Securing Internet of Things (IoT) Services Involving Network Operators

May 2017

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address 5G, the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The adoption of Internet of Things (IoT) services is rapidly growing. IoT services can provide significant advantages to consumers, enterprises, and government institutions. It is important that as IoT services are designed and delivered, full account is taken of the security considerations both to protect the IoT service itself and to prevent IoT equipment becoming a source of attacks against other service users.

In some cases, the network operator's role in delivering IoT services is simply to provide connectivity and there is no direct technical or business partnering between the operator and the IoT service provider. In other cases, the network operator may take a more active role where the IoT service includes technical and business aspects under the control of the network operator. In this report, several different scenarios are introduced that characterize different relationships and levels of partnering that may exist between a network operator and an IoT service provider. In these scenarios, shared responsibility for securing the service may exist and consequences of security failures may be felt by both the network operator and the IoT service provider. The security implications of the various scenarios are discussed and practices that can be used to proactively address security in these scenarios are provided.

No part of this document should be taken as normative. Its purpose is to document practices that may be helpful to the development of good solution security. As each situation is different, it is necessary for the security approach to be chosen by the parties involved appropriately for their service, priorities, and circumstances.

2 Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

ACL	Access Control List
API	Application Programing Interface
ARA	Architectural Risk Analysis
ATIS	Alliance for Telecommunications Industry Solutions
CPE	Customer Premises Equipment
IoT	Internet of Things
IPSO	Internet Protocol Smart Objects
LWM2M	Lightweight Machine to Machine
M2M	Machine to Machine
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NoT	Network of Things
OCF	Open Connectivity Foundation
OIC	Open Internet Consortium
OMA	Open Mobile Alliance
RPK	Raw Public Key

PSK	Pre-Shared Key
SIM	Subscriber Identity Module
SM	Security Module
SMS	Short Message Service
SW	Software
VNF	Virtual Network Function
WWW	World Wide Web
XMPP	Extensible Messaging and Presence Protocol

3 Overview of Market Segments

3.1 Example Scenarios for IoT Service Offers by Operators

Many IoT services are provided by organizations that focus purely on IoT activities and treat connectivity (either over Wi-Fi or cellular) as a dumb pipe. However, more sophisticated IoT services – especially those involving many devices distributed over a wide area – benefit from closer attention being paid to connectivity aspects. The following scenarios consider cases where network operators are involved in the provision of IoT services either to leverage the value of their brand or to take advantage of their wide-area connectivity assets.

Typically, an IoT service will involve communications, device, and network (cloud)-based elements. Network operators are well equipped to provide connectivity but may choose to work with third parties to provide the other solution elements. There are a variety of different scenarios for the relationship between the network operator and third party IoT partners. Each of these scenarios has different security implications.

3.1.1 Operator develops, brands, and markets its own service

In this scenario, the operator takes complete responsibility for all aspects of the IoT service. Though the operator owns and manages the complete service, it may procure hardware and software elements from third parties and integrate them into the service. In particular, network operators will work with hardware vendors to build IoT devices.

For example, home broadband operators may provide home gateway devices or set top boxes as part of their package. With users' permission, these devices may monitor their electrical supply voltage and AC frequency. This data may be collected by the operator and supplied to power companies to allow them to assess the health of their distribution network in real-time.

In this type of scenario, the operator acts as the technical design authority for the complete service. As such, the operator should apply good security practices during the service design. This should include a full assessment of the security implications of the service design and the creation of a cybersecurity risk management plan.

Where the operator includes hardware or software from third parties in the solution, the operator's security assessment should define the security requirements placed on these elements. The operator should then audit these elements to ensure that they meet the identified security requirements.

3.1.2 Operator procures a partner's solution; brands and markets the service directly to customers

In this scenario, the operator sells an IoT solution developed and operated by a third party using the operator's brand. The operator makes no technical changes to the IoT solution.

This scenario is most likely to arise when the operator wishes to have additional services to offer as part of their package. For example, the operator may extend their home broadband service by offering additional services such as home security monitoring. Technically, the home security solution is provided by an existing third party.

In this scenario, the network operator is dependent on the third party for the cybersecurity of the service being marketed under their brand. In order to protect their interests, the network operator should ensure that the third parties solution has an effective approach to cybersecurity. This may be done, for example, by requiring the third party to share their cybersecurity risk management plan and by auditing the third party's compliance to that plan.

Some areas of cybersecurity planning may fall under joint responsibility in this model. In particular the handling of public relations during a cybersecurity incident requires coordinated activity by the network operator and the third party solution provider.

3.1.3 Operator provides access and other network services for an IoT/M2M partner to bundle and market to their customers – Co-branded services

In this scenario, the operator sells access and other network services to an IoT/M2M partner. The IoT/M2M partner will bundle with their solution and sell as a co-branded service or a joint enterprise. When effectively done, co-branding provides a way for companies to combine forces so that their marketing efforts work in synergy. The IoT/M2M partner benefits from the operators existing customer base and marketing.

In this scenario, the operator is basically providing the backbone and would be responsible for the normal day-to-day cybersecurity on their existing network. The IoT/M2M partner would be responsible for the cybersecurity planning for the IoT/M2M solution.

Overall cybersecurity should be reviewed and part of the contract/agreement by both parties in this model. Due to the co-branding, a cybersecurity incident could have negative impacts on the network operator and/or the third party solution provider. Again in particular the handling of public relations during a cybersecurity incident requires coordinated activity by the network operator and the third party solution provider.

3.1.4 Operator provides access and other network services for an IoT/M2M partner to bundle and market to their customers - Operator and IoT/M2M provider each have an independent relationship with customers

In this scenario, the operator provides the access and other network services that enable an IoT/M2M service. The network provider and third party solution provider will each independently own the relationships with their respective customers.

In this scenario, both the operator and the third party are responsible to provide cybersecurity planning as well as validation of the others plan. Overall cybersecurity should be reviewed and part of the contract/agreement by both parties in this model.

A cybersecurity incident on either the network provider or the third party provider would have a negative impact on both. Again in particular the handling of public relations during a cybersecurity incident requires coordinated activity by the network operator and the third party solution provider.

3.2 Protecting Brand Value when providing IoT Services

As discussed above, IoT services may include elements from several different sources. All these elements contribute to the overall security of the service. Where operators market IoT services under their band any security failures will inevitably be associated with the operator's brand wherever the security vulnerability originated. This is particularly true because most network operators have a high profile in their operating countries and spend heavily on brand development.

While the brands of third party providers of service elements are less at risk in the event of a security breach, it is still possible that they will receive negative publicity if they become associated with a security failure. Therefore, third parties that offer solution elements should still have an independent cybersecurity management plan.

In order to protect their brands, operators marketing IoT services should have their own cybersecurity management plan as described in the previous scenarios. This will manage the risk of cybersecurity incidents. This plan should include a section dealing with incident response that includes the management of public relations during and after a cybersecurity incident. The cybersecurity plan should include a plan to enable service restoration following a cybersecurity incident.

4 Survey of Existing Work on IoT/M2M Security

The need to improve security for IoT/M2M applications has been widely recognized in the industry. There are a number of relevant activities summarized in the following table. During the analysis it was found that the various working groups have generally produced one of two types of recommendation. Some working groups produce general guidance on IoT security that is not tied to a specific technology platform (e.g., the work by the Cloud Security Alliance). These are labelled with a "G" in the table below. Other working groups define specific technology platforms to support IoT services that include platform-specific security features (e.g., oneM2M). These are marked with a "P" in the table below.

Table 4.1: Working Group Activities Relevant to IoT Cybersecurity

Working Group (Active Since)	Charter	Comments	Type G=General P=Platform
IPSO Alliance (Sep 2008)	Establish *Internet Protocol (IP)* as the network to interconnect smart objects and allow existing infrastructure to be readily used without translation gateways or proxies.	Extensively reuses existing, industry standard, IP protocols. We did not find significant, original, security content.	G
IoT-A (2010-2013)	Developed an architectural *reference model* to allow seamless integration of heterogeneous IoT technologies into a coherent architecture to realize 'Internet of Things' rather than 'Intranet of Things'.	This project was conducted as part of the EU's research agenda and aimed to define a framework for later industry consideration rather than create normative specifications for commercial application. Its security recommendations may be a useful input to security modelling.	G
AllSeen Alliance (2013)	Collaborate for an open, universal IoT software framework across devices and industry applications, based on AllJoyn *open source project*, originally developed by Qualcomm but now released to community developers.	See write-up below.	P
Industrial Internet Consortium (Mar 2014)	Accelerate development and adoption of *intelligent industrial automation* for public use cases.	The Industrial Internet Consortium has excellent participation from a variety of industry vertical sectors. Their published security guidelines are useful for their application domain and compatible with the approach in this document.	G