

A Comprehensive review of Security and Privacy teaching in Informatics

David Aspinall

1st March 2016

Background

Teaching of security topics in the undergraduate computer science curriculum is now recognised as being vital for all students. Our students go on to work in companies that manage valuable data or personal information at large scale, and the old view that “security is someone else’s problem” no longer holds water. Security (and privacy) understanding needs to be designed into socio-technical systems from the start. Regulation is increasing.

The **ACM 2013 Computing Curricula**¹ introduced *Information Assurance and Security* (IAS) as one of two new Knowledge Areas and has extended security related topics in most other Knowledge Areas, stating that IAS is “unique . . . the topics are pervasive throughout other Knowledge Areas”. There is a recommended total of 74.5 *core* lecture hours in the curriculum for IAS-related topics.

As expected, CS2013 was an influence on BCS who are now also raising the importance of teaching security, see their 2015 press release *Cybersecurity to Become Core Component of UK Computing Degrees*². Through CPHC, BCS are organising a series of meetings across the UK this year to consider curricula changes (I am attending one in Edinburgh on 7th March). In our last accreditation, we were encouraged to increase the security component of our teaching.

In my view, although it is not yet a strong focus of new curricula, we need to also need to improve teaching of (computer science aspects of) **privacy**. There is a connection to ethics and professional issues (which BCS have also pointed out that we are weak on), although there are also important technical aspects (e.g., information leakage, metadata). Privacy thinking is becoming an important part of cybersecurity design.

Proposal

I propose to convene a small working group to:

1. **Survey** where security and privacy topics in our current courses are taught, or where there is an opportunity for modifying or extending courses to meet the requirements of the new curricula being discussed. The focus will especially be on Years 1 and 2, where (as far as I know) there is little coverage at the moment.
2. **Propose recommendations** to BoS for curriculum modification, comparing our current status quo with emerging best practice. It may be possible to “fast track” some changes (e.g., adding new lectures taught by security faculty, or sections to existing lectures) to bring them online for 16/17, without changing DPTs, although formal (or more extensive modification) will require longer.

I will invite people to join (or give advice to) the WG including at least the security teaching staff (Arapinis, Kiayias, Vaniea), current course organisers for Y1 and Y2 (or nominees), HoT and those responsible for accreditation and TQA (previously: Murray, Longley). I expect to convene a small number of meetings from late March-June. Recommendations and progress will be reported to the first autumn meeting of the BoS in the next session.

¹<http://www.acm.org/education/CS2013-final-report.pdf>

²<http://www.bcs.org/content/ConMediaFile/26056>