April 2013

Beecham Research

Towards Right-Sizing Security for M2M Solutions:
A Practical Approach

Researched and Published by
Beecham Research Ltd.

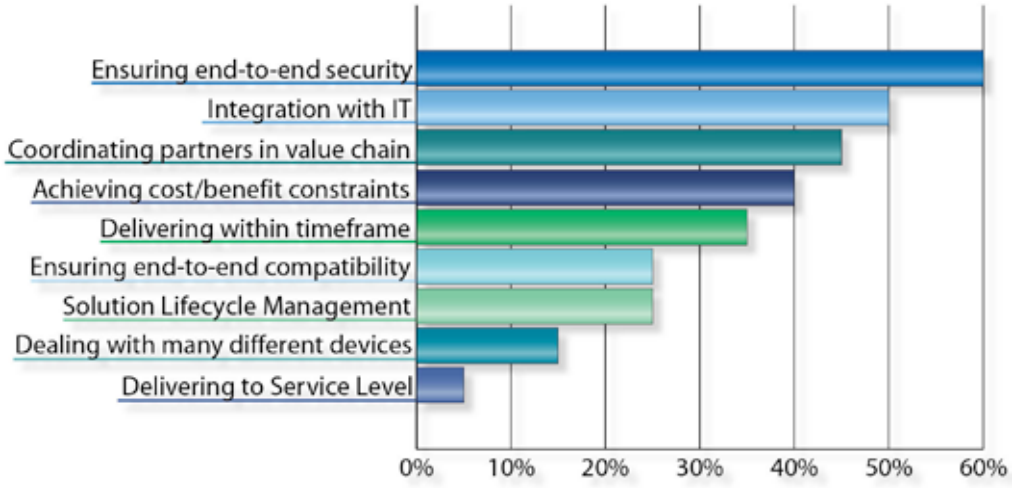
Security for M2M solutions is a current research focus for Beecham Research, with a report due in early Q2 2013 that identifies a new balance and new opportunities emerging in the market. This white paper discusses the issues and approaches to security in M2M that are making a real difference.

M2M SOLUTION SECURITY A HIGH PRIORITY

A recent survey conducted by Beecham Research of leading M2M solution providers in North America, Europe and AsiaPac found that ensuring end to end security was their highest priority for current M2M projects. This is indicative of the growing requirement.

Figure 1: Beecham Research Survey of leading M2M providers

Which of these are the top 3 priorities for delivering M2M projects today?



Source: Beecham Research for Oracle, Sept 2012

Reports of data loss and corruption, access intrusion and distributed denials of service are growing at an alarming rate. For example for Industrial Control Systems, in 2011, the year after the discovery of Stuxnet, over 5 times as many vulnerabilities were reported compared to the previous 5 years. These discoveries of new vulnerabilities doubled again in 2012. These and other documented examples of security breaches illustrate the potential for harm. For this reason, security solutions for all manner of IT projects including those in M2M are

> *. . . in 2011, over 5 times as many vulnerabilities were reported compared to the previous 5 years. These doubled again in 2012 . . .*

gaining in importance.

M2M systems comprise a complex chain of connected systems and devices; hence the M2M community is right to be concerned about their increasing targeting by attackers, particularly via the Internet. For this reason, end to end M2M security has shot up the priority list. Whilst there has been an aversion in the market to discuss security issues openly, and the threat of hacking M2M-based operations is relatively low at present – this state of affairs is unlikely to continue. A major attack could have a significant impact on M2M market development and public trust.

A major attack could have a significant impact on M2M market development and public trust.

However the meaning of a system's security and requirements are not fully understood. Despite much talk about 'end to end' security, the 'ends' are not always clearly defined. Security is too broad and eclectic a concept to define, and its definition and implementation depend on its value to the solution. As security solutions are defined by the perceived threat or threats of the system in question, the meaning and requirements for security are different in different M2M vertical market segments.

In business critical applications/operations, data security and the physical integrity of remote devices tend to be paramount. Hence any failure that prevents delivery of the service is a threat. By contrast, in consumer applications such as telehealth and smart metering for example, the security of personal information is already becoming an issue of greater concern. New risks arise when devices are inextricably linked in an M2M delivery chain; for example, a persistent identifier could link the data back to the device from which it was collected or back to an individual. Moreover, connected objects communicate at a far faster rate than humans, and any adverse effects can arise independently, resulting in damage before it can be mitigated.

EVOLVING 'ELEMENTS OF SECURITY'

Many past and current M2M solution developments have provided both connectivity and security through the use of the secure capabilities of the SIM cards within embedded cellular modules, and at the other end of the M2M solution through the security in the cellular wireless network. In fact, the module plus the SIM has been rightly seen to provide sufficient security for the demands of those systems and their perceived threats.

An M2M solution chain is complex with multiple suppliers, technologies and communications, and will likely grow in complexity. As M2M solutions have become more widespread and more critical, more areas are identified where security needs to be added. For example, some connected devices' embedded systems developers have identified a need for encryption and decryption of varying strengths from sensors; here, the first approach, which can be sufficient for many M2M solutions, is to integrate off the shelf chips that provide encryption and decryption.

As pressures on the level of required security increase, many have recognised that the protection of secured communication subsystems does not extend to all parts of the remainder of the supply chain. M2M solutions are increasingly incorporating 'Elements of Security' at different points in the supply chain. These may involve hardware, operating systems, embedded security and the application layer and other parts, and are being independently developed by several different supply chain players for a variety of needs.

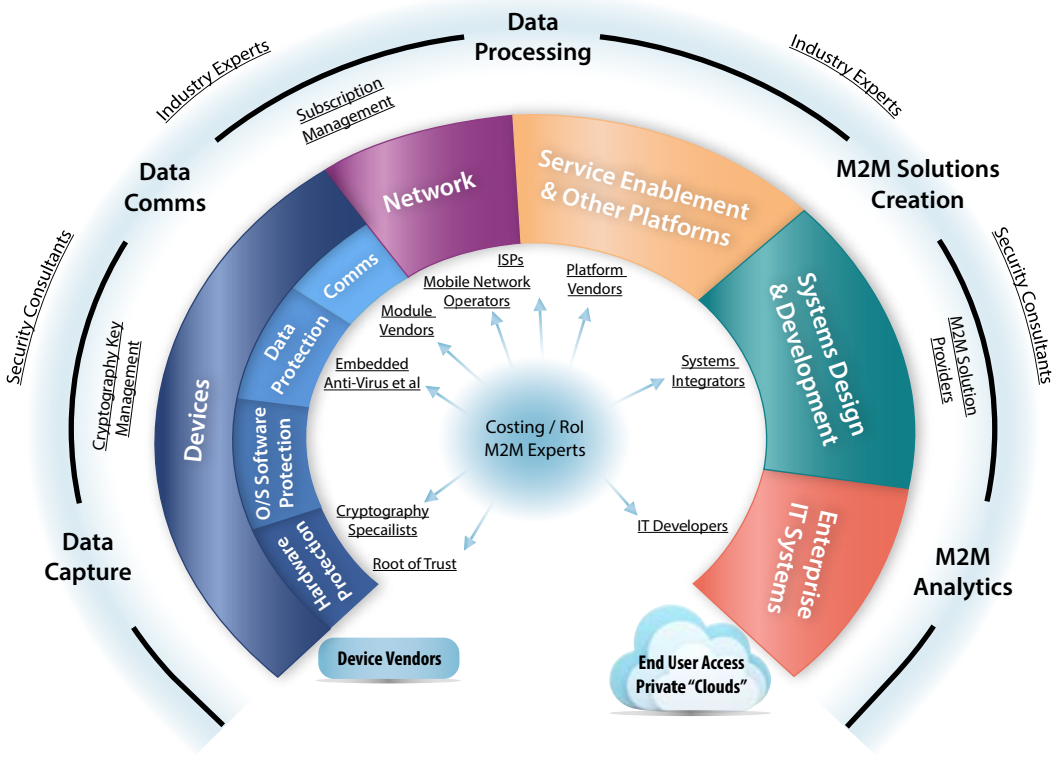
KILLING THE M2M PATIENT ?

Assuring end to end M2M security will likely involve more than one specialist vendor in these 'Elements of Security'; the challenge is for the multiple elements provided by these vendors to be dynamically linked together to form an end to end chain, in order to mitigate a specific threat. Identifying the nature of that threat will be key, and will necessitate input from sector specific experts. We should not forget the role of the customer and end user: suppliers of technology may provide design expertise, but customers and ultimately end users must understand their business and the business implications of these design choices.

Security breaches could occur not only within the domains of the participants, but also as data is passed between them. Hence M2M solutions must guarantee sufficient security protection at the boundaries and interfaces between the different domains that are part of the overall solution, comprising devices, networks, M2M platforms and enterprise systems. Beecham Research's recent research shows that many organisations are considering how to integrate their M2M solutions with strategic corporate systems. This would extend both the M2M delivery chain and the corresponding 'Elements of Security' overlay to incorporate enterprise systems.

> *If the reaction to the new security threats is simplistically to add even stronger protection, then the costs of that additional security will result in M2M solutions that are not economically viable.*

Figure 2: Diagrammatic Representation of the M2M solution supply chain, with participants and suppliers, including those providing 'Elements of Security'



Source: Beecham Research 2013

Whilst as we saw above 'Elements of Security' are being independently improved by several different supply chain players, some will overlap with Elements of Security with a wider remit or application. However if existing and future supply chain members each try to strengthen the security capabilities of their particular area and products, this could lead to duplication of some capabilities.

Moreover, if the reaction to the new and various security threats is simplistically to add even stronger protection, then the costs of that additional security will result in M2M solutions that are not economically viable, in other words, killing the 'M2M patient'. M2M solutions have been and will continue to be sensitive to costs, and the economics of a solution will vary between sectors and applications.

Hence the future success of a secure M2M solution will require careful consideration and validation of all parts of the chain.

TABLE: Mapping M2M solution development with 'Elements of Security' development

Processes in creating an M2M solution	Standard M2M solution component development activities	Elements of Security special activities
Planning and Designing including cost analysis	Standard good practice in development	Security requirements-based risk analysis
Create network of devices/modules	Standardised devices/modules	Secured chips, semiconductors, devices/modules
Create communications link	Connectivity supplied by telecoms/wireless/wired operators	Additional network/SIM security, incorporating secure upgrading, support
Incorporate hardware	Standard Hardware	Hardware ID secured with Secure Element and others
Incorporate sof tware, operating systems, platforms	Standard components, subscription management	Software protection, data protection
Storage	Standard components	Secured and safe storage
M2M solution integration/testing	Industry-wide expertise, standard techniques	Specialist solution-based expertise, security-focused testing
Business operations/ applications	IT systems; data analytics	Application layer security e.g. data protection, user ID and privacy, passwords

Source: Beecham Research 2013

In the table, the left hand column shows the processes in creating an M2M solution, from planning and designing the solution, through creating a network of devices for data capture, to creating enterprise IT systems with secure end user access. The central column lists standard solution development activities that apply to all M2M solutions, whilst the right hand column lists activities in creating specific Elements of Security for a particular M2M solution.

Security of identity for machines is already an important part of ensuring that connected devices sending data are a true part of the M2M solution. As we move towards the Internet of Things, where Beecham Research studies are showing that the consumer is increasingly in the loop, the importance of ID verification for human users of the systems will rapidly increase.

CREATING THE SECURE SUPPLY CHAIN

Secured M2M solutions will therefore have two layers: the conventional M2M supply chain with its players, and an overlay composed of a chain of 'Elements of Security'. This chain will encompass all parts from the devices, networks, enterprise systems as well as the interfaces between these domains. Once identified, the security supply chain players will need to carry out their activities, ranging from:

- Defining the requirements and if applicable, regulations, for their M2M application area
- Planning the secure end to end M2M system, starting with an assessment of the impact of security requirements, with the participation of all supply chain members. This means identifying security issues at the start using risk analysis and similar techniques, and incorporating effective mitigating controls so as to avoid the risks without losing the benefits
- Designing, then testing the system to ensure that these controls work as intended.

Privacy by design or privacy by default is a much talked about methodology to ensure data protection. Data protection has caught the attention of regulators of late, particularly in Europe, and these are ramping up rules to penalise both providers and users who do not conform. The academic community is doing much to develop techniques to this end. However complete privacy has proved to be unattainable, hence choices must be made to prioritise needs so as to make the solution affordable and realistic.

Complete privacy has proved to be unattainable, hence choices must be made to prioritise needs so as to make the solution affordable and realistic.

Even when designing-in security, compliance with best practices is required for designing, developing and testing new hardware and software. All manufactured products must today conform to quality standards. It is generally recognised that building-in quality from the start of the development process may cost resources and money, but developers need to balance the ultimate cost of non conformance, e.g. security breaches and the forfeiting of customer trust and goodwill, with the cost of preventing these errors (cost of conformance).

Certification services are also spreading to enable compliance with different regulations in the many different M2M applications. Such services have long been part of quality assurance in standard commercial system developments. A secure M2M solution is the same as any large enterprise system in that it requires testing, quality assurance and sometimes certification, depending on the industry. Even in M2M vertical markets with minimal regulation, solution providers should provide evidence of sufficient protection for customers, and provide a structure for the qualification of suppliers and the assignment of responsibility for their products.

Hence successful futures for M2M solution security will depend on understanding and right sizing the security features that are implemented. These futures will also depend on the players – who often use different versions of 'technospeak' and are trained in different disciplines - being able to work together effectively to deliver the end to end solution. In this regard, it is interesting to note that the survey in Figure 1 also found that coordinating partners in the value chain is a high priority.

In the future, regulatory constraints will demand that levels of security required in M2M applications such as telemedicine and smart metering be specified precisely, and how and where that security will be implemented. As lawmakers in different countries place differing levels of importance on issues such as privacy protection, even more variations will be introduced, with which M2M solution developers will need to comply.

TOWARDS A RATIONAL APPROACH

In order to be prepared to rise to this challenge, a rational approach is needed, rather than a panic response. This approach should be based on:

- Understanding that security is an evolving field and the time line over which security service requirements will manifest themselves in the market and become commercially viable – and mandated by regulators.
- Understanding key security requirements in specific industries
- Identifying the ways present and new market players can work together effectively. A framework for understanding needs to be developed
- Understanding how M2M solution providers will satisfy customer security requirements, either through the use

> of internal resources or via specialist suppliers, and using standard or proprietary solutions. This suggests the possible emergence of new types of specialist supplier of Elements of Security. If these new suppliers operate in several market verticals, their solutions will need to be standardized to work across these.

As part of Beecham Research's continuing research into Security for M2M solutions a report will be published in early Q2 2013 that explores these security issues and the business opportunities they create.

The report will present the wider range of current and emerging future opportunities and the associated needs for correctly addressing right-sizing of security for systems of connected devices. Also covered will be the new opportunities for adding value and generating improved revenues through security related services.

The report will also explore how the M2M security landscape is changing as the needs of end-to-end security rapidly change.

Read the report and you will hear about: the business potential in interactions in security between M2M market players old and new; and the new business models, balance and opportunities that can, and must, be created in M2M solutions security.

For more details on the report and how to order it contact us at
M2MSecurity@beechamresearch.com