

Issues and Business Opportunities in Security for M2M Solutions

Table of Contents

1. Introduction
 - 1.1 Defining Security
 - 1.2 The Heart of Security for M2M - and the Focus of this Report

2. Executive Summary

3. M2M Solution Security a High Priority
 - 3.1 Reactions Incompatible with M2M Business Models
 - 3.2 Variations in Understandings of Security

Driving Forces in M2M Security

4. M2M Solution Supply Chain - Relation to Elements of Security

5. Right-Sizing of Security for M2M
 - 5.1 Security is Always a Compromise

6. Threat & Risk Analysis
 - 6.1 M2M Data - Example of Variability and Complexities of Risk
 - 6.2 Architecting Security, Building Successful M2M
 - 6.3 When is Risk Analysis Needed?
 - 6.4 Role of Leading Security and Risk Consultants
 - 6.5 Consultancy Market Gap for Smaller Scale M2M Projects
 - 6.6 DIY for In-House Lower Risk M2M Projects
 - 6.7 Evaluating & Averting Risk in Installation, Operations and Maintenance Phases

7. Importance of Security Standards and Regulations
 - 7.1 M2M Applications Benefitting from Informal Standardisation
 - 7.2 Standards & Regulations for Verticals
 - 7.2.1 Moving from New Verticals to New Standards
 - 7.3 Standards for M2M and its Security
 - 7.4 Certification

Reference Resources: Views from Industry Perspectives

8. Views from Industry Perspectives

8.1 Current and Future Best Practice - Increasing Collaboration

8.2 Views from in and around:

M2M Service Platform Providers	Mobile Network Operators	Module Manufacturers
Enterprise IT Systems	Connected Device Makers	System Integrators
ICS and SCADA Systems	SIM Card Manufacturers	Embedded Systems
Chip Level Subsystems	Cryptography Specialists	

The Market Opportunity: Value and Elements of Security

9. Evolution of Elements of Security Technology

10. Value of Security

10.1 The Costs

10.2 The Direct Returns

10.3 The Indirect Returns

10.4 Future of Security as a Service

10.5 Market Opportunity - Forecast

Future Steps in Security

11. The Shape of Things to Come

11.1 Emerging M2M Solutions Crossing Multiple Domains

11.2 Emerging Influences on Security from Embedded Systems Experience

Utilising Embedded Systems Approaches to Operating Systems

Long Lifetime Connected Devices Demand Security Updates

11.3 Moving Towards the Internet of Things

Increasing Complexity - Increasing Security Needs

High Volumes of Connected Devices - Standard Basic Security

Experimental IoT Connected Devices and Security Incompatibilities?

The Threat and Promise of DIY Maintenance

Adding the Consumer to the Mix

Towards Constrained Devices

12. Towards a Rational Approach to M2M Security

Profiles of Market Players

13. Profiles of Market Players

ARM Holdings

Cryptography Research Inc

Gemalto

ILS Technology

Numerex

Trusted Labs

Axeda Corporation

Digi International

Giesecke and Devrient

INSIDE Secure

Praesidium

Wind River

Codenomicon

Elliptic Technologies

Green Hills Software

Neul

Sierra Wireless

14. Glossary

Table of Figures

- Figure 1: Beecham Research Survey of Leading M2M providers
- Figure 2: Diagrammatic Representation of the M2M Solution Supply Chain
- Figure 3: Elements of Security and the Supply Chain
- Figure 4: Industry Linked Security Standardising Organisations
- Figure 5: Actors in and Around New Verticals and New Standards
- Figure 6: Differentiated Security Market Players - The Tip of the Iceberg
- Figure 7: Not All M2M Solutions Are Created Equal
- Figure 8: Elements of Security - M2M Original Core Focus
- Figure 9: Elements of Security - M2M Connected Devices Defence
- Figure 10: Elements of Security - M2M's Expanding Boundaries
-
- Table 1: Mapping M2M Solution Development with Elements of Security Development
- Table 2: Illustrating Type of Security Risk by Vertical Application

Total number of pages (excl. TOC): 138

Achieving M2M solution security is not just desirable – it is also absolutely necessary, but at what cost?

Issues and Business Opportunities in Security for M2M Solutions provides a comprehensive examination of the challenges and opportunities in M2M solution security, including:

- An exploration of threat and Risk Analysis, with an assessment of risks for different vertical markets and all different applications
- Introducing new concepts related to a holistic view of solution security, including how to make a success from Elements of Security
- Profiles of 17 leading market players in different parts of the overall value chain, illustrating their approach to key security issues
- Views from the industry on current and future best practices
- Definitions and projections of revenue opportunities for different segments of the overall M2M solution security market to 2018
- An analysis of the value of security and balancing cost versus risk
- An exploration of the importance of security standards and regulations: What is happening now and what needs to happen next?
- Assessment of:
 - The impact of emerging M2M solutions crossing multiple domains
 - Moving towards the Internet of Things
 - Emerging influences on security from embedded systems experience

Issues and Business Opportunities in Security for M2M Solutions will be of interest to:

- M2M solution experts identifying potential for new partnerships/areas where their expertise and capabilities can enable new market growth
- Elements of Security specialists who see the opportunities, obstacles and mechanisms to wider adoption of their products
- System Integrators who see those areas where their capabilities will be in increasing demand
- Risk and Threat Security consultants who see the potential in extending their M2M involvement or engaging with M2M for the first time
- Embedded Systems specialists who can start to map their expertise and products into the M2M and IOT spaces

- IOT innovators who see strategic security risks threatening the commercial success of their products – how they can address these
- Suppliers of Security as a Service who see threats such as DIY maintenance and accelerating opportunities – catalysing new business models
- Market players in the M2M value chain and the future IOT who can identify business opportunities, collaborations and more
- Market players who see the ways in which standardization is being built and can be influenced and utilized
- Business and strategy developers

SAMPLE PAGES

1.2 The Heart of Security for M2M - and the Focus of this Report

Many of these points emerge from the analysis in this report, but are important to understand up-front as they shape the heart of all issues and opportunities for Security in M2M.

The points outlined have also shaped what has proven meaningful and valuable to report.

There is no single approach to the implementation of Security in all M2M Solutions. Therefore no single analysis is complete in itself as a description of present activities and future possibilities.

There are different security approaches being taken by many market sectors to address different threats, trust requirements, specific needs of verticals, communications methods and more in the appropriate ways.

What is more, many of the better planned current security approaches contain valuable lessons for planning in the M2M Security sector. Hence many vertical market sectors can benefit from the expertise of security capabilities currently applied in other sectors.

In addition, there are opportunities for improvement through commercial relationships, collaborations and acquisitions. In the complex world of security expertise, it is often best to rely on established experts rather than building all of those capabilities internally.

In this report, several expert views and methods are described in the level of detail needed to engage with these opportunities for progress. Full understandings of those approaches have been gathered and can be presented where required; in our view, this is preferable to creating a large report that presents in detail the entire range of M2M security approaches.

Principles to remember:

The highest value of Security is in the things that it enables

Without sufficient Security there can be no trust and no privacy

Security measures alone can not guarantee trust or privacy

Security can enable business success (and without it businesses will fail)

As with any weapon of defence or attack, the outcome is dictated by how you choose to use it and what you are trying to defend or defeat

especially damaging to businesses where risk-averse clients demand independent reassurance of their correct choices in security architecture & capabilities. In that latter case, this market gap can lead to some M2M projects being infeasible.

6.6 DIY for In-House Lower Risk M2M Projects

Some M2M projects with low complexity and lower security risks are being tackled in-house by organisations which are relatively inexperienced in M2M. There have been many examples where, given a common approach of ignoring security in the project planning stages, even lower security risks have become a potentially damaging threat. Such risks and threats are likely to increase in coming years, as they are increasing throughout the worlds of connected devices.

At the most basic level, there appears to be gap in the understanding and experience of M2M security issues by these M2M solution builders. Nonetheless, some consultants with extensive M2M and security expertise, such as Nick Hunn of Wi-Fore, have advocated a systematic approach to this sort of project that has proved successful.

Although there is a need to learn how to plan the security architecture of such lower complexity M2M products, excellent progress can be made through a security risk assessment using RMADS (Risk Management and Accreditation Document Sets). In utilising that manual process the architect is effectively asking "What do I need?" in all appropriate areas and "What do I need to implement at each stage?"

This approach based around RMADS has even been made to work for M2M solutions requiring significant levels of security.

6.7 Evaluating & Averting Risk in Installation, Operations and Maintenance Phases

Amongst other complexities, it is important to keep in mind the risks posed to the security of M2M solutions by choices and actions taken during all of the installation, operations and maintenance phases.

There is evidence of evaluated security risks being invalidated by those actions. Evaluating the associated risks with additional focus on these potential actions is an essential step, but putting policies and procedures in place to avoid such vulnerabilities is also needed.

For example, in order to reduce installation costs or to improve installation speed, decisions such as retention of default passwords in network connecting devices



Issues and Business Opportunities in Security for M2M Solutions:

About Beecham Research

ABOUT BEECHAM RESEARCH

Beecham Research is a leading market analyst and consulting firm that has specialized in the development of the rapidly-growing M2M/Internet of Things market worldwide for over a decade, since 2001. Based in Cambridge UK and in Boston US, we actively participate in initiatives aimed at achieving M2M market development and growth. Recent research has included two market-leading and widely supported studies on M2M Cloud-Based Platform Services and a study of the worldwide Satellite M2M market contracted by the European Space Agency. Ongoing research includes new business models for the Internet of Things, Healthcare and other vertical sectors. Visit www.beechamresearch.com for more information.

In conducting our research, we cover 9 key industry sectors and their associated devices including all principle technologies for connecting them – both fixed line and wireless. We offer customized market analysis and consulting services including subscription-based services tailored to individual company needs.

Contact us at:

Email: info@beechamresearch.com

Tel: +44 (0)845 533 1758 Fax: +44 (0)845 533 1762

ABOUT PROF. JON HOWES, TECHNOLOGY DIRECTOR

Jon Howes is based in the UK and is Technology Director at Beecham Research. Before joining Beecham in 2011, Jon led his own NEuW Limited consultancy team since 1993 building products and services based on new semiconductor and other advanced technologies for clients around the world, in sectors as wide-ranging as automotive, smart grid and healthcare. Leading R&D and marketing activities with Fujitsu and Ferranti in the preceding years, Jon helped launch many types of products including some of the first GSM solutions. He combines a strong technical background – particularly in wireless, semiconductor technologies and system software – with deep market knowledge of M2M-related sectors and is an expert in M2M solution security. His Professor title is a result of his past work in delivering Industry and Markets insights at the University of Newcastle in the UK, and highlights his continuing links with leading research institutions.

