How to Hack a Smart Meter and Kill the Grid

And then all the lights went out.

Last week was a watershed for the embedded security community, and by implication everyone else. Bloomberg announced that rogue chips had been found on the motherboards of servers sold by Super Micro Computer to companies like Amazon and Apple. Whoever had added these during the manufacturing process would have acquired the ability to control and access data from the servers when those companies installed them. For the first time, it appeared there was evidence that the supply chain could be disrupted. That meant hacking was happening during the manufacturing process, before the products had even left the production line.

Up until now, hacking has predominantly been viewed as getting malicious code into a device which is "clean", by exploiting security flaws in its code. That's what's happened with every PC virus; attacks like the WannaCry ransomware, and state sponsored attacks such as Stuxnet and the recently discovered attempt by Russian hackers to infiltrate the Organisation for the Prevention of Chemical Weapons in The Hague. Although the concept of hacking a product before it has shipped has been discussed for years, the Bloomberg report signals that we've moved from academic debate to reality.

There is still debate about whether the report is correct. Apple and Amazon deny much of the detail, but its publication has started people looking more closely at the supply line and concluding that whether or not it is true, the way we design, subcontract and manufacture complex electronic products today means that it is possible. If it is true, this attack was probably commercial, where a company or a state wanted to discover what leading global companies were doing. What is more worrying is the prospect of a future where malicious state actors target infrastructure with the aim of crippling a country. Which brings me to smart meters.

I've always been concerned about the vulnerability of the British smart meters to hacking at the manufacturing stage. The reason for that concern is that these meters contain an OFF switch which allows power to be disconnected by the energy supplier. This is a convenience for them, as they no longer need to send someone round to gain access to a building. However, if it were ever hacked, the hackers could turn off millions of meters at the same time. That could be used to destroy the electricity grid.

Saleh Soltan, a researcher in Princeton's Department of Electrical Engineering, has written a number of good papers demonstrating how the majority of the grid could be brought down by hacking that results in just 1% change in electricity demand. Because it's currently very expensive to store electricity, generation is carefully matched to expected demand. If that demand varies rapidly, the grid will attempt to shut down to prevent damage, but if the change is rapid and unexpected, the resulting surges as individual elements turn on and off may cause damage, which can cascade causing widespread blackouts. Restoring power can be even more damaging as the grid doesn't know what is connected and turned on, so can't anticipate what the demand will be. Again, there is the potential for damage to critical portions of the grid if demand can be suddenly increased. Once you get past a certain level of damage, the task of repairing the grid and restoring reliable, universal supply can take years

I've always been concerned at this risk; that a programmer working for a meter manufacturer could write code which would cause tens of millions of meters to switch off a certain time. If a quarter of domestic smart meters turned off together, you could be looking at an instantaneous demand change of up to 15%, an order of magnitude greater than the 1% Saleh thinks will kill the grid. That is something that no electricity grid has been designed for. There is a reason that military planners target power stations – removing electricity cripples a nation for years, as we've seen in Iraq. That makes the grid a very interesting target for any malicious state actor.

So far I've failed to get anyone involved in the UK program to understand this risk. The energy suppliers' concept of hacking is limited to people bypassing or fooling individual meters to try and minimise their bills. Historically, their approach to hacking has been to move meters outside. That wasn't just to make meter reading easier, it's also because it's a disincentive to bypass the meter; what you might do privately in your under-stairs cupboard is less attractive when you're in full view of everyone on the street. When I've raised the possibility of a rogue programmer deliberately adding malicious code to a smart meter during its development, the only response has been "Why would someone do that"? Challenging that with "Why would someone drive a lorry into a group of pedestrians?", or "Why would someone fly a plane into a trade centre?" don't seem to compute. Those involved with the smart metering program have difficulty expanding their world view from a single student or householder trying to defraud them of a few pounds to an organisation or cause trying to destroy an economy.

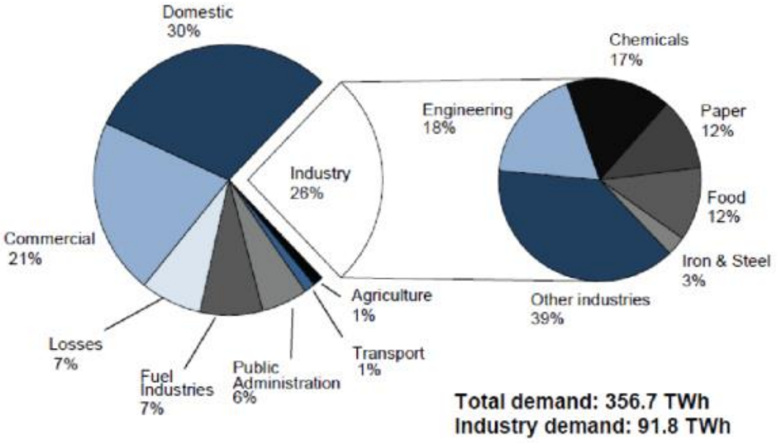
What is most worrying is that it's potentially very easy. So here's a quick tutorial on how to hack a smart meter and kill the grid.

First, get a job with a smart meter manufacturer. That shouldn't be difficult, as they're pretty desperate. All you really need for that is to have a basic knowledge of ZigBee. I only class myself as a hobbyist programmer, but I've been offered jobs by two smart meter companies as a systems architect. (I have declined.) Then think about what you want to add to the smart meter code.

Let's start off simple and just add a few lines of code that disconnect power to the home at a predetermined date. Smart meters have real time clocks, which should be regularly synchronised, so it's not difficult to get millions of them to switch off within the same mains cycle. You want to make sure that once you've disconnected the household supply, the energy companies can't turn it back on, reset the meter or upload new firmware, so add a few more lines to turn off the comms, or just overwrite the authentication keys. Make sure you hide the code so that no-one spots it and you're done. Because the GB metering spec is so complex, there are plenty of places to hide your few lines of code. DECC and BEIS have provided a very big haystack to let you hide your needle. You want to make sure your code is not overwritten by any subsequent firmware upgrade, so it's probably worth popping it in something which is likely to stay static, like the cluster library, or, if you can get to it, the bootloader. If you get the chance, put it in ROM. Job done.

To get the best chance of doing damage, you can do better than just disconnecting the supply by turning it back on again a few hours later and repeating that sequence a few times. That will really confuse anyone trying to restart the grid and probably cause more damage. The Government helpfully publish data about domestic demand and sector demand to help you work out when to do that.

If we look at sector demand, domestic electricity usage accounts for about 30% of total consumption on average. For the first turn-off, you want to find a time when domestic demand is at its greatest proportion of the total generation to inflict the maximum percentage change. At weekends, the industrial and commercial usage will be much lower, so a good starting point would be a Sunday.



Moving on to daily domestic usage data, peak demand is between 6 and 8 o'clock in the evening, so if you target 7 o'clock on a Sunday in January you'll probably find that the domestic demand accounts for around 60% of the total. If a quarter of domestic smart meters turn off at that point, you got maximum bang for the buck with an instantaneous drop of demand of about 15%. Nobody in the history of grid design has ever planned for that.

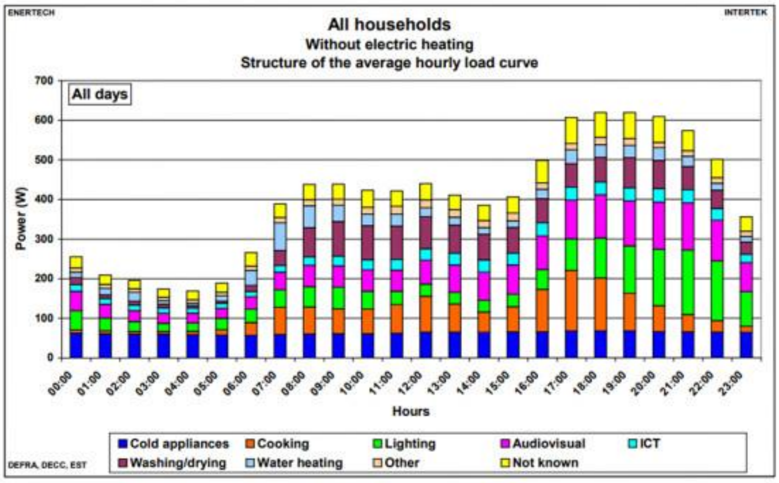


Figure 1 Structure of the average hourly load curve – All days – All households - Without electric heating

Have another look at the data to determine your next step, which is to turn all of the smart meters back on the next morning. Industrial and commercial users will have tried to come back on line, possibly a little later than normal because of the ongoing power cuts and the difficulty everyone will have had getting into work, so delay the reconnection until 11.30 am. If the grid has been brought back up this should generate a very unwanted additional 8% to the demand. Program a few more ON/OFF transitions over the next few days and then disconnect the supply and corrupt the boot loader in the smart meter. That makes it difficult for anyone to manually update the meter firmware, so they'll have to replace it. Except there's nothing like enough spare meters to replace all of the bricked ones, so 7 million homes remain without power just as the British winter starts to bite

This is the simplest hack. You program every meter to go through the same process, at the same time a couple of years in the future. As there are only three or four smart meter suppliers, just getting in and subverting one should give you control of a quarter of homes, which is more than enough. It's a sleeper hack which will either wait until its appointed time and cripple the country, or it could be a criminal hack, where the Government is alerted to it just before the date and blackmailed for a fix.

There should be tests in place to try to ensure that nothing malicious, or even just erroneous has been added to the code. I've yet to hear evidence that that is being done. The simplest test for the hack described above is to set the real time clock to a date in the future and leave the meters running with that false time. If you have fifty test meters, each with the current date set a month apart and constantly running, that would alert you to this sort of hack. I don't think that sort of testing is happening. It also assumes the hacker isn't clever. If they decide to play cat and mouse, they'll think of the tests you might run to discover corrupted code, attempt to detect those tests and turn off the hack whilst your test is running. In this case all they'd need to do is look for the RTC being reset. If you think that's science fiction, it's exactly what Volkswagen did with their emissions testing – they identified the difference between a test run and a normal drive and changed the settings for the conformance test. Within the industry that sort of tweak is far from unknown.

Smart Meters have an external wireless connection, so that opens up the opportunity for a firmware hack which could be externally activated, allowing the hacker to turn meters on or off as desired. That's a lot more complex, not least because the external comms element is in the communications hub, which then uses ZigBee to communicate with the meter. This would need firmware to be hacked in both devices to allow a disconnect message to be transferred, as well as allowing external communication with the GPRS modem. If the modem module itself were to be hacked, it would probably be undetectable, as no-one is likely to be vetting the modem code.

What the Bloomberg report has highlighted is the fact that this can be done. What I've described above doesn't need any complex hardware changes, but just one rogue programmer. We're constantly told that our smart meters are secure, but even the GCHQ pronouncements to that effect only talk about the risk of external hacking, not internal hacking during the design and manufacturing process. We now need to consider security models which no longer limit attack vectors to external hackers, but look seriously at the consequences of internal hacking and how to protect against that.

In many ways, this is an article I would have preferred not to write, but neither do I want to be the person saying "I told you so" when the lights go out. I have no doubt that what I've described above could be done. It may already have been done. It is highly unlikely, but this is a potential infrastructure risk that makes a no deal Brexit look like a new Garden of Eden; wreck the grid and you are back to a third-world economy that can probably only support a population of five million. It solves the immigration issue – we'll all be refugees trying to get into Europe.

There's an easy solution – remove the disconnect option from smart meters. It's only there because energy suppliers want their lives to be easy. That's the problem with the whole of the GB smart metering program – it's been debased to the point where it only benefits the suppliers and has thrown away the wider benefits, but not the risk and costs to consumers. The Bloomberg report is yet another wake-up call that tells us that it is time to stop the current deployment and do smart metering properly.

Nick Hunn

October 2018
www.nickhunn.com

Download and share this article from http://bit.ly/killthegrid