Information Security Research at UCL

M. Angela Sasse

University College London, UK

Research Institute for Science of Cyber Security

www.ucl.ac.uk/cybersecurity/

Academic Centre of Excellence for Cyber Security Research

http://sec.cs.ucl.ac.uk/ace_csr/

Background: UK Initiative in Cyber Security

- 2011: UK National Cyber Security Strategy
- 11 Academic Centres of Excellence in Cyber Security Research (ACE-CSR)
    - Belfast, Birmingham, Bristol, Cambridge, Lancaster, Imperial College, Newcastle, Oxford, Royal Holloway, Southampton, UCL
- Studentships from GCHQ – 10 in 2012, ???
- 2 Centres for Doctoral Training for Cyber Security Research

Global Centre for Cyber Security Capacity-Building

- FCO-funded
- Find out “what works, where, under which circumstances” in cyber security, as a basis for enhancing capacity and collaboration
- Led by Prof. Sadie Creese
- Multi-disciplinary – based at Martin School at Oxford
- Bringing together researchers and practitioners, range of organisations

Research Institutes

- 2 Research Institutes funded by EPSRC/GCHQ/BIS
- Science of Cyber Security (coordinated by UCL)
- Automated Program Generation & Verification (coordinated by Imperial)
- Call for 3rd one imminent

Research Institute in Science of Cyber Security

- Funded by GCHQ in partnership with the Research Councils' Global Uncertainties Programme (RCUK) and the Department for Business Innovation and Skills (BIS)
- £3.8 M over 3.5 years
- Virtual Institute
  - 4 projects involving 7 universities
  - coordination activity (Research Director Prof. Angela Sasse)
- Advisory Board

Goal of the RI

- allow leading academics in the field of Cyber Security from across the UK
  - to work together
  - to connect them with the collective expertise of
    - industry security experts, and
    - international researchers
- most emphatically multi-disciplinary research
- *Science* of Cyber Security

Here comes the science bit …

1. *"How secure is my organisation?"*
2. *"How do we make better security decisions?"*

- Evidence-based:
  - – Establish a map of substantive, empirically based knowledge, and fill the gaps
  - – Identify/develop a set of suitable methods for cyber security research, and for companies
- Shift from craft to evidence-based security

Key questions

1. What risks are we dealing with?
2. What is the data we need? How do we persuade industry to give us access to the data we need?
3. How should we measure? How do we make sure we use these measurements correctly?
4. How do we model risks and countermeasures? How do we evaluate and improve the models?

Obstacles to collaboration within RIs

- Time-frame and format of projects
- The usual inter-disciplinary problems
- Incentives for competition larger than incentives for collaboration?
- No expectation of continuity (?)

Industrial Collaboration

- Difficult to impossible for RIs because of contracts imposed
  - uncertainty and delay puts collaborators off
  - (potential) sensitivity of research makes industrial collaborators reluctant to give access
- What's left?
- Direct contracts (so company imposes constraints
- Faculty awards
  - Nice: prestige, meeting with other faculty members
  - Don't pass the Linda-Evangelista-of-Research test, teaching oriented

Collaboration outside RI

- Manifold, strong collaboration with US – but difficult to get genuine joint funding
- EU funding – many opportunities, but administrative overhead puts many off
- Programmes with developing, BRICs countries – tend to be one-off programmes, no continuity