A GENISYS GROUP Publication

THE UK'S FASTEST GROWING CORPORATE TECHNOLOGY DIGITAL MAGAZINE
Packed with news, opinion, debate and reviews by expert analysts you can trust

CIOTODAYUK.COM

CIO TODAY UK

innovation for tomorrow, today

MARCH 2015 MONTHLY

Don't Be Next!

HOW TO STOP THE NEXT HACK ATTACK

ALSO IN THIS ISSUE

The Data Privacy Officer's Role

UK Virtualisation Viewpoint

Bringing Order To Incident Response

PLANET OF THE THINGS

IoT and the challenge to security

– **DR HONGWEN ZHANG**, Chair CEF Security Committee explains -

STEPHEN HAWKING TOUCHED A NERVE when he reiterated his warning about the danger to humanity posed by artificial intelligence. In May last year he and a group of leading scientists had said: "Whereas the short-term impact of AI depends on who controls it, the long-term impact depends on whether it can be controlled at all. All of us should ask ourselves what we can do now to improve the chances of reaping the benefits and avoiding the risks."

Futuristic artificial intelligence may seem a far cry from today's Internet of Things (IoT), but in both cases the fundamental problem is about the uncertainty and risks of scaling complexity. Early experiments on the interactions between very simple elements – analogous to termites obeying a few basic rules – showed how surprisingly intelligent behaviour begins to emerge as the number of elements increases. Putting an emphasis on "surprisingly" – rather than "intelligent" – means that we are not predicting some malevolent intelligence to emerge from the growing network of smart fridges, but rather that we may find ourselves facing unexpected consequences by adding billions of relatively simple devices to our already complex Internet.

Even before we get on to those surprising consequences, however, there is the all-too-predictable certainty that criminal minds are already planning ways to exploit the IoT and create new forms of cyber-attack. The 2013 holiday season saw a smart, Internet-connected fridge sending out spam as part of a junk mail campaign that had hijacked more than 100,000 connected devices. But why should this be any more worrying than the existing threat of botnet-launched spam campaigns?

IOT – THE ADDED CHALLENGE

The first big difference lies in the sheer number of devices that could be, and eventually will be, connected. The world's population is around seven billion people, and already there are many more devices than that connected to the Internet – although estimates seem to vary considerably. According to IDC's estimation the number of connectible devices approaches 200 billion while the number of sensors (e.g., the accelerometer in a smart phone) that track, monitor, or feed data to those things is already more than 50 billion, with scientists talking about trillion-sensor networks within 10 years. Of those 200 billion things around 20 billion are already connected, and the number is predicted to reach 30 billion connected devices by 2020. So the first problem is not so much about the impact of any particular thing as about the possibility of unpredicted responses or vulnerabilities emerging out of sheer complexity.

The second big difference, and the one posing more immediate risk, is the fact that most of the devices now being connected are new to the IT arena. Whereas each new computer added to the Internet comes with some degree of malware protection built into its operating system, things like smoke detectors, security alarms and utility meters come from a different culture: traditionally they were either autonomous units or else, if they were connected, it was on a closed, dedicated network. Fire alarms were installed by one company, control and instrumentation networks came from a different vendor, the electricity meter was installed by the power supplier and none of these networks overlapped. While computers and IT systems have for many years been fighting off attacks, none of these simple devices joining the IoT have inherent defences and they remain wide open to cyber-attack.

The risk is not only that the particular function could be compromised – say fire alarms disabled before an arson attack – but the IoT could provide a weak link or point of entry to an otherwise strong security chain. The infected fridge continued sending out spam mail without drawing attention to itself, because its normal operation was not affected. Despite this relative vulnerability, the most publicised attacks so far on IoT control systems have penetrated the system via IT: attackers using simple phishing-style means to breach the perimeter and then target privileged access accounts. As well as gaining access to databases and high value systems, this approach lets them use the same privileges to reach control systems and whole new opportunities for sabotage and cyber war.

That brings us to the third difference. A lesser difference, but potentially the most dangerous of all, is that many of the things joining the IoT have more of a direct physical role than the computers, game consoles and databanks currently populating the Internet. When the Stuxnet worm closed down some thousand centrifuges at Iran's Natanz nuclear facility in 2010, IT departments all over the world woke up to the fact that a cyber-attack could cause actual physical damage. This was not simply an attack generating a signal to shut down the centrifuge, but one designed to force changes in the centrifuges' rotor speeds that could lead to destructive vibrations and internal damage – causing far more serious delays to the nuclear program than any simple shut down.

A couple of years ago we heard about a breach affecting Telvent control system designed to be used with "smart grid" networks. The attackers installed malicious software on the network and also accessed project files for its

OASyS DNA system – designed to integrate an electricity company's IT network with the grid control systems so that legacy systems and applications can communicate with the new smart grid technologies. There was nothing inherently wrong with OASyS DNA: it was a highly sophisticated system in use since the late 90s, but it was never designed to connect to the Internet.

Project files provide a clever way to spread malware because vendors have full rights to modify customers' systems through the project files. The files hold a lot of customer-specific system data, so an attacker could also use the project files to study a customer's operations for vulnerabilities in order to design further attacks on critical infrastructure. The Stuxnet attack was a sophisticated example of how a project file was studied to discover how the centrifuges were controlled and then the file was modified so that they were now behaving in a different, harmful manner.

So the IoT adds enormous extra scale to the already crowded Internet, and it also adds extreme diversity. On the one hand we are networking highly critical systems: industrial and utility grid control systems that could cause widespread damage or economic harm if breached; critical healthcare and remote medical devices containing sensitive personal data or responsible for life support; navigation and control systems for connected cars, air traffic control and so on. At the other extreme we have small low-cost monitoring devices, meters, wearable devices, simple switches for remote control of household lighting etc.

With such a range of devices it would be unrealistic to insist that every "thing" joining the IoT should have its own built-in defences. The latest malware signature has some sixty million records and to be sure of identifying it by current pattern matching techniques would require 3-4 Gb RAM. A more sophisticated defence is provided by behavioural analysis – studying how the code behaves when quarantined in a "sandbox" environment. Such analysis of behaviour for signs of malignancy is what computer scientists call an "NP Complete" problem – or what the layperson would call "extremely difficult".

Reducing operational costs is one major driver for IoT connection – so adding sophisticated cyber-security to a ten-dollar switch would be hopelessly uneconomical. There is no way that we can realistically defend the IoT on the militia model, where every device is armed against attack – so how is it possible to provide adequate protection across such a vast and diverse cloud?

How to disinfect the Internet of Things
Security is at the centre of the five key challenges being addressed by the CloudEthernet Forum (CEF), spelled out under the acronym VASPA, namely: Virtualization, Automation, Security, Programmability, and Analytics. The CEF, established in 2013, is an industry organization embracing every type of cloud stakeholder – including major users as well as cloud service providers, network service providers, equipment manufacturers, system integrators and software developers.

The most promising approach so far to securing the cloud, and so the IoT, is to adopt the SDN principle and consider the traffic flow as a virtual network, rather than a string of hardware elements, and so define a distinct "security layer" to orchestrate Security as a Service.

Today's Internet has been compared to a water supply without any guarantee of purity, leaving responsibility for filtering and sterilizing the water to the customers. Internet users are expected to install their own anti-virus software, firewalls and other forms of security. Security as a Service, however would mean providing traffic that is already decontaminated – so even the most humble connected switch on the IoT could benefit from the most sophisticated security that would be provided by the network itself.

On the network scale, deep packet inspection, pattern recognition coupled with a constantly updated cloud databank of emerging attack signatures, behavioural analysis and other costly high-level malware defences become an economic proposition. For individual users, and most client companies, such levels of security would be way beyond budget. Provide Security as a Service and let your customers order whatever level or type of security they need for their business, knowing it will always be up to date and maintained in peak condition.

Security as a Service provides a very attractive revenue stream, and it must be the ultimate added-value proposition for building customer loyalty and reducing churn. □