An Architectural Risk Analysis for Internet of Things (IoT) Services

March 2019

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global Information and Communications Technology (ICT) companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, machine-to-machine (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.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

Table of Contents

1 Executive Summary

The adoption of internet of things (IoT) services has accelerated enormously as multiple industries have recognized the extent to which IoT services can provide significant advantages to consumers, enterprises, and government institutions. Given the wide range of IoT-based services and products, their rapid entrenchment into daily life, and the increasingly sensitive and critical roles they can play, security must be a top consideration.

Protecting IoT services and applications requires a solid and well-founded set of security defenses that have been selected to provide the necessary (and—it is hoped—sufficient) safeguards against those threats deemed to pose the greatest risks to the service, its users, and the service providers. A risk assessment that identifies vulnerabilities in a quantifiable manner is a necessary first step in constructing a sensible IoT security posture. This paper has been written to address the fundamentals needed to perform risk assessments for IoT assets.

This report uses the *ATIS Security Architectural Risk Analysis (ARA)*[1] to establish a framework for assessing a generic IoT asset's cybersecurity risk. That asset might be an application, a service, or something else. Its primary function might be to collect and manipulate data, or it might be to perform some task, simple or complicated. It might be a standalone device, or it might work in coordinated fashion with a few or many other applications, services, or machines. It might be a low-level spoke in a wheel, or it might be a critical component of some vast mechanism. As an IoT "thing," it could be nearly anything, and for the purpose of this analysis, exactly what it is does not matter. It is simply "the asset."

This paper establishes the fundamentals that permit an examination of the risks to the asset from cyber-attacks that might be launched from anywhere, with a wide range of intents. The ATIS ARA methodology has been applied, with the following results:

1. This report provides a risk-assessment framework that is successful for:
   - Recognizing that IoT assets share many common features that differentiate them from non-IoT networked assets.
   - Identifying primary, secondary, and other IoT real-world assets, in accordance with the ARA methodology.
   - Establishing a complete set of consistent and useful attributes for each IoT asset. In working through the methodology, the authors have also established new criteria for determining the correctness of a set of attributes; namely, that they constitute a complete set—i.e., that for a given asset, the attributes listed are all there are; and that they be orthogonal in the sense that attacks on a given attribute must not bleed over to other attributes.
   - Providing a reasonable subset of the attacks to each of those assets. According to the ARA methodology, this is done by delineating the list of possible attacks against each of the asset's attributes based on how each attribute can be exploited (the so-called *exposures* of the attribute). This report shows how the ARA methodology is used to pinpoint the attacks and attack classes to which each attribute is exposed.

2. The report provides a simple though plausible example of how the ARA can be applied to an IoT asset.

One major benefit of an ARA risk assessment is that its results identify specific security mitigations that can address the most serious threats. As a result, it can suggest the best expenditure of time, money, and resources to fortify an asset to mitigate the most serious risks. In the case of IoT assets, the size, complexity, and perhaps cost to the user all put strict limits on how much development time, effort, and money can be directed towards security. Thus, the capability to assess the risk provides immense value to designers, architects, and planners as they go through their respective tasks of bringing an IoT asset into existence. The framework developed in this report offers a mechanism for using the ARA methodology to make that happen more directly because it has been tailored to the IoT landscape.

[1] *Cybersecurity Architectural Risk Analysis Process*. ATIS-I-0000057. May 2017. Alliance for Telecommunications Industry Solutions; Washington, DC.

2 Introduction

The emergence of IoT-based services is already creating explosive demand for new devices and applications. According to *Forbes*,[2] a 2017 survey predicted 20 billion connected devices globally by the end of 2018, with steady (rather than explosive) growth through the year. *Business Insider*[3] projects that "there will be more than 55 billion IoT devices by 2025, up from about 9 billion in 2017." It goes on to predict "that there will be nearly $15 trillion in aggregate IoT investment between 2017 and 2025, with survey data showing that companies' plans to invest in IoT solutions are accelerating."

The growth forecasts in terms of dollars are probably a more telling indication of the explosion of interest in and adoption of IoT than raw numbers of devices would ever be. The devices themselves, which include connected cars, machines, meters, wearables, and other consumer electronics, will be connected to the internet or to private network environments and will need robust security mechanisms (such as the capability to clearly assert an identity that can be authenticated by the network and/or application appropriate for that device).

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.

IoT device types range from simple, small sensors to complex, large systems such as connected vehicles, which contain dozens of IoT devices. Regardless of the form factor or level of sophistication, devices must connect to IoT application servers or client devices via one or more intermediate networks. For example, the device may connect via private or public networks using a variety of connection mechanisms such as:

- Wired access via a physical connection (e.g., Ethernet cable to a local network).
- Wireless unlicensed private access (e.g., Wi-Fi or Bluetooth to a private network).
- A public licensed spectrum wireless access using standard 2G, 3G, 4G, or 5G radio technologies.
- Public wireless access provided by network operators using unlicensed spectrum technologies such as Wi-Fi, Citizens Broadband Radio Service (CBRS), and MulteFire™-based networks.
- Other wide area networks using various Low Power Wide Area Network (LPWAN) technologies.

In some cases, the device may connect to the network via an intermediate gateway device.

Given the wide variety of device types and access methods coupled with the large numbers of devices being deployed, network security concerns voiced by many experts[4,5,6] are well founded. This paper looks more closely at network-related security aspects of the IoT domain, with a specific focus on the security risks associated with IoT devices and services.

---

[2] Newman, Daniel. "The Top 8 IoT Trends for 2018." *Forbes*. December 19, 2017.

[3] Newman, Peter. "There Will Be More Than 55 billion IoT Devices by 2025—These Are the Biggest Drivers For Adoption." *Business Insider*. July 27, 2018. https://www.businessinsider.com/internet-of-things-report?op=1

[4] Meola, Andrew. "How the Internet of Things Will Affect Security & Privacy. *Business Insider*. December 19, 2016. https://www.businessinsider.com/internet-of-things-security-privacy-2016-8

[5] Palmer, Danny. "IoT Security: Where Do We Go from Here?" *ZDNet*. November 13, 2018. https://www.zdnet.com/article/iot-security-why-everyone-needs-to-step-to-ensure-the-security-of-the-internet-of-things/

[6] Zorz, Zeljka. "IoT Security: The Work on Raising the Bar Continues." *HelpNetSecurity.* August 22, 2018. https://www.helpnetsecurity.com/2018/08/22/iot-security-challenges/

2.1 Document Purpose

With an awareness of IoT security on the rise, methods to provide protection to the devices, the services, the data, and the users of all three must start with an understanding of the risks that IoT-based technologies introduce or exacerbate. It is generally agreed that a risk assessment is a necessary step that should predate the design of solutions and the creation of solutions architectures, so that correct security solutions can be designed in up front and a comprehensive security architecture can be crafted to dovetail with the overall solution architecture itself. This document provides a starting point for assessing the risks associated with IoT solutions. To do so, it applies the ARA to general IoT solutions involving network operators. Through this process, threat modeling techniques are applied to ensure proper security considerations are part of the solution by design.

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.

2.2 Scope and Context

The ARA methodology is expected to help network operators, application providers, and their third-party partners and suppliers to assess the robustness of their IoT architecture by identifying key points where security controls are needed to thwart potential threats and the associated risks. Prior to applying the ARA process, it is necessary to establish a context that supports the application of the process.

IoT solutions involving network operators may engage four players or actors, illustrated in figure 2.1, in providing the IoT service:

- The IoT device management entity handles processes such as providing device configuration and fault-management services. The IoT device might be a single physical device, a gateway, or a controller for a multitude of sensors or actuators. The IoT device might be directly connected to the network operator via a WAN interface to cellular (2G, 3G, 4G, or 5G). Or it might be connected via a LAN, which in turn connects to a wireless or wireline network via a gateway/modem element.
- The network operator that provides the network service.
- One or more identity providers that certify the identity of the device for network, application, or management authentication and/or authorization purposes. For WAN access, this entity is often the network operator. However, roaming cases exist where a home network provides authentication services to a visited network. Separate identity providers may also exist to provide application- or management-specific services.
- The application provider that provides a service based on IoT device communication. The application provider will often utilize servers to provide the IoT application. Client devices may also be enabled on behalf of the application domain to connect directly to IoT devices.