Acadamh Ríoga na hÉireann
Royal Irish Academy

Martin Hynes
European Science Foundation
1 Quai Lezay Marnesia,
Strasbourg, 67080
France

12 November 2018

Re: Royal Irish Academy Discourse with Máire O'Neill

Dear Martin,

On behalf of the Academy, I would like to thank you for your reflective and considered response to Máire O'Neill's Discourse on Wednesday, 7th November 2018.

Your contribution to the success of the event is greatly appreciated.

Yours sincerely

Michael Peter Kennedy
President

19 Dawson Street, Dublin 2 / +353 1 6762570 / info@ria.ie / www.ria.ie
Professor Michael Peter Kennedy, President Professor Patrick M. Shannon, Secretary Professor Stephen J. Gardiner, Treasurer

Securing connected devices: An arms race

by Martin Hynes, 7 November 2018

Good evening, and thank you to Professor Maire O'Neill for such an enthusiastic and comprehensive summary of a very complex field. Thank you also to RIA Secretary, Prof. Pat Shannon and to all of you for giving me an opportunity to respond.

The subject under discussion is rather closer to practice than I feel comfortable with.
Imagine a time when you could open car doors and activate the ignition with a screwdriver and one could overcome a flat battery by starting the car with a push. If there were other problems, some fiddling with the points or spark plugs would usually resolve it. That was my time.
By contrast, some recent thriller movies portrayed a senior White House employee driving along over the Potomac Bridge. Suddenly the steering wheel is wrenched from his grasp and the car lurches into the parapet, killing the occupants instantly. This might seem like science fiction; I fear that it is not. As a plot twist, it is like an example of Beelzebub ex machina.

When I returned to Ireland I purchased a hybrid car, one designed to reduce total emissions whilst providing similar utility to diesel cars. I had experienced at first-hand the enormous pollution caused by ICE and diesel vehicle in a valley environment with little wind. The atmosphere was observably polluted and whole cities and towns had restricted access to polluting vehicles based on varying criteria. Speed limits on motorways were reduced at times of high pollution.
My own type of vehicle provided remote control in order to set up services such as pre-heating the cabin or to determine charging times; for instance at off-peak rates or when solar PV was available.
Unusually, the car is supplied with an embedded router—its own WiFi system which is always on. It has been demonstrated[i] that this can be used to hack into to the control systems—not just to open the doors, switch on the lights and switch off the alarm, but to potentially control functions such as steering and brakes. Apparently, it is also possible to geolocate the vehicle using publicly available portals. These are not comforting thoughts. It is only mildly reassuring that it is somewhat less dramatic than has been demonstrated on the Jeep Cherokee[ii].

Moving from the personal observation to matters closer to a real "arms race", I find it fascinating to observe that the most recent UK aircraft carrier, the Queen Elizabeth, as yet has no aircraft! The first landings of aircraft on the giant vessel took place in the US in August last. It is expected that the UK will purchase a squadron of 12 F35B fighter aircraft from the USA for the carrier.
What is really interesting about the F35B aircraft is the proposed maintenance arrangements. The only engine overhaul facility will be in Turkey, whilst avionics repairs can be carried out in Deeside, North Wales.
Reported on the e-journal "The Register", the Autonomous Logistics Information System (ALIS) is the main monitoring system. ALIS tracks every component on the aircraft; it determines in real time the state of the aircraft, allows viewing of flight plans, and the review of each jet's entire history from the moment it leaves the factory.

Controversially, it also sends each jet's history back to the US, regardless of which country actually owns that aircraft: now this really calls to mind an Arms Race. Is there any guarantee that some hidden features (or bugs) do not exist?
One can imagine a situation in which remote control would disable or limit vehicle performance under certain conditions. In this instance I can appreciate that a national cyber security initiative would be fully justified and cost a tiny fraction of the overall investment.

In the original definition of arms race, it was seen as a competition between nations to develop and accumulate weapons. There seems to be lots of evidence that government supported entities are doing exactly that in relation to cyber weapons with tailored toolkits being stockpiled. For example, Microsoft's VP Brad Smith in the context of the WannaCry attack:
"We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage."

This gives rise to an interesting reflection: whose role is cyber security? Larger nations have significant programmes and investments in various aspects of cyber security. How much of that investment has been dedicated to insecurity or vulnerabilities?
I am not familiar with specific national efforts here, but IDA Irealand has an interesting infographic on the range of companies working on the topic with investments here[1]. I am aware that there is a National Cyber Security Centre as a component of the Department of Communications, Climate Action and Environment, but I have yet to understand its scope of work.

At a more collective level, UNESCO has a series of initiatives on the topic.

The Electronic Frontiers Foundation claims to be "The leading nonprofit defending digital privacy, free speech, and innovation." It has been an effective lobby in the past.

It seems that this continuing warfare is a big boy's game, not something that the consumer can reasonably expect to address at any meaningful level. Is there therefore a trade off between cost and security?

For the sake of example, it is clear that mobile phones have moved from "Connecting People" as the good old Nokia jingles used to say, to connected ***things***. I detest when Google tells me "welcome home" or "how did you enjoy shopping" just a little less than the times when it remembers where I parked my car.
I accept trade offs in privacy for enhancement of performance: but am I also leaving myself vulnerable to attacks? Even more unsettling, would I even know that I had been hacked?

Many will have seen that you can purchase a mobile telephone secured by a group backed by famous names in internet security like Phil Zimmerman. In commenting on the sales

[1] https://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security

performance of what is sold as the Blackphone and the Silent Circle service, Zimmerman quipped about consumers:

"They'll say 'Give me liberty, or give me death! But I don't want to pay $50"

Zimmerman explained that they had to reorientate the company towards security conscious business users. They still serve individual consumers, but you would need to be seriously concerned regarding security to pay the additional capital as well as monthly service charge.
I have often wondered whether you would be specifically singled out for scrutiny in the event that you used such a phone: you would be like a moving telephone SIM card without all the other data more usually associated with it.

In this way, there seems to be a premium to be paid to suppliers who have the capacity and integrity to "go to bat" for you when one of the many vulnerabilities have been identified and need to be acted upon. Note here that I seem to have unconsciously accepted that all devices have some vulnerability; it just has not yet been identified or publicised.
It cannot have hurt the sales of one provider when they steadfastly resisted efforts of the authorities to force them to provide access to a telephone that had been secured with a suspect's fingerprints. Perhaps it goes to reinforce Professor O'Neill's postulate when the impasse was resolved by the authorities purchasing a service from a third-party to hack the 'phone. The arms cache of suitable weapons was available in this situation.

Looking back at the role of specialist cyber security programmes, might it be feasible to ban insecure devices? If one accepts the idea that there is no such thing as a secure device, only once where the vulnerabilities have not yet been discovered, then there might be an argument to be made to force providers to recall those which have been demonstrated to exhibit serious vulnerabilities.

Allow me a moment to speak of unintended consequences. In his 2014 book "To Save Everything Click Here" Eugeny Morozov gave a whole spectrum of examples of how projects that seemed initially appealing gave rise to unintended consequences. A simple example was the desire to plot reported petty crimes on a map. It was observed that as the data was populated people started looking at house values in areas with high reported crime rates; it came to devalue houses in certain areas. As a result, fewer crimes were reported and thus the project came to be self defeating.

An example I experienced myself was the installation of CCTV cameras in a domestic situation. It seems desirable to be able to monitor your house and security arrangements remotely. However, if you can do it it is almost certain that miscreants can also monitor your home, determine times that people are there and act accordingly in their own interests.
Whilst one might not characterise the book as an enjoyable read, it is an exhaustive catalogue of unintended consequences and a persuasive call to think critically about the benefits and risks of "being digital".

As more and more devices become interconnected, we can see the benefits and the downsides. I had a system that controlled the heating in our home. It had a very nice interconnection with a weather forecasting service whereby it could modify starting times

depending on predicted weather in our area. I could also start and stop as well as set temperatures on the system remotely depending on conditions and expected occupancy. However, it relied on WiFi connectivity and as more and more SSIDs came on line and the channels became congested it started to become less reliable. A lightening strike finally killed it and we are back to good old stand alone time-switches. One last point in relation to this lightening experience is related to the solar storm of 1859- that named the Carrington event. As devices are more interconnected and interdependent, what resistance and resilience can we expect in the event of another significant solar storm?

In relation to our "smart thermostat" I suppose the consequences of a hacking in that particular application is not especially severe. However, I am of a generation when I really do not like the idea of something listening into our conversations and perhaps providing data to persons unknown. I note that the latest Mac laptops have a physical shut-off switch for the microphones when closing the lid. Providing data on our energy and other consumption habits and monetising information that we have not consciously give away I also find objectionable.

It is in this context that Prof. O'Neill's discourse is timely. As a citizens, we need great assurance of our security as these devices proliferate. We have a NCT service for our cars, a certification system for our electrical and gas installations; do we need a third party imprimatur for our connected devices?

I very much look forward to the discussion.

---

[i] https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/
[ii] https://www.motor1.com/news/57221/jeep-cherokee-susceptible-to-hacking/