Executive Summary

Security is critical to the success or failure of the Internet of Things and Machine-to-Machine markets. Recently the critical flaws identified at the heart of the Internet, such as the Heartbleed bug, have highlighted engineering fallibility. The successful attacks in industrial M2M, such as Stuxnet, have highlighted hereto hidden aspects of cyber warfare. Plus attacks on consumer IoT in connected lighting and white goods, have demonstrated the broad capability for attacks and the rapid impact of fear on consumers as they react to perceived loss of control to cyber criminals. These issues, challenges and fears, justified or not, will have significant potential impact on market adoption of IoT technology and its ultimate success or failure.

The goal of this report is to highlight a key set of security recommendations and requirements across the industry, stretching from device implementation through to the high-value cloud services required to support the Internet of Things. It is expected that these recommendations should be considered by executive leadership plus general management responsible for IoT within device and service vendors, alongside industry visionaries.

The target users of IoT devices and associated services are open to strong debate within the industry. These users include “Main Street” Consumers who will consume large volumes of connected home goods, and who already are alerted to security concerns through the mainstream press; through to more technically able Professional IoT Consumers, who will integrate and maintain large scale systems. Further users include technical experts within both IoT and M2M domains who may have significant teams available to them.

Security is fundamental in enabling the implementation of solutions for all of these user groups. It is required to enable the development, deployment and maintenance of systems in factories and in homes; it underpins the majority of the high value services to be evolved in the cloud and on devices; it is critical in assisting the management of liabilities across system implementation; and it is essential in providing a common framework to enable the growth of multi-vendor solutions.

Security is therefore a critical feature of all solutions and must be considered early in the marketing and engineering cycles of devices, software and services. The consumer experience in these domains is king, and therefore security must be both tightly integrated and practically invisible to ensure the best consumer experience.

The threat from cyber-attackers cannot be ignored in this marketplace and governments are already working with cross-industry forums to help close the knowledge gap and define the problems we face together. The timeline to deliver secure IoT and M2M is short and the need for open frameworks, driven by broad

interoperability is critical. This report is informed by these developments and the application of critical security controls to the Internet of Things arena.

Key recommendations included in this report include the following:

- Enhanced frameworks & interoperability

While a number of standardization efforts are underway inside the industry, most notably AllSeen Alliance and Open Interconnect Consortium, there is still significant effort required to ensure interoperability.

Most notably interoperability needs to be established around Identification, Authentication and Encryption, but then needs to extend to remote device management, updates and frameworks that support long term service provision for multi-vendor and multi-network solutions.

- The implementation of "Security First" development processes

To ensure costs and complexity are minimized it is critical that security be well architected from the start of the process, encompassing hardware, software and services.

It is therefore critical that device and system designers maintain a very clear vision of the users and how these people expect systems to operate and be supported in their homes or premises. To achieve this it is important to have a clear vision of the technical security requirements that is shared throughout the industry in an open, free and unlimited manner.

It is recommended that the industry develop clear use case analysis of system implementation, from industrial and professions IoT users, through to technology agnostic and technology illiterate end users.

- Lifecycle management

A key finding of the report is the need to support many IoT systems, in-situ, over a number of years and the impacts this has on security.
Most notable is the need to create systems with the resources to enable a remote, yet highly robust, patching and updating system that will ensure as threats evolve the systems can themselves extend capabilities.
Further the need to initially deliver strong defences needs to be mirrored by the assumption that at some time, and in some way, these defences will be breached and therefore a mechanism is required to reset, regain control and remediate the problem.

- Enablement of value added services

Security should not be seen as a cost, rather it is a necessary mechanism to enable a set of highly valuable extended services that requires specific hardware and firmware hooks within the system.

Examples of these services include, but are not limited to:

Advanced system management – Visualisation and ownership tools that enable end users to build and manage systems from numerous vendors inside a single package, while also ensuring data boundaries are instantiated properly.

Policy management – Ensuring that only people or devices with suitable credentials are enabled to access systems or make changes, based on sets of known of future criteria.

Anti-malware – In a world beyond existing anti-virus software the need to monitor systems for threats and ongoing attacks is critical. The ability to enable heuristic analysis within large systems, or even meta-systems is critical.

Big data analytics – The ability to analyze large data sets is critical to the deliver of next generation services from governments, companies and other organizations. To enable analytics we have to ensure privacy and maintain specific data boundaries to ensure individuals continue to control their data. Only with the right infrastructures can this be supported.