Maintaining the Focus on Cybersecurity in UK Higher Education

Tom Crick[1], James H. Davenport[2], Alastair Irons[3], Sally Pearce[4] and Tom Prickett[5]

[1]Swansea University (thomas.crick@swansea.ac.uk)
[2]University of Bath (j.h.davenport@bath.ac.uk)
[3]Sunderland University (alastair.irons@sunderland.ac.uk)
[4]BCS, The Chartered Institute for IT (sally.pearce@bcs.uk)
[5]Northumbria University (tom.prickett@northumbria.ac.uk)

September 2019

In this article we explore some of the challenges facing university-level cybersecurity education in the UK, with a focus on the benefits of BCS degree accreditation…

Introduction

In August, a Harvard Business Review article [1] postulated that "*Every Computer Science Degree Should Require a Course in Cybersecurity*", provocatively stating that cybersecurity is eating the software world and arguing that systematically addressing the problem of security begins with educating software developers at scale. It is hard to disagree with the intent of this suggestion. Alongside organisations such as the UK's National Cyber Security Centre, the BCS has been promoting this position for a number of years through its accreditation and policy activities, and it is positive to see our concerns highlighted to a wider international audience. As our recent paper [2] argues, cybersecurity is too important to be left to specialists and thus should be seen as an essential component of computer science, software engineering, and many other IT-related degree programmes.

This article explores some of the challenges raised in our paper, related to the teaching of cybersecurity in UK universities, and provides a progress report regarding BCS efforts to promote the development of cybersecurity knowledge in accredited degree programmes.

Some Challenges

Resources

Databases form a core part of all computer science degree programmes. From a security perspective, SQL injection is still a major concern: ranked number one in the Open Web Application Security Project (OWASP) Top 10, and has been in the Top 10 since at least 2003. A range of common undergraduate database textbooks were analysed as part of a 2019 project [3], showing that injection attacks are generally not covered; small wonder it continues to be an issue in the wild.

Our related research from 2017 [4] shows that Java is still the most commonly taught introductory programming language at UK universities. But many Java books do not cover security in depth, applied to real-world contexts. If you want to know more about security,

you need to delve into the documentation of the package/API being used, as well as a range of unofficial or informal resources. Recent work [5] analysed 503 posts from Stack Overflow, with 53% focusing on Java's Spring Framework; of these, 45% were related to authentication. A key example to illustrate our concerns was that, by default, Spring enables protection against cross-site request forgery (CSRF). But all the accepted answers to CSRF-related failures simply suggested disabling the check. There were no negative comments or concerns raised about this, and indeed a typical response was "*Adding* `csrf().disable()` *solved the issue!!! I have no idea why it was enabled by default".* Needless to say, disabling security mechanisms to remove frustrating errors is not a strong foundation for developing secure software and systems.

A further study [6] considered 30 popular web programming tutorials and found six had SQL injection weaknesses, and three had cross-site scripting (XSS, number seven in OWASP's Top Ten) weaknesses. A follow-up search on GitHub found 820 instances of these fragments, of which 117 were verified manually to be vulnerable — 80% of which were open to SQL injection attack.

Faculty

We clearly need high quality learning and teaching in UK universities, especially in technical domains. But cybersecurity skills are in short supply, in both industry and academia. The demand for cybersecurity skills in industry makes it increasingly difficult for academia to attract academics with current knowledge, practical experience, research background and academic aspirations. As universities expand their cybersecurity provision, it is not uncommon to find multiple jobs across the career path advertised at the same time; however, this displaces the faculty problem rather than solving it.

The Role of BCS Accreditation

Enough of the challenges — what is being done about them? Industry, higher education, government and the relevant professional bodies have collaborated on the development of a set of guidelines which aims to benefit education and wider society, as discussed in a previous issue of ITNow [7]. These guidelines -- "*Cybersecurity Principles and Learning Outcomes*" -- published in June 2015, established a baseline of common knowledge and example learning outcome domains for cybersecurity within degree programmes, as well as guidance on embedding the concepts.

Since 2015, the BCS has been expecting accredited degrees to be compliant with the cybersecurity guidelines. Universities are visited on a quinquennial basis, but a full cycle of accreditation visits has not yet taken place following this change in requirements. However, we have observed that the majority of visited institutions have now either adjusted their curricula to extend the coverage of cybersecurity or have a plan in place to do so, with a minority requiring encouragement to do so.

From the start of the Autumn 2015 term, up to and including the Summer 2019 term, the BCS has carried out 82 accreditation visits, including five international visits (two in South Africa and one each in Brunei, Cyprus, and Ireland). The BCS identified that action was required to

address concerns related to cybersecurity at 23 institutions; thus, 59 institutions were already delivering cybersecurity in line with the BCS expectations.

Long-term actions ('*At Threshold*' judgements) were expected from 14 institutions (six in 2015/16, three in 2016/17, and five in 2018/19); 13 of these judgments were across all programmes, while one was specifically against a generalist Masters-level programme. This indicates that the BCS will expect adjustments to have taken place before the next accreditation visit. It also acknowledged that adjustments had been made as part of periodic curriculum redesign processes; however, the adjusted programmes had not yet been delivered, so the evidence base was incomplete in terms of how cybersecurity was assessed.

Short term actions were thus required from nine institutions; the outcomes of these actions were as follows: (*i*) of the eleven undergraduate programmes involved, all were approved '*At Threshold*'; (*ii*) of the nine undergraduate programmes involved, eight were approved and one refused; (*iii*) of the five undergraduate programmes involved, all were approved '*At Threshold*'; and (*iv*) of the three undergraduate programmes involved, all were refused; and (v) a further five, which at the time of writing the outcome was not known. From a pedagogic perspective, good practice was identified at three universities by the following commendations:

"*The second-year project provides an opportunity for exploring security aspects in depth with an industrial use case.*"

"*Hacktivity and related learning and teaching approaches*"

"*Cyber Security Centre which permeates both the course and supports external links and opportunities for students.*"

Looking Ahead

It is now clear that a BCS-accredited degree programme will include cybersecurity knowledge, with the BCS focused on improving the UK's cybersecurity skills capability. However, there are challenges ahead in terms of improving the resources upon which degree provision depends and developing the cybersecurity skills base within universities.

As a final point, is it sufficient to leave cybersecurity to computer scientists and software engineers? Should it be the sole preserve of those who work with technology? Or like similar discussions regarding artificial intelligence, how can we ensure wider engagement and responsibility? We hope this is a conversation that will continue to develop and evolve.

References

[1] J. Cable. *Every Computer Science Degree Should Require a Course in Cybersecurity*. Harvard Business Review, 27 August 2019. https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity

[2] T. Crick, J. Davenport, A. Irons, and T. Prickett. *A UK Case Study on Cybersecurity Education and Accreditation*. In Proc. of IEEE Frontiers in Education Conf., 2019. https://arxiv.org/abs/1906.09584

[3] C. Taylor and S. Sakharkar. `'; DROP TABLE textbooks;-` *An Argument for SQL Injection Coverage in Database Textbooks*. In Proc. of ACM SIGCSE 2019, p191–197, 2019.

[4] E. Murphy, T. Crick, and J. H. Davenport. *An Analysis of Introductory Programming Courses at UK Universities*. The Art, Science, and Engineering of Programming, vol. 1(2), no. 18, p1–23, 2017.

[5] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. Arango Argoty. *Secure coding practices in Java: Challenges and vulnerabilities*. In Proc. of 40th IEEE/ACM Int. Conf. on Software Engineering, p372– 383, 2018.

[6] 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, 2017.

[7] A. Irons, N. Savage, C. Maple, A. Davies, and L. Turley. *Cybersecurity in CS Degrees*. ITNow, vol 58, p56–57, 2016.