Squirrels, Grid Security and a Stuffed Rudd

Or how taxidermy might save the grid.

Probably the most effective way for any terrorist group or belligerent power to cripple a Western nation and bring it to its knees is to destroy its electricity grid. Without power, most of the infrastructure will crumble into chaos within a few weeks. Manufacturing would come to a standstill, along with healthcare, transport, banking, mobile communications and retail. That was seen in Iraq, where 70% of the generating capacity was destroyed during the Gulf war, in what has been described as a crime against humanity. At that time, grid destruction relied on physical means – dropping bombs on power stations and sub-stations. As we integrate more electronics and software into the grid, you no longer need expensive munitions to blow things up – terrorists can do it from a computer.

It's two years since I last wrote about the cybersecurity issues within the GB smart meter rollout. At that time the response from the industry was dismissive. In the past six months, three things have happened which bring the risk back into focus. We've seen the first major grid cyber attack in the Ukraine; secondly, smart home owners with Nest thermostats have discovered that firmware updates can stop them operating and the third is that reports have come in of smart meters in the UK which have stopped working. None of that means our grid is going to be hacked tomorrow, but they all point out that what has been dismissed as impossible may not be quite so difficult as the industry and DECC would like to believe. Despite that, heads are still firmly in the sand as the UK Government continues to press ahead with a smart metering programme that is not so much climate-friendly as terrorist-friendly.

So what have squirrels got to do with grid security? There is a lot of talk going on about energy security in the UK, but it has little to do with the security of our national infrastructure, as opposed to the simple maths of making sure that we have enough generating capacity to meet demand. When the subject of cybersecurity is raised there is little informed debate. Earlier this year, the

media, along with a number of grid "experts" had great fun with the report that squirrels cause more power outages than hackers. There's even a cybersquirrel website where you can track the incidents. As a result, the cute little rodents have now entered the popular culture of the industry, such that real security issues get dismissed with trite squirrel references.

That distracts from the problem, which is that we now have some real security issues. At the end of last year, Kiev suffered serious blackouts. These were blamed on Russian hackers attempting to disrupt the Ukrainian grid. Whoever was responsible, they managed to shut down around a quarter of the country's substations for six hours. Details are still sketchy, but it appears that malware was injected into utility computers to turn them off. The belief is that the malware managed to send control messages to the substations. As those would have been valid commands from the central control system, the substations would have performed an orderly shut-down without causing any permanent harm to the grid. Hence the attack is annoying, but not one that would result in lasting damage. In its wake, cybersecurity experts are warning that 2016 is likely to see an increase in attacks in the utility sector.

The second issue that we have seen, or rather which Nest thermostat owners have seen, is the effect of bugs in downloaded firmware. At around the same time as the Ukraine attack, Nest thermostats around the US started to turn off, leaving their owners to face freezing homes. That problem was caused by an undetected bug in a software upgrade which had been applied automatically. The bug caused the internal battery to drain, presumably because it pulled more power than many of the devices could scavenge from the control wiring. In the UK, Hive had a similar problem, where an app upgrade directed thermostats to ramp the temperature up to a sweltering 32 deg C. Both were rectified after a week, but consumers realised that their thermostats were not as smart or reliable as they had assumed.

I'm sure the new software that was deployed in both of these cases was thoroughly tested, but it demonstrates how difficult it is to reproduce all of the different variables when you have lots of devices in lots of different situations. In other words, it's very difficult to be sure a software update is bug free, even when you have confidence in your programmers. As I said in my previous article, it's easy to imagine a rogue programmer working for a meter manufacturers being able to insert malicious code which would turn millions of meters off at the same point in the future. That's possible, because all of the smart meters being installed in Britain allow the utility to remotely disconnect your electricity and gas at the flip of a switch. If hackers turned off a million electricity meters in one go, that would cause serious damage to the grid. Turning them all on again a few days later would do even more damage, as restoring power when demand is unknown is particularly problematic and can burn out equipment on the grid, which gives a rogue programmer lots of scope to bring large parts of the country to its knees.

The point here is that it's very difficult to be 100% sure about an end-to-end system like this. Hive and Nest are a lot more experienced with this that our smart metering companies. They also have the advantage that they own all of the system. They designed the thermostats, the servers and the applications themselves, so they know how they all fit together. In contrast most GB domestic smart meter installations will have a gas and electricity meter designed by two different companies, the communications hub that connects them to the cellular network designed by a third; a switching centre – the DCC, designed and operated by a fourth with a cellular network operator in the middle, then a server application written by a fifth company, none of which have the level of skills and understanding which Nest had. So there's a strong chance that they will get it wrong at some point, giving an opportunity for a hacker to get in.

The third issue is a report that the Daily Mail picked up about a smart gas meter which stopped working. It told the story of Martin Thompson, a British Gas customer who had smart gas and electricity meters installed. Three months later, on a very cold March morning the gas meter turned his gas off. An engineer came round, blamed the battery (which is supposed to last fifteen years) and reset the meter. Ten months later, on another cold day, it died again. Another engineer came around and put in a new smart meter, but this one couldn't talk to the British Gas servers. It worked, but wasn't very smart. So in February a third engineer came round to replace it with a working meter. If that reminds you of Flanders and Swann's "The Gasman Cometh" I've already provided an updated version.

The serious point about this is that two meters had software issues, but in both cases they appear to have been treated as mechanical errors. It is quite possible they were just bad batteries, but in the world of secure, connected devices, faults like this should set alarm bells ringing, as embedded software which fails either indicates bugs which needs to be fixed, or more worrying, bugs which may open up security vulnerabilities. I have tried to find out from British Gas and DECC whether they have any reporting process in place for these cases and so far I've failed to find anyone who understands what I'm talking about. I just get a repeat of "why worry - it must have been a bad battery".

I don't actually think this is complacency - I suspect it is mostly naivety. Our electricity companies are not high tech. They care passionately about reducing outages, but it's a largely manual concern – it's about sending people out to cut down foliage, repair power lines and clear up after the occasional unlucky fried squirrel. It's why they like the squirrel analogy – they understand squirrels, whereas they don't really understand hackers. Utilities have a very physical mindset, not a technical or intellectual one and probably don't realise the firmware risks. Their concept of smart meter security is about people fiddling their meter readings, not terrorists bringing down the entire grid. That's brilliantly illustrated in British Gas' submission to the House of Commons' Science and Technology's call for evidence on smart metering, where they say that "Security is an issue British Gas takes extremely seriously. We store smart meter readings in the same way we do all our customers' personal information, which is all protected by the Data Protection Act". It's a bit like someone walking into the lion enclosure at the zoo saying "I'll be all right – I know I'm allergic to cat fur, but I've taken some anti-histamine".

These three separate examples show that the smart metering programme needs to look more closely at the security risks. We need to question whether the benefit to utilities of having a remote disconnect has been weighed up against the risk of hacking and major grid disruption? We need to question whether firmware is being written as safety critical software? My experience is that in this industry it is not. And we need to understand whether there is enough expertise within DECC and our utilities to manage and assess the security requirements of the deployment. If the answer to any of these questions is no, we should stop the programme.

In the past I've found that writing objective, technical articles about the problems with the smart metering programme has had little effect other than a few sage nods of agreement, which is why I've resorted to taxidermy in the hope that it might highlight the fact that pursuing the current course could well leave us stuffed. It won't just be the grid that is stuffed, it looks increasing likely that the career of our Secretary of State for Energy and Climate Change could be on the line as well. If it's any consolation to Amber, she won't be the first Rudd to be stuffed, as it appears the Victorians got there first.

This fine specimen of Scardinius Erythropthalmus, or common rudd, is currently available from Ayre & Co. for a mere £325. If there's a caring soul within DECC, they might want to contribute a small part of the £1.3 million in bonuses they picked up last year to purchase it and place it in the foyer of Whitehall Place as a cautionary warning to our Lady in Charge of Energy Policy. It would be the most visible example yet that anyone there has any awareness of the potential security consequences of the GB Smart Metering Programme.

Nick Hunn

April 2016

nick@nickhunn.com

+44 7768 890 148

You can read my previous articles about GB energy policy and the smart metering programme here.

Read more on my Creative Connectivity blog.