Input to:
Horizon 2020 Workshop

Chris Mitchell

Information Security Group
Royal Holloway, University of London

www.chrismitchell.net

What is the question?

- Considering what research to fund is probably not the right question.
- Need to start by considering what the big problems are in cyber security.
- Then look at what needs to be done to fix them.
- If part of the answer is ‘more research needed on x’ then fund such research, but also need to do the other things.
- Indeed, more research is likely to be only a very small part of the picture ...

Background

- Look at one problem I see as being a big deal ...
- We have plenty of good security technology, including for example:
  - a wide range of internationally standardised cryptographic algorithms, many of which have mathematical security proofs;
  - a broad portfolio of internationally standardised general purpose security protocols, again many of which have security proofs;
  - an established set of secure system development methods and tools, use of which should help to minimise risks of security vulnerabilities arising from poor design and implementation of systems;
  - experience in some industry sectors (notably the PC sector) painfully derived from having to clean up the mess from not taking notice of the need for security in the first place.

Falling through the cracks ...

- Despite this rich base of security technology:
  - systems are very commonly designed which do not use the state of the art security technology (a big gap);
  - recent experience suggests that implementers are doing a very bad job of implementing security-relevant protocols, even if they are well-specified and well-designed (a yawning chasm);
  - more generally, developers are simply not building with security in mind (whether or not security functionality is explcitily involved).

Fixing the problems

- What can be done to close these gaps?
  - **Scope the problem**: look at current products and systems and test them – e.g. US work on looking a security of cars.
  - **Create development aids**: develop public domain tools, systems, and processes to enable system designers to make better systems and test them.
  - **Educate industry**: develop better undergraduate curricula in engineering and computing; run education events for practitioners.
  - **Make it happen**: develop standards, regulations, codes of practice ...

How can we do things better?

- Find better ways of exploiting the understanding of major security problems that exists in academia.
- Don’t just fund large research projects … look at ways of engaging academia in development of guidelines, codes of practice, free tools, etc.
- It needs money, but perhaps small beer compared to other costs?
- Potentially major benefits in terms of informing future research.