Security is emerging as a key differentiator – both for ourselves and our customers

One of the prices of success of almost any kind is an increased exposure to risk – and the M2M/IoT sector is no different. But where do these emerging vulnerabilities lie and what can we, our customers, and the wider business community do to mitigate and control those risks, now and into the future? Robin Duke-Woolley, CEO of specialist M2M/IoT market analysis and consultancy company Beecham Research, recently discussed these issues with Gilli Coston, chief strategy officer and EMEA managing director for Wyless.

RD-W: Security has gained strongly in importance for M2M and IoT solutions over the last couple of years in particular. Why do you think that is?

GC: Security is a moving target and an area where we all need to be vigilant for our customers. At one time, M2M solutions were thought to be secure enough because connected objects were little known and not a specific target for hackers. M2M has raised its profile and the IoT is making security centre stage in many implementations. As soon as a solution becomes mission critical for an enterprise, the risks of security breaches increase enormously. In addition, things we have taken for granted turn out to have vulnerabilities. The Heartbleed security vulnerability issue, for example, allows any sensitive data that would normally be protected by SSL/TLS encryption, even private keys, to be stolen. Heartbleed did not impact on Wyless technical resources but it did indicate that any device, host, or resource could, eventually, be exposed to an immediate vulnerability. Security cannot be taken for granted and this is an area Wyless is continually monitoring and adapting to.

RD-W: There is a tendency for people to view the need for security rather negatively as just a cost that has to be borne. Is it right to treat it like that?

GC: It is true that security can be seen as a cost and therefore may be resented or perceived as a grudge purchase. As M2M and IoT become more embedded in our ways of life, security has never been so important for our industry.

In addition, it is the overall connected environment that has changed and grown in importance and, with it, the potential vulnerabilities and risks. This translates into a rich hunting ground for hackers and a shared ▶

Reproduced from M2M Now Magazine

"Security is a moving target and an area where we all need to be vigilant, for our customers."

set of risks that can impact everyone. So we should view the need for security as an essential part of the project specification and one that has to work just like any other part of the overall solution. When seen from this angle, what could be seen as a 'resented cost' suddenly has the potential to become more of an opportunity for competitive differentiation. It is an area that Wyless has worked on to build particular capabilities that our customers see as of real value within our solutions.

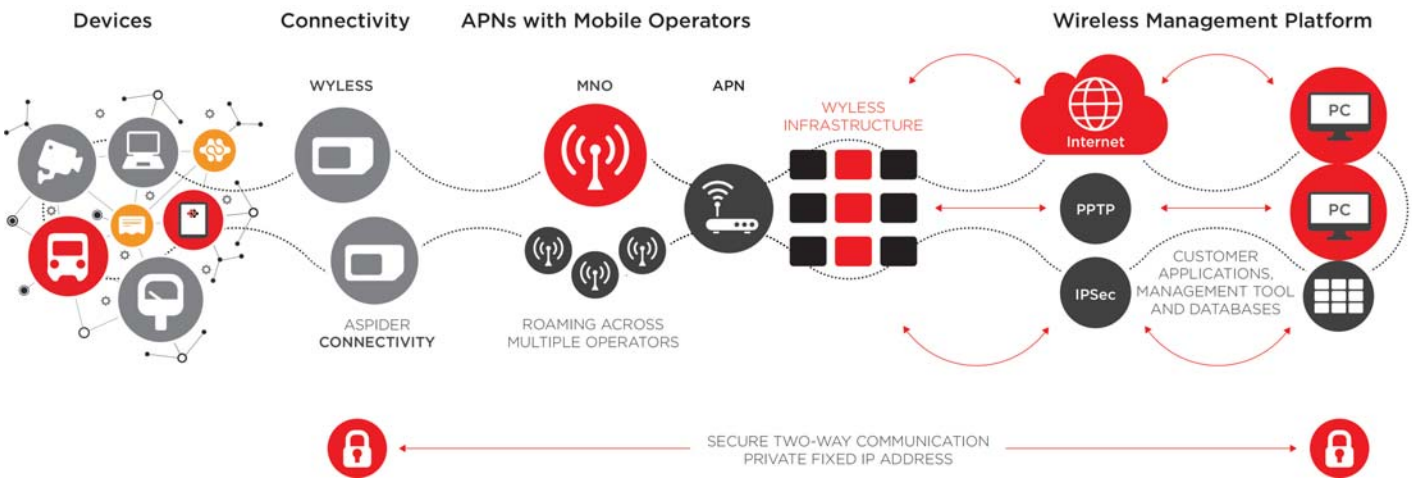
RD-W: So, what's the overall approach that Wyless is taking with security?

GC: We offer end-to-end security for M2M and IoT solutions, and we look at this from both a horizontal and a vertical perspective. To enable the horizontal perspective, we take security seriously at every level, from the most fundamental physical security of our data centres to the highest-level aspects of our network, software and service layers. One example of this involves building a secure wall around a business environment, but enabling remote access by authorised users and devices. To implement this we use two data communications technologies – PPTP (Point-to-Point Tunnelling Protocol) client-server and IPSec site-to-site VPNs (Virtual Private Networks). With PPTP, individual users can initiate a VPN and establish traffic to devices on the fly. With IPSec, one or more sites can be linked to the devices over a private, permanent connection. That means it isn't necessary to have public IP addresses, which in our view should be avoided wherever possible.

In addition, we implement the most stringent security policies that we can, along with robust encryption. Wyless has a particular capability in this area through our acquisition last year of ASPIDER M2M who are based in the Netherlands. We developed an end-to-end security solution specifically for M2M communications that employs state-of-the-art cryptographic technologies. The current version supports symmetric-key cryptography, with public-key asymmetric cryptography coming to cover other needs. As far as we know, Wyless is one of the very few companies to employ ▶

Gilli Coston, chief strategy officer and EMEA managing director, Wyless

Wyless offers end-to-end security for M2M and IoT solutions, looking at this from both a horizontal and a vertical perspective



this sort of robust technology for M2M security. The security keys for this are stored on the SIM card, so the M2M modem retrieves keys from the SIM, sends encrypted data to the server, which then decrypts the data using the same key. The same process also works the other way, sending data to the modem.

RD-W: That covers the horizontal perspective, which is essentially common across all solutions. What about the vertical perspective?

GC: Apart from the SIM-based cryptography which is pretty unique to Wyless, the horizontal perspective essentially runs along traditional lines. What is different with these is that they are available directly from us. When you look at different verticals such as utilities, automotive, city infrastructures and so on, there's an increasing need to cater for the unique requirements that are specific to that sector. This focuses thinking on what is really appropriate for each application. Security needs for different applications may not be the same. By tailoring security to individual sectors and applications, we can provide exactly the right levels and layers of security meaning that the costs involved are applied precisely according to need.

Implementing pragmatic and grounded approaches that work in the real world is our goal. You need to get away from theory and put it into practice. This means that there's a need to get right down to the detail involved in each vertical and demonstrate how it really works and benefits the users.

RD-W: Can you have too much security for an application? Is there a risk of losing the cost-effective perspective?

Security is a moving target and an area where we all need to be vigilant for our customers

GC: Security for each solution needs to be "right-sized" so that costs are appropriate for that particular solution. In practice, this means applying different levels of security for different reasons, with some being more costly than others because of the potential damage that could be caused by a breach. An easy example of this is a mission critical application, such as controlling a smart grid. Compare this with a much simpler application, such as monitoring humidity levels in a field, for example. The two are clearly not equivalent in terms of the potential damage caused by a breach. It is more justifiable to have a higher level of security for the smart grid application, rather than trying to provide the same high level of security for both. To do so would probably make the field monitoring application financially non-viable. For each application, the cost of the security being provided needs to be weighed against the potential damage of a breach.

RD-W: Taking this point a bit further, do you see different security challenges facing IoT solutions compared against traditional M2M solutions?

GC: M2M is generally embedded in enterprise processes. The applications typically have clear specifications and architectural requirements and the end-to-end security requirements are clearly defined. The economics are bounded and it is usually pretty clear whether an application needs - or can sustain - a high level of security and the associated costs. Secure communication is a fundamental requirement and solutions are most often created in-house or by a number of trusted partners working together. ▶

Reproduced from M2M Now Magazine

With the Internet of Things, there are many developers and devices involved who are usually working independently. Security can often be an afterthought, rather than specifically defined in advance and communication often involves unsecured cloud environments. Looking at security from this perspective, new services and applications are continually being created that often draw on sources of information that were originally designed for another purpose. This is a completely different and much more dynamic security challenge than we have seen in the M2M world to date.

Consider the hacking opportunities that come with millions of connected remote devices that have a long life span of ten years or more. During that time security vulnerabilities may increase and those devices become hackable. What happens next? Their current security arrangements may need to be updated and remotely managed with new security updates being provided. To achieve this with millions – or even billions – of devices, standards are an essential ingredient.

The fact that there are currently limited security standards for M2M applications has not slowed market growth down. It is predictable that in IoT there may not be sufficient means of interoperating securely in large numbers and we therefore must consider what impact this may have on future IoT growth. It could be profound.

RD-W: What are the issues that need to be addressed to move forward with all this?

GC: These are issues for the industry to resolve together as a community. For example, how do we work together to provide consistent security solutions, from end to end? How do we do that so it doesn't just add extra layers of cost and duplication? If it is too costly, users then have to start making decisions about what elements to leave out to bring budgets back in line, or choose to reduce the overall functionalities to achieve those savings. These are not really decisions that we should be asking executives to make.

When faced with these sorts of questions, discussions inevitably revolve around the need to create new standards. There is no doubt that standards are required in order to fully develop what will increasingly become a large scale, consumer-oriented market. Standards typically take a long time to come about and the market is not going to just wait for that to happen. So, there's an increasing need for market players to work together more informally in the meantime.

We need to take account of the many issues that come from new technologies being introduced all the time, which in turn create new ways of doing things, which then themselves create new security and privacy issues. How can overall security be maintained while these changes are being introduced? In other words, how do you ensure you have security in your end-to-end solution in a world that's constantly changing? It requires a constant assessment of the security implications of changes as they are made, but not in a way that slows down or hinders the introduction of new ideas and new methods. This is a challenge that the whole industry has to resolve.

RD-W: So, what's the key message from all of this?

GC: Make security cost effective enough to enable the mass adoption of IoT and M2M solutions and ensure it's achievable through good practical and directly relevant standards that benefit all our customers. We must keep what is inherently a very complex area as simple and as cost effective as possible. We must focus on and understand the actual needs of businesses and consumers in all their rich variety and help them to achieve those ends by applying new and innovative technologies – but in implicitly secure ways.

Gilli Coston is chief strategy officer and EMEA managing director for Wyless. Gilli spent over twenty years at O2 and Telefonica, with her final position being as General Manager of M2M for Telefonica O2 UK. After that, she joined consulting firm CGI. Gilli is the Wyless Board member for the International M2M Council (IMC).

We must keep what is inherently a very complex area as simple and as cost effective as possible

Reproduced from M2M Now Magazine