The All Party Parliamentary Engineering Group

07 November 2017

Hacking – can the huge data breaches be prevented?

Discussion over lunch in the Cholmondeley Room, House of Lords

Chair – Professor the Lord Broers

Speakers:

- Professor Andy Hopper CBE, Professor of Computer Technology and Head of the Department of Computer Science and Technology at the University of Cambridge
- Dr Alistair Beresford, Reader in Computer Security at the Computer Laboratory and an Official Fellow at Queen's College, University of Cambridge
- James Hatch, Director of Cyber Services at BAE Systems Applied Intelligence

---

Introduction

Lord Broers, Chairman of the group, began by thanking everyone for attending, then introduced the three speakers.

Professor Andy Hopper CBE's research interests include computer networking, pervasive and sensor-driven computing, and using computers to ensure sustainability of the planet. He has pursued academic and industrial careers simultaneously, working both at the Computer Laboratory and the Department of Engineering at Cambridge and as co-founder of thirteen spin-outs and start-ups. In recent years the companies he co-founded have received five Queen's Awards for Enterprise. He is Chairman of RealVNC Group. Professor Hopper is a Fellow of the Royal Academy of Engineering and of the Royal Society, and former president of the Institution of Engineering and Technology. He was made a CBE for services to the computer industry in 2007, and received the Royal Society Bakerian Medal this year. He has been elected Treasurer of the Royal Society from December 2017.

Dr Alistair Beresford's work examines the security and privacy of large-scale distributed computer systems. Within this broad area, he is currently interested in the security and privacy of networked mobile devices, such as smartphones, tablets and laptops. He examines the security of the devices themselves as well as the security and privacy problems induced by the interaction between mobile devices and cloud-based Internet services. He approaches this through the critical evaluation of existing products, by designing and building novel prototype technologies, and by measuring human behaviour.

James Hatch leads BAE Systems advisory and technical services in cyber security across Europe. This business covers all industry sectors but with a particularly strong presence in financial services, telecommunications, energy and central government. The services provided cover security strategy, assessment, improvement and integration. As well as his advisory work, James has direct experience of information security management in financial services and central government. He has also led

major business change projects in technology heavy domains, including setting up the Telecom Regulatory Authority of Egypt, re-engineering the management information of a major mortgage lender and modernising a state-owned financial services business.

Professor Andy Hopper CBE

Professor Hopper had recently released a report on hacking and the associated security risks. To produce this report he had to work with individuals from different fields in order to produce recommendations on (the prevention of) hacking and its implications.

There were three different groups working on the report: academics, industry experts and security servicemen. This created issues because the academics and industry experts would come up with a solution, only then for the security services to say that it would not work without being at liberty to say why (because it was classified information).

Everyone and everything is moving online which means that everything has a digital presence. From your social media presence to the digital presence of the trees on the street that will be logged in a computer somewhere. This means that the security threat grows ever more serious: as everything becomes digitally integrated, so everything becomes 'hackable'.

Professor Hopper went on to list some of the recommendations of the report. These included increased security measures, however these would need to be enforced and the question remains open as to who. He added that Government legislation needs to adapt to the changing technological landscape.

Dr Alastair Beresford

Dr Bereford began by talking about updates – individuals need to make sure that they update their software, which he terms 'patching'. He made the important point that every single piece of software has some kind of problem with it. There is always a back door into the system- its creators might not know it at the time, but it is there. It is through this back door that hackers can get into your computer and use it for illicit means. It is not only the software contained in the physical device, but also the data kept in cloud-based services, that are at risk.

There need to be continual software updates in order to patch up the holes in the software which allow breeches. The problem is that the economic incentives are not aligned with this necessity. In a software or tech company, you have two choices. On the one hand, you could use your tech engineers to fix the existing problems with your current device and associated software, which will not increase revenue. Alternatively, the company could allocate the resources towards making sure the next device is better which will bring in a new source of revenue and patch up the problem. Therefore it is much more likely that the tech firm will do the latter. This is dangerous for those people who don't buy the second device. Some software is very effective and so doesn't need much patching; this is because it uses end-to-end encryption, which is used by things like Whatsapp.

Dr Beresford suggested that this is an issue that should involve the Government, as we might need to have legislation that obligates companies to patch up software so that individuals are not left vulnerable to cyber-attacks.

James Hatch – BAE Systems

James Hatch gave the business perspective on the hacking problem, which he stressed was an important point of view to consider.

Security systems should no longer be thought of as a national issue because security threats are no longer national. They have gone beyond geography and therefore regulation needs to do the same. To some extent this has happening. If you get mugged on the street, you go to the local police. However, when something goes wrong with your technology, you call the company responsible rather than the police. Generally these companies are very international and so we can see the shift away from the national to the international.

Part of James Hatch's job is to contain major hacking breeches or attempted breeches. The biggest marker of success, he argued, was to make sure that the hacking events don't get wide coverage. If people don't know it happened then he has done his job right.

Q&A

Q - Is it possible to be anonymous on the internet?

A – Dr Beresford: Dr Beresford stated that he thought people believed that they are far more anonymous on the internet than they actually are, and that anonymity was the default position. However, he argued that the internet was more like being in a market square – you are in a crowd but still identifiable.

A - James Hatch: James stated that it is possible to be close to anonymous but it takes a lot of time and effort. He did however raise the point that, if you were so inclined, you could use a distant internet café and pay in cash to achieve the same ends.

Q - Has Bitcoin presented added difficulty to cyber security given its untraceability?

A – Dr Beresford: Whilst we cannot see the identity of a person who is using bitcoin, it is possible to trace its movements. It presents a different challenge.

Q – Should there be a psychological angle considered when discussing hackers?

A – James Hatch: James confirmed that psychology was certainly part of their considerations when it comes to cyber security, especially when understanding the motivations of the hackers.

A – Dr Hopper: Dr Hopper stated that there had been a lot of psychological consideration in security design, right down to the colour of the padlock which indicates that a certain website is secure.

Q – Is it possible that new more secure forms of passwords actually won't be taken up as they are not user friendly?

A – James Hatch: James agreed with the question and said that if security methods involve a significant degree of effort for the user they may discourage their use. However, he acknowledged that there have been developments in more functional security technologies, such as the facial recognition software we now see on iPhones.

Q - Does the responsibility to be secure lie with the consumer, with business or with the government?

A - Dr Hopper: Dr Hopper argued that some responsibility must lie with all three, but also made the point that businesses need to create a new framework for what is expected in terms of cyber security.

A – James Hatch: James made the point that there is a conflict when it comes to businesses implementing security systems because the people who they collect data from may not necessarily be the people who fund the organisation.