Information Security in the undergraduate curriculum

Chris Mitchell
Royal Holloway, University of London
www.isg.rhul.ac.uk/~cjm

Background I

- Some years ago, computer hacking was mainly done for fun.
- Today, organised crime is driving serious attacks on corporate and end user systems; a huge variety of malicious software and attack techniques now available.
- Systems many of us rely on in our daily lives are under constant attack by malicious criminal gangs.

Background II

- IT industry has recognised the paramount importance of restoring trust and security to today's computing environments.
- E.g., in 2003, Microsoft formed the Trustworthy Computing Academic Advisory Board, to advise on security, privacy and reliability issues – RHUL is unique amongst UK universities in being represented on this board.

Background III

- Huge risks to personal and corporate data have also been recognised by the UK government.
- Aug 2007: House of Lords (UK Government) Science and Technology Committee Report on Personal Internet Security points out:
  - The Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's 'bad guys' belong to organised crime groups, are highly skilful, specialised, and focused on profit.

Background IV

- 2008 White Paper on Secure Software Development, published by UK Government's Technology Strategy Board-supported *Cyber Security Knowledge Transfer Network*, states:
  - It is evident that many of the [IT security] problems [that] we [have] encountered would have been mitigated and sometimes removed completely if the software on ICT systems had been developed with fewer software flaws and better security design.
  - This is a neglected area in the UK in that there are some very good examples of best practice but these are few and desperately need to be shared so all can benefit.

Background V

- In June 2009, the Prime Minister presented to Parliament a Cyber Security Strategy for the United Kingdom.
- Key theme of which is to ‘improve knowledge and capabilities’ in the area.

Masters-level education I

- All organisations are now being forced to take security and privacy threats seriously.
- Yet these efforts have been hampered by serious shortages of suitable staff.
- To date, the role of universities in addressing this pressing need has primarily been in underlying research and delivering masters courses aimed at developing information security experts.

Masters-level education II

- Such specialists are, of course, essential, and these courses play a vital role in providing staff for information security departments of companies and government departments worldwide.
- Royal Holloway continues to play its part, with its Information Security masters programme which, when launched in 1992, was the first programme of its kind.

New directions I

- However, it is becoming clear that educating a small core of security specialists is not enough.
- All IT staff need to be aware of the huge security risks arising from everyday decisions, including when writing software, procuring and configuring products, or integrating complex IT systems.

New directions II

- A huge proportion of threats to our information processing infrastructure arises from vulnerabilities introduced into software through programming or configuration shortcomings.
- So **undergraduate computing education** must play a key role.

BSc Computer Science (Information Security)

- At Royal Holloway we have taken on this challenge by introducing a ground-breaking undergraduate programme in Computer Science (started in 2007).
- This degree programme is designed to help address the urgent need for greater security awareness
- Huge opportunities exist for security-literate software developers, system administrators, and IT managers.

Content I

- One key element of this new degree programme is a course on secure software, the development of which was funded by Microsoft, reflecting their belief in the importance of this topic.
- The first cohort of students from this programme will graduate in 2010, and will enter a job market where there is an ever-growing need for security-aware staff.

Content II

- Students in the programme take a ‘standard’ Computer Science first year.
- The 2nd year is 75% standard Computer Science and 25% Information Security, including:
  - a general introduction to all Information Security topics; and
  - a group software development project on a security-related subject.

Content III

- The 3rd and final undergraduate year is 50% Computer Science and 50% Information Security.
- Topics include:
  - software security;
  - trusted computing;
  - a major individual project on a security topic.

The future

- We can expect to see rapid growth in degree programmes offering a more substantial security component.
- For the moment, the numbers of graduates with a high degree of security-awareness is small, and the prospects for such graduates seem rosy indeed.

Questions?

- Please contact me at:

  c.mitchell@rhul.ac.uk