THE
ROYAL
SOCIETY

Emerging cybersecurity research challenges

4 November 2013

1 Privacy and online surveillance

Current debates about surveillance and protecting the privacy of the common citizen create an opportunity for the Royal Society to provide independent and credible analysis of relevant technological aspects of the debate. Specific areas of interest include (but are not limited to) data mining, data analysis, context analysis, as well as the legal frameworks associated with these activities.

2 Privacy and security in its wider socioeconomic context

There is an opportunity to explore new behavioural and economic approaches and incentive structures to cybersecurity so that privacy by design and security by design can become technological norms. Privacy and security are often neglected or even seen as undermining business models. Yet connectivity is becoming pervasive. Everything from automobiles to power stations to healthcare will be online and one firm's marketing mechanisms may be another firm's critical security vulnerability. It will become impossible to define privacy and security separately for each device, each small area of operations or each process. Privacy and security should become embedded in technologies by default so that users will not have to learn new protocols for each specific product or service, but many business pressures will cause systems to fall short of this ideal. It may therefore be of value to develop mechanisms that can alert users to security problems and give them more situational awareness.

3 Biologically-inspired cybersecurity and the sustainability of the internet

Analogies between computer viruses and biological pathogens create the opportunity for cybersecurity to learn from the dynamics of certain biological systems, such as immune systems and epidemics. For example, one area of particular interest concerns Moving Target Defence whereby systems are built so that they can still operate effectively even in a compromised environment. Continuing the analogy, cyberspace faces sustainability challenges that may be similar to those facing the natural environment. Someone who connects an insecure machine to the Internet is a bit like someone who cooks their food on a coal fire; they impose costs on others. This creates the opportunity to better understand the nature and dynamics of the cyber ecosystem through environmental models of cyberspace. Creating new threat and mitigation models will be an important aspect to this field.

4 Extracting high levels of information from data with assured levels of privacy and trust

Many companies and government departments hope to improve their services by analysing massive sets of personal data, such as medical records, shopping baskets and bank transactions. Privacy and trust then become major issues with the increasing emergence of Big Data analytics, for example. To preserve privacy, organisations often promise to anonymise the data. Yet, as the Royal Society highlighted in its recent report, *Science as an open enterprise*, this is very difficult to do effectively, and the growth in the amount of data available online makes it ever easier to re-identify personal information from which the obvious identifiers, such as name and date of birth, have been scrubbed. Doing anonymity better is a research problem that may have urgent practical applications.

5 Cyberphysical systems

The rise of smart grids, networked process control systems and the internet of things more broadly pose major security challenges to protect this infrastructure. These systems are different from prevailing information technologies in many ways. They are built for longevity that exceeds that of an average IT system; many systems are built to last more than 20 years. These systems are designed with an emphasis on physical operations and often include a significant legacy component. Research is necessary to define security features, understand threats and design mitigations for this environment.

6 International collaboration

This project is keen to consider the potential for international collaboration with UK researchers on these research challenges whilst recognising different funding and collaborative models involved in working with researchers in the EU versus the USA and elsewhere.

7 Commercialisation

The commercial exploitation of academic research is often claimed to be inadequate, yet there are clusters of successful spin-out companies in various parts of the UK. There remains strong interest and emerging opportunities to develop this commercial potential whilst ensuring that curiosity driven research is not compromised.

8 Responsible research and innovation

Growing public concerns about both privacy and fraud mean that a debate about cybersecurity research is timely. Debates about technology frequently react to products and services as they enter the marketplace. This is often too late. An inclusive and reflective debate could explore the ethical and legal challenges facing researchers in a field which is often at the centre of challenges over control of technologies, markets and personal information. Specific challenges include the management of the dual use potential of cybersecurity research and the disclosure of security flaws during the conduct of research.