March 2017

Future risks; the evolution of cybercrime

If you own an internet-connected car, a smart TV or a smart watch, a smart fridge, a WiFi doorbell, a smart home heating or cooling system, a connected home security system, or any one of thousands of other available connected devices and accompanying apps, you are already participating in the Internet of Things; and so is your personal data.

Mark Johnson, The Risk Management Group

If there is any certainty to be found in the dynamic world of cybercrime and internet security, it is that when change happens it happens quickly, often as a phase transition from one known tactic to a completely new and unexpected one. Cyber-criminals have numerous motives, from committing fraud, extorting payments and selling stolen data, to bringing down web sites or even whole networks, attacking national infrastructure and supporting terrorist or military actions. But whatever their motive, one need is common to all; access to systems and the data they hold. So, as the infrastructure that stores and processes data evolves the threat evolves at the same pace. To predict what that future threats might look like, we need to focus on the technological changes that are happening all around us.

The Internet of Things

Whether you wear it on your wrist, watch it in your living room, use it in your kitchen, or drive it to work, the internet-connected smart device is already a reality in the lives of many of us. If you own an internet-connected car, a smart TV or a smart watch, a smart fridge, a WiFi doorbell, a smart home heating or cooling system, a connected home security system, or any one of thousands of other available connected devices and accompanying apps, you are already participating in the Internet of Things; and so is your personal data.

You may at some point have looked at what happens to your web browsing and social media data in the big data market, but you now need to think about ‘bigger data’. Everywhere you go, everything you say to a smart device, how fast you walk, where you stop, what you look at, who you call or message when you do, how you feel about it, what it makes you want to purchase, how much you're willing to spend; all this and more is being deduced, extrapolated, charted, estimated, predicted, shared, sold and enriched, second-by-second, minute-by-minute, every hour of every day on a worldwide basis by the huge organisations that provide you with these low-cost technologies and free online services, partly in order to capture this data.

But those devices, those apps, are no different from the devices and apps hackers have been infecting, hijacking and disabling for decades. The devices contain microprocessors no different from those in your laptop. The apps contain code and store data no different from that held on your hard drive. Those apps and that data will be attacked in the same fashion as they have always been; in fact, the attacks have already started.

In 2016, the Mirai network of infected machines was created by hackers who specifically targeted Internet of Things devices, infecting over 145,000 of them, mainly Webcams. Fridges and other systems have also been infected. The Mirai 'botnet' was then used to send massive volumes of data to victim's web servers in what is known as a distributed denial of service attack (DDoS). Unable to handle the traffic volume, some of the internet's most popular websites went down temporarily. There is nothing to stop this happening again and future attacks could be even more severe. How long would your business survive without its web presence?

Drone-jacking

Last week reportedly saw the first confirmed use of armed drones by ISIS, during the ongoing battle for the city of Mosul in northern Iraq. If validated, this represents another phase transition in the technical security domain. Drones have already been used by criminals in the UK, most notably to carry drugs and weapons into prisons, but the widespread unlawful use of drones has remained a topic for science fiction novels. Now we must prepare to contend with the risk of hostile surveillance and data theft by micro-drones, deployed by hackers or competitors.

Drone technology is not the property of any one government or industry. When a large delivery organisation prepares to roll out drone-based services, it needs to think long and hard about the potential risks. Will criminals deploy their own drones, with nets hanging beneath them, to intercept and capture delivery drones? Is it conceivable that hackers will develop the ability to hijack drones remotely and redirect them? Can a delivery drone with a solid, heavy cargo, be diverted and used as a weapon, perhaps to bring down an aircraft?

Not only are these scenarios plausible, but an entire anti-drone industry has already sprung up, before drones have even come into widespread commercial usage. On the military front, drone swarms are being proposed to counteract the anti-drone defences of the enemy. This may all turn into a zero-sum game, in which the business case for flying anything of value through the air to a customer's premises will evaporate in the face of tens of the challenge from thousands of technical wiz-kids and their home-grown drone interceptors.

I've got you under my skin

Have you ever had your cat or dog chipped? We chipped our cats when we purchased them and we installed a cat flap in the back door that reads the chip and only lets our cats into the house. The chip is tiny; you even can't feel it under the cat's skin. Our vet reads the chip with a handheld device and the data on the chip includes our names, our address, phone numbers, email addresses and, of course, the cat's name.

But wait! That's a lot of personal data to put inside an animal that roams the streets and fields and which might end up anywhere. I've just realised my cats are internet of things devices too and that I have put my data out there again. Luckily, cats are difficult to catch. I just hope nobody can read the chips from a distance…

Let's focus on the evolving uses of this technology for a moment. A chipped pet is one thing, but what about a chipped human? Are there any scenarios in which this might happen? What about chipped soldiers; their officers might see real value in being able to track them minutely, or in being able to identify their remains. Chipped prisoners? Possibly a no-brainer. Chipped kids? I would probably have opted for that, if I had been given the option.

It would certainly have been much easier than trying to hide a friend finder app on a teenage child's mobile phone without them noticing! But I'm only joking… or am I?

It might come as a surprise to learn that there are already companies that have chipped their employees – on a voluntary basis, naturally. The chips support access control, location monitoring, the transfer of business card data to mobile phones, and even mobile payments in the staff canteen. Yes, mobile payments via a chip under the skin of a human are a reality in a few locations. The future is now.

So, what does this imply. The answers are obvious. Chips will be hacked and the data stolen. Chips will be cloned so that imposters can pose as employees. Chips will be infected with malware to spy on their users. And chips will be fried; remotely destroyed to deny service to their hosts and to damage security controls at their employer's sites.

In conclusion

The takeaway from all of this is very simple. Everything we already know about cyber-security, about encrypting sensitive data, updating our systems and anti-malware applications, training our staff, hardening our networks and locking down vulnerable ports and services, testing security, planning for failures, ensuring resilience; all these things are equally important when it comes to the Internet of Things, the use of drones, implants within the body, or any of the other emerging technologies, including robotics and nano-technology. There is nothing new under the sun, but what is also well demonstrated is our unfortunate collective failure to learn the lessons of the past. Let's hope we can do better this time.