PREPARING FOR THE BLACK SWAN

Mike Ahmadi *discusses the importance of utilities security and why the Internet of Things changes everything*

Utilities are just coming online now. In this new connected world, utility providers understandably want to seize the innovations that the rest of the world is so eagerly getting their hands on. This wouldn't be a problem if it weren't for the fact that we lived in an age where hacking a power plant was possible.

In 2015 and 2016 hackers shut down power to thousands in the middle of a Ukrainian winter. This matters because the US Government now openly admits that foreign powers are attempting to gain access to America's energy grid control rooms every day; it matters because we are currently in the process of connecting decades-old infrastructure in an environment which is swimming with threats that it was never designed to protect against.

Engineers have not always played well with computer scientists. Not only are these different disciplines, they are different mindsets with different aims, different cultures and, of course, different technologies. Engineers might plan for accidents and failures while cyber security professionals plan for attack. There are wildly different industry standards for each discipline, and very few standards at all for the burgeoning field of the Internet of Things (IoT), which is increasingly weaving its way into utility environments. Those two worlds are now colliding.

EVOLVING LANDSCAPE

Much of the IT that's used in utilities infrastructure was previously air gapped, operating without fear that a hacker might find its way in. From that point of view, systems are often built for availability and convenience, not for security. Their creators rarely considered how a user might have to authenticate to a network to prove that they're a trusted actor. That might have been acceptable in the past, but now we have a landscape littered with outdated machines weighed down with insecure code that are unequipped for modern IT threats. Retrofitting those systems and bolting on security after the fact, won't solve all those security problems and replacing them entirely is sure to be an expensive, uncomfortable and almost impassable road for many to take.

Furthermore, those once-isolated IT infrastructures now risk doubling down on those problems, by being connected to an environment that is groaning with threats and opportunistic adversaries searching for the next easy target.

Now, utilities are looking to take advantage (or even become part of) the IoT, a trend which describes the increasing computerisation of physical objects. In the home this could mean things like connected cars, baby monitors connected to a parent's smartphone and doorbells informing homeowners who is at their door, even when they're not home.

Exciting as these new innovations might sound; evidence mounts every day of the IoT's insecurity. Whether it's hardcoded passwords, an inability to authenticate its outward and inward connections or an inability to update, there is little argument about their security. These products are often rushed to market without a thought for this important factor.

THE AVERAGE TIME BETWEEN A COMPANY BEING BREACHED AND ITS DISCOVERY IS 191 DAYS

Enterprises and governments are seizing the IoT as a way to transform the way they do business, and utilities are doing the same. Large infrastructures will increasingly be made up of IoT endpoints and sensors – able to relay information to its operators and radically improve the overall function of utilities. Unfortunately, in the rush to innovation, eager adopters often ignore the glaring security problems that shiny new inventions often bring with them.

In an industrial or utilities environment the IoT means something that is similar at a descriptive level, but radically different in real-world impact. A connected doll is one thing, a connected power plant is another entirely.

Admittedly, the results of a hack on a utility seem the stuff of science fiction. There are, however, plenty of examples we can look to. Stuxnet, the virus which destroyed the Iranian nuclear programme is just one. The aforementioned attacks on the Ukrainian power grid could be another. Furthermore Western governments now admit that foreign actors are attempting to hack their utilities on a daily basis.

Security patrols outside a nuclear plant in France

But if this is such a big problem, you might ask, then why hasn't it happened more often? Why haven't we heard about such potentially devastating attacks even more? Well, the fact is that many won't know they've already been hacked. Many organisations go for weeks, months and often years without realising that an attacker has been lurking within their systems. The Ponemon Institute has found that the average time between an organisation being breached and the discovery of that fact is 191 days, nearly half a year. This is especially true if one of those aged legacy systems has no way of telling what is anomalous.

Others may just hide their breach, as many organisations do. Such attacks are often embarrassing, especially with the regulatory implications and public backlash that a cyber attack on a utility brings with it.

Furthermore, most attacks are often not catastrophic events. They are commonly attempts to gain data or access to a critical system. For most, that's a valuable enough goal to pursue. Edging into the more destructive possibilities of such an attack would essentially be an act of war and not many cyber criminals want to earn the attention – or the ire – of a nation state.

The notion of the black swan – a situation that is hard to predict and seems wildly unlikely, but has apocalyptic implications – fits perfectly here. We don't know when, how or if such an event might happen but we had better start preparing for it. Even if the likelihood of such an event is small, the cost of not preparing for it will be much higher. The IoT adopters in the utilities sector need to start preparing for that black swan.

Public Key Infrastructures (PKIs) using certificates will allow utilities to overcome many of these threats, providing unparalleled trust for an often hard

Picture credit: Getty

to manage network. It's been built on interoperable and standardised protocols, which have been protecting web-connected systems for decades. It offers the same for the IoT and the utilities sector.

PKIs are highly scalable, making them a great fit for industrial environments and utilities. The manner in which many utilities will be seizing hold of the IoT is through the millions of sensors that will feed data back to operators and streamline day-to-day operations, making utilities more efficient. The sheer number of those connections and the richness of the data flowing through them make them hard to manage, hard to monitor and hard to secure.

A PKI ecosystem can secure the connections between devices, the systems and those that use them. The same goes for older systems, which have been designed for availability and convenience, but not for the possibility of attack. Users, devices and systems will also be able to mutually authenticate between each other, ensuring that behind each side of a transaction is a trusted party.

SYSTEMS ARE OFTEN BUILT FOR AVAILABILITY AND CONVENIENCE, NOT FOR SECURITY

The data that is constantly travelling back and forth over those networks is encrypted under PKI using the latest cryptography. Attackers that want to steal that data will find that their ill-gotten gains are useless when they realise they can't decrypt it.

Further ensuring the integrity of that data is code signing. When devices need to update over the air, code signing lets you know that the author of the updates is who they say they are and that their code hasn't been insecurely tampered with since they wrote it. Secure boot will also prevent unauthorised code from loading when a device starts up. PKI will only allow secure, trusted code to run on a device, hamstringing hackers and ensuring the data integrity that utilities require.

PREPARED FOR ANYTHING

The possibilities of an attack on a utility can sometimes seem beyond the pale. Just a few years ago a hack on a power grid seemed almost impossible. Today, news of IoT vulnerabilities regularly fills headlines around the world. The full destructive implications of this new situation have yet to be fully realised, but just because all we see are white swans, it doesn't mean a black one isn't on its way.

Even if it doesn't arrive any time soon, people will soon start demanding these security provisions from utilities companies. The Federal Energy Regulatory Commission (FERC) has recently fined a utility company that was found guilty of 127 different security violations $10 million. The company wasn't named, but pressure groups have recently mounted a campaign, filing a petition with FERC to publicly name and shame it. Moreover, with the advent of the General Data Protection Regulation and the NIS directive last year, utilities now have to look a lot closer at the way they protect their data. All over the world, governments are looking at how to secure the IoT, especially when it comes to the physical safety risks involved. Utilities security matters because utilities hold a critical role in the functioning of society. It is just as important that they be dragged into the 21st century, as they are protected from it. PKIs can offer a way to do just that ●

Mike Ahmadi, DigiCert VP of Industrial IoT Security, works closely with automotive, industrial control and healthcare industry standards bodies, leading device manufacturers and enterprises to advance cyber security best practices and solutions to protecting against evolving threats.

The US Government openly admits that foreign powers are attempting to gain access to America's energy grid control rooms every day

Picture credit: Shutterstock.com