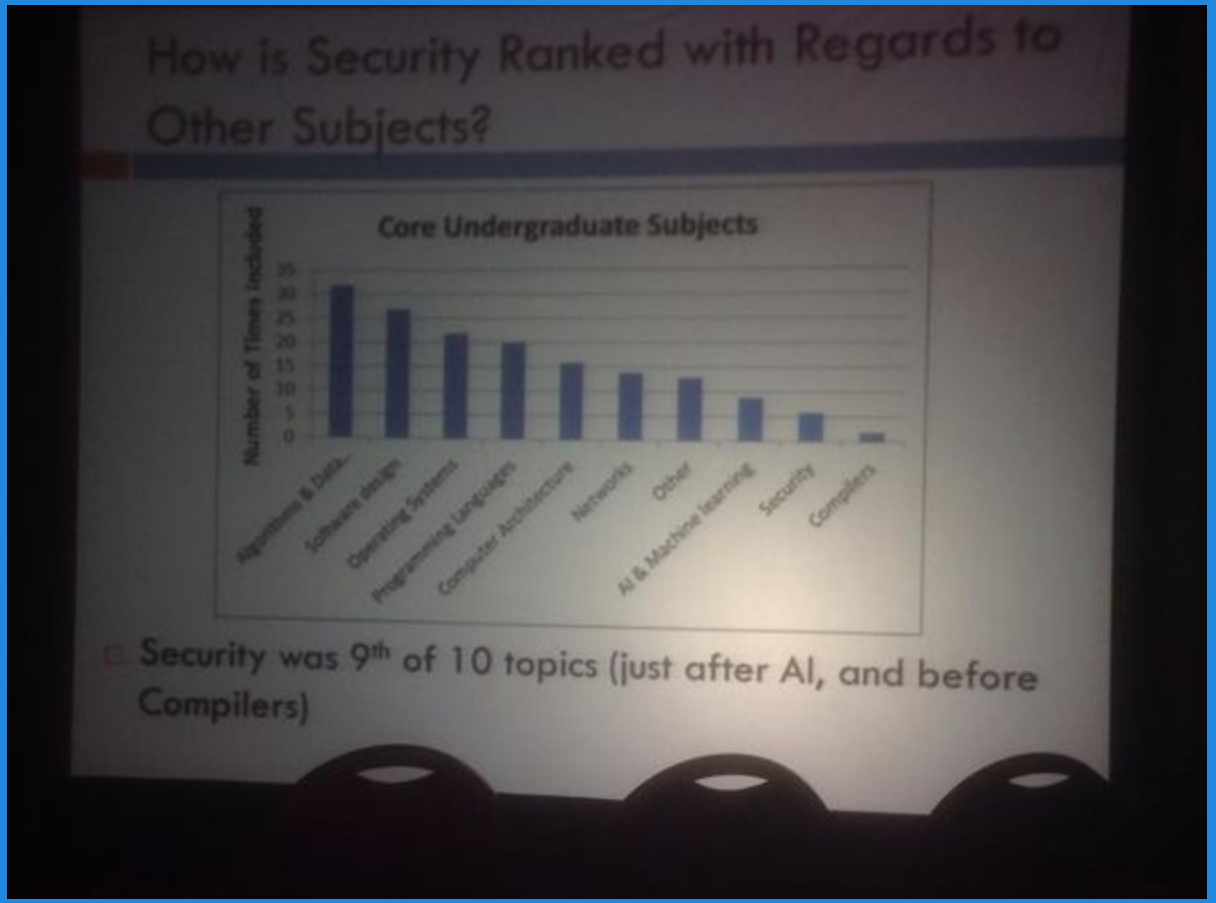
# The Blame Starts with Computer Science Curricula

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 academialand 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 valuable




@sambowne: Security's importance as rated by CS Dept. Chairs #HOPEX

# 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.

**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

# 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 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

**Evan Peck**
@EvanMPeck

Follow

@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

# The Need

- Make students think #whatcouldpossiblygowrong; violate invariants, preconditions
- “Thinking like a bad guy” 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

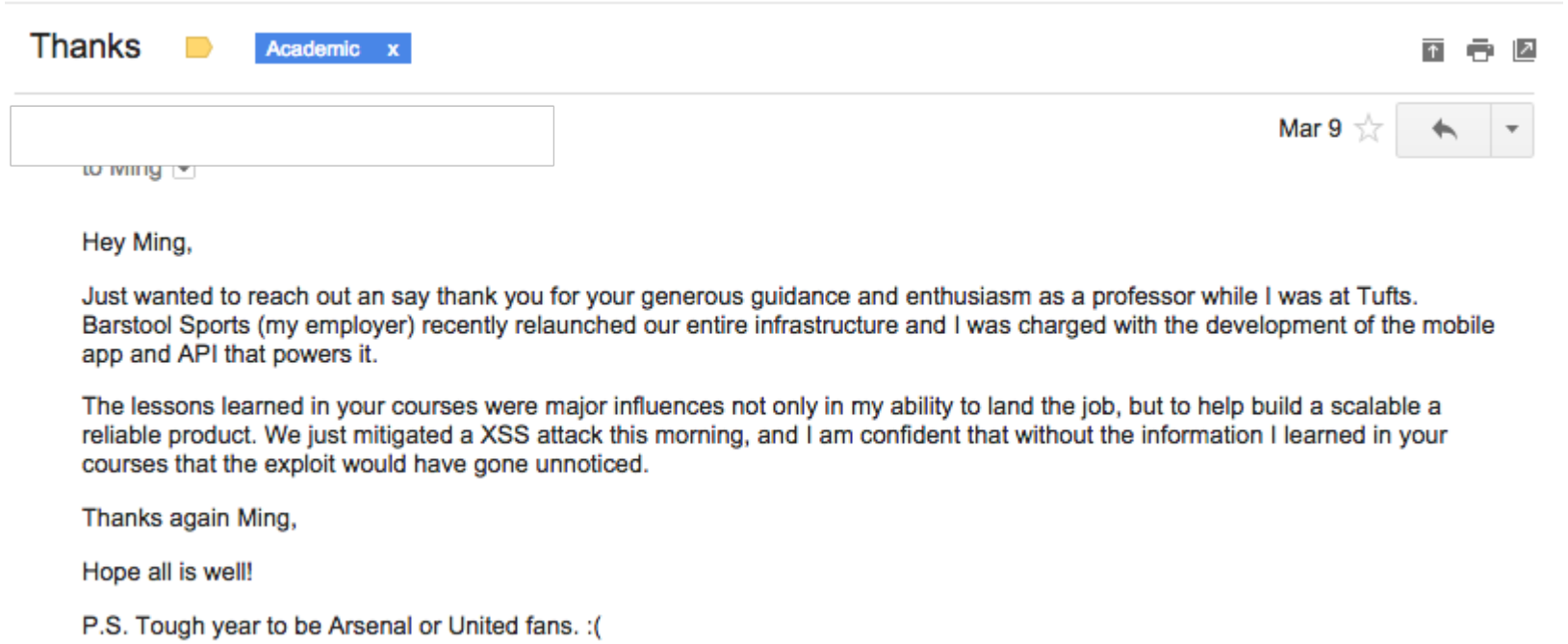
# Example 1: Data Structures

- 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: 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

# 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.

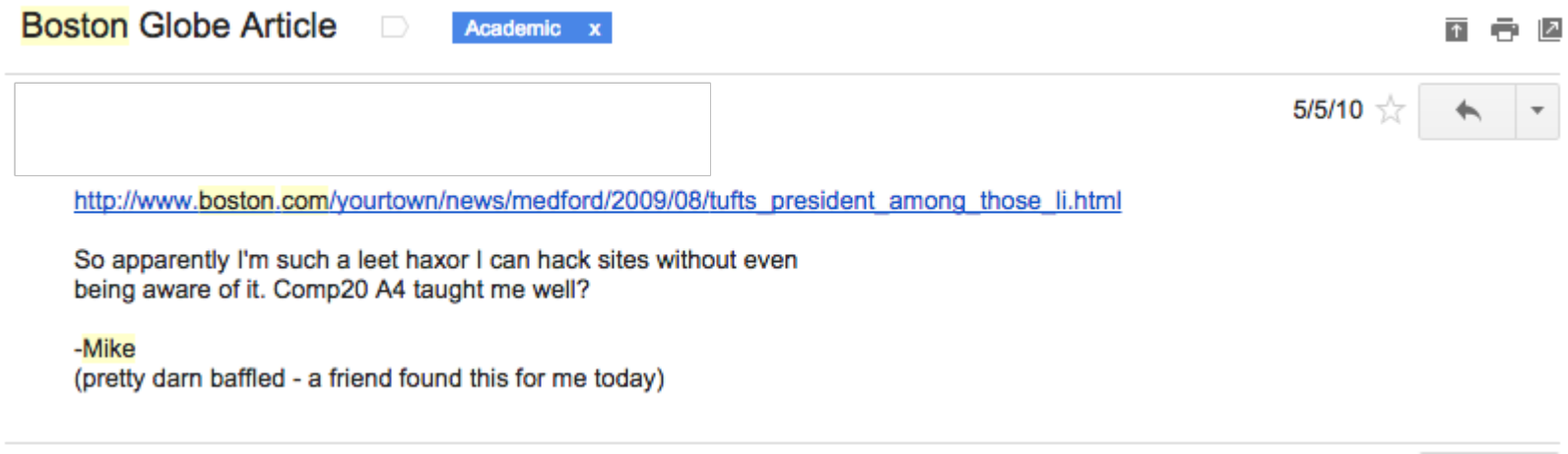
Thanks again Ming,

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



# 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

# Challenges Ahead

- *This is an area where we really need help*
- 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 bad guy
- Do not use only traditional teaching and learning techniques for courses
- Provide mentorship and networking opportunities
- What else?

# Resources and References

- 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
- https://www.defcon.org/html/defcon-22/dc-22-speakers.html#Erven
- 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-T9asfmPmD7uGIPxSjw&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
- http://searchsecurity.techtarget.com/opinion/McGraw-asks-whos-in-charge-of-medical-device-security