{* THE CHANNEL *}

https://www.theregister.co.uk/2014/06/23/hold_interthreat/

Traffic lights, fridges and how they've all got it in for us

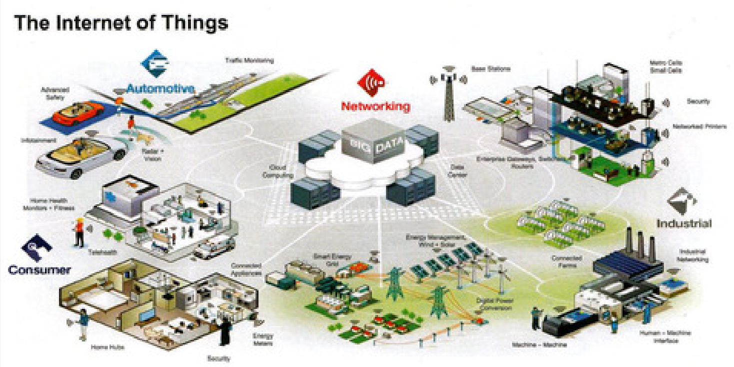
Interthreat of things

MON 23 JUN 2014 // 11:06 UTC

69 GOT TIPS?

Tom Brewster BIO EMAIL TWITTER

SHARE ▼



No doubt many of The Reg’s readers are tired of the term “the Internet of Things”. It is both a nebulous term and a vague idea. What it attempts to encapsulate is the masses of networks of automated machines that didn’t traditionally have connectivity, working to manage the environment around them, supposedly for the benefit of everyone.

Typical examples are fridges that notify users when something’s not right with the groceries inside, smart energy systems that manage heating to maximise efficiency and a toothbrush that reports oral hygiene habits to dentists.

It’s a brave new world, one rife with possibility for businesses hoping to make money from things that weren’t profitable before they were able to interact with the internet. The problem with giving objects IP addresses, however, is that they become exploitable. And in the world of embedded devices, if hackers hit them, they might be able to cause serious damage.

“The Internet is now woven into the fabric of our lives, literally in some cases, as connectivity is embedded into everyday objects,” says David Emm, senior security researcher at Kaspersky Lab. “The result is that we can be touched in more ways than ever by those who wish to subvert technology. The risks include theft of data by an attacker or manipulation of that data so that incorrect information is sent.”

This was highlighted in April by researcher Cesar Cerrudo, from consultancy IOActive, when he uncovered vulnerabilities in devices helping manage traffic lights. The flaws, which revolved around improper validation of data, would allow a hacker to head out on the streets, hook up to the affected machines from a laptop and trick the lights into sticking on a colour, or changing unexpectedly. That could cause some nasty traffic, or much worse.

Another piece of IOActive research from this year uncovered problems in Belkin WeMo home automation power switches. It claimed a malicious outsider could cause house fires by exploiting the flaws, which Belkin subsequently said it had fixed.

Much has also been made of software weaknesses in SCADA (supervisory control and data acquisition) systems. These manage various pieces of critical infrastructure and can be easily identified via device search engine Shodan. As SCADA systems are used to control nuclear plants, transport systems like railway tracks and water utilities, it’s pretty apparent something needs to be done to secure them, yet many remain replete with vulnerabilities.

One shouldn’t, of course, get too mired in the FUD (fear, uncertainty and doubt). One can count the number of genuinely malicious IoT attacks on a single hand. Researchers have shown themselves to be a tad hasty in talking up the IoT threat too. After Proofpoint said connected fridges had been involved in sending out reams of spam messages earlier this year, Symantec waded in to note that the fridges weren’t actually to blame. Instead, the fridges sat behind home routers using Network Address Translation. The fridges were simply sharing the same IP address as infected PCs, which were the devices responsible for the spam.

Indeed, the current IoT threat is not severe. With cyber terrorism still something of a myth, it will only become a huge problem if the “things” start processing financial data. That’s when the interest of real criminal hackers will be piqued.

Why so insecure?

But to get bogged down in FUD is to miss a pertinent point: the potential for harm is very real. “IoT devices are insecure, in the security community we know this. While these devices are not controlling or containing anything of real importance their threat is relatively low. However, as they get more and more pervasive and have more and more importance the greater the threats become,” says Michael Jordon, research director at Context Information Security.

To prove that point, Context recently purchased five devices, all of which can be found in the home but can’t be named for responsible disclosure reasons, and hacked them “with relative ease”, says Jordon.

“This shows that security is not currently on the requirements list for IoT devices. The devices and manufacturers cannot be named as these devices currently have no fix for the issues that we found, but they are being worked on,” he adds.

“Interestingly, the smaller the company the more seriously they take the security issues - they know that one bad story about the fact that their only product is insecure would sink their company.”

It’s not just security that’s a concern either. Privacy is likely to come further under threat if everyday devices within the home and across towns and cities can be compromised for surveillance operations, whoever is carrying them out. Given the now-tarnished reputation of UK and US intelligence agencies, it would be no surprise if they were already investigating ways to use embedded devices for scooping up data on the general populace.

But any hacker crew could become an arm of Big Brother, if the current landscape is anything to go by. James Lyne, global head of security research at Sophos, has been poking around with IoT devices too, purchasing a large selection of devices including CCTV, webcams and baby monitors. He found a lot of issues which could be exploited to snoop on people.

Of the 11 different camera products he tested, four didn't support encryption at all, meaning any username and password could be intercepted and the camera compromised. Three were vulnerable to Heartbleed, five had default credentials even when an account was created during setup and seven were open to multiple categories of web application attacks, Lyne says. Most of them automatically negotiated network access to the web using UPNP, itself a protocol that has been shown to be flawed in the past, he adds.

Lyne also tested a number of faults in home automation systems, using existing research. He says he managed to cause desk lamps to explode by exploiting weak control channels in power devices.

“I'm sure there are more devious use cases I have yet to discover,” says Lyne, who believes the future of IoT is not looking bright from a security perspective. “Internet of Things devices tend to have poor updating infrastructure and aren't prepared to react and rectify the serious faults that may be discovered during their years of service.

“We are adopting the Internet of Things, but the ecosystem isn't ready to do it right. Given we aren't likely to slow our charge to adopt new fancy devices they had better learn quickly or they will give cyber criminals huge power in the physical world, not just digital.”

One of the biggest concerns is that old problems are being carried into the new hyperconnected world. “It is scary to think how many devices around us that we have just accepted and ignore as a 'black box device' when really they are a computer running old software - ancient versions of Linux not being uncommon - with basic security failures like default passwords, unpatched and simply exploitable software and web vulnerabilities that make it feel like 2005,” adds Lyne.

“The scary thing is that these flaws are tragically similar to the flaws I've seen in industrial infrastructure and control systems. From the innocuous device to the powerful, life and limb impacting infrastructure, there is a lot of work to do in security beyond the PC.”

Protective measures

Addressing the problems now should help ease the threat of IoT hacks. The first thing is to push manufacturers to ensure security and privacy by design, says David Emm, senior security researcher at Kaspersky Lab. It's important that manufacturers of such devices, and the organisations implementing them, ensure that security is built in. The first step is to be aware of the potential risk; this can be more difficult if the device manufacturer and the implementation are not being carried out by the same organisation, he adds.

“For example, a car manufacturer may not be responsible for the technology that brings Internet connectivity into the car – or that's used to drive it – in the future. Similarly, it's unlikely that the connectivity built into smart meters will be developed by power companies themselves.

“Not only does this mean that security may not be automatically be 'top of mind' from the start, but deployment of any firmware updates may be beyond the means of the implementer."

Fortunately, there are a number of groups who are working to create such good practices amongst IoT vendors. The Build It Securely initiative, established by a number of researchers including Zach Lanier of Duo Security, is providing information for companies to help embed security in their processes. It also includes advice on setting up bug bounty programs to reward vulnerability researchers, thereby encouraging firms to make their products more secure.

“This isn't a service, this is kind of like OWASP, we're just providing resources,” Lanier says. “Here's some education on how security researchers work, here is some research to make your stuff more secure.”

Then there’s I Am The Cavalry, a project set up by Josh Corman, which describes itself as “a global grassroots organisation that is focused on issues where computer security intersects public safety and human life”. It will act as a hub for research on the Internet of Things and will hope to coordinate efforts to secure the connected machines that surround us.

It’s also lobbying US government to act on the issues. Corman tells me he has been spending time on Capitol Hill this year, speaking with a number of politicians about what can be done to make the digital controls running everyday machinery less vulnerable to hackers.

Should we slow down IoT?

But even these admirable initiatives will find it hard to cover off the majority of vulnerabilities. Perhaps encouraging corporations and government entities to slow the rise of the Internet of Things would also be wise, so hackable machines don’t form a significant part of our quotidian existence.

Emm and others believe there’s little chance of that happening. There are simply too many economic opportunities. “If this were a government project, or one sponsored by a single company, it might be. But what's driving this is economics – the drive for efficiency and productivity. The benefits that flow from an Internet of Things are much more evident than the potential dangers.”

That’s why Gartner is predicting the number of IoT devices, excluding PCs, tablets and smartphones, will hit 26 billion units installed by 2020. That represents an almost 30-fold increase from 0.9 billion in 2009. This will open up vast revenue streams for businesses, as IoT product and service suppliers are expected to generate revenue exceeding $300bn, mostly in services, by that same year. In a world still reeling from the downturn that started in 2008, which government wouldn’t want to spur on IoT development?

Jordon also says there’s no chance of IoT being slowed down, but manufacturers have the tools available to them to secure their creations. They just need to be convinced to use them. “People will still buy the products either because they are ignorant to the threats or assume that no one would hack into them. The security community needs to help and encourage the manufacturers of IoT devices to accelerate the process of maturing the security of their products,” he adds.

“The lessons have already been learnt on modern OSes. The mitigation techniques are out there and secure development lifecycles are well documented. IoT developers have access to the answers, if end users force them to use them.”

People have the power to make IoT safe. They just need to be told to exercise that power. ®