Insights into IoT Security



Insights into IoT Security

Security, Data Protection, and Privacy are key topics for those discussing the Internet of Things.

With limited standards currently in place for developers of consumer products and business left to define their own security measures, the progression of these issues is fundamentally linked with the progression of the IoT as a successfully industry.

We spoke to CA Technologies and NetIQ on how they are tackling the new issues that increased connectivity, BYOD and contextual technology are throwing up, hoping their experience would provide some insight into IoT security, as well as what the future holds for Industry 4.0.



If you have insights or opinions on this topic, we'd love to hear them.
Join the discussion in our LinkedIn group or tweet us @techx15.

ca technologies

NetIQ®

TECH X Digital business. Digital life.



Holger Reinhardt

Director of Emerging API Technologies

CA Technologies

Holger Reinhardt is responsible for developing business strategy and partnerships around the IoT, M2M, and Big Data for CA Technologies API Management and Security business.

He has an MS in Computer Science and an MBA in Entrepreneurship, and has been programming since he was 14 years old. He is also co-founder and chief developer of launchd.io.

ca technologies



Holger Reinhardt

Director of Emerging API Technologies

CA Technologies

How different is the security challenge posed by IoT as opposed to more traditional device connection?

Emerging connections and Internet of Things do not really add new or fundamentally different threats, they simply create a much larger attack surface.

But connected things do have specific characteristics which increase the potency of any existing exploit, and that is a potential inability to upgrade and longevity. The former is driven by the need to keep production and running costs low and the latter by simple economics of the product lifecycle.

Some phone vendors have been ingenious to get us to upgrade our smartphone every other year or so – but I strongly doubt that this economic model is scalable to appliances or smart homes. Without the ability to upgrade or replace, potentially compromised 'things' will create a latent security thread.

Consider it another form of an increasing long tail of vulnerabilities.

ca technologies

Is there a risk that adoption of the IoT will lead to corners being cut over security as manufacturers compete over price?

I don't think that it is merely a risk, but today's reality.

And it is not just about price competition. It also is due to apathy and disinterest. Partly to blame are the lopsided economics of who bears the costs if a breach occurs. In particular in the consumer space the costs are borne by the individual consumer, not the vendor. Given that why would a company invest into making their products especially secure?

But consumers and users are not blameless either - security is one of those attributes consumers claim to care for in survey after survey - but the reality is that they do not seem to be willing to work at it or pay for it. If the consumer is not willing to pay more money for a secure product, and the company does not pay for the costs if a breach happens – where does the incentive to invest into security come from?

Should it be the governments and regulators responsibility to impose tighter restrictions and ensure adherence to security protocols?

When it comes to Internet of Things and similar areas of technical revolution, instilling regulation too early in the market could hinder innovation. But the freedom to innovate doesn't mean security can be ignored.

Vendors must find the balance of security and business enablement and growth, and consumers must determine how much risk they are willing to endure. Will they install a drop camera for their home, yet neglect to secure their wireless network and manage the device access?

And what role do you foresee standards bodies such as Hypercat or the IIC playing?

Standards bodies are great arenas where stakeholders can exchange and test ideas. The outcome is often a boon for the industry in the form of best practices.

ca technologies

"instilling regulation too early in the market could hinder innovation."

How did your company respond to the challenge of BYOD?
Are you experiencing the so-called 'BYOA' trend now?

We see this all the time with our customers. Employees are consumers too and are starting to expect to be treated as such in terms of convenience and ease of use. Enabling this trend is the phenomenal success of APIs as means of integration and access to business assets. As an API Management and Security vendor we are helping business to enable secure access to assets and services using APIs.



ca technologies

How do you encourage your employees/customers to adopt security best practices?

One of our market differentiators is that we are offering security 'guard-rails' for mobile app developers with our Mobile API gateway. These guard rails are embedded in our mobile client SDK which connects seamlessly and securely to our API Gateway. The mobile SDK abstracts and encapsulates authentication and authorization for the app developer and enables him to focus on the task at hand – which is to build a world-class app. In other words he can speed along building his App while the Mobile SDK acts as guard rail to enforce compliance with the company's security policies on user, app and device authentication and authorization. This enables corporate IT to do its job of protecting access to the company's assets and services while stepping out of the way of the app developer to create cool, sticky apps for customers and employees.

TECH X Digital business. Digital life.

70% of devices use unencrypted network services

90% of devices collect at least one piece of personal information.

Nearly **145,000** new malicious programmes for mobile devices were discovered in 2013.

That's **3** times 2012's figure.

In **2014**, the number of mobile-connected devices will exceed the world's population.



Sources:
HP IoT Research Study (goo.gl/O5ir2A)
Cenzic Application Vulnerability Trends Report 2014 (goo.gl/BUBg0Y)



Geoff Webb

Director of Solution Strategy

NetIQ

Geoff is responsible for the NetIQ Information Security, Identity and Acess and IT Operation Management solutions.

He holds a combined bachelor of science degree in computer science and prehistoric archaeology from the University of Liverpool and boasts over 20 years experience in the tech industry, having held management positions at Credant Technologies, FutureSoft, SurfControl and JSB.

NetIQ®

How different is the security challenge posed by IoT as opposed to more traditional device connection?

There are really three significant differences when we think about the security implications of the IoT devices.

1. The first is that these devices are likely to be deeply embedded and in many cases, always on. So rather than having a small number of devices that we interact with occasionally, the IoT really drives a large number of devices that are pretty much embedded in our daily lives, or in the fabric of the infrastructure around us. What that means is that the potential for impact from misuse of these devices is very much greater – we're not talking about your laptop sending out spam email if you get careless, but potentially something of the scale of city-wide interruptions to critical services, entire regions losing power, or massive breaches of personal data. If we get it wrong, the impact is significant.

2. The second difference is the nature of the devices themselves. Rather than much heavier devices like PCs, or even tablets or smartphones, the IoT will be composed predominantly of far lighter weight devices such as sensors embedded in buildings, industrial devices, or our homes. These light weight "things" will be simpler, which is good from a security perspective, but also generally far more difficult to update and patch in the event of a vulnerability being discovered, which is obviously bad.



3. The third difference is the scale of the IoT.

There will be many orders of magnitude increases in the complexity of interactions between these devices above anything we see today. With so many more devices interacting in ways that are difficult to foresee today it's hard to plan appropriately for the security implications. In other words, the biggest problem is that we don't know what the biggest problem will be. Certainly there are good efforts under way to try to keep things as secure as possible – Weightless, and other communication standards will hopefully force encryption of information as it is moved between devices, but that's a relatively small part of the overall picture. If the device itself is under attack, then encrypting what leaves it may not solve the problem. Similarly, creating new methods of communication (again standards such as Weightless, and others like it) potentially add huge value in so far as they make the IoT far more extensible by innovative use of whitespace communications, but they also introduce new elements in the security puzzle, and attackers often exploit any weakness in the added complexity to make attacks. So there's always a trade-off.



Is there a risk that adoption of the IoT will lead to corners being cut over security as manufacturers compete over price?

I think the real risk is that security is neglected or added as an afterthought. Many of the creators of the IoT device will likely come from backgrounds where info-sec is not part of the culture. These are likely to be manufacturers of industrial devices, building sensors, medical devices, even domestic appliance creators. So they are going to need to "buy in" security skills and thinking to keep their devices safe, and without strong motivation to do so from day one, ***they may simply consign the problem to the "nice to have" pile.***



NetIQ®

Should it be the governments and regulators responsibility to impose tighter restrictions and ensure adherence to security protocols?

Regulators have had a huge impact on the security of enterprise and governmental IT systems. Whether that's privacy standards or industry specific standards such as PCI DSS – the effect of imposing standards forces organisations to take security seriously. Of course, no standard can fix the overall problem by itself, but with appropriate enforcement, they do form a good baseline. With something as pervasive as the IoT, and indeed, something that may well have national security implications, there is clearly a role for governments to address best practices, and to enforce minimum standards for securing the IoT.

And what role do you foresee standards bodies such as Hypercat or the IIC playing?

Standards like Hypercat are certainly welcome when it comes to creating a more workable IoT – part of the value of the IoT will be the interoperability of devices being used in ways that we don't currently anticipate. In fact, you could argue that the ability to combine sensors and devices in ways that they weren't originally intended for will drive the long-term value and enable us to solve complex problems in ways we haven't yet thought of.



How did your company respond to the challenge of BYOD?
Are you experiencing the so-called 'BYOA' trend now?

What makes BYOD (and BYOA, plus all the other BYO's) interesting is that they really exemplify the long term shift in power from the data centre to the office worker.

One of the most common strategies I've seen be successful is to gradually open the door to Bring Your Own, so that the risk management aspects of each step can be better understood. That said, it's a challenge, because once people can bring their own mobile devices it becomes very difficult to reign in control over things like cloud services and applications.

Nevertheless, as difficult as it is to maintain control once the doors are open, it's far better than the alternatives of no control whatsoever (and the appalling risk implications of that) or trying to lock everything down which simply won't fly in the long run.



How do you encourage your employees/customers to adopt security best practices?

Policies, communication, and education are the most critical elements of getting employees, or anyone else, to adopt security best practices. In the first case, policies should clearly lay out what is and isn't expected and acceptable. The problem is that while policies look good on paper, they are often not top of mind when it comes to solving day to day business challenges. So communication is critical too – explaining and reminding why we have the policies we do, and letting employees see that the company they work for takes security, and data privacy, seriously. Finally education is of course important – it's one thing to expect people to do the right thing, but unless you show them how, it's simply not going to be effective. Good education doesn't have to be scaremongering, nor does it have to feel draconian – rather it should focus on the right way to get the job done, in order to meet their personal goals, while still protecting the company, its data, and its customers. Encouragement is the key here – we humans tend to react negatively to being told 'no' all the time, and going down that route with security training simply breeds resentment. It's far, far better to reward people for doing the right thing, and encourage the rest of the business to do the same.



Insights into IoT Security

We hope you enjoyed this look into some of the issues surrounding the Internet of Things. We'd love to hear your opinions on the topic, why not...

Start a discussion with us on LinkedIn

Or come have a chat with us on Twitter at @TECHX15.

You might like to stay in the loop with our weekly IoT newsletter

Or, for some more information, please visit our website: techxx.net



With thanks to:

ca technologies

NetIQ®

Cover Photo courtesy of Nan Palmero