institute of CODING

bcs The Chartered Institute for IT

CyberSecurity in UK Higher ed.

James H. Davenport

18 October 2019

With Tom Crick, Alastair Irons, Tom Prickett

Who are we?

- British Computer Society: the Chartered Institute for IT. Mission “Make IT good for society”. See https://www.bcs.org/
- A learned and professional society, that also does accreditation: think ACM+ABET.
- The Institute of Coding: a joint Government and industry initiative to improve digital skills at university level (*not* necessarily in universities) in England: funded 2018-2020, led from Bath. See https://instituteofcoding.org/

There’s a dichotomy in demand

- Cybersecurity specialists: many estimates of the size of the shortage, but always huge
- The “generalist” programmer, designer etc. needs to know “some Cybersecurity” (recognised in ACM 2013 and BCS equivalent)
- Note that there’s a limit to the mess that a Cybersecurity expert can clean up retrospectively:

✓ check for buffer overflows and certain leakages

X fix bad design decisions (no framework to check for CSRF; unencrypted passwords, logging in the wrong place [Facebook!] etc.)

Educational Resources

Case Study: SQL Injection[1]

- A study of the 7 database textbooks used by 44 of the top 50 US departments.
- 5 had no mention of the SQL Injection, which is #1 in the OWASP “Top 10” list of weaknesses, and the cause of many current breaches
- Of the two that did, the discussion in the more popular one was seriously flawed

Educational Resources

Case Study: Java[2]

- Many Java textbooks go nowhere near security applications (credit card processing, username/ password handling etc.) despite their ubiquity
- The documentation of the APIs for the various packages tend to assume that the reader knows the basics, and wants to use *this* API.
- Hence the novice programmer is driven back to informal resources.

Informal Resources such as StackOverflow

- [3] Focused on functionality and “getting it working”
- Consider Cross-Site Request Forgery (CSRF)
- By default, Spring protects against this
- All the accepted answers to CSRF-related failures simply suggested disabling the check, with no comments on the downsides
- [4] took top 30 tutorials (via Google)
- 6 had SQL Injection weaknesses, 3 CSRF
- 820 instances of these fragments on Github, of which 117 were verified manually to be vulnerable
- These resources *need* to come with a health warning

UK Timeline for CyberSec[5]

UK Government Strategy	November 2011
Three workshops of industry academic and government – guidelines development	2013-June 2015
UK Government report Cybersecurity Skills, Business Perspectives and Government's Next Steps Report Released	March 2014
Council of Professors and Heads of Computing (CPHC) Identifies Cybersecurity as one the top 3 concerns in Computing	April 2014
Joint Development of White Paper from CPHC and The International Information Systems Security Certification Consortium (ISC)2	April –November 2014
Extended Cybersecurity Criteria included in BCS Accreditation Guidelines	June 2015

Timeline for implementation

Cybersecurity Principles Roadshow: March-April 2016

All institutions expected to be fully compliant: Sept 2020

Status (autumn 2018)

- 70 Higher Education Institutes visited under this regime
- 54 Higher Education Institutes compliant
- 12 Higher Education Institutes requiring long actions (for next visit)
- 4 Higher Education Institutes requiring short term actions

Curricula guidelines (2015)

Coverage is mandated of:

- Information and risk
- Threats and attacks
- Cybersecurity architecture and operations
- Secure systems and products
- Cybersecurity management.

In the light of our findings, where should this go?

How to teach?

[6] suggests three ways:

1) Adding a course in software security to an existing curriculum;
2) Adding specialized security courses as a track to an existing curriculum;
3) Integrating security into every [relevant] course in the curriculum.

In the light of “everyone”, (2) by itself won’t do. The author prefers a mix of (1) and (3).

What next for accreditation??

- Check appropriateness of books (or how deficiencies are handled). Shouldn’t be necessary, but see SQL and [1]
- Check students’ attitudes to informal resources
- ?? Insist that there’s some practical Cybersecurity work ??
  - implementing a password system
  - Hacker curriculum
  - Digital Forensic investigations
  - Apply security standards to a practical task
  - etc

Any questions?

References

[1] Cynthia Taylor and Saheel Sakharkar. ';DROP TABLE textbooks; — An Argument for SQL Injection Coverage in Database Textbooks. In Proc. of SIGCSE 2019, pages 191-197, 2019.

[2] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. Arango Argoty. Secure coding practices in Java: Challenges and vulnerabilities. In IEEE/ACM 40th Int. Conf. on Software Engineering, pages 372-383, 2018.

[3] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl. Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security. In 38th IEEE Symposium on Security and Privacy, pages 121-136, 2017.

[4] T. Unruh, B. Shastry, M. Skoruppa, F. Maggi, K. Rieck, J.-P. Seifert, and F. Yamaguchi. Leveraging Flawed Tutorials for Seeding Large-Scale Web Vulnerability Discovery. In Proc. of 11th USENIX Workshop on Offensive Technologies (WOOT 2017), 2017.

[5] Alastair Irons, Nick Savage, Carsten Maple, Adrian Davies, and Lyndsay Turley. Cybersecurity in CS Degrees. *ITNow*, 58:56-57, 2016.

[6] O. Ezenwoye, Integrating Security into Computer Science Curriculum. Proc. FIE 2019.