FCC TAC Cybersecurity Working Group

Applying Security to Consumer IoT Devices Subcommittee

Technical Considerations White Paper
December 2015

Release Version 1.1
12/4/2015

Table of Contents

Acronyms

AES	Advanced Encryption Standard
APU	Accelerated Processing Unit
BSIMM	Building Security In Maturity Model
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Team
CoAP	Constrained Application Protocol
CPS-PWG	Cyber-physical Systems Public Working Group
CSA	Cloud Security Alliance
CTA	Consumer Technology Association
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring system
DDS	Data Distribution Service
DHS	Department of Homeland Security
DOT	Department Of Transportation
DTLS	Datagram TLS
FCC	Federal Communications Commission
FPGA	Field-Programmable Gate Array
FTC	Federal Trade Commission
GPRS	General Packet Radio Service
HMAC	keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IPC	Inter-Process Communication
IPSO	IP for Smart Objects Alliance
IoT	Internet of Things
IRM	Identity Relationship Management
LAN	Local Area Network
LTE	Long-Term Evolution
MQTT	Message Queue Telemetry Transport Protocol
M2M	Machine to Machine
MCU	Microcontroller
NIST	National Institute of Standards and Technology
NOI	Notice of Inquiry
NSF	National Science Foundation
NVD	National Vulnerability Database
OASIS	Advancing Open Standards for the Information Society
OEM	Original Equipment Manufacturer
OIC	Open Interconnect Consortium
OWASP	Open Web Application Security Project
PAN	Personal Area Network
PSP	Platform Security Processor
REST	Representational State Transfer
RTOS	Real Time Operating System
SASL	Simple Authentication and Security Layer
SCC	Standards Coordinating Committee
SDLC	Systems/Software Development Life Cycle
SN	Sensor Network
SoC	System on a Chip
SSL	Secure Sockets Layer
TAC	Technological Advisory Council
TLS	Transport Layer Security
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver/Transmitter
UPnP	Universal Plug and Play
XMPP	Extensible Messaging and Presence Protocol
WG	Work Group
XSS	Cross Site Scripting

1. Executive summary

For 2015, the FCC Technological Advisory Council Cybersecurity Work Group was requested to examine the special cybersecurity challenges posed by the emerging Internet of Things, and to suggest actionable recommendations to the FCC with focus on the security and protection of IoT consumer products. In particular, the FCC asked the Work Group to address six questions related to this charter. This paper is loosely structured around these questions.

Media reports of security breaches on consumer IoT products have become a frequent occurrence. These reports range from actual breaches by hackers with real financial goals, to "proof of concept" demonstrations by white-hat hackers, to concerns based on the terms in product license agreements. Hackers have an array of tools freely available, and in the meantime the manufacturers have not treated device security as a priority. It should be no surprise that the working group found that the hackers have the lead at this time.

However, industry does appear to be moving in the right direction. The working group found evidence of consortia and alliances specific to security, trade associations and standards development groups working in device security, "best practice" recommendations, and a growing array of development tools and processors available with security features.

Through the TAC Cybersecurity Work Group's research we identified a list of key findings.

<u>Key Findings:</u>

- Spectrum:
  - Many IoT devices use spectrum allocated and regulated by the FCC
- Identified Gaps:
  - A CSA survey reveals that IoT investors and technology startups are not prioritizing security
  - There have been many security gaps publicly identified in existing IoT solutions
  - Many traditional device manufacturers lack cybersecurity expertise and need to implement secure systems/software development life cycle (SDLC) processes
  - Due to long development cycles, insecure products will continue to enter the market for a period of time
  - For many types of IoT devices, physical access cannot be restricted, thus devices that expose critical information on internal nodes can be compromised
- How industry is addressing these gaps:
  - Industry organizations acknowledge IoT security gaps and are prioritizing security-related technology and best practices
  - There are many publicly available best practices that provide excellent guidance on IoT security, both from a technology and process perspective
  - Processor manufacturers are responding to market needs by providing small system on a chip (SoC) processors that include security features
- Standards:
  - There are a wide variety of technology standards and how security is addressed within these standards

    - Some organizations do not permit review of security requirements without alliance membership, or NDA, etc.; these barriers limit open review by security researchers and the broader industry
    - Many standards allow for different security implementations, some less secure than others
- Compliance/Testing:
    - There are a number of industry organizations providing compliance requirements and testing that includes security for the technology promoted by the organization
- Best Practices:
    - There are multiple industry best practices available, including documents from CTA, CSA, NIST, FTC, DHS, OWASP, etc. (see the Best Practices section for more details)
    - A few examples of specific best practices:
        - Techniques such as internal data encryption and the use of security-hardened chipsets should be leveraged to stop determined hackers, especially when physical access cannot be controlled
        - Communications of user names and passwords (UN/PW) should be encrypted
        - Password management should be more robust, e.g., different passwords for each device

2. Purpose and Scope

a. Purpose

The 2015 FCC Technological Advisory Council Cybersecurity Working Group addressed three topics as directed by the FCC. This document captures the results of analysis done by the subcommittee created to address Topic 2 – Securing IoT Consumer Products.

The FCC posed the following six questions to the Working Group:

1. What are the underlying technologies (e.g., WiFi, ZigBee, GPRS, LTE) that dominate the IoT space, and what security vulnerabilities and challenges do they present in the IoT environment?
2. What other security challenges face IoT consumer products? For example, to what extent does lack of physical security pose a threat to unsupervised IoT devices? Explain.
3. What is the industry doing to secure and protect battery-operated and resource-constrained (i.e., minimum computing power and memory) M2M devices, which cannot encrypt its data?
4. How are the IoT/M2M stakeholders addressing those security challenges and vulnerabilities, and what are the gaps?
5. What is the potential impact of these security challenges on the future of IoT/M2M industry, the end user and the economy, especially when IoT devices become fully integrated in all of our systems, including our critical infrastructures?
6. What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of M2M/IoT devices and systems?

Various sections of this document (as marked in the headings) will address each of these questions.

b. Scope

The Subcommittee created the following scope and direction to address the FCC's questions:

- Start by leveraging valuable work produced by the 2014 TAC IoT Working Group
- Examine the cybersecurity challenges posed by the emerging Internet of Things, and suggest actionable recommendations with particular focus on the security of IoT consumer products
- Understand IoT security challenges, e.g., securing unsupervised resource constrained devices
- Investigate how stakeholders are addressing security challenges today, identify the gaps, and understand the potential impact of these challenges to the future of the IoT industry where IoT devices become fully integrated in all of our systems

3. Reference model

The term "Internet of Things" has been used without definition, has been defined, and has been swapped out for other variants (such as Internet of Everything, Industrial Internet of Things, and M2M). To discuss security in this context, we show a reference architecture (see Figure 1). This basic structure shows the IoT from several points of view:

1. **Hierarchy**
   In the left-most portion of the Figure, there are three top-level hierarchical elements.

   The Cloud/Data Center represents the distributed network of servers and networking gear making up the Internet and cloud storage and processing, away from the local Thing.

   The Gateway represents the interface between the Internet and the device (or "Thing"). This Gateway is the interface between the public WAN-side network (that is, the Internet) and the private or LAN-side intranet[1]. Additionally, the Gateway may also bridge between technologies; the Thing may not use IP addressing or may be on a proprietary RF link.

   The Devices & Sensors are the Things in the Internet of Things. These Things have embedded processors and communications links.

   Note that some devices may be able to serve multiple roles in the above described hierarchy. For example, the sophistication and flexibility of modern smartphones is such that they can act as both Devices & Sensors (e.g. the smartphone's accelerometer or GPS based location providing sensor data) and Gateways (e.g. providing the interface between a Bluetooth enabled fitness wristband and a cloud based back end).

2. **Goals**

[1] In the case of IPv4 devices. Over time, IPv6 is expected to replace IPv4, especially for the vast number of devices. However, a gateway device to the public Internet is still required for most types of Things.

Manage Devices: A main requirement of the IoT is the ability to monitor and control the Things from the Internet.

Understand the System: In order to protect network integrity, someone must know enough about the system to monitor for attacks and to keep the system updated.

Protect Communications: Various types of attacks rely on compromising communications between Things, between a Thing and local computing (including the user's smartphone), between a Thing and the cloud, or between local computing and the cloud.

Protect Devices: Devices may be vulnerable to hands-on (physical access required) attacks or remote attacks. Understanding threats and mitigations at the device level is essential.

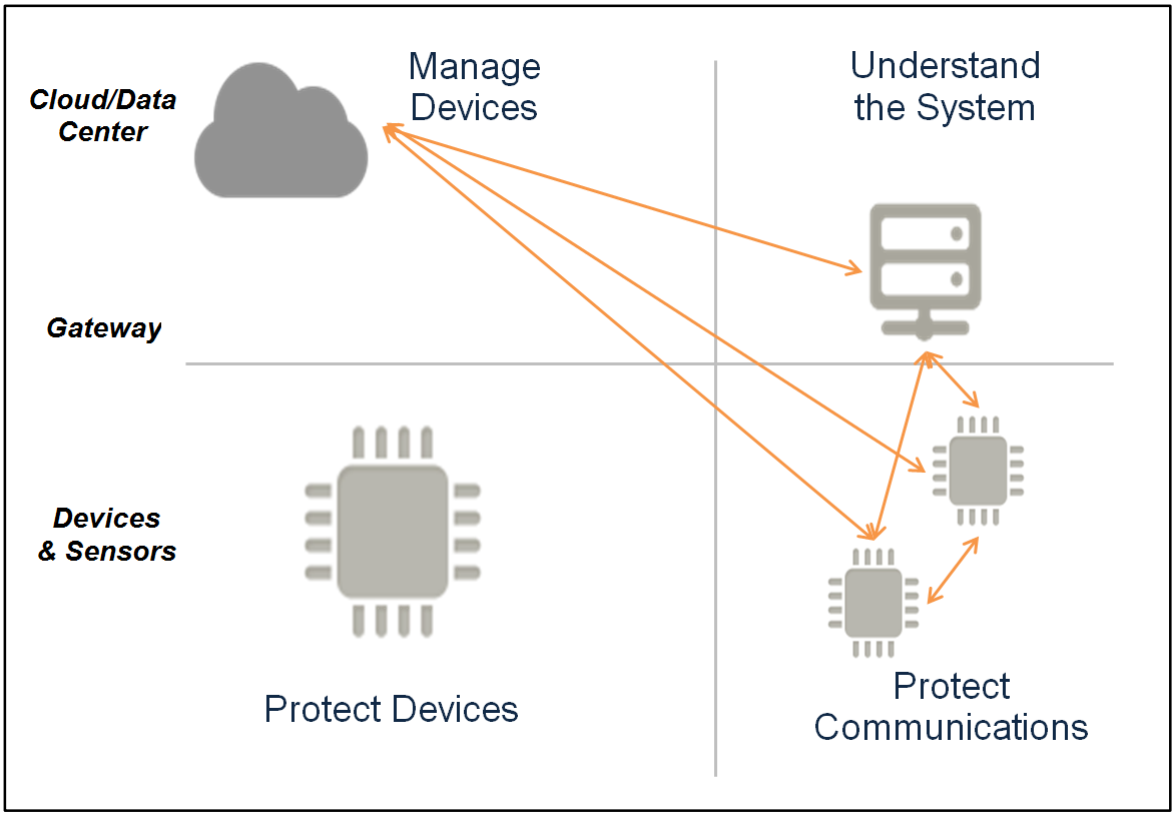

Figure 1: Reference architecture highlighting four main goals of a security-hardened IoT system.

In the following sections, this white paper will consider the industry landscape that supplies and supports this architecture; the underlying technologies and the security challenges faced by manufacturers.

4. Industry landscape

The team evaluated various industry activity related to IoT security. The groups fall into 4 general categories:

- IoT industry group – companies and individuals interested in promoting IoT processes and practices including creating technical conformance practices and performing conformance tests
- Mobile industry group – companies and individuals interested in promoting mobile phone and network processes and practices extending those to IoT; this is separate from IoT industry groups primarily because they are mature and well known to the FCC and the TAC membership
- Standards organization – create technical standards
- Government organization – US government organizations with interest in policies and technologies related to IoT

There is significant activity going on at the industry level. The industry recognizes that security is an issue and is putting a priority on providing a secure IoT environment. The various groups are described in more detail in this section with the intention that this could help the FCC should it decide to reach out to these groups for more information.

With the exception of the IETF, all of these organizations are membership run. For the most part activity within the organization is proprietary, available to members only and cannot be shared publicly. In most cases this makes evaluating their effectiveness with regard to ensuring security difficult.

a. IoT Industry Groups

Allseen Alliance

Allseen Alliance[2] consists of over 185 companies focused on IoT devices and software. Their goal is to enable industry standard interoperability between products and brands with an open source framework that drives intelligent experiences for IoT. They also provide conformance requirements and testing.

Allseen's Security 2.0 allows applications and devices to validate access based on owner policies. The AllJoyn Core Permission Management component provides enforcement including mutual authentication. The Allseen Security Manager supports key management, permissions, and application manifest to let the user authorize interactions for the application.

Cloud Security Alliance

[2] https://allseenalliance.org/

CSA[3], established in 2008, is a not-for-profit organization promoting education and best practices around securing clouds. CSA's mission is to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing". In 2013, CSA actively participated in the TAC Cybersecurity Working Group's activities around cloud security.

The CSA Mobile Working Group recently published security guidelines for IoT early adopters (discussed later in this document). This IoT effort has focused on those areas where traditional enterprise security efforts may fall short for IoT use cases – e.g. difficulty in applying perimeter security, the challenges associated with mass quantities of devices, privacy concerns, mobility, and platform security limitations

Consumer Technology Association

The Consumer Technology Association[4] (CTA)™, formerly the Consumer Electronics Association (CEA)®, is the trade association representing the $285 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

CTA conducts market research, industry outreach and education in many industry verticals that collectively make up the IoT. These include audio and video (smart TV, wireless audio systems); automotive (connected car, driverless car); digital imaging (connected cameras and printers); health and fitness (connected wearables, connected health & wellness products, "lifestyle"[5] products); Tech Home (smart home security, HVAC and home entertainment controls); and Wireless and Accessories (smartphones, smartphone-connected devices).

CTA also works on particular topics that cut across industry verticals. For example, CTA conducts membership working groups on privacy policy. Recently, this group developed voluntary best practices for wellness data that preserve the ability to innovate while creating strong consumer privacy protections. CTA's working groups tackle related issues such as spectrum, accessibility, and medical device regulation as well. CTA has recently formed a member IoT Working Group.

Industrial Internet Consortium (IIC)

The IIC[6] was founded in March 2014 by AT&T, Cisco, GE, Intel and IBM. It is not a standards organization and was created to accelerate growth of the industrial Internet by coordinating

[3] https://cloudsecurityalliance.org/
[4] www.cta.tech
[5] "Lifestyle" is a category of (typically connected) devices that fit the daily living and health and wellness needs of a specific demographic, such as seniors, children, and families with pets.
[6] http://www.iiconsortium.org/

ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards that lead to transformational business outcomes. It evaluates and organizes existing standards to; 1) advocate for open standard technologies, and 2) influence the global standards development.

Two relevant working groups at IIC are the Reference Architecture and Security Working Groups. The Reference Architecture WG's goal is to align the industry to a common end-to-end Industry IoT reference architecture with clearly defined constituent components and interfaces. The Security WG charter is defining a security and privacy framework to be applied to technology adopted by the IIC. The framework will establish best practices and be used to identify security gaps in existing technology.

The CTO of IIC is also the co-chair of the NIST Cyber Physical Systems Public WG Reference Architecture Subgroup.

IP for Smart Objects (IPSO) Alliance

The Internet Protocol for Smart Objects (IPSO) Alliance[7] is a global forum including many Fortune 500 high tech companies and noted industry leaders. Since 2008 IPSO has been serving as a thought leader for communities seeking to establish the Internet Protocol (IP) as the network for the connection of Smart Objects and devices for IoT and M2M applications. The IPSO Alliance provides a foundation for industry growth by providing education, promoting the industry, generating research, and creating a better understanding of IP and its role in the Internet of Things. Its primary goals are to promote IP, to enable investment in innovation, to uphold the IP standards, and to enable IP-based interoperability. Its objective is not to define new technologies, but to document the use of IP-based technologies.

Open Interconnect Consortium (OIC)

Founded by Atmel, Dell, Intel, Samsung Electronics and Wind River among others, the OIC[8] is developing specifications, certifications & branding to deliver reliable interoperability. This standard expects to be an open specification that anyone can implement and is easy for developers to use. It will include IP protection & branding for certified devices (via compliance testing) and service-level interoperability. There will also be an Open Source implementation of the standard. This Open Source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

As an example of some consolidation activity within the IoT consortium space, the OIC announced[9] in November 2015 that it was acquiring the assets of the UPnP ((Universal Plug and

[7] http://www.ipso-alliance.org/
[8] http://openinterconnect.org/
[9] http://openinterconnect.org/oic-news-releases/open-interconnect-consortium-increases-membership-with-upnp-forum-agreement/

Play) Forum. Both groups communicated the move would benefit their consortiums as well as the burgeoning Internet of things (IoT) space.

Thread Group

The Thread Group[10] is a not-for-profit organization responsible for the market education around the Thread networking protocol and certification of Thread products. Thread is an IP-based wireless networking protocol providing the best way to connect products in the home. With Thread, product developers and consumers can easily and securely connect more than 250 devices into a low-power, wireless mesh network. The Thread group was founded in part as a result of Google's acquisition of Nest, and the need to ensure interoperability certifications.

Thread recently announced product certification testing that will include security testing. "Thread products will be tested to validate device behavior for commissioning, networking functionality, security and operation in Thread's network, and may bear the "BUILT ON THREAD" or "THREAD CERTIFIED COMPONENT" logo to help consumers and product developers identify them on the market."[11]

Underwriters Laboratories (UL)

UL[12] is known for creating many safety related standards, including (but not limited to) the safety of industrial control devices, electrical appliances, building products, wire & cable, and electrical/electronic appliances. More recently, UL has expressed interest in pursuing industry certification in the area of IoT device security. In October of 2015, the Cybersecurity IoT TAC sub- group had an opportunity to discuss with UL their evolving efforts around this topic.

UL is working on an IoT security program called the Cybersecurity Assurance Program (CAP) pilot. UL's goal is to help vendors manage risk by helping them reduce SW vulnerabilities and raising security awareness. The CAP scope includes both product assessment (e.g. SW vulnerabilities, the use of security controls), and organization assessment (e.g. SW lifecycle process, including patch management). The first focus is in ICS (Industrial Control Systems) and medical devices, with a planned launch by 1Q2016. The program is intended to be voluntary, with vendors incentivized to participate in a manner similar to other UL certification initiatives.

Some additional points extracted from our UL discussions:

- The CAP program focuses on software for now, with future iterations looking at hardware implementations.
- The TAC group inquired about the challenge of UL getting access to proprietary software from vendors. UL indicated it is viewed as a trusted partner and companies are usually receptive to sharing their source code under NDA. Black box testing is also possible if the source code is not provided.

[10] http://threadgroup.org/
[11] Thread Group press release, "Thread Group Launches Product Certification", 2015-11-11, available at http://threadgroup.org/Default.aspx?Contenttype=ArticleDet&tabID=94&moduleId=492&Aid=83&PR=PR
[12] http://ul.com

- The CAP pilot program includes product testing (known vulnerabilities, fuzzing, malware, security controls), penetration testing (ports, external services), and process audit (patch management).
- The CAP full program will greatly expand on the areas of focus, including static/dynamic code analysis, wireless interfaces, SDLC, supplier controls, and risk management.
- Regarding current status (as of 4Q2015), UL has put out a draft of their requirements to a pilot set of collaborating companies for review. They have begun testing of their draft and are pursuing customers (participants).
- Sources of requirements include CAPEC (Common Attack Pattern Enumeration and Classification). CAPEC was established by DHS as part of the Software Assurance strategic initiative of the Office of Cybersecurity and Communications (CS&C).
- Another source of requirements is CWSS (Common Weakness Scoring system). CWSS is another DHS sponsored initiative, part of the Common Weakness Enumeration (CWE) project within DHS' Cybersecurity and Communications Software Assurance program.
- The NIST National Vulnerability Database (NVD) is leveraged for the known vulnerabilities part of CAP
- When asked about consortia participation, UL indicated it is a member of the IIC (Industrial Internet Consortium).
- UL plans to target the automotive market after it completes its work in the ICS and medical markets.
- The process of putting together the CAP pilot is relatively closed thru 1Q2016. A broader panel of participants will be used after the pilot.
- There is some focus on networking devices (e.g. routers, switches, etc,) with inclusion of wireless interfaces. This aspect of UL's work may be of special interest to the FCC.

b. Mobile Industry Groups

CTIA – The Wireless Association

CTIA-The Wireless Association[13] (originally known as the Cellular Telephone Industries Association) is an international nonprofit membership organization that has represented the wireless communications industry since 1984. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products. CTIA does not set standards, but they do work with standards bodies to gain alignment and consensus within the industry.

The relevant areas where CTIA would be a benefit are the Cybersecurity Working Group (CSWG) as well as the Privacy Working Group (PWG). The CSWG focuses on all aspects of cybersecurity that affects the industry and its members, as well as legislative and government efforts around cybersecurity that might impact the membership. The PWG is also focused on privacy issues both within the industry and in government. Both of these groups are looking at IoT and the respective focal issues.

[13] http://www.ctia.org

GSMA

The GSMA[14] represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organizations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

GSMA IoT Security Guideline Document Set[15]
This document is one part of a set of GSMA security guideline documents that are intended to help the nascent "Internet of Things" (IoT) industry establish a common understanding of IoT security issues. The set of non-binding guideline documents promotes methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services.

The structure of the GSMA security guideline document set is shown below in Figure 2. It is recommended that this document, (i.e. the overview document) is read as a primer before reading the supporting documents.

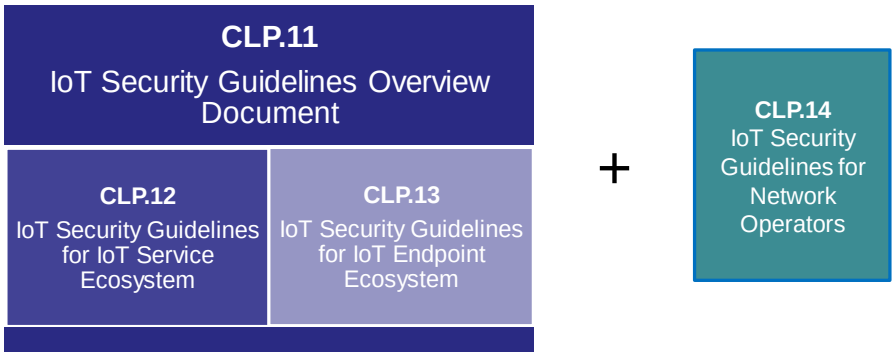

Figure 2 - GSMA IoT Security Guidelines Document Structure

Network Operators are advised to read GSMA document CLP.14 "IoT Security Guidelines for Network Operators"[16] which provides top-level security guidelines for Network Operators who intend to provide services to IoT Service Providers to ensure system security and data privacy.

oneM2M

The purpose and goal of oneM2M[17] is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware

[14] http://www.gsma.com
[15] http://www.gsma.com/connectedliving/wp-content/uploads/2015/10/CLP.11-DRAFT-IoT-Security-Guidelines-Overview-Document-V0.11.pdf
[16] http://www.gsma.com/connectedliving/wp-content/uploads/2015/10/CLP.14-DRAFT-IoT-Security-Guidelines-for-Network-Operators-V0.1.pdf

and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. Initially, oneM2M shall prepare, approve and maintain the necessary set of Technical Specifications and Technical Reports for:

- Use cases and requirements for a common set of Service Layer capabilities;
- Service Layer aspects with high level and detailed service architecture, in light of an access independent view of end-to-end services;
- Protocols/APIs/standard objects based on this architecture (open interfaces & protocols);
- Security and privacy aspects (authentication, encryption, integrity verification);
- Reachability and discovery of applications;
- Interoperability, including test and conformance specifications;
- Collection of data for charging records (to be used for billing and statistical purposes);
- Identification and naming of devices and applications;
- Information models and data management (including store and subscribe/notify functionality);
- Management aspects (including remote management of entities);
- Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between:
    - Application and Service Layers
    - Service Layer and communication functions

Under the scope of oneM2M, the Security WG has the overall responsibility for all technical aspects related to security and privacy within oneM2M. The Security WG performs the security analysis of the oneM2M system architecture and applies best practices to derive technical solutions, including but not limited to authentication, encryption and integrity verification. The WG will determine the resulting requirements for oneM2M system integrate security into the oneM2M system architecture and specify the security protocols. Also, the security group will specify the means for provisioning and protecting sensitive data (e.g. security credentials) and to enable their management.

c. Standards Organizations

CTA

CTA is accredited through the American National Standards Institute and maintains approximately 70 committees, subcommittees and working groups for approximately 1,100 participants. Vertical categories include audio and video, portable/handheld, in-vehicle and home networking, and home systems installation. CTA recently published best practices for manufacturers and for installers for securing consumer IoT devices in the connected home.

[17] http://www.onem2m.org

IEEE

IEEE has numerous standards related to IoT:

> **SCC42**[18] leads the coordination of IEEE standardization activities for technologies related to transportation, especially in the areas of connected vehicles, autonomous/automated vehicles, inter- and intra-vehicle communications, and other types of transportation electrification. These technologies include but are not limited to Mobile Apps, Sensor Networks, and Communications that allow human to vehicle, vehicle to vehicle, vehicle to infrastructure, vehicle to platform, and vehicle to everything exchange of information and data. Where standardization needs exist, the SCC will develop guides, recommended practices, standards, and common definitions of terms.
>
> **802.11**[19] is a set of Media Access Control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands.
>
> **802.15.4**[20] (Low Rate WPAN) deals with low data rate but very long battery life (months or even years) and very low complexity. The standard defines both the physical (Layer 1) and data-link (Layer 2) layers of the OSI model.

IETF

The IETF[21] is a long-standing standards setting body for technologies supporting Internet infrastructure. There are numerous working groups that are directly addressing the needs of IoT systems involving transport, messaging, and security

Kantara Initiative

Kantara Initiative[22] provides support and standards development work in the identity management disciplines. Work includes: Identity Relationship Management, User Managed Access, Identities of Things, and Minimum Viable Consent Receipt. Kantara Initiative connects a global, open, and transparent leadership community.

Kantara is now, and has historically, focused on user privacy features of new and existing protocols and frameworks.

[18] http://standards.ieee.org/news/2014/ieee_scc42_transportation.html
[19] http://standards.ieee.org/about/get/802/802.11.html
[20] http://standards.ieee.org/about/get/802/802.15.html
[21] https://www.ietf.org/
[22] https://kantarainitiative.org/

OASIS (Advancing Open Standards for the Information Society)

OASIS[23] is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS presently supports several technical committees that are employed in IoT systems today:

- OASIS Advanced Message Queuing Protocol (AMQP) TC
- OASIS Message Queuing Telemetry Transport (MQTT) TC
- OASIS Open Building Information Exchange (oBIX) TC

OASIS also supports several security related technical committees, many of which will be applicable to IoT systems.

d. Government Organizations

NIST Cyber-physical Systems Public Working Group

The National Institute of Standards and Technology is a non-regulatory agency of the US Department of Commerce. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

The NIST Cyber-Physical Systems Public Working Group[24] (CPS PWG) was formed in 2014 to develop and implement a new cyber security framework dedicated to cyber-physical systems (of which IoT is a part), however, the initial focus was not consumer IoT. NIST has been broadly looking at the CPS space, with 175 participants and growing. The National Science Foundation (NSF) has also funded academic groups for the CPS draft framework.

For reference, NIST's definition of CPS is repeated here:

> "*Cyber-physical systems (CPS) are smart systems that include co-engineered interacting networks of physical and computational components. These highly interconnected systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use.*"

[23] https://www.oasis-open.org/
[24] http://www.cpspwg.org

5. Applying security to consumer IoT devices

a. Underlying technologies and their challenges

The IoT is composed of many layers of technologies, each with its own set of security challenges. An IoT-based ecosystem consists of the physical devices that are deployed at the edge, as well as the gateways and services that those devices interact with to perform a fully threaded set of functions.

i. Hardware

An individual IoT device is composed of many layers of technology as well. Hardware components include the microcontroller (MCU) that provides the computing capability, transceivers that support communication using a variety of protocols, and the boards that bring these components together. Batteries represent another aspect of IoT hardware, although in some cases power may be drawn directly from a larger device that the IoT component is hosted within.

Hardware-based sensors are used to provide a device the ability to sense various aspects of its environment. There are numerous types of sensors available to support a variety of purposes. Along with sensors, IoT devices may implement various types of actuators, which provide a means to act on the environment.

Challenges related to Hardware

1. Hardware vs. Software Security

IoT devices are physical things, and it is often easy to acquire those things through various means. Researchers and malicious actors that are interested in reverse engineering an IoT device often simply need to buy one from a retail establishment. In other cases, they can be acquired through theft as they are left in open environments to perform their functions.

This ready availability of IoT devices for reverse engineering purposes is of significant concern because today's devices typically lack the advanced security features inherent in more complex computers. While laptops typically implement hardware security mechanisms such as Trusted Platform Modules (TPMs), highly constrained IoT devices are not capable of incorporating these into their designs. These highly constrained devices typically rely upon software-based security services to protect sensitive material held on the device. The use of a software-based module instead of a hardware security module increases the risk associated with the capture and reverse engineering of an IoT-device.

2. Exposed Test and other physical Ports

Ports on IoT devices can provide an attack vector for malicious parties attempting to break into a device. One example is the exposure of Universal Asynchronous Receiver Transmitters (UARTs), which are often used for debugging the device. Since many IoT devices are often left in exposed environments, the risk of an attacker obtaining a device and investigating device

internals is high. Exposed UARTs allow an attacker to interface directly with the hardware, using a simple cable and terminal emulation software. Attackers can then open a shell which oftentimes provides root access to the device. This access is not always protected by a username/password combination. In other instances where access is password-protected, it is often only protected by a well-known username/password combination.

3. Limited Tamper Response Capabilities

More robust devices often include some form of tamper resistance, which in some cases can be used to zeroize sensitive material on the device. Most IoT devices do not support this functionality, allowing researchers and malicious parties to access the internals of the device.

ii. Operating systems

Operating systems for IoT devices have become commonplace. There are dozens of Real Time Operating Systems (RTOS) available for use. Some examples of RTOS' used in support of the IoT include:Tiny OS, Contiki, Mantis, LiteOS, FreeRTOS, SaphireOS, Brillo, Embedded Linux, mbedOS, VXWorks, LynxOS, and Ubuntu Core. IoT-based operating systems are often configured with applications that run on top of them and then uploaded as images to the actual hardware. In many instances, the size of the operating system is significantly limited, with some operating systems taking up only 10KB of space.

Challenges related to Operating Systems

1. Out of Date Software

Oftentimes, embedded operating systems are built by obtaining the latest code from a code repository (e.g., gitlab). The operating systems are then uploaded to the target IoT platform for use. In order to keep the latest version of operating system, processes have to be in place to continually perform these updates.

2. Default or non-secure accounts and keys

Oftentimes as the quantities of IoT devices within any particular net grows, the account passwords and keys for each of the devices are duplicated. It is important that organizations that deploy IoT devices make sure that operating system accounts are given unique passwords and that keys used by the OS as authenticators are unique to each device.

iii. Messaging protocols

Messaging protocols allow for IoT devices to communicate with each other, with gateways and with services. These messaging protocols are run on top of lower layer communication protocols. Examples of messaging protocols include the Constrained Application Protocol (CoAP), the Message Queue Telemetry Transport Protocol (MQTT), the Data Distribution Service (DDS), and the Extensible Messaging and Presence Protocol (XMPP). Some of these protocols offer IoT or Sensor Network (SN) tailored-versions.

These protocols offer varying capabilities for secure configurations. In most cases, devices that implement these protocols should also support the use of security protocols such as Transport Layer Security (TLS) or Datagram TLS (DTLS), while at the same time making use of the security controls available within the messaging protocols themselves. As an example, MQTT offers the ability to use passwords, but without a lower layer confidentiality service, those passwords would be sent in the clear.

Other messaging protocols provide additional authentication capabilities. For example, CoAP offers designers the ability to use certificates, raw public keys or shared secrets for authentication purposes. The selection of the appropriate mechanism depends on a number of factors, however leveraging shared secrets across many different devices opens security concerns related to reverse engineering.

Challenges Related to Messaging Protocols

Protocol	m2m Authentication Options	Security Discussion
MQTT	username/password	MQTT allows for sending a username and password, although recommends that the password be no longer than 12 characters. Username and password are sent in the clear, and as such it is critical that TLS be employed when using MQTT.
CoAP	preSharedKey rawPublicKey certificate	CoAP supports multiple authentication options for device-to-device communication. Pair with Datagram TLS (D-TLS) for higher level confidentiality services.
XMPP	Multiple options available, depending on protocol	XMPP supports a variety of authentication patterns via the Simple Authentication and Security Layer (SASL – RFC4422). Mechanisms include one-way anonymous as well as mutual authentication with encrypted passwords, certificates and other means implemented through the SASL abstraction layer.
DDS	X.509 Certificates (PKI) using RSA and DSA algorithms. Tokens	The Object Management Groups Data Distribution Standard (DDS) Security Specification provides endpoint authentication and key establishment to perform subsequent message data origin authentication (i.e., HMAC). Both digital certificates and various identity / authorization token types are supported.
HTTP/REST	Basic Authentication (cleartext) (TLS methods) OAUTH2	HTTP/REST typically requires the support of the TLS protocol for authentication and confidentiality services. Although Basic Authentication (where

		credentials are passed in the clear) can be used under the cover of TLS, this is not a recommended practice. Instead attempt to stand up a token-based authentication approach such as OAUTH 2.

iv. Communication technologies

The TAC IoT sub-group investigated key communications technologies focusing on wireless. We've divided the technologies into four categories:

- Mobile/WAN – mobile technologies used for wide area networks, which cover a large geographic area, we categorized this separately from WAN because mobile technologies are extremely familiar to the FCC and TAC members
- WAN – wide area network, non-mobile technology covering a wide geographic area
- LAN – local area network, covers a relatively small geographic area, such as a residence, building or campus
- PAN – personal area network, covers a small geographic area ranging from centimeters to a few meters

The matrix below identifies the technology, the category, the organization that manages it, and notes related to the technology or the organization.

Technology	Organization	Category	Note
LTE	3GPP	Mobile/WAN	3GPP/3GPP2 creates global standards to mobile networks
GPRS	3GPP	Mobile/WAN	"
UMTS	3GPP	Mobile/WAN	"
CDMA	3GPP2	Mobile/WAN	"
LoRaWAN	LoRa Alliance	WAN	Originally developed by Cycleo, acquired by Symantec
Weightless–N/W	Weightless SIG	WAN	Developed by Neul, acquired by Huawei
802.11	IEEE	LAN	Widely used wireless LAN technology referred to commonly as Wi-Fi
802.15.4	IEEE	LAN	Many other protocols are based on 802.15.4 technology
6LoPAN	IETF	LAN	Based on 802.15.4
ZigBee	ZigBee Alliance	LAN	Based on 802.15.4
Thread	Thread Group	LAN	Based on 802.15.4
Z-Wave	Z-Wave Alliance	LAN	Focused on home automation
Sigfox	Proprietary	LAN	Developed and managed by Sigfox
Bluetooth	Bluetooth Alliance	PAN	Widely used wireless PAN technology
Bluetooth LE	Bluetooth Alliance	PAN	Bluetooth technology developed specifically for low energy IoT applications

NFC	NFC Forum	PAN	Focused on proximity, 10cm or less
WAVE IEEE 1609	IEEE	PAN	Focused on vehicular environment
ANT/ANT+	ANT+ Alliance	PAN	Developed by Garmin, focused on health sector
DASH7	DASH7 Alliance	PAN	Focused on RFID

Challenges related to Communications Technologies

Evaluating these technologies is somewhat difficult because the standards documents are proprietary to the organization that manages them (with the exception of the IETF). In addition, since committees create standards they typically allow multiple implementations. Some implementations may be less secure than others. Thus a solution can be standards compliant yet not as robust as it may need to be.

Some security gaps however have become public, allowing us to summarize them.

Zigbee provides both network and application level authentication (and encryption) through the use of Master key (optional), Network (mandatory) and, optionally, Application Link keys. It allows for the temporary exposure of keys while provisioning a new device.

Due to the need for simplicity in Bluetooth devices it is common for manufacturers to use the same password for all like devices. For example a particular manufacturer may use the password 1234 for all of its Bluetooth headphones. The protocol also allows for other more secure solutions.

Bluetooth provides authentication services through two different device pairing options, Standard and Simple Pairing. The Standard pairing method is automatic; the Simply pairing method includes a human-in-loop to verify (following a simple Diffie-Hellman exchange) that the two devices display the same hash of the established key. Bluetooth offers both one-way as well as mutual authentication options. Bluetooth secure simple pairing offers 'Just works', 'Passkey entry' and 'Out of Box' options for device-device authentication.

Bluetooth-LE introduces to the Bluetooth world a two-factor authentication system, the LE Secure Connections pairing model which combines – based on device capability – several of the available association models available. In addition, Elliptic-Curve Diffie Hellman is used for key exchange.

b. Device security challenges

i. Insecure environment

The deployment of IoT devices within insecure environments opens the device up to many attacks that would not be seen in a corporate environment. These attacks primarily allow for adversaries to take advantage of exposed physical interfaces on the device, however they also allow attackers to attempt to circumvent the security applied to wireless protocols.

In situations where an attacker has been able to reverse engineer a device, critical data such as shared symmetric keys may be compromised. In this case, the attacker would likely have access to all data held within other devices that share the same key. Identifying default passwords on a reverse-engineered device would also lead to the ability to easily compromise like-devices within a network.

We have already seen new approaches to performing reconnaissance on IoT devices. Researchers have attached a sensor to an unmanned aerial system (UAS) that listens for Zigbee beacons and then maps out the devices.

ii. Lack of physical security

IoT devices often suffer from a lack of stringent physical security. In some cases, outer casings may be applied that provide tamper-evidence, however this is not always possible. Additionally, the ability to take positive action (tamper-resistance) given a tamper detection is not always present. This, along with fielding in insecure environments contributes to the ability to gain access to data hosted on the device.

iii. IT security is new to many manufacturers

IT security is a specialized discipline that those in the computer industry have taken many years to embrace. For IoT device manufacturers that have never had to deal with security concerns, it is understandable that they would often lack the skills required to engineer and develop products in a secure manner. Many device manufacturers that are adding connectivity to their portfolios have begun to build the skill sets necessary to understand the security weaknesses inherent in connected devices. There is still a gap however as some products have long-lead product cycles which will lead to a continued influx of insecure devices onto the market. For organizations that continue to lack the security expertise needed to begin securely developing their products, there are many 3rd party organizations that offer security evaluation services for a fee or even at no charge.

iv. Lack of SDLC robustness

Many developers follow Agile[25] principles when developing their IoT products. There are security gaps in typical Agile processes such as “scrum”, that often have to be filled in order to inject and track security requirements within the development life cycle. This is coupled with the often lack of developer security expertise which can lead to vulnerabilities in code. Organizations developing consumer or enterprise IoT devices should follow best development security practices, which include peer code reviews and code analysis. Penetration tests against the final products in a representative environment should also be conducted.

[25] https://en.wikipedia.org/wiki/Agile_software_development

v. Lack of interoperability in protocols

The wide variety of IoT related protocols have necessitated the use of protocol-specific gateways and translators in many instances. These gateways add complexity to the network environment and extend the attack surface for malicious actors. As standardization in messaging and communication protocols continues, the need for these additional components will decrease.

vi. Security is not a business driver

The Cloud Security Alliance (CSA) conducted a survey of technology startups in 2015 to better understand their motivations related to security of IoT developments. Results from the survey showed understandably that investors and technology startups are not concerned with the security of their products. They are instead focused on getting their products to market quickly and ensuring that core functionality works as expected.

IoT lends itself better than most technologies to being heavily led by startups and small businesses, as IoT products do not pose high barriers to market entry, and thrive on innovation. With this segment of developers not focused on product security, it is probable that the resulting products will introduce new security challenges into the marketplace soon.

In addition, security is often viewed as a consumer inconvenience and/or complication that is perceived to drive up support costs, diminish user friendliness, etc. Password usage is an example of the trade-offs that can occur between security and usability - the simpler and longer lived the password, the easier it is for the user to remember (and for the adversary to guess). The challenge is for future technical solutions to achieve both increased security *and* a good user experience whenever possible.

vii. Low cost point increases pool of potential hackers

As discussed in other parts of this paper, the low cost of typical IoT devices, especially consumer devices, makes it simple for both researchers and malicious actors to acquire and spend time analyzing the security protections built into each device. This allows for the systematic discovery of security vulnerabilities related to both the hardware and software, knowledge of which can then be used to exploit weaknesses in operational environments.

c. Progress on resource constrained devices

Device designers need support from the ecosystem to produce security-hardened products. Low-end nodes often do not require high-end processing power for the core mission of monitoring field conditions, controlling infrastructure or managing a medical device. Such typical low-end processor designs in the past were not designed to be security hardened.

The requirement has changed. The market is responding with a variety of small system-on-a-chip (SoC) processors that include security features:

> *"On the lower end of the design scale, such a device may consist of a low-cost System on Chip (SoC) with around 100,000 gate equivalents including on-chip memory and basic peripherals. Such platforms will typically support a simple firmware and software environment tailored to the particular usage scenario. Supervisor/usermode separation as well as memory protection based on range/permission registers or simple memory lock bits may be available. However, advanced hardware security mechanisms such as virtualization or secure co-processors are typically too expensive in terms of silicon real estate or power consumption."*[26]

Virtually every manufacturer targeting the IoT has examples of security-hardened but low-end building blocks available to developers. As "low-end" means different things in different markets, some devices listed vary in capacity. However, all have additional features to protect against bad actors.

ARM processors are used at a variety of levels from smaller single-core processors to the higher-end multi-core processors used in modern smartphones. ARM's TrustZone standard is widely used by ARM licensees to provide security-hardened solutions. From the ARM website,

> *"ARM® TrustZone® technology is a system-wide approach to security for a wide array of client and server computing platforms, including handsets, tablets, wearable devices and enterprise systems…TrustZone technology is tightly integrated into Cortex®-A processors but the secure state is also extended throughout the system via the AMBA® AXI™ bus and specific TrustZone System IP blocks. This system approach means that it is possible to secure peripherals such as secure memory, crypto blocks, keyboard and screen to ensure they can be protected from software attack."*[27]

One example of TrustZone support is the AMD Platform Security Processor (PSP) category of products.[28] Examples of PSP-enabled products include the G-Series, announced last year at Computex.[29] Low power nodes can be supported by AMD's Low-Power Mobile APUs with an ARM Cortex-A5 and ARM TrustZone® technology.

Freescale ARM-based products offer a combination of hardware and trusted firmware which OEMs may use as a root of trust to create trusted systems.[30]

ARM is not the only secure platform game in town. Intel's TrustLite security framework provides hardware to protect software on low-cost embedded devices. TrustLite is a scalable architecture that can include runtime isolation of software modules, secure exception handling,

---

[26] http://www.icri-sc.org/research/projects/trustlite/
[27] http://www.arm.com/products/processors/technologies/trustzone/index.php
[28] S. Kester, interview with Chip Design Magazine, http://chipdesignmag.com/sld/blog/2014/06/30/deeper-dive-iot-security/ , 2014-06-30
[29] http://www.amd.com/en-us/press-releases/Pages/amd-expands-g-series-2014jun04.aspx
[30] http://www.freescale.com/about/technology-programs/security-technology/trusted-systems-technology:NETWORK_SECURITY_INT_SEC

secure inter-process communication (IPC) and secure peripheral I/O to support sophisticated usages like secure user input and secure execution of 3rd party (untrusted) code.[31]

Altera FPGAs and SoCs support hardware crypto acceleration and secure remote in-field upgrades. Configuration firmware is protected using the advanced encryption standard (AES) and a 128-bit or 256-bit key.[32] A non-volatile key option offers design protection against Secure against copying, reverse engineering, and tampering[33]

Analog Devices (ADI) has connectivity products for IoT with features such as hardware acceleration for cryptography, and secure booting of ADI MCUs to in-circuit read protection of on-chip memories. ADI also offers customer-specific security features, depending on the customer requirements. [34]

Infineon offers hardware-based products supporting device integrity checks, authentication and secure key management. The company has shipped nearly 20 billion security controllers worldwide. The product portfolio ranges from "basic authentication products (OPTIGA™ Trust) to advanced implementations (OPTIGA™ TPM, OPTIGA™ Trust P and OPTIGA™ Trust E) protecting integrity, authenticity and confidentiality of information to enable security in the IoT. Further highlights include M2M, Fido, boosted NFC, USB, RFID and My-d™ as well as CIPURSE™ innovations."[35]

Texas Instruments' CC430F61xx series are microcontroller SoC configurations that combine an RF transceiver and other peripheral functions with a CPU and memory. To support security-conscious design, the SoC family also includes a 128-bit AES security accelerator.[36]

These are only a few examples. As mentioned, virtually every major manufacturer offers IoT platforms with secure options.

Clearly, IoT devices can have security features like encryption. In the short term, developers of lowest-end applications would be wise to limit the data and attack surface presented by unsecured devices. However, in the mid-term to long-term, Moore's Law will make even the lowest-end devices potentially capable of such security hardening.

d. What are security gaps

Articles around IoT security concerns are commonplace within technology based news streams. One only has to Google "IoT security gaps" to find a myriad of press articles on automobiles being hacked, Internet enabled garage door openers being compromised, baby monitors being abused, etc.

---

[31] https://securityledger.com/2015/11/intel-updates-iot-platform-with-security-in-mind/
[32] https://www.altera.com/solutions/technology/iot/overview.html
[33] https://www.altera.com/products/fpga/features/stx-design-security.html
[34] http://design.avnet.com/axiom/analog-devices/
[35] http://www.infineon.com/cms/en/applications/chip-card-security/internet-of-things-security/
[36] http://www.ti.com/lit/ds/symlink/cc430f5137.pdf

Rather than attempt to create an exhaustive list of perceived security gaps, this section is intended to provide a snapshot of the more commonly referenced gaps as of late 2015. The topics below build upon the gaps already introduced earlier in this section.

Gap case study: baby monitors

The security analytics vendor Rapid7 performed a September 2015 case study around baby monitor security vulnerabilities[37]. Radid7 selected baby monitors for study since they are positioned in the market as security devices (which makes it reasonable to expect them to be held to a higher security standard), are internet accessible, and are built from general purpose components that make their analysis likely applicable to other consumer IoT devices.

In the case study, Rapid7 found and documented these vulnerabilities:

- Inadequate access control: authenticated users at one baby monitor's website could view details of any other user
- Backdoor credentials: Two vendors had devices shipped with hardcoded credentials in the firmware, allowing access to the device OS (requires physical access to the device)
- Web session hijacking: One vendor's website was vulnerable to reflective and stored cross site scripting (XSS)
- Insecure streaming: insecure transport could allow attackers access to access video streams
- Authentication bypass: an arbitrary account can be set up, giving an attacker a means to access a targeted monitor
- Privilege escalation: A regular user can easily escalate their privileges on the device to administrative level

Rapid7 reported the discovered vulnerabilities to the affected vendors and CERT. They observed a wide range of responses from the vendors, from being impossible to contact, to being very receptive to Rapid7's findings.

Observations from the 2015 DEF CON Security/hacking conference

Some members of the TAC IoT security sub-group attended DEF CON 23[38] in August of 2015. DEF CON is a rather unique security conference, held annually in Las Vegas. It attracts many people from the hacker community as well as security professionals. Most of the DEF CON presentations focused on how hackers and researchers compromised various types of systems, and how such attacks could be mitigated in the future.

IoT vulnerabilities were popular topics throughout the conference, with several publicized "how-to" attacks on vehicles, Linux powered rifles, medical devices, and video cameras. Many of the attacks dealt with vulnerabilities associated with accessibility of the device firmware for analysis (e.g. searching for hardcoded passwords/keys), and the lack of protections around the firmware

[37] https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf
[38] https://www.defcon.org/html/defcon-23/dc-23-index.html

update process. If one were to attempt to identify the top IoT related gap at the conference, it would likely be around some device manufacturers failing to adequately design in safety measures around firmware, such as the lack of digital signatures protecting the integrity of the firmware.

OWASP Top Ten identified gaps

Industry initiatives around IoT security have identified many gaps in recent years. One frequently referenced study is the *OWASP (Open Web Application Security Project) Internet of Things Top Ten Project*[39]. The project is intended to help manufacturers, developers, and consumers better understand IoT security issues, and to enable users to make better security decisions when building, deploying, or assessing IoT tech. It defines the top ten security surface areas presented by IoT systems, and provides information on threat agents, attack vectors, vulnerabilities, and impacts associated with each. Its 2014 list of top 10 concerns is listed below:

1. Insecure web interface
2. Insufficient authentication/authorization
3. Insecure network interfaces
4. Lack of transport encryption
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software/firmware
10. Poor physical security

Insecure network interfaces, lack of transport encryption, and poor physical security relate closely to the questions the FCC provided the Cybersecurity TAC WG at the beginning of the 2015 TAC calendar year. The OWASP effort also lists remediation steps for the listed concerns. This will be addressed further in the best practices section of this document.

e. How is industry addressing gaps

As awareness and urgency of addressing security gaps in IoT has increased, both established and emerging private sector capabilities are beginning to emerge and mature. However, these efforts to date are largely focused on perimeter security, rather than being directly incorporated into software development practices of consumer devices.

Transmission confidentiality methods are largely well established, but are not always used for consumer products. This may be due to constrained computing resources or lack of mature software development practices. Multiple industry efforts are underway to produce guidelines and best practices to better inform manufacturers. CSA conducted a survey of startups

[39] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

developing IoT devices, where they found that most had little focus on security, prioritizing functionality and time to market.

There are numerous efforts underway to enhance authentication capabilities of devices, within multiple standards organizations.

Data retention and governance best practices remain nascent, but industry and public sector efforts are emerging to encourage appropriate levels of data handling practices, including creation or amending consumer privacy regulations.

One area where little progress has yet been made is around consumer access control visibility and consumer administration of access control policies. While many individual devices provide such tools, a consumer has no true holistic perspective for all devices (in a home, for example). This is partly due to many competing standards, each of which implements access control methods in different ways. Another contributing factor is that robust policy management is getting increasingly complicated, as more and more devices are network connected, and risk causing consumer confusion.

Security coalition groups are taking a leadership role:

- IamtheCalvary[40] - focused on security for the automotive industry
- Builditsecure.ly[41] - focused on security guidance for device manufacturers
- Securing Our Cities - coalition focused on developing guidance to secure connected cities
- Kantara Initiative - focused heavily on Identity Relationship Management and naming of things
- Cloud Security Alliance - focused on guidance for enterprise adoption of the IoT

The Industry Landscape section of this document provides some additional details on existing or planned outputs for some of these private and public consortia.

f. Potential impacts of security challenges

Failure of industry to implement robust security practices has the potential for severe consequences, both to businesses and consumers. Consider the outcome of historical security breaches. That risk is amplified with the enormous growth in cyber physical systems drastically increasing the overall attack surface.

While historical breaches harmed consumers indirectly from businesses, cyber physical breaches may also result in direct digital or physical harm to consumers, from compromised home networks, connected vehicles, connected medical devices, or other systems that were not previously network connected.

[40] https://www.iamthecavalry.org/
[41] http://builditsecure.ly/

If these breaches are serious enough, with broad impact to businesses and consumers, it may result in harm to the economy, consumer confidence and consumer safety. This is especially true for failures in most industrial applications, such as energy, utilities, and transportation.

g. Best practices

There is no shortage of security best practices to be found on the Internet. Within the last twelve months, several best practices initiatives have emerged specifically on the topic of IoT security. This section is intended to call out some of the more commonly referenced best practices, but is clearly not meant to be an exhaustive list. The reader is encouraged to download the referenced best practices for more details, since this section only highlights some of the more salient points from each initiative.

BuildItSecure.ly

BuildItSecure.ly is a community initiative run by security professionals from a variety of IT security companies such as Rapid7, AttackIQ, Optiv Security, and IOActive. One of its stated purposes is to curate informational resources to help educate IoT vendors on security best practices. BuildItSecure.ly has also partnered with Bugcrowd[42], which leverages crowdsourcing for product penetration testing and bug discovery.

The BuildItSecure.ly website[43] serves as a collection point for security best practices for IoT implementers. Currently the website points to a document titled *"An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond"* from the UK based information assurance firm NCC Group. The site also contains links to a FTC document titled *"Careful Connections: Building Security in the Internet of Things"* , CSA's *"Security Guidance for Early Adopters of the Internet of Things"* and the OWASP *Internet of Things Top Ten Project* (these last three references are described later in this section).

CTA best practices paper

CTA recently published CTA-TR-12, "*Securing Connected Devices for Consumers in the Home*". This paper uses the BSIMM[44] (Building Security In Maturity Model) as a basis for maturing corporate processes towards best practices across-the-board. BSIMM is a study of existing software security initiatives. By quantifying the practices of many different organizations, it is possible to describe the common ground of security best practices that are shared by many companies, as well as the variation that makes each unique.[45] Companies can study BSIMM to evaluate their own practices and compare to other organizations' most common 112 best practices.

[42] https://bugcrowd.com/
[43] http://builditsecure.ly/#resources
[44] https://www.bsimm.com/
[45] https://www.bsimm.com/about/

The second half of CTA-TR-12 deals with Threats and Mitigations, including a "top ten" list of developer "to-do's" such as "prevent wireless sniffing" and "restrict password guessing", with information and references on each item.

Cloud Security Alliance

The CSA released "*Security Guidance for Early Adopters of the Internet of Things"* [46] in April 2015. This document provided a set of recommendations generated by a cross-industry set of CSA members. The guidance provided information on IoT threats to individuals and organizations, challenges to secure IoT deployments, and a set of recommended security controls.

The recommended security controls focused on enterprise design and deployment of IoT systems and included:

1. Analyze privacy impacts to stakeholders and adopt a Privacy-by-Design approach to IoT development and deployment.
2. Apply a Secure Systems Engineering approach to architecting and deploying a new IoT System.
3. Implement layered security protections to defend IoT assets.
4. Implement data protection best practices to protect sensitive information.
5. Define Life Cycle Security Controls for IoT devices.
6. Define and implement an authentication / authorization framework for the Organization's IoT Deployments.
7. Define a Logging and Audit Framework for the Organization's IoT Ecosystem.

The CSA released a second report in September 2015 – "*Identity and Access Management (IAM) for the IoT"*[47], which provided additional focused recommendations related to IAM, including:

1. Integrate your IoT implementation into existing IAM and GRC governance frameworks in your organization.
2. Do not deploy IoT resources without changing default passwords for administrative access.
3. Evaluate a move to Identity Relationship Management (IRM) in place of traditional IAM.
4. Design your authentication and authorization schemes based on your system-level threat models.

DHS Security Tenets for Life critical embedded systems

[46] https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[47] https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

The Department of Homeland Security recently released a security guidelines paper on "life critical embedded systems"[48]. This term is defined in the paper as "devices whose failure or malfunction may result in serious injury or death to humans, loss or severe damage to equipment, or environmental harm".

The DHS paper has relevance to the 2015 TAC work since consumer IoT devices such as vehicles and medical devices would arguably fall under the working group's scope. What makes the DHS document worth noting is its focus on tenets that will help mitigate the risks associated with devices that could inflict bodily harm when these devices misbehave. Examples include specifying the need for the creation of threat models and the designing of products that fail safely. For reference, the tenets are summarized below:

1. General Security
    a) Systems MUST have documented threat models.
    b) Systems MUST be engineered to fail safely.
    c) The data usage, safety, and privacy aspects of life critical embedded systems MUST be clearly documented in lay terms.
    d) Devices MUST only run hardened code.
    e) Devices MUST enforce l east privilege.

2. Communications Security
    a) All interactions between devices MUST be mutually authenticated.
    b) Continuous authentication SHOULD be used when feasible and appropriate.
    c) All communications between devices SHOULD be encrypted.

3. Boot-time Security
    a) Devices MUST NEVER trust unauthenticated data and code during boot-time.
    b) Devices MUST NEVER be permitted to run unauthorized code.

4. Run-time Security
    a) Devices MUST mitigate run-time security risks, including malicious data.
    b) Devices SHOULD NEVER trust unauthenticated data during run-time.
    c) When used, cryptographic keys MUST be protected.

5. Managing Life Critical Embedded Systems Securely
    a) Devices and systems MUST be built to include mechanisms for in-field update.
    b) Devices and systems for managing updates MUST be mutually authenticated and secured.

6. Security for Back-end Systems
    a) Systems communicating with life critical embedded system devices MUST be protected in accordance with industry best practices.

7. Monitoring for Advanced Threats
    a) Systems MUST be monitored for threats capable of defeating or avoiding these tenets.

[48] https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf

Federal Trade Commission

A FTC document titled *"Careful Connections: Building Security in the Internet of Things"*[49] provides guidance to makers of IoT devices/systems for taking reasonable steps toward addressing security. The paper starts with describing some fundamental steps, such as encouraging a culture of security, risk management, defense-in-depth, and avoiding the use of default passwords (unless consumers are forced to change them during setup).

The paper goes on to call out several other considerations which are highlighted here:

- Use common security techniques such as encryption, the use of salt (random data for cryptographic functions), and rate limiting
- Designing products with authentication in mind
- Protecting device interfaces
- Limiting permissions
- Testing of security measures
- Making default settings more secure
- Looking for opportunities to educate consumers on making sensible security choices
- Considering methods to inform consumers of security updates on existing products
- Monitoring free databases for the latest in identified vulnerabilities
- Implementing "bug bounty" programs
- Using setup wizards to help consumers configure security features

The paper concludes with a thought provoking paragraph for device makers, which is worth repeating here:

> *"Right now, many companies still think of security as primarily defensive – behind-the-scenes precautions to help prevent the what-ifs. But the Internet of Things offers entrepreneurs an opportunity to showcase the steps they're taking to keep information safe. The likely winners in the burgeoning Internet of Things marketplace are companies that out-innovate the competition both on the effectiveness* ***and*** *security of their products."*

NIST Cyber-Physical Systems Public Working Group (CPS PWG)

As mentioned in the industry scan section of this document, the NIST CPS PWG was formed in 2014 to develop and implement a new cyber security framework dedicated to cyber-physical systems. The CPS PWG recently released a draft framework[50] for review. The framework covers many topics, including Cybersecurity and privacy. Several Cybersecurity/privacy challenges and opportunities are addressed, with the following recommendations enumerated:

[49] https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf

[50] http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf

1. Realistic attack models should utilized, including simulation for deception and DoS attacks
2. Methods to detect deception attacks launched by compromised sensors and system controllers
3. Autonomous attack detection/mitigation means are needed, given the impracticalities of injecting humans into the decision making process of typical CPS deployments, where real-time decision making algorithms are required
4. Rational advisory models should be utilized to ensure the survivability of CPS systems
5. Estimates of performance and integrity indicators of the CPS communication networks are needed
6. Security principles such as diversity and separation of duty should used in combination with built in physical/analytical redundancies of CPS systems

OWASP Top Ten IoT

The OWASP Top Ten project was already discussed in the gaps section of this document. The same OWASP initiative also listed several options for mitigating these risks. The OWASP IoT website not only addresses way of developers to mitigate the raised issues, bit also provides guidance for testing methodology on how to discover product weaknesses after they are implemented. In addition, the OWASP website[51] provides links to more details on risk mitigation from the perspective of manufacturers, developers, and consumers.

The OWASP website points out that IoT security is not just about the device, the network, or the client. There are many surface areas involved, and each one must be evaluated. The goal is to have a broad approach, covering topics such as devices, the cloud, apps, network interfaces, software, the use of encryption, authentication, physical security, and I/O ports.

Rather than regurgitate all the detailed information on the very informative OWASP website, links are provided to both the design/development and product testing guidelines to the top 10 identified issues:

Overall top 10 guidance:
https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Testing guidance: https://www.owasp.org/images/2/2d/Iot_testing_methodology.JPG

Symantec

Symantec published a document in early 2015, titled, "Insecurity in the Internet of Things"[52]. The paper described the results from Symantec's analysis of 50 smart home devices available today. The study found that no devices enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks. Nearly 20% of the mobile apps used to

[51] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
[52] https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf

control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. Many other common vulnerabilities were noted.

The paper pointed out that all of the potential weaknesses are already well known to the security industry. The paper also described several mitigation techniques for both end users and manufacturers to help improve security. These best practices are listed below.

For users:

- Use strong passwords for device accounts and Wi-Fi networks
- Change default passwords
- Use a stronger encryption method when setting up Wi-Fi networks such as WPA2
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Be careful when buying used IoT devices, as they could have been tampered with
- Research the vendor's device security measures
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available
- Use devices on separate home network when possible
- Ensure that an outage, for example due to jamming or a network failure, does not result in a unsecure state of the installation
- Verify if the smart features are really required or if a normal device would be sufficient

For manufacturers:

- Use SSL/TLS-encrypted connections for communication
- Mutually check the SSL certificate and the certificate revocation list
- Allow and encourage the use of strong passwords
- Require the user to change default passwords
- Do not use hard-coded passwords
- Provide a simple and secure update process with a chain of trust
- Provide a standalone option that works without internet and cloud connections
- Prevent brute-force attacks at the login stage through account lockout measures
- Secure any web interface and API from bugs listed in the OWASP List of Top Ten Web vulnerabilities
- Implement a smart fail-safe mechanism when connection or power is lost or jammed
- Where possible, lock the devices down to prevent attacks from succeeding
- Remove unused tools and use whitelisting to only allow trusted applications to run
- Use secure boot chain to verify all software that is executed on the device
- Where applicable, security analytics features should be provided in the device management strategy

The paper concludes by pointing out that in the near future, a variety of devices will be connected to consumers' home networks, which will lead to more intelligent smart hubs that allow commands based on logical conditions. The presence of these hubs likely means one device can trigger the shutdown of another. This makes the smart hub an ideal central point of attack, and adds to the challenge of securely deploying multiple smart devices in a secure

fashion at home. The paper's intent is to help address this challenge through the described threat mitigation techniques.