An exploration of Internet of Things cyber security

I am very grateful to Santander and Royal Holloway for making my visit to the Global Internet of Things Summit in Bilbao possible and giving me the opportunity to supplement my Information Security MSc studies.

The Internet of Things (IoT) is an infrastructure of interconnected objects, people or systems. These "things", or smart IoT devices, process and react to physical and virtual information, using the internet. Smart devices are widely used, by consumers and in industry, and from the very small and limited in scope (lightbulbs, smoke detectors, webcams, thermostats) to massive, safety-critical systems controlling water treatment plants, electricity generation plants and industrial manufacturing. But although already widely used, the IoT is only just beginning its revolutionary impact on society.

The IoT is part of what is sometimes called the Fourth Industrial Revolution, in which just as with other industrial revolutions, new technologies are being introduced which disrupt traditional ways of doing things, relatively fast and within a single generation, causing both positive and negative impacts on society and particularly the workforce. Bilbao, fittingly, has been undergoing its own revolution, since its iron industry declined in the early 1980s. A hybrid of old and new, the city is rebuilding and reinventing itself as a post-industrial smart city. Bilbao is a participant in wider European initiatives in IoT which aim to solve collective problems using techniques such as energy management, building retrofits, urban sharing platforms and citizen engagement.

Guggenheim Museum

The Summit had a substantial focus on solving the security challenges IoT devices give rise to, caused for example by the separation of cyber security during product development. Manufacturers race to bring new smart devices to market but many slip between the gaps of different laws and so are unregulated. If manufacturers are not held liable, they have little incentive to improve security or provide a method of updating the software which becomes obsolete quickly so devices like smart thermostats built to last for a long time become potentially hackable.

Another obstacle on the horizon is the likelihood of objects (machines or systems) becoming data processors once artificial intelligence (AI) is widely adopted. When this happens, systems will make decisions on behalf of humans, based on colossal amounts of data. The machines will have no accountability. Devices will be autonomous and we will not understand or be able to trace back and find out why they made specific decisions. Therefore there is an urgent need to protect the data on which these decisions are made.

Ethical and even philosophical questions arise. A cross-disciplinary approach was proposed for cyber security. IoT initiatives were presented in terms of their societal benefits with emphasis on "experimentation", usually associated with science, while technology traditionally refers to "testing". Terms such as cross-fertilisation and open ecosystems were used.

The language of IoT

But thankfully the cyber security problems of IoT were not perceived to be insoluble. Insecure PCs and mobile phones were fixed and in time we will also fix IoT weaknesses and there were a number of proposals for doing this. Much work is being done collaboratively across Europe, including the following initiatives and proposals:

- Certification of IoT devices to aid consumers and businesses in choosing solutions
- The EU funded ARMOUR project is investigating the use of labelling of devices at manufacture, and using blockchain for trust in Decentralised Autonomous Organisations
- The 6LoWPAN communication protocol running over IPv6 for internet connectivity on the smallest of smart devices with limited battery power was reviewed
- Installing forensics-gathering nodes for evidence for demonstrating liability is an unsolved problem being investigated

- A future trend identified was self-protection, where individuals will take the initiative, while a non-technical trend identified was "retropia", where a pre-digital way of life is embraced
- The need for a security version of GDPR was identified to shift the responsibility for securing devices from the consumer to the manufacturer/supplier.

Gateway of the Honorable

From the perspective of a tourist it is sometimes hard to find harmonious views in Bilbao. The scenery is eclectic, with impressive historical buildings converted into public art spaces contrasting with noisy, large-scale building works. These contrast again with neat and compact green spaces, part of Bilbao's regeneration plan to create micro-spaces for social integration in city neighbourhoods as part of a new spirit of eco-urbanism. Unflinching sculptures reflecting the city's industrial past are dotted around; bold statements of confidence and renewal looking forward rather than back. What struck me about Bilbao was its infectious buzz; the city's clearly cohesive inter-generational population were busy enjoying the city's culture and commerce.