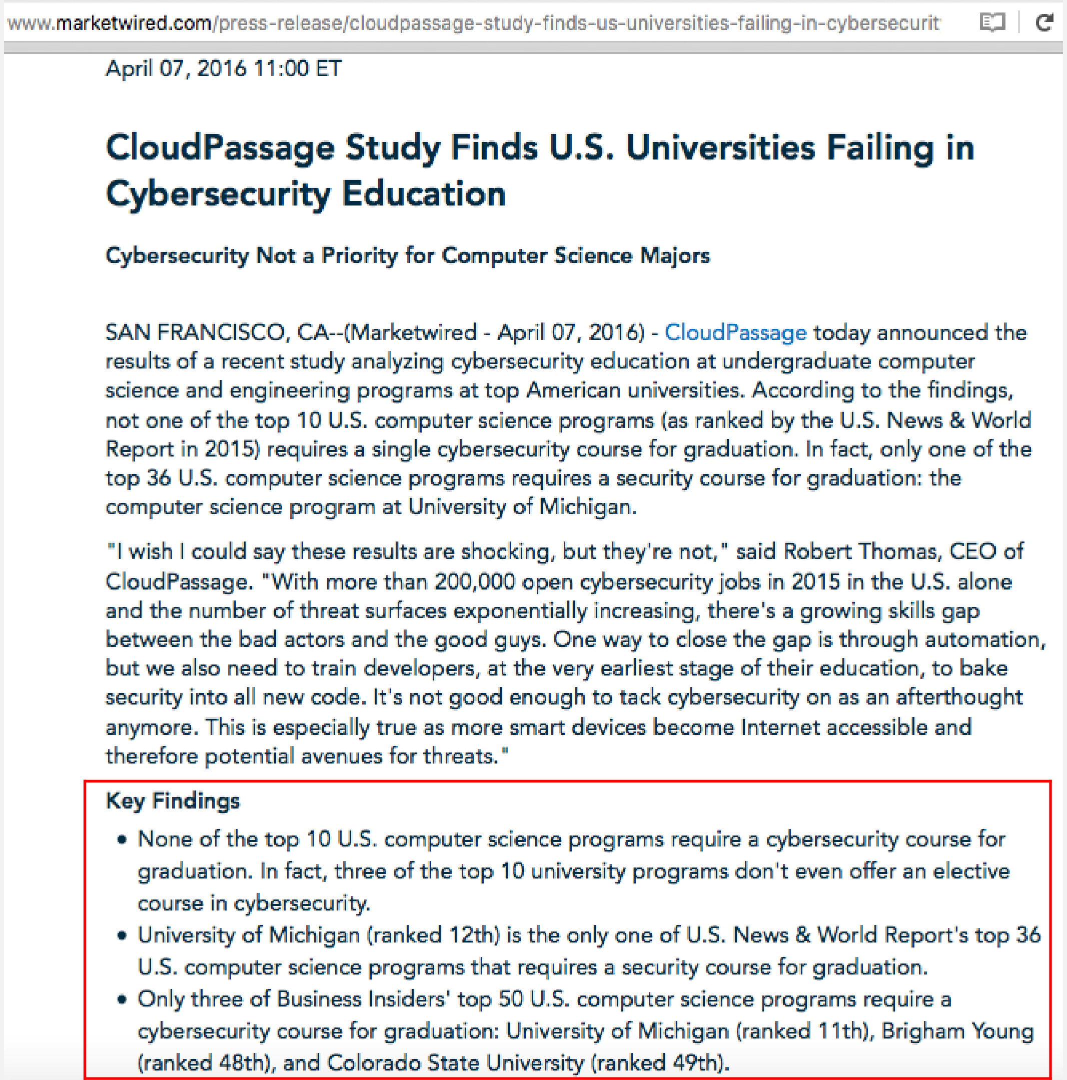
Kelly Jackson Higgins
News

New study reveals that none of the top 10 US university computer science and engineering program degrees requires students take a cybersecurity course.

There's the cybersecurity skills gap, but a new study shows there's also a major cybersecurity education gap -- in the top US undergraduate computer science and engineering programs.

An analysis of the top 121 US university computer science and engineering programs found that none of the top 10 requires students take a cybersecurity class for their degree in computer science, and three of the top 10 don't offer any cybersecurity courses at all. The higher-education gap in cybersecurity comes amid the backdrop of some 200,000 unfilled IT security jobs in the US, and an increasing sense of urgency for organizations to hire security talent as cybercrime and cyber espionage threats escalate.

April 7, 2016


www.marketwired.com/press-release/cloudpassage-study-finds-us-universities-failing-in-cybersecurit

April 07, 2016 11:00 ET

CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education

Cybersecurity Not a Priority for Computer Science Majors

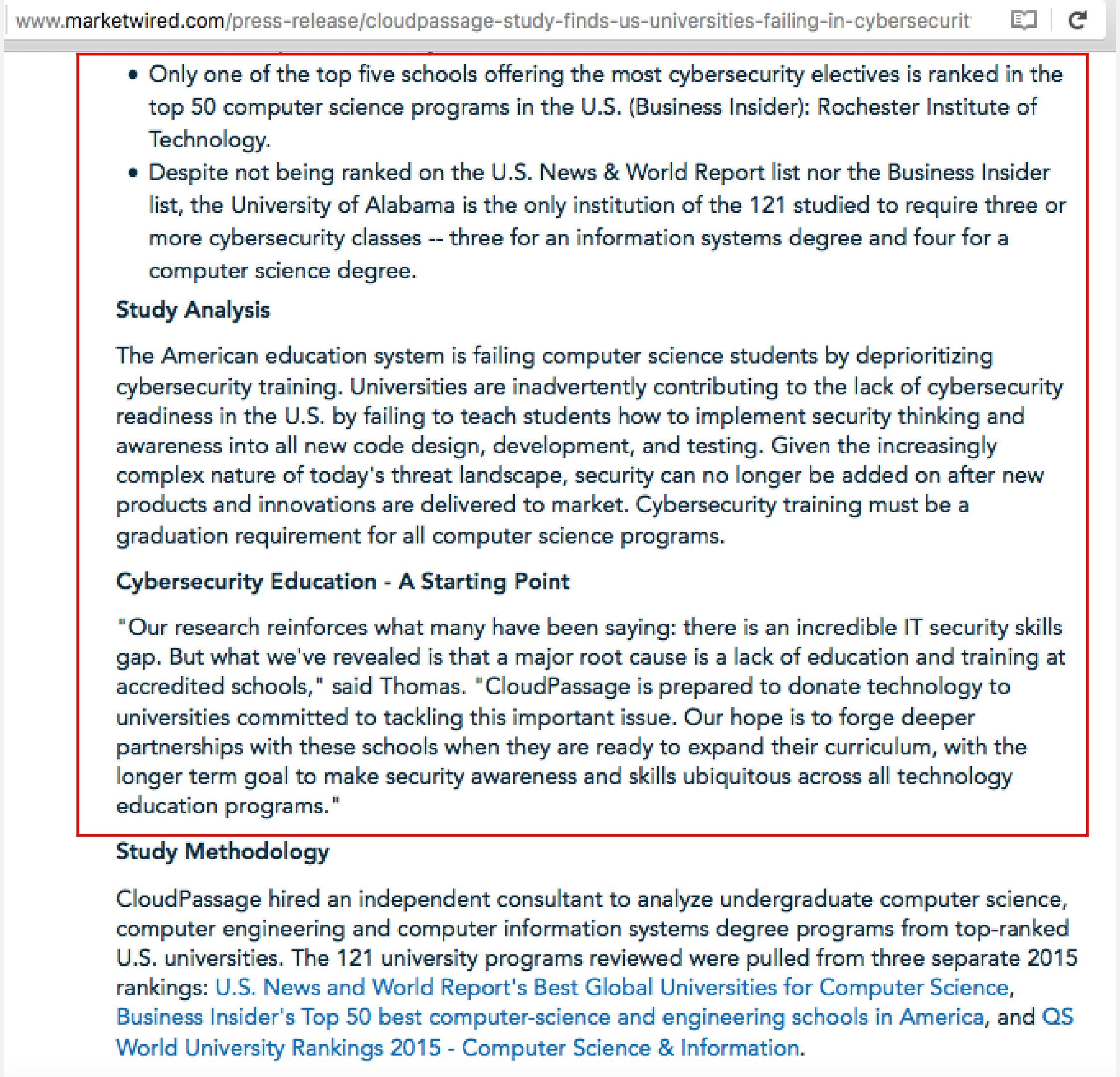
SAN FRANCISCO, CA--(Marketwired - April 07, 2016) - CloudPassage today announced the results of a recent study analyzing cybersecurity education at undergraduate computer science and engineering programs at top American universities. According to the findings, not one of the top 10 U.S. computer science programs (as ranked by the U.S. News & World Report in 2015) requires a single cybersecurity course for graduation. In fact, only one of the top 36 U.S. computer science programs requires a security course for graduation: the computer science program at University of Michigan.

"I wish I could say these results are shocking, but they're not," said Robert Thomas, CEO of CloudPassage. "With more than 200,000 open cybersecurity jobs in 2015 in the U.S. alone and the number of threat surfaces exponentially increasing, there's a growing skills gap between the bad actors and the good guys. One way to close the gap is through automation, but we also need to train developers, at the very earliest stage of their education, to bake security into all new code. It's not good enough to tack cybersecurity on as an afterthought anymore. This is especially true as more smart devices become Internet accessible and therefore potential avenues for threats."

Key Findings

- None of the top 10 U.S. computer science programs require a cybersecurity course for graduation. In fact, three of the top 10 university programs don't even offer an elective course in cybersecurity.
- University of Michigan (ranked 12th) is the only one of U.S. News & World Report's top 36 U.S. computer science programs that requires a security course for graduation.
- Only three of Business Insiders' top 50 U.S. computer science programs require a cybersecurity course for graduation: University of Michigan (ranked 11th), Brigham Young (ranked 48th), and Colorado State University (ranked 49th).

April 7, 2016


www.marketwired.com/press-release/cloudpassage-study-finds-us-universities-failing-in-cybersecurit

- Only one of the top five schools offering the most cybersecurity electives is ranked in the top 50 computer science programs in the U.S. (Business Insider): Rochester Institute of Technology.
- Despite not being ranked on the U.S. News & World Report list nor the Business Insider list, the University of Alabama is the only institution of the 121 studied to require three or more cybersecurity classes -- three for an information systems degree and four for a computer science degree.

Study Analysis

The American education system is failing computer science students by deprioritizing cybersecurity training. Universities are inadvertently contributing to the lack of cybersecurity readiness in the U.S. by failing to teach students how to implement security thinking and awareness into all new code design, development, and testing. Given the increasingly complex nature of today's threat landscape, security can no longer be added on after new products and innovations are delivered to market. Cybersecurity training must be a graduation requirement for all computer science programs.

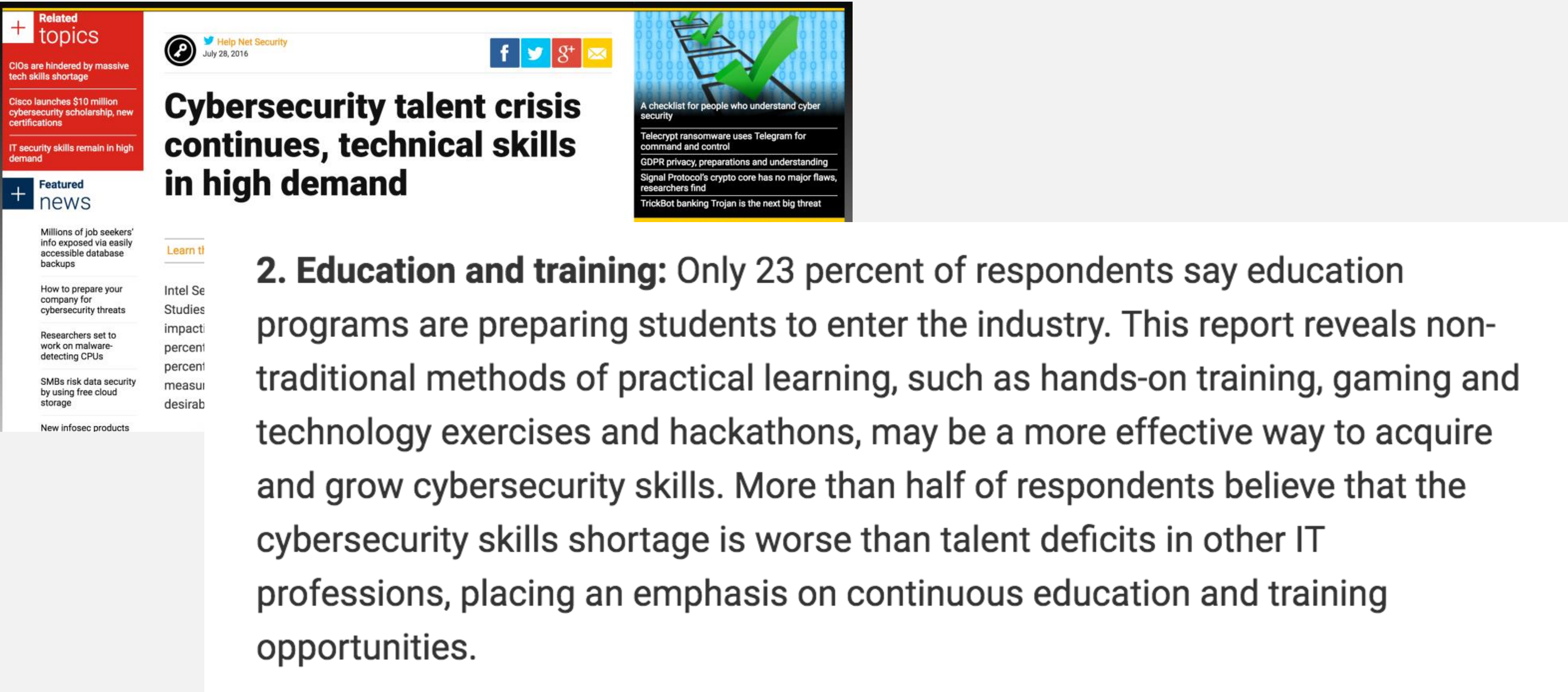
Cybersecurity Education - A Starting Point

"Our research reinforces what many have been saying: there is an incredible IT security skills gap. But what we've revealed is that a major root cause is a lack of education and training at accredited schools," said Thomas. "CloudPassage is prepared to donate technology to universities committed to tackling this important issue. Our hope is to forge deeper partnerships with these schools when they are ready to expand their curriculum, with the longer term goal to make security awareness and skills ubiquitous across all technology education programs."

Study Methodology

CloudPassage hired an independent consultant to analyze undergraduate computer science, computer engineering and computer information systems degree programs from top-ranked U.S. universities. The 121 university programs reviewed were pulled from three separate 2015 rankings: U.S. News and World Report's Best Global Universities for Computer Science, Business Insider's Top 50 best computer-science and engineering schools in America, and QS World University Rankings 2015 - Computer Science & Information.

April 7, 2016



Related topics

CIOs are hindered by massive tech skills shortage

Cisco launches $10 million cybersecurity scholarship, new certifications

IT security skills remain in high demand

Featured news

Millions of job seekers' info exposed via easily accessible database backups

How to prepare your company for cybersecurity threats

Researchers set to work on malware-detecting CPUs

SMBs risk data security by using free cloud storage

New infosec products

Help Net Security
July 28, 2016

Cybersecurity talent crisis continues, technical skills in high demand

Learn th

Intel Se
Studies
impacti
percent
percent
measur
desirab

A checklist for people who understand cyber security

Telecrypt ransomware uses Telegram for command and control

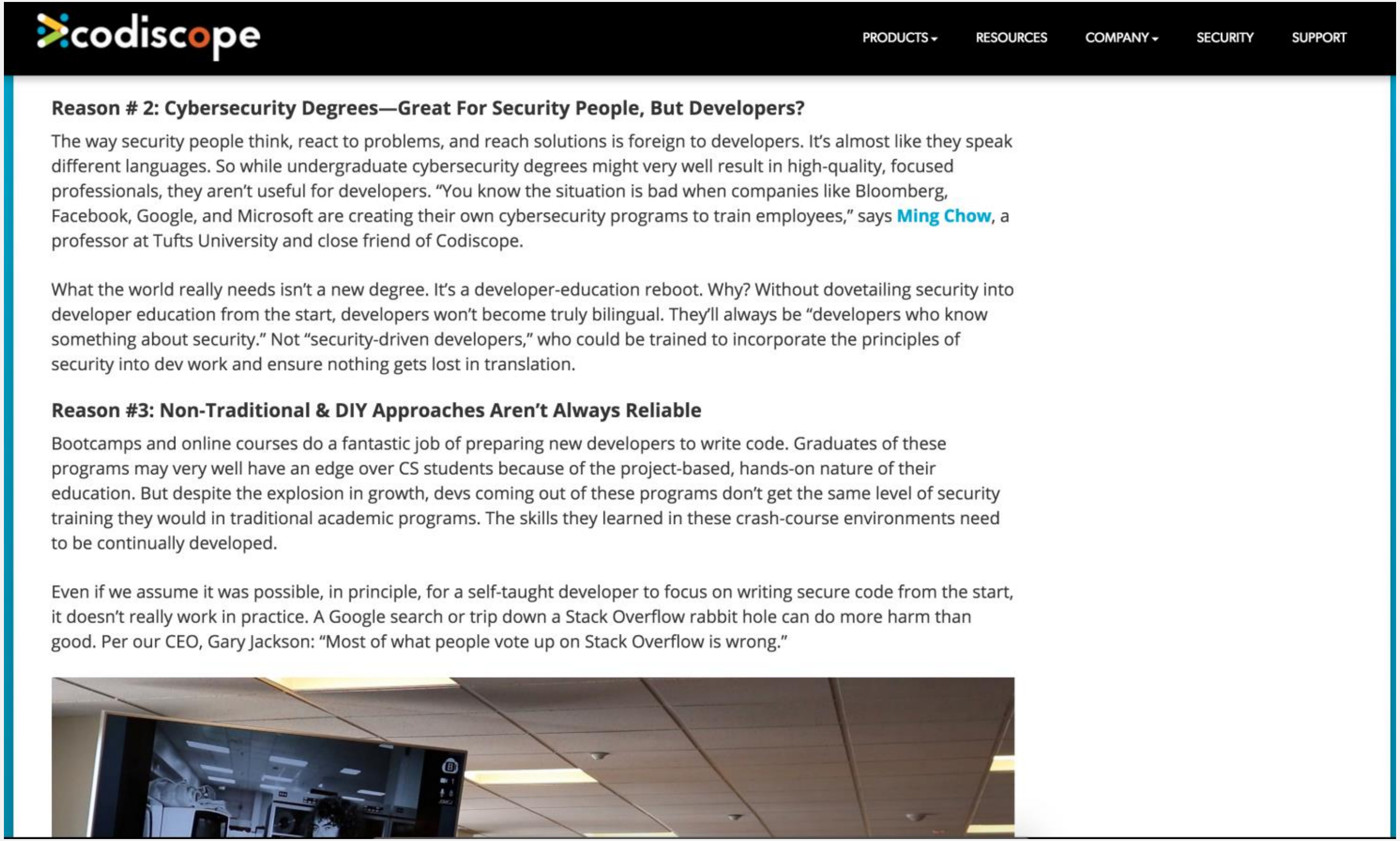
GDPR privacy, preparations and understanding

Signal Protocol's crypto core has no major flaws, researchers find

TrickBot banking Trojan is the next big threat

2. Education and training: Only 23 percent of respondents say education programs are preparing students to enter the industry. This report reveals non-traditional methods of practical learning, such as hands-on training, gaming and technology exercises and hackathons, may be a more effective way to acquire and grow cybersecurity skills. More than half of respondents believe that the cybersecurity skills shortage is worse than talent deficits in other IT professions, placing an emphasis on continuous education and training opportunities.

Source (July 28, 2016): https://www.helpnetsecurity.com/2016/07/28/cybersecurity-talent-crisis/



Reason # 2: Cybersecurity Degrees—Great For Security People, But Developers?

The way security people think, react to problems, and reach solutions is foreign to developers. It's almost like they speak different languages. So while undergraduate cybersecurity degrees might very well result in high-quality, focused professionals, they aren't useful for developers. "You know the situation is bad when companies like Bloomberg, Facebook, Google, and Microsoft are creating their own cybersecurity programs to train employees," says **Ming Chow**, a professor at Tufts University and close friend of Codiscope.

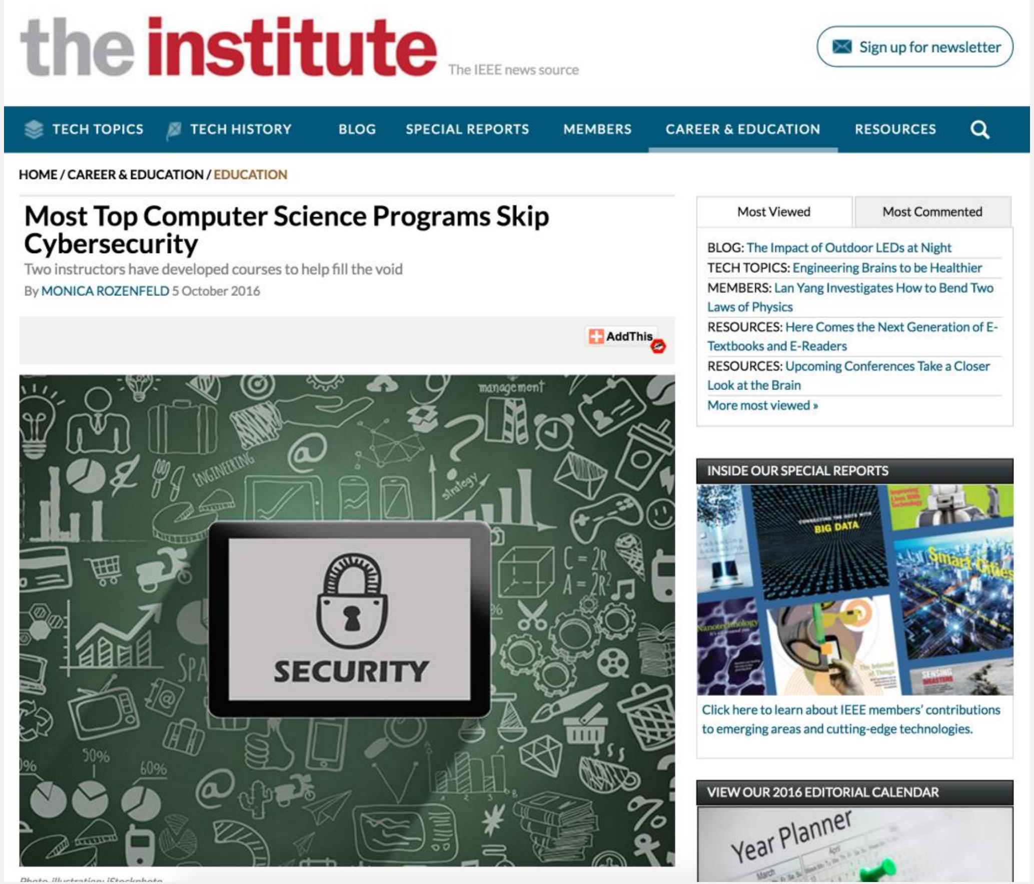
What the world really needs isn't a new degree. It's a developer-education reboot. Why? Without dovetailing security into developer education from the start, developers won't become truly bilingual. They'll always be "developers who know something about security." Not "security-driven developers," who could be trained to incorporate the principles of security into dev work and ensure nothing gets lost in translation.

Reason #3: Non-Traditional & DIY Approaches Aren't Always Reliable

Bootcamps and online courses do a fantastic job of preparing new developers to write code. Graduates of these programs may very well have an edge over CS students because of the project-based, hands-on nature of their education. But despite the explosion in growth, devs coming out of these programs don't get the same level of security training they would in traditional academic programs. The skills they learned in these crash-course environments need to be continually developed.

Even if we assume it was possible, in principle, for a self-taught developer to focus on writing secure code from the start, it doesn't really work in practice. A Google search or trip down a Stack Overflow rabbit hole can do more harm than good. Per our CEO, Gary Jackson: "Most of what people vote up on Stack Overflow is wrong."

Codiscope's blog article "Why Security Isn't Taught in Schools (And What We Can Do About It)"
https://codiscope.com/cybersecurity-not-taught-schools/



HOME / CAREER & EDUCATION / EDUCATION

Most Top Computer Science Programs Skip Cybersecurity

Two instructors have developed courses to help fill the void

By MONICA ROZENFELD 5 October 2016

Photo illustration: iStockphoto

Most Viewed | Most Commented

BLOG: The Impact of Outdoor LEDs at Night

TECH TOPICS: Engineering Brains to be Healthier

MEMBERS: Lan Yang Investigates How to Bend Two Laws of Physics

RESOURCES: Here Comes the Next Generation of E-Textbooks and E-Readers

RESOURCES: Upcoming Conferences Take a Closer Look at the Brain

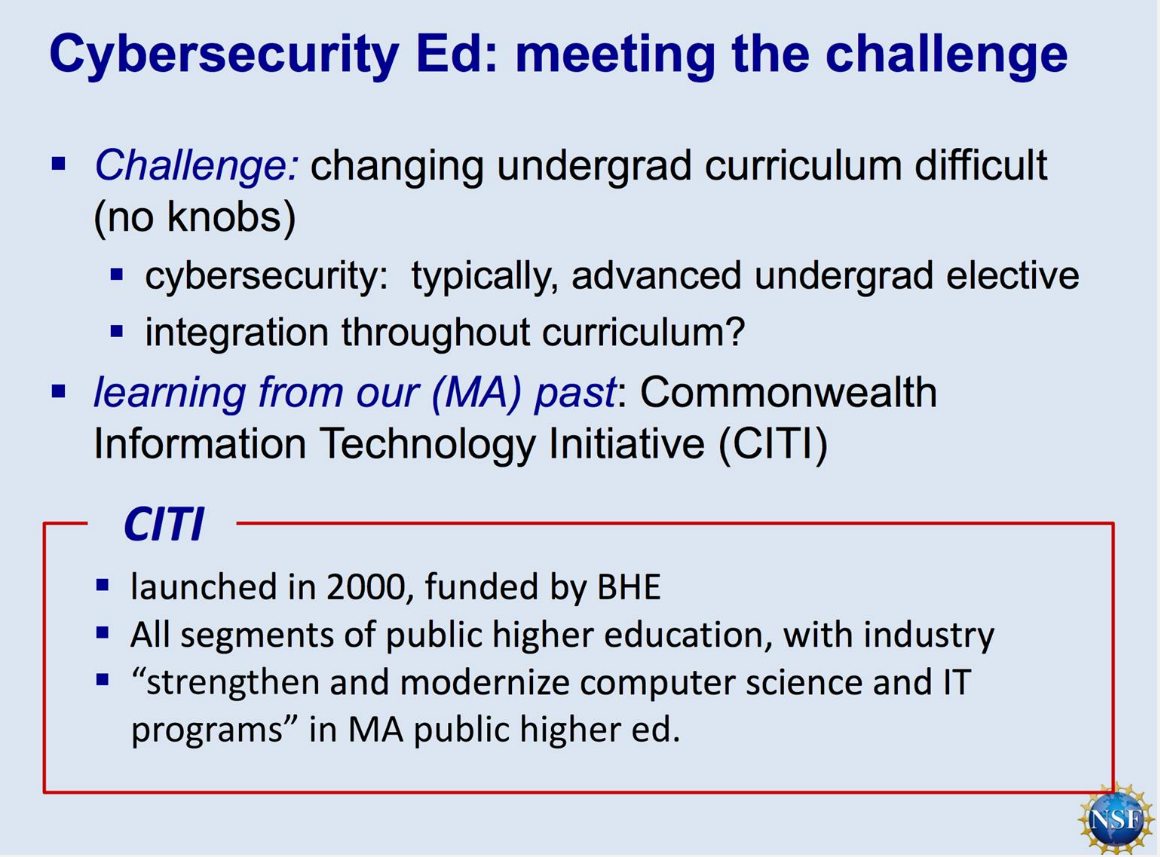
More most viewed »

INSIDE OUR SPECIAL REPORTS

Click here to learn about IEEE members' contributions to emerging areas and cutting-edge technologies.

VIEW OUR 2016 EDITORIAL CALENDAR

In IEEE: The Institute (October 5, 2016) http://theinstitute.ieee.org/career-and-education/education/most-top-computer-science-programs-skip-cybersecurity



Cybersecurity Ed: meeting the challenge

- *Challenge:* changing undergrad curriculum difficult (no knobs)
  - cybersecurity: typically, advanced undergrad elective
  - integration throughout curriculum?
- *learning from our (MA) past*: Commonwealth Information Technology Initiative (CITI)

CITI

- launched in 2000, funded by BHE
- All segments of public higher education, with industry
- "strengthen and modernize computer science and IT programs" in MA public higher ed.

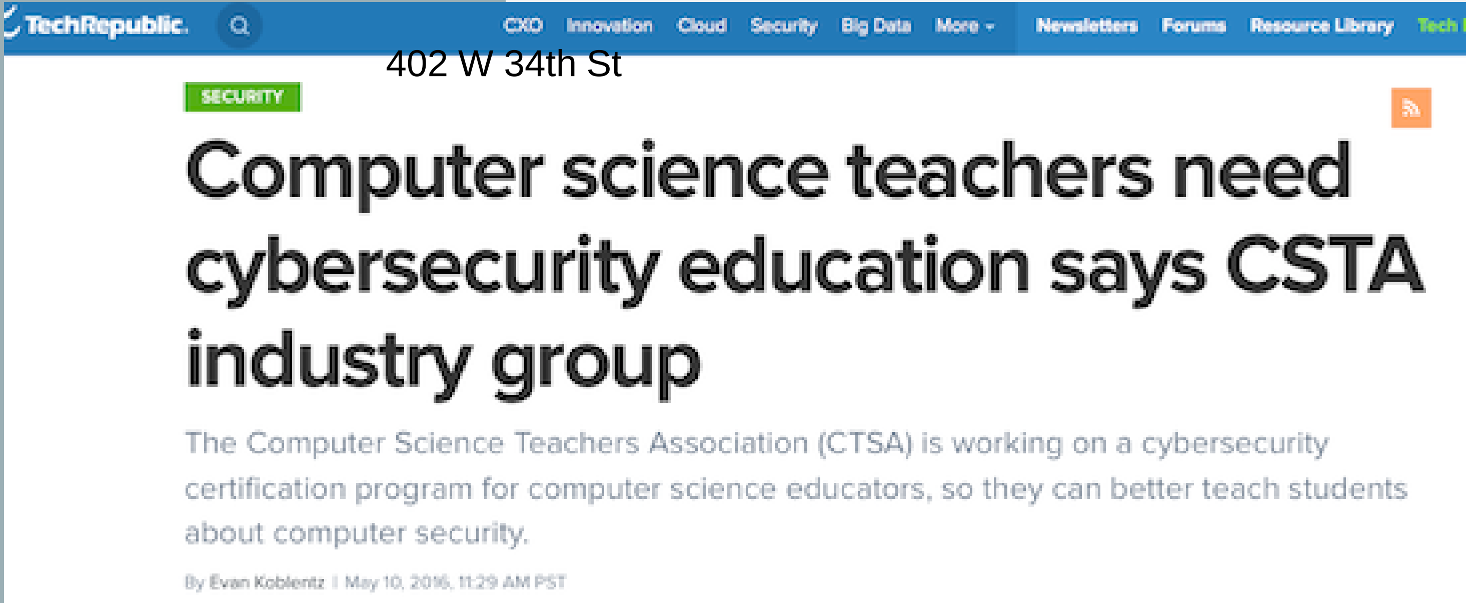
From Dr. James Kurose, Assistant Director, Computer and Information Science and Engineering Directorate, NSF at Innovations Partnerships Network (IPN) Conference on December 9, 2015

From The Computer Science Teachers Association (CTSA)http://www.techrepublic.com/article/cs-teachers-ramping-up-cybersecurity-education/

http://www.csteachers.org/

csta | Computer Science Teachers Association

402 W 34th St



SECURITY

Computer science teachers need cybersecurity education says CSTA industry group

The Computer Science Teachers Association (CTSA) is working on a cybersecurity certification program for computer science educators, so they can better teach students about computer security.

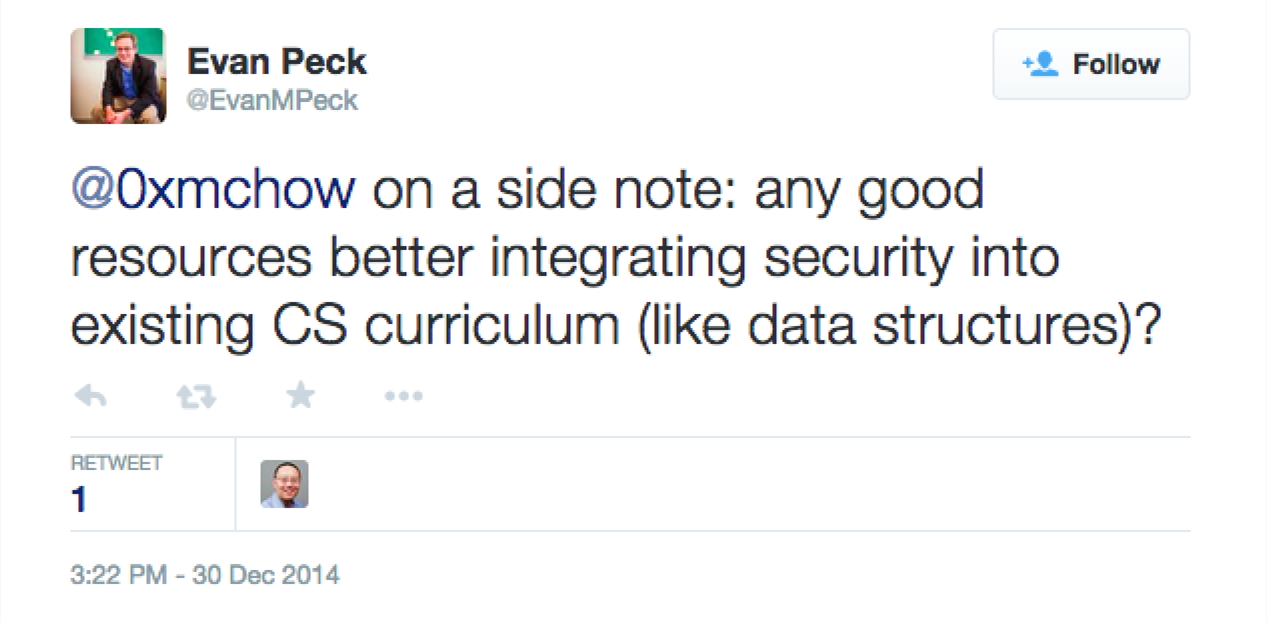
By Evan Koblentz | May 10, 2016, 11:29 AM PST

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.**"



Evan Peck
@EvanMPeck

@0xmchow on a side note: any good resources better integrating security into existing CS curriculum (like data structures)?

RETWEET
1

3:22 PM - 30 Dec 2014

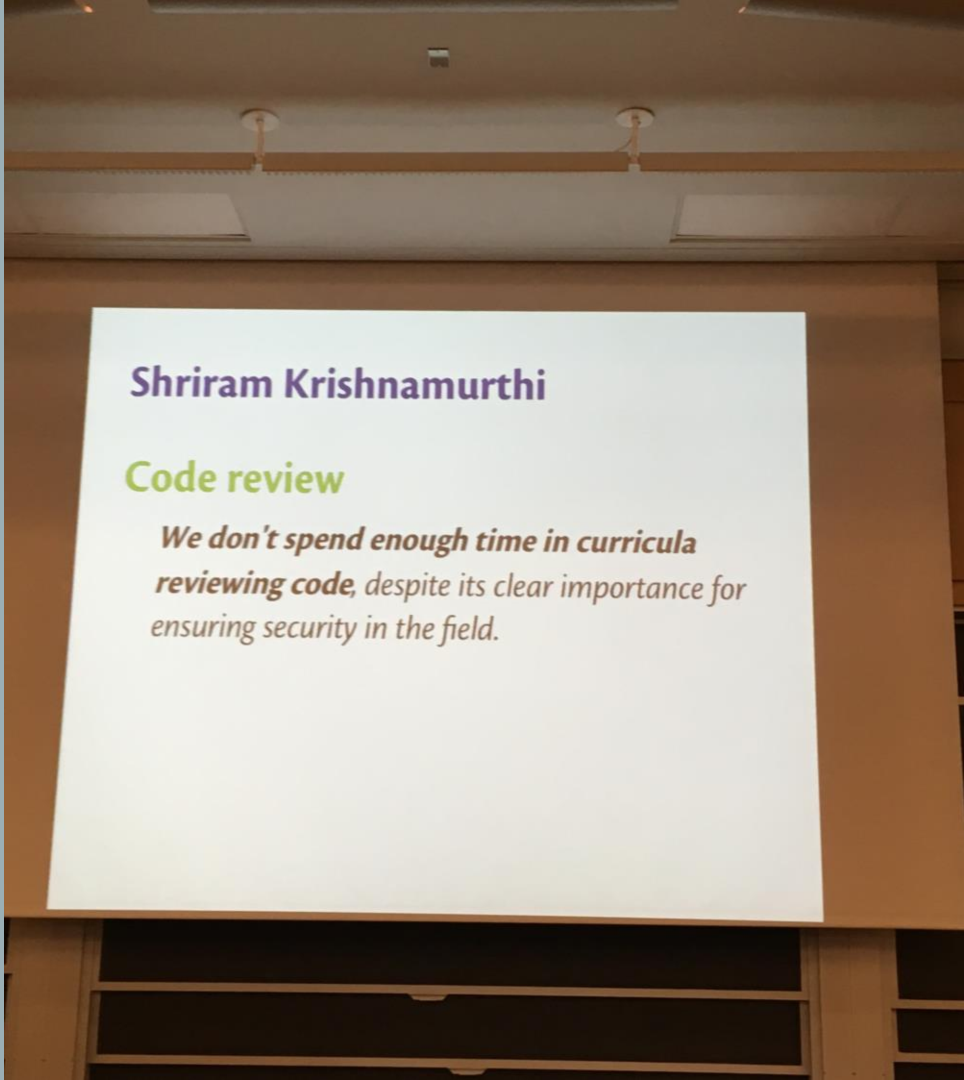
EXAMPLES AND SUCCESS STORIES

- Collection of ideas and pictures at end of slide:
  - Web Programming
  - Senior Capstone / Software Engineering
  - Healthcare
  - Game Development
  - Mobile Development
  - Machine Structure and Assembly Language
  - Programming Languages

NEED: REAL AND ”VALUABLE” ASSIGNMENTS

- Capture The Flag (CTF) games
- Code reviews
- Conduct risk assessments, metrics
- Create information security policies
- Research papers on information security topics that students care about
- Peer reviews of assignments
- Mock-interviews that can be used at student’s organizations
- ”Personal engagement project”(e.g., attend local security events/webinars and discuss)

From New England Security Day Spring 2016, April 28th, Security Education Panel



Shriram Krishnamurthi

Code review

We don't spend enough time in curricula reviewing code*, despite its clear importance for ensuring security in the field.*

FACEBOOK'S RECENTLY OPEN SOURCED CTF

"Career Advantage

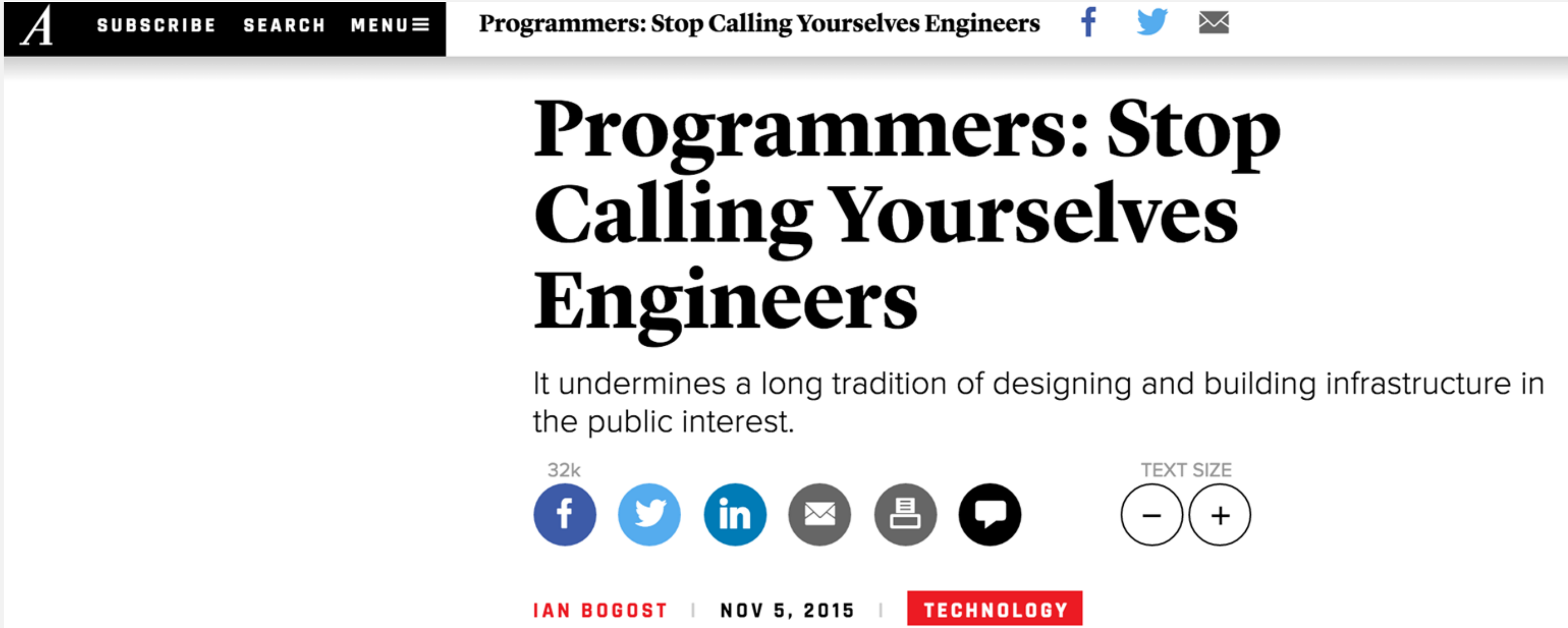
Not only do CTFs have the ability to teach more technical skills than you'll get in an average computer science program, they can also help you break into the security industry. When I started looking for full-time positions, I found security job interviews to be a lot like CTF challenges, which made it easier for me to demonstrate my technical skills --- and I was able to make an impact from day one.

When I joined the Facebook security team last year, it was in large part because of the experience I gained through CTFs. When I was a student at the University of Michigan, the TA for my security class introduced me to CTFs, which exposed me to a fun and practical side of security that I didn't get in class."

Source: https://www.facebook.com/notes/facebook-ctf/facebook-ctf-is-now-open-source/525464774322241/

ONLY THE TIP OF THE ICEBERG

There's much more…



Programmers: Stop Calling Yourselves Engineers

It undermines a long tradition of designing and building infrastructure in the public interest.

IAN BOGOST | NOV 5, 2015 |

THE TITLE OF ENGINEER

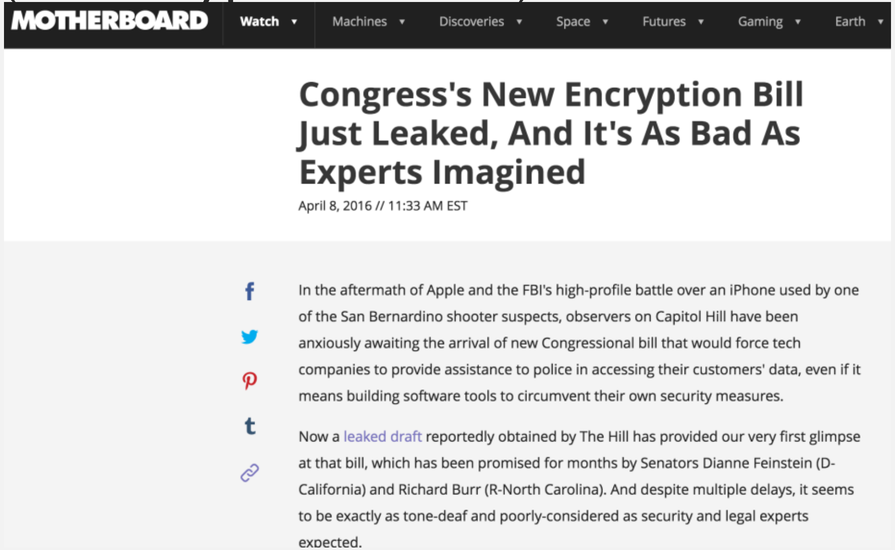
"The title "engineer" is cheapened by the tech industry.

Recent years have seen prominent failures in software. Massive data breaches at Target, Home Depot, BlueCross BlueShield, Anthem, Harvard University, LastPass, and Ashley Madison only scratch the surface of the cybersecurity issues posed by today's computer systems. The Volkswagen diesel-emissions exploit was caused by a software failing, even if it seems to have been engineered, as it were, deliberately."

Source: http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/?single_page=true

FURTHER SECURITY EDUCATION GAPS

- Awareness that software has critical infrastructure, has life-and-death implications
- Policy and leadership (see encryption debates)



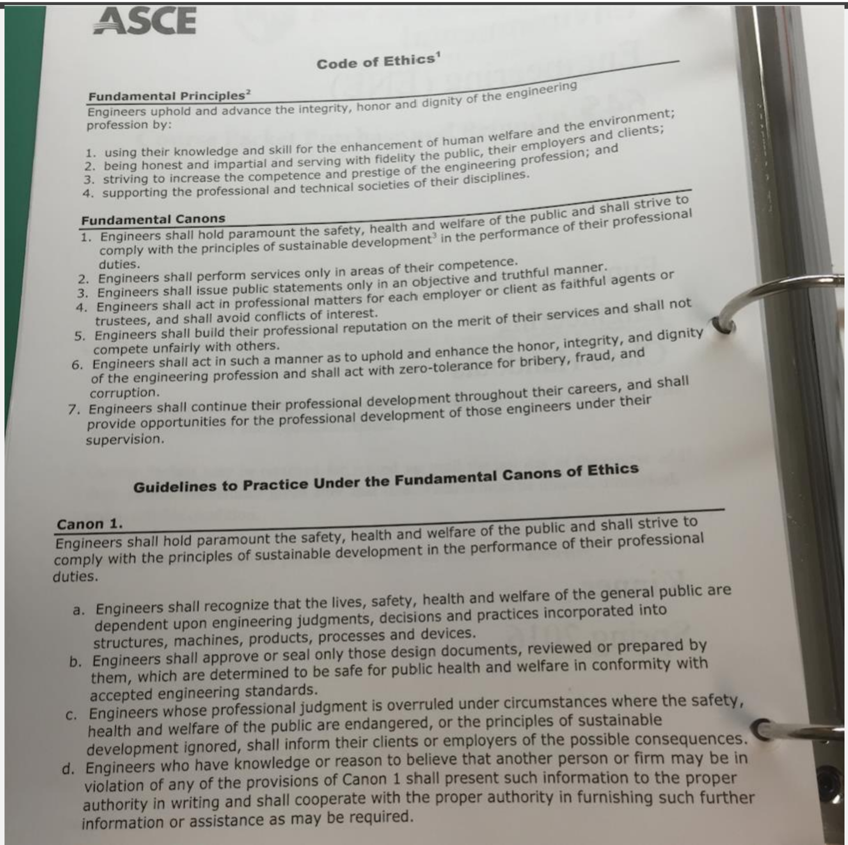
Congress's New Encryption Bill Just Leaked, And It's As Bad As Experts Imagined

April 8, 2016 // 11:33 AM EST

In the aftermath of Apple and the FBI's high-profile battle over an iPhone used by one of the San Bernardino shooter suspects, observers on Capitol Hill have been anxiously awaiting the arrival of new Congressional bill that would force tech companies to provide assistance to police in accessing their customers' data, even if it means building software tools to circumvent their own security measures.

Now a leaked draft reportedly obtained by The Hill has provided our very first glimpse at that bill, which has been promised for months by Senators Dianne Feinstein (D-California) and Richard Burr (R-North Carolina). And despite multiple delays, it seems to be exactly as tone-deaf and poorly-considered as security and legal experts expected.

THE NEED: FOLLOW THIS MODEL?



ASCE

Code of Ethics[1]

Fundamental Principles[2]

Engineers uphold and advance the integrity, honor and dignity of the engineering profession by:

1. using their knowledge and skill for the enhancement of human welfare and the environment;
2. being honest and impartial and serving with fidelity the public, their employers and clients;
3. striving to increase the competence and prestige of the engineering profession; and
4. supporting the professional and technical societies of their disciplines.

Fundamental Canons

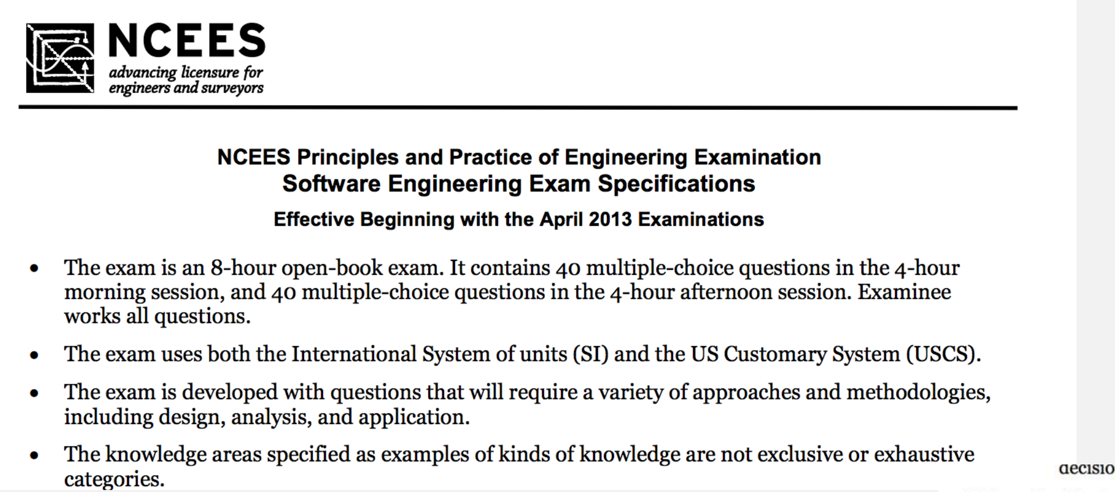
1. Engineers shall hold paramount the safety, health and welfare of the public and shall strive to comply with the principles of sustainable development[3] in the performance of their professional duties.
2. Engineers shall perform services only in areas of their competence.
3. Engineers shall issue public statements only in an objective and truthful manner.
4. Engineers shall act in professional matters for each employer or client as faithful agents or trustees, and shall avoid conflicts of interest.
5. Engineers shall build their professional reputation on the merit of their services and shall not compete unfairly with others.
6. Engineers shall act in such a manner as to uphold and enhance the honor, integrity, and dignity of the engineering profession and shall act with zero-tolerance for bribery, fraud, and corruption.
7. Engineers shall continue their professional development throughout their careers, and shall provide opportunities for the professional development of those engineers under their supervision.

Guidelines to Practice Under the Fundamental Canons of Ethics

Canon 1.

Engineers shall hold paramount the safety, health and welfare of the public and shall strive to comply with the principles of sustainable development in the performance of their professional duties.

a. Engineers shall recognize that the lives, safety, health and welfare of the general public are dependent upon engineering judgments, decisions and practices incorporated into structures, machines, products, processes and devices.
b. Engineers shall approve or seal only those design documents, reviewed or prepared by them, which are determined to be safe for public health and welfare in conformity with accepted engineering standards.
c. Engineers whose professional judgment is overruled under circumstances where the safety, health and welfare of the public are endangered, or the principles of sustainable development ignored, shall inform their clients or employers of the possible consequences.
d. Engineers who have knowledge or reason to believe that another person or firm may be in violation of any of the provisions of Canon 1 shall present such information to the proper authority in writing and shall cooperate with the proper authority in furnishing such further information or assistance as may be required.

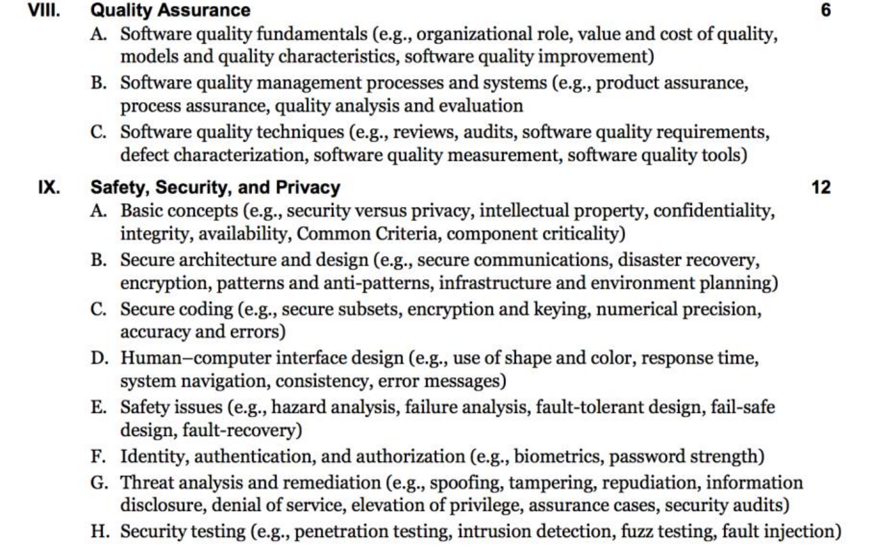


NCEES
advancing licensure for engineers and surveyors

NCEES Principles and Practice of Engineering Examination
Software Engineering Exam Specifications

Effective Beginning with the April 2013 Examinations

- The exam is an 8-hour open-book exam. It contains 40 multiple-choice questions in the 4-hour morning session, and 40 multiple-choice questions in the 4-hour afternoon session. Examinee works all questions.
- The exam uses both the International System of units (SI) and the US Customary System (USCS).
- The exam is developed with questions that will require a variety of approaches and methodologies, including design, analysis, and application.
- The knowledge areas specified as examples of kinds of knowledge are not exclusive or exhaustive categories.



decisions under uncertainty)

VIII. Quality Assurance 6

A. Software quality fundamentals (e.g., organizational role, value and cost of quality, models and quality characteristics, software quality improvement)

B. Software quality management processes and systems (e.g., product assurance, process assurance, quality analysis and evaluation

C. Software quality techniques (e.g., reviews, audits, software quality requirements, defect characterization, software quality measurement, software quality tools)

IX. Safety, Security, and Privacy 12

A. Basic concepts (e.g., security versus privacy, intellectual property, confidentiality, integrity, availability, Common Criteria, component criticality)

B. Secure architecture and design (e.g., secure communications, disaster recovery, encryption, patterns and anti-patterns, infrastructure and environment planning)

C. Secure coding (e.g., secure subsets, encryption and keying, numerical precision, accuracy and errors)

D. Human–computer interface design (e.g., use of shape and color, response time, system navigation, consistency, error messages)

E. Safety issues (e.g., hazard analysis, failure analysis, fault-tolerant design, fail-safe design, fault-recovery)

F. Identity, authentication, and authorization (e.g., biometrics, password strength)

G. Threat analysis and remediation (e.g., spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege, assurance cases, security audits)

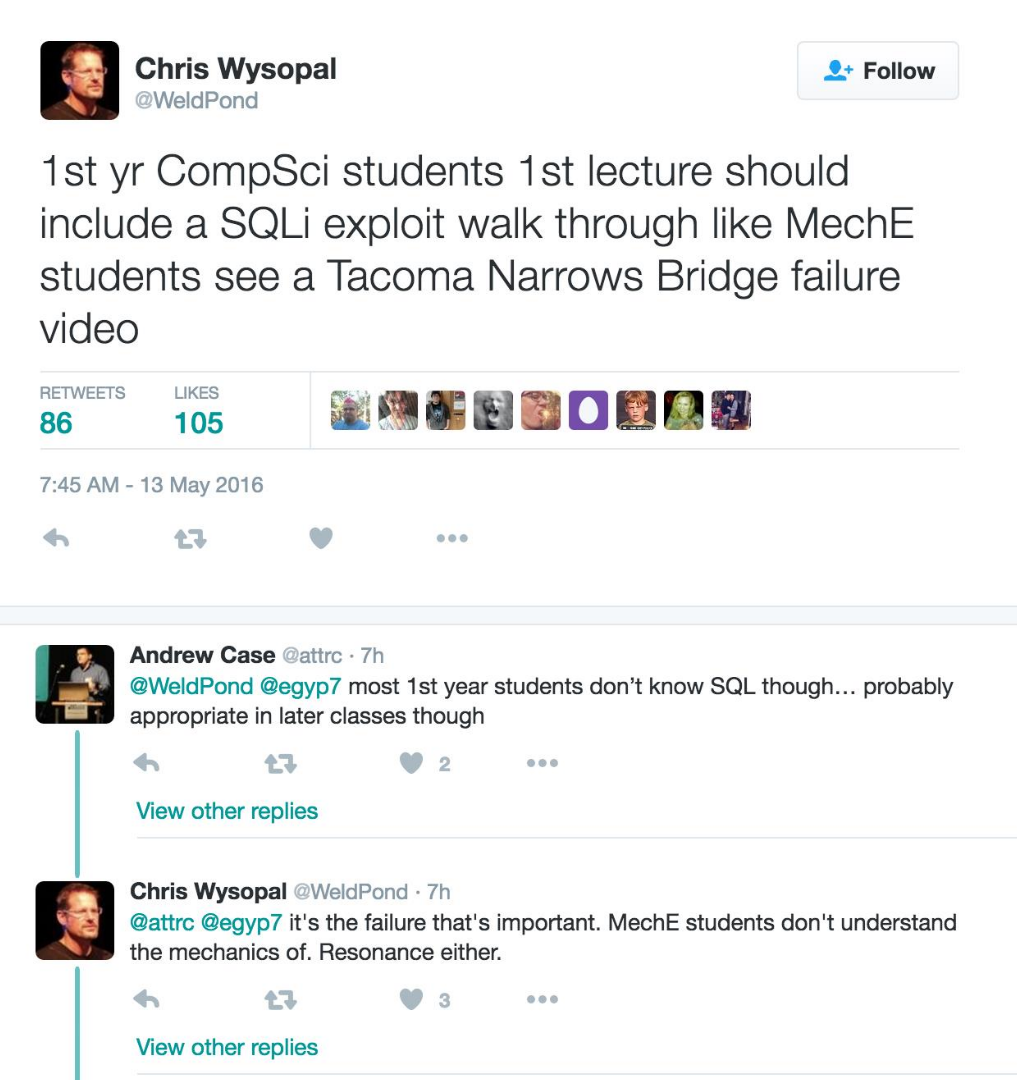
H. Security testing (e.g., penetration testing, intrusion detection, fuzz testing, fault injection)

HOW TUFTS IS ADDRESSING THE POLICY GAP

- Tufts can make global contributions to this nascent field by leveraging our existing strengths in Diplomacy, International Relations, Political Science, Computer Science, and Active Citizenship.
  - Side note: Boston College founded a new MS in Cyber Security and Policy in January 2016 but without much help with from Computer Science as the program does not have emphasis on Security in curriculum (special thanks to Kevin Powers)
- Step 1: A bridge professorship in Cyber Security and Policy between School of Engineering and The Fletcher School (only two schools)
- Step 2: Joint Computer Science and Political Science course on Cyber Security and Cyber Warfare (accepted; will run in spring 2017)
  - The point: get undergraduates informed
- Step 3: Start Certificate and Masters Programs

HOW BRANDEIS IS GOING TO ADDRESS THE POLICY GAP

- Proposed:
  - Open up healthcare information security systems course to all Brandeis students as it is a required course in the healthcare medical informatics program. (Make course an elective course for all people outside the program) who want to learn
    - High School?
    - Undergraduate?
  - Development of new course to incorporate student projects and work directly with students throughout course
  - Provide the ability to have course every semester so that course does not fill up
  - Incorporate additional required information security and elective courses in to other Brandeis programs?
    - To ensure security is throughout lifecycle rather than bolted on.
  - Certification program
  - Integration with departments



Chris Wysopal
@WeldPond

1st yr CompSci students 1st lecture should include a SQLi exploit walk through like MechE students see a Tacoma Narrows Bridge failure video

RETWEETS 86
LIKES 105

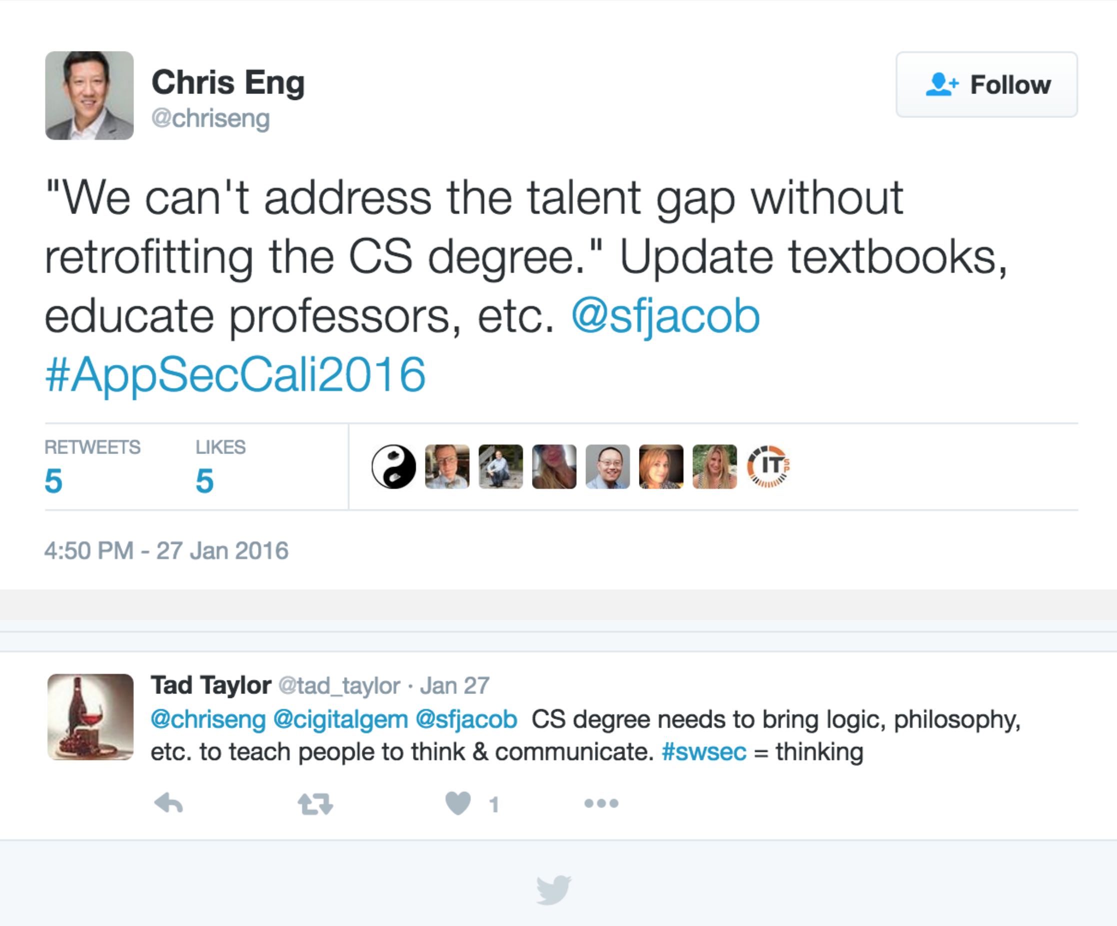
7:45 AM - 13 May 2016

Andrew Case @attrc · 7h
@WeldPond @egyp7 most 1st year students don't know SQL though… probably appropriate in later classes though

2

Chris Wysopal @WeldPond · 7h
@attrc @egyp7 it's the failure that's important. MechE students don't understand the mechanics of. Resonance either.

3



Chris Eng
@chriseng

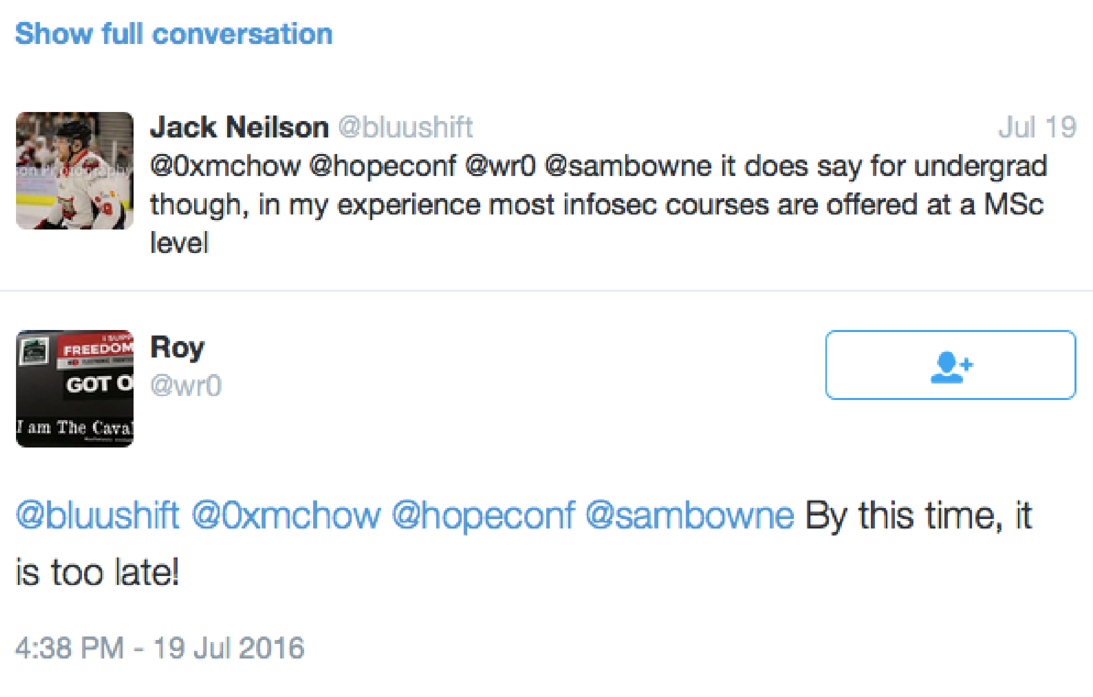
"We can't address the talent gap without retrofitting the CS degree." Update textbooks, educate professors, etc. @sfjacob #AppSecCali2016

RETWEETS 5 LIKES 5

4:50 PM - 27 Jan 2016

Tad Taylor @tad_taylor · Jan 27

@chriseng @cigitalgem @sfjacob CS degree needs to bring logic, philosophy, etc. to teach people to think & communicate. #swsec = thinking



Show full conversation

Jack Neilson @bluushift Jul 19

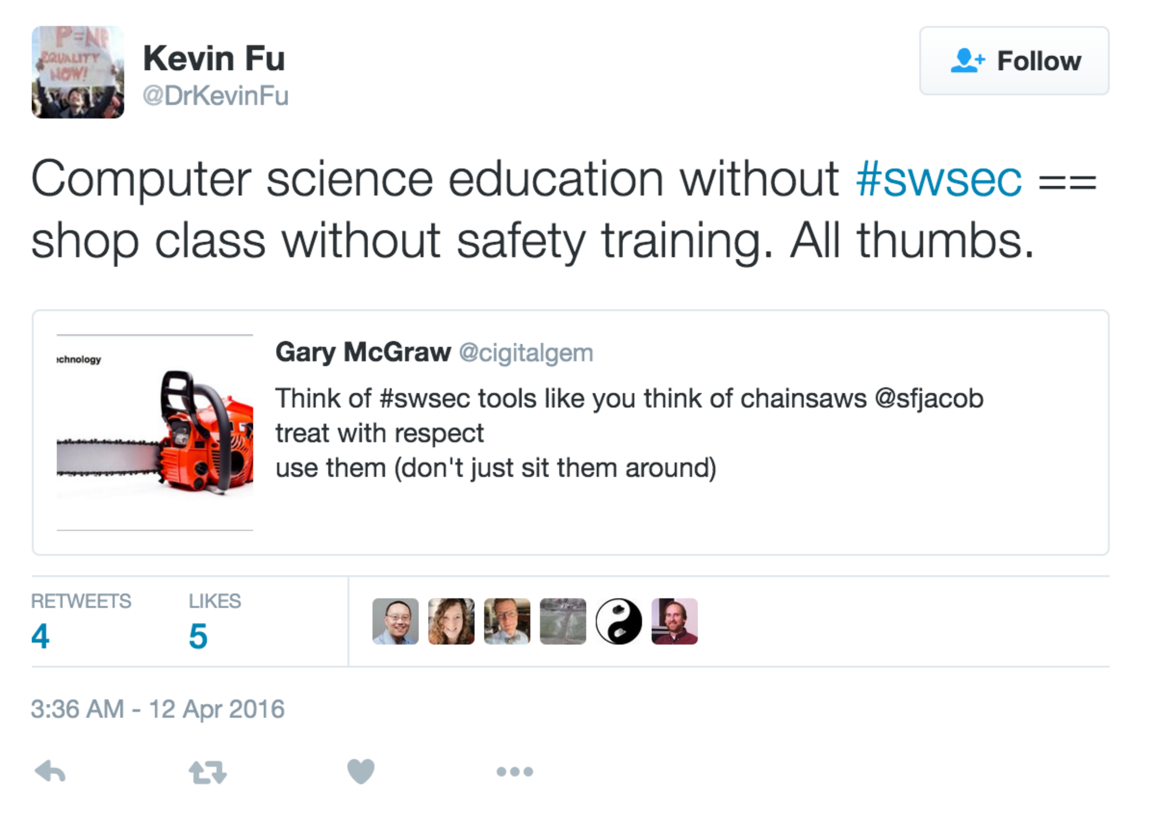
@0xmchow @hopeconf @wr0 @sambowne it does say for undergrad though, in my experience most infosec courses are offered at a MSc level

Roy
@wr0

@bluushift @0xmchow @hopeconf @sambowne By this time, it is too late!

4:38 PM - 19 Jul 2016

FACT TO THE MATTER IS



Kevin Fu
@DrKevinFu

Computer science education without #swsec == shop class without safety training. All thumbs.

Gary McGraw @cigitalgem

Think of #swsec tools like you think of chainsaws @sfjacob
treat with respect
use them (don't just sit them around)

RETWEETS
4

LIKES
5

3:36 AM - 12 Apr 2016

COLLECTION OF EXAMPLES

EXAMPLE: 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: WEB PROGRAMMING

- The full-stack: HTTP, HTML5, CSS, JavaScript, server-side, data persistence using database(s)
- Build client and server, then break. Since spring 2014, 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: USING EXISTING FRAMEWORKS

- HIPAA Security versus HIPAA Privacy
- NIST, ISO, HITRUST, GRC
- Ethics, privacy, segregation of duties
- Local, state and international laws
- CIS
- PCI, HITECH
- Healthcare terms like PHI, PII, EHR, etc.

EXAMPLE: SENIOR CAPSTONE PROJECT / SOFTWARE ENGINEERING

- Exercise: think of abuse cases in the specification and design phases
- Deliverable: technical risk analysis table for capstone project (in the fall)
- From @chriseng: "Undergraduate CS projects should be subjected to security testing" @sfjacob #AppSecCali2016 (/cc @0xmchow) https://twitter.com/chriseng/status/692510469442117634

EXAMPLE: APPLICATIONS OF INFOSEC. IN HEALTHCARE

- Concept of "not bolted on . . ."
- How to test and monitor software applications (reverse engineering)
- Evaluate information security tools
- Review existing/new IoT devices and its uses
- Create an incident response checklist and how to respond
- OWASP Top 10 & OWASP Mobile Security Project

EXAMPLE: GAME DEVELOPMENT

- Issues taught: cheating in games, virtual economies, and abusing online games (https://tuftsdev.github.io/GameDevelopment/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/security.html

EXAMPLE: EMERGING ISSUES IN HEALTHCARE

- Review of current events on a weekly-basis
- Review/ Discussion Questions of students' feedback of ongoing and past information security events
- Threat vectors / FBI warnings and lists of healthcare breaches, Verizon DBIR, Mandiant Report
- Opportunities to network with colleagues and present at conferences
- Awareness of new technologies like implantable medical devices, PHR

EXAMPLE: MOBILE MEDICAL DEVICES AND APPS

- 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/engineeringreality

EXAMPLE: INTRODUCTION TO COMPUTER 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: HEALTHCARE INFORMATION SECURITY SYSTEMS AT BRANDEIS

- Syllabus runs the broad spectrum: healthcare information security, privacy, application security, incident handling, threat modeling, healthcare medical devices, IoT, mobile applications
- Real hands-on assignments: Analyze your organization’s information security program, analyze existing security tools, create your own ISP, conduct risk assessments, research additional information security topics, write paper(s) and have two students give feedback to your paper
- Discussion on weekly news and security events
- Guest speakers from the field

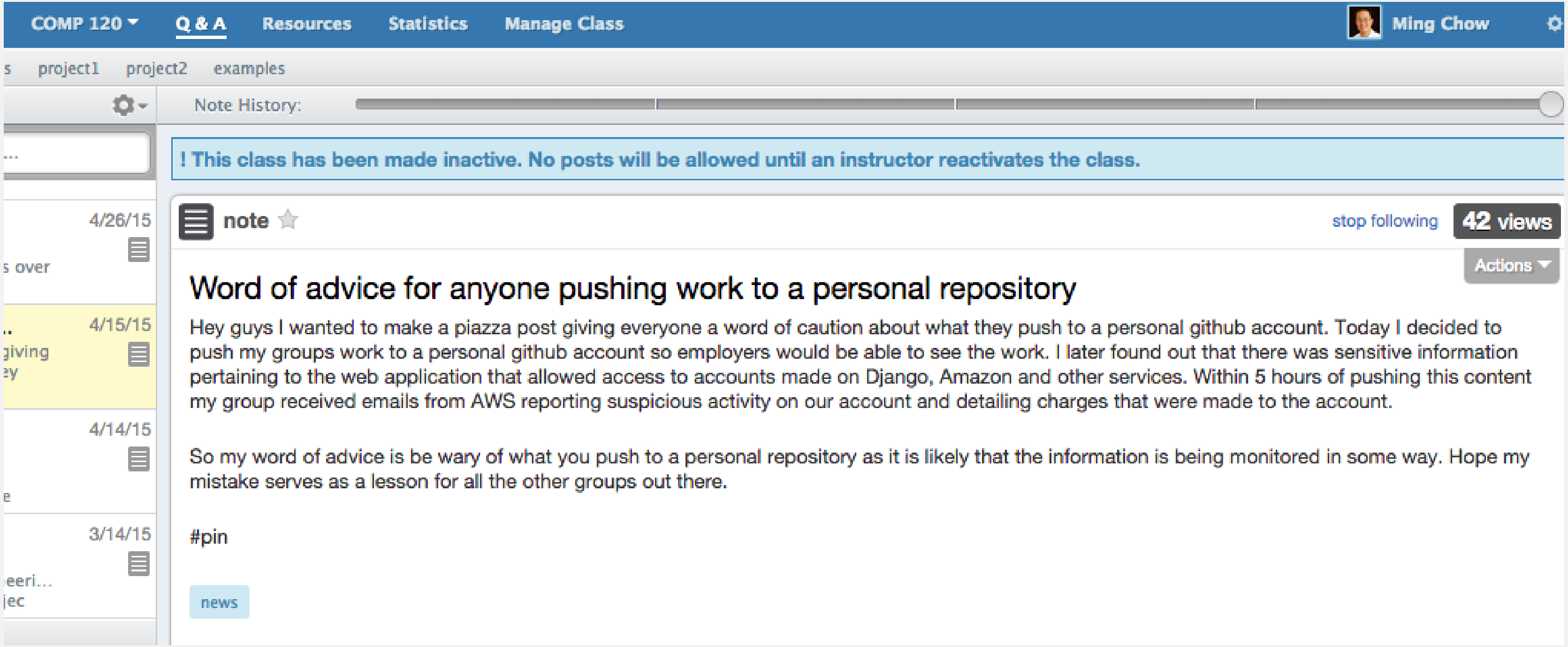
EXAMPLE: MACHINE STRUCTURE AND ASSEMBLY LANGUAGE PROGRAMMING

- Reverse engineering (e.g., “binary bomb”)
- Buffer overflow

EXAMPLE: PROGRAMMING LANGUAGES

- Langsec
- Build it, break it, fix it model (competition: https://builditbreakit.org/)
- “The Security of Programming Languages” (http://www.cs.tufts.edu/comp/116/archive/fall2015/chamilton.pdf)
- http://www.cs.dartmouth.edu/~sergey/langsec/

SUCCESS STORIES



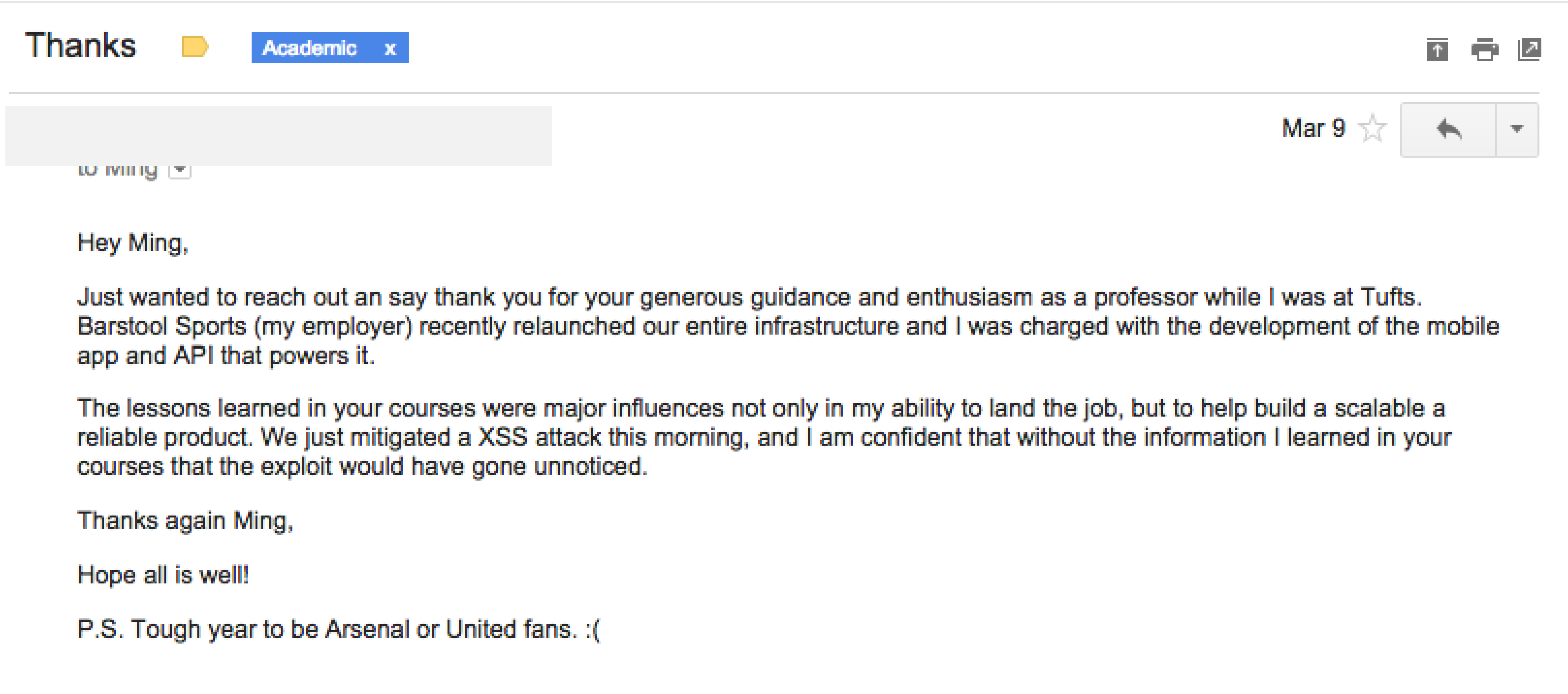
! This class has been made inactive. No posts will be allowed until an instructor reactivates the class.

Word of advice for anyone pushing work to a personal repository

Hey guys I wanted to make a piazza post giving everyone a word of caution about what they push to a personal github account. Today I decided to push my groups work to a personal github account so employers would be able to see the work. I later found out that there was sensitive information pertaining to the web application that allowed access to accounts made on Django, Amazon and other services. Within 5 hours of pushing this content my group received emails from AWS reporting suspicious activity on our account and detailing charges that were made to the account.

So my word of advice is be wary of what you push to a personal repository as it is likely that the information is being monitored in some way. Hope my mistake serves as a lesson for all the other groups out there.

#pin



Thanks

[redacted]

Mar 9

Hey Ming,

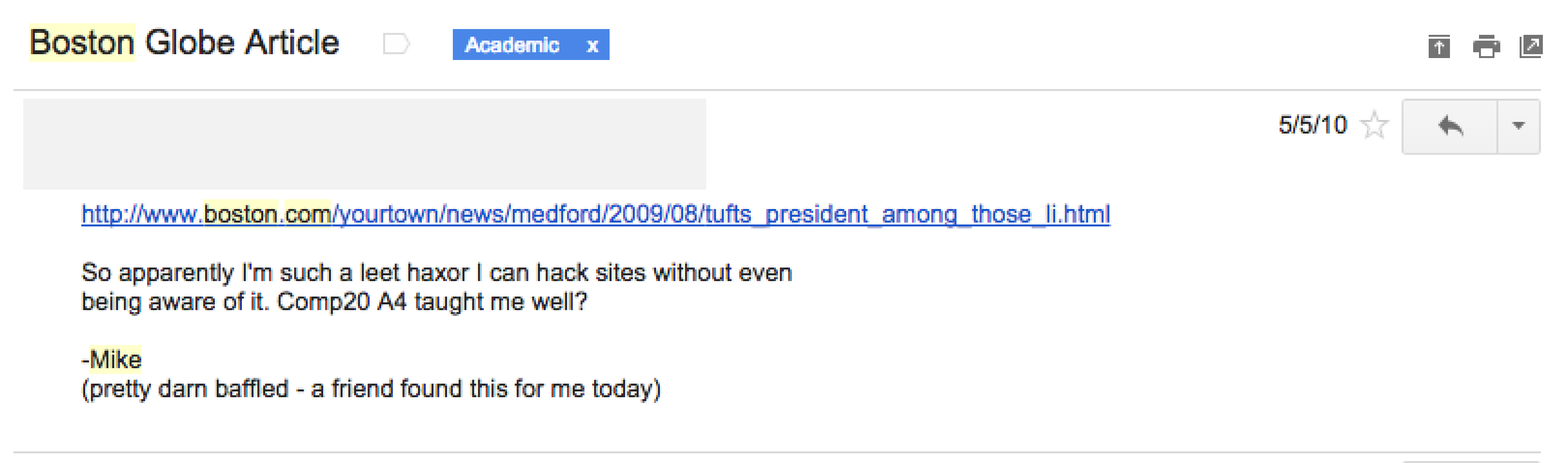
Just wanted to reach out an say thank you for your generous guidance and enthusiasm as a professor while I was at Tufts. Barstool Sports (my employer) recently relaunched our entire infrastructure and I was charged with the development of the mobile app and API that powers it.

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. :(



Boston Globe Article

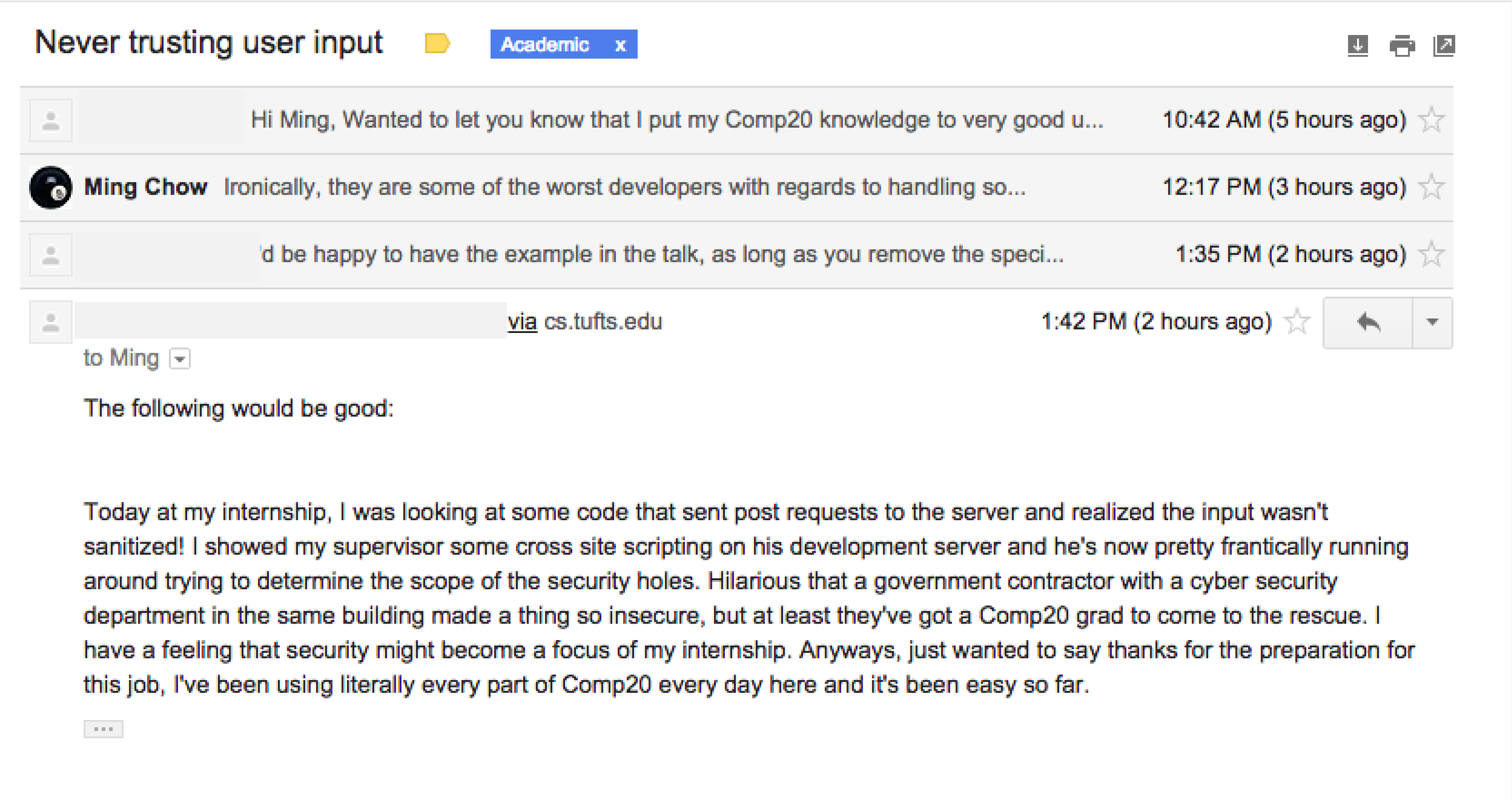
[redacted]

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)



[redacted] 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)

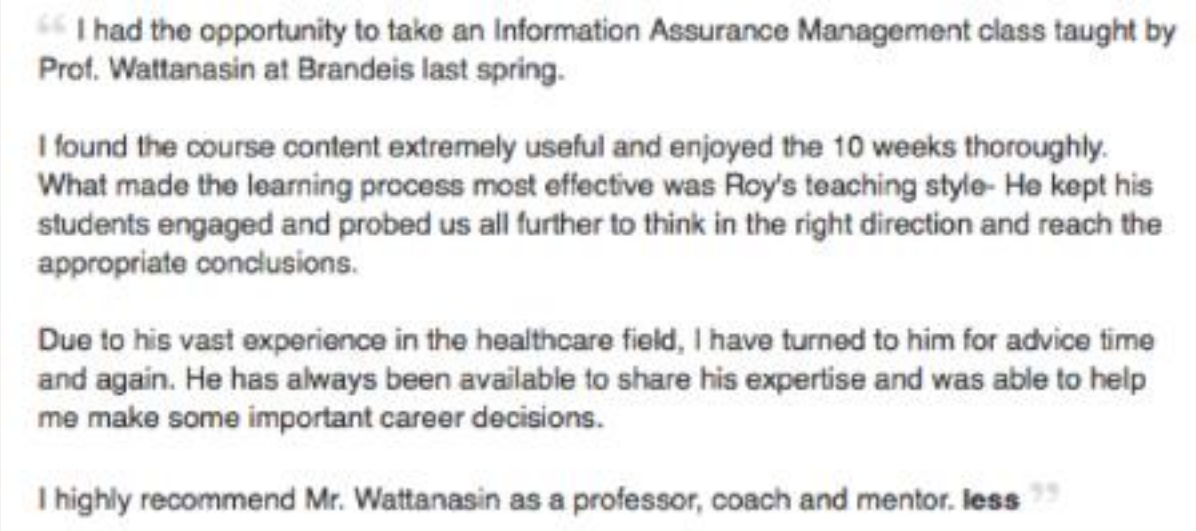
[redacted] 'd be happy to have the example in the talk, as long as you remove the speci... 1:35 PM (2 hours ago)

[redacted] 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.

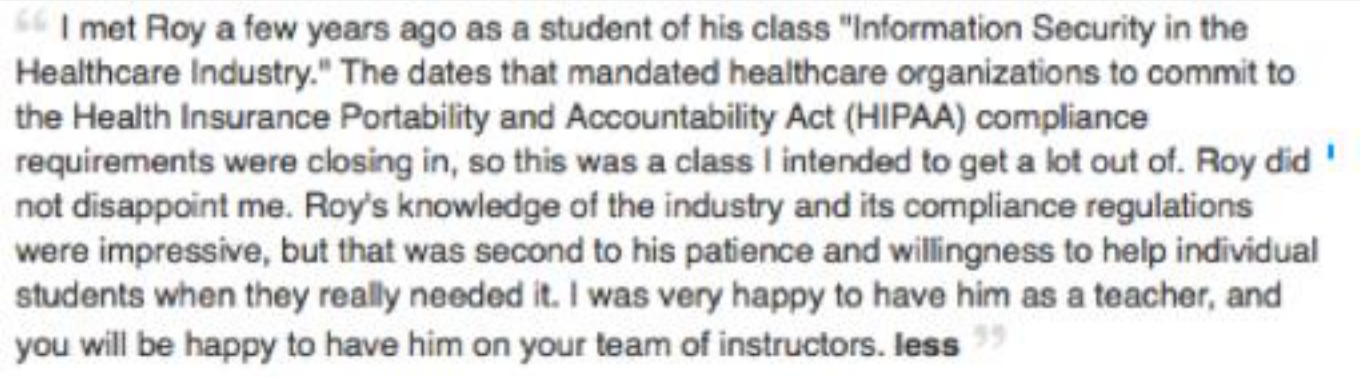


“ I had the opportunity to take an Information Assurance Management class taught by Prof. Wattanasin at Brandeis last spring.

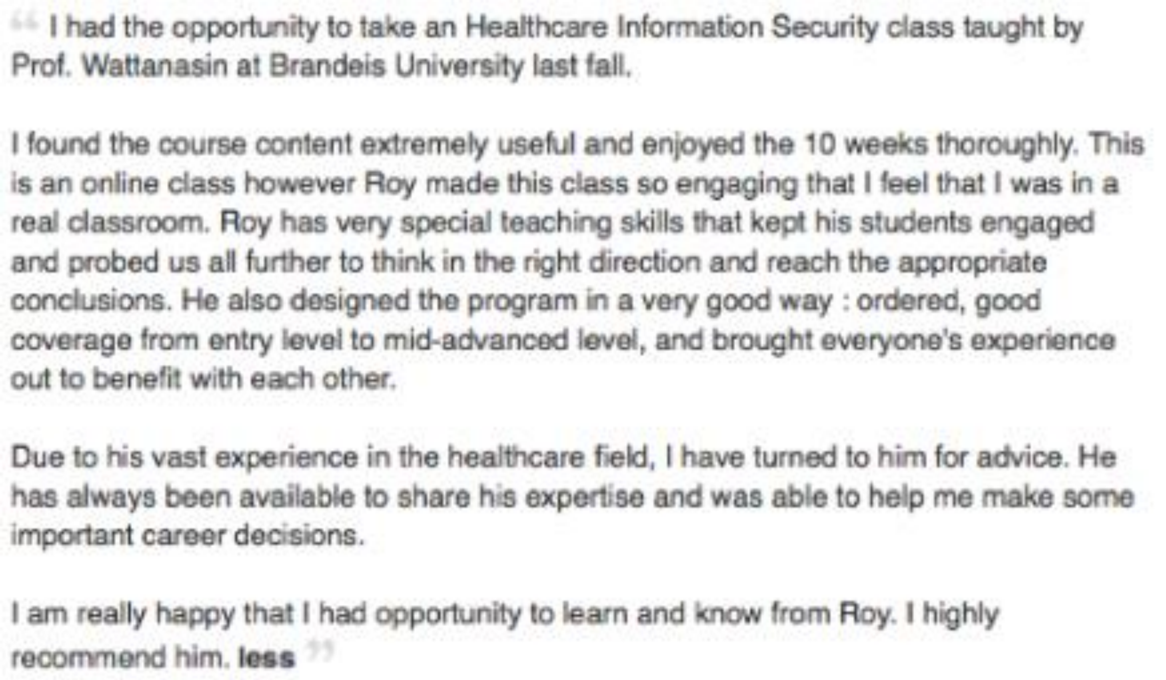
I found the course content extremely useful and enjoyed the 10 weeks thoroughly. What made the learning process most effective was Roy's teaching style- He kept his students engaged and probed us all further to think in the right direction and reach the appropriate conclusions.

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** ”



“ 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** ”

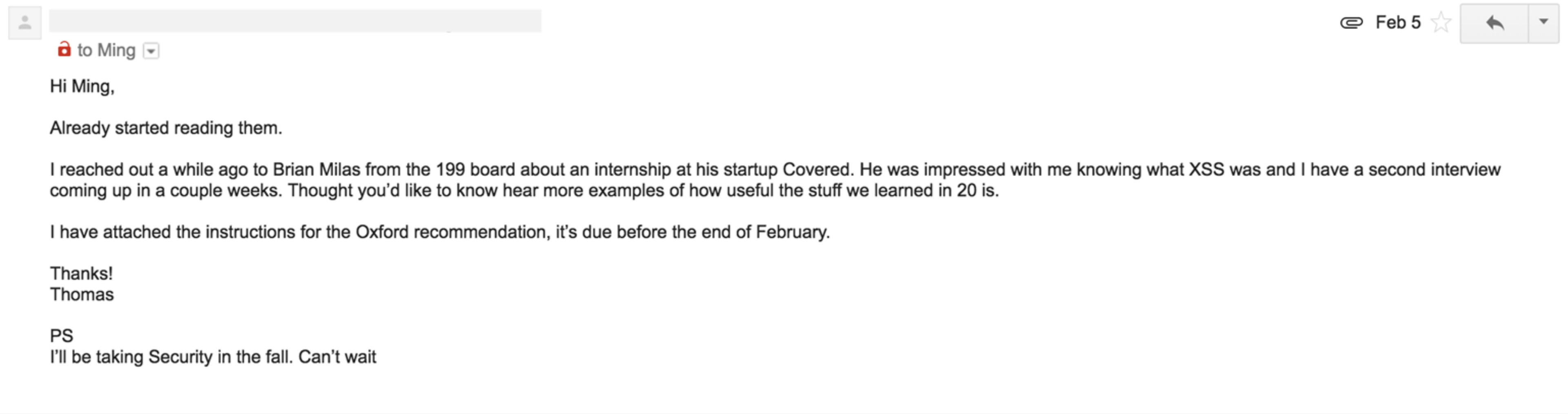


“ I had the opportunity to take an Healthcare Information Security class taught by Prof. Wattanasin at Brandeis University last fall.

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** ”



[redacted]

to Ming

Feb 5

Hi Ming,

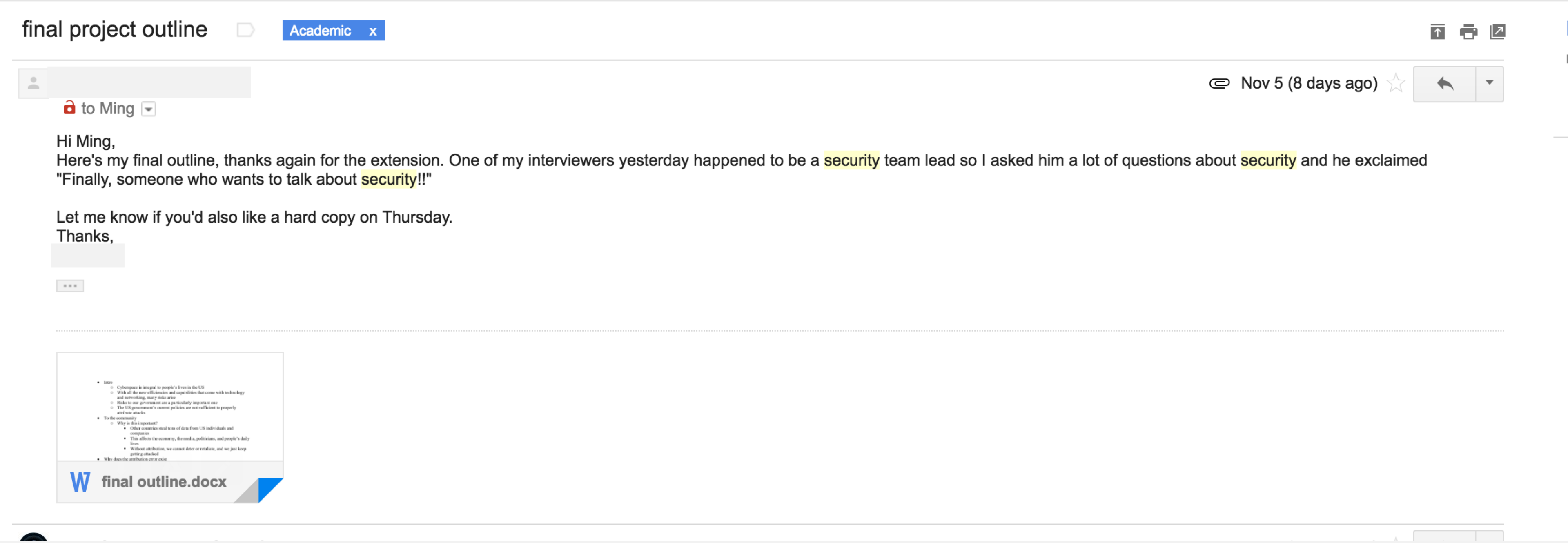
Already started reading them.

I reached out a while ago to Brian Milas from the 199 board about an internship at his startup Covered. He was impressed with me knowing what XSS was and I have a second interview coming up in a couple weeks. Thought you'd like to know hear more examples of how useful the stuff we learned in 20 is.

I have attached the instructions for the Oxford recommendation, it's due before the end of February.

Thanks!
Thomas

PS
I'll be taking Security in the fall. Can't wait



final project outline

[redacted]

to Ming

Nov 5 (8 days ago)

Hi Ming,
Here's my final outline, thanks again for the extension. One of my interviewers yesterday happened to be a security team lead so I asked him a lot of questions about security and he exclaimed "Finally, someone who wants to talk about security!!"

Let me know if you'd also like a hard copy on Thursday.
Thanks,
[redacted]

- Intro
  - Cyberspace is integral to people's lives in the US
  - With all the new efficiencies and capabilities that come with technology and networking, many risks arise
  - Risks to our government are a particularly important one
  - The US government's current policies are not sufficient to properly attribute attacks
- To the community
  - Why is this important?
    - Other countries steal tons of data from US individuals and companies
    - This affects the economy, the media, politicians, and people's daily lives
    - Without attribution, we cannot deter or retaliate, and we just keep getting attacked
- Why does the attribution error exist

final outline.docx

THANK YOU

Questions ?

Ming Chow (@0xmchow, mchow@cs.tufts.edu)
Roy Wattanasin (@wr0, websecr@gmail.com)

RESOURCES AND REFERENCES

- “[HOPE X] How to Prevent Security Afterthought Syndrome” https://www.youtube.com/watch?v=iLiQqii0c9E
- Zatko, Sarah. "Rethinking the Role of Security in Undergraduate Education." IEEE Security & Privacy 14.2 (2016): 73-78.
- http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/?single_page=true
- http://www.theatlantic.com/technology/archive/2015/12/the-moral-failure-of-computer-science/420012/
- http://www.massinsight.com/wp-content/uploads/2015/12/IPN-Conf-2015_Kurose.pdf
- http://www.darkreading.com/vulnerabilities---threats/top-us-undergraduate-computer-science-programs-skip-cybersecurity-classes/d/d-id/1325024
- https://tuftsdev.github.io/WebProgramming/notes/blangenberg.pdf
- http://www.scmagazine.com/updated-cybersecurity-being-overlooked-by-american-universities-report/article/488233/
- http://www.irongeek.com/i.php?page=videos/teaching-hacking-at-college-sam-bowne
- https://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-bownpdf
- 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
- https://www.defcon.org/html/defcon-22/dc-22-speakers.html#Erven
- https://cdn.ncees.org/wp-content/uploads/2012/11/SWE-Apr-2013.pdf
- http://www.techrepublic.com/article/cs-teachers-ramping-up-cybersecurity-education
- https://twitter.com/McGrewSecurity/status/583997726930694145
- https://twitter.com/tottenkoph/status/584009115887775744
- https://twitter.com/SwiftOnSecurity/status/592469306069266435
- https://twitter.com/tottenkoph/status/584014539932348417
- https://twitter.com/EvanMPeck/status/550069351601037313
- https://twitter.com/DrKevinFu/status/719836696834084864
- https://twitter.com/tottenkoph/status/584014539932348417
- https://twitter.com/chriseng/status/692509993023700993
- https://twitter.com/WeldPond/status/731133193303261187