NTIA IoT Security Upgradability and Patching

Existing Standards, Tools and Initiatives Working Group (WG1)

Catalog of Existing IoT Security Standards Version 0.02

Draft

Acknowledgements

This publication was developed by the Existing Standards, Tools & Initiatives Working Group (WG1) as a part of the National Telecommunications & Information Administration (NTIA) Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching with representatives from the private, professional, and government communities in an ongoing effort to produce a Catalog of IoT security-related standards, policy and guideline references. The authors of this document would like to acknowledge those individuals who contributed significantly to the development of this publication, including:

Contributor names go here....

Table of Contents

1. Introduction

The NTIA IoT Security Upgradability Existing Standards, Tools and Initiatives Working Group undertook a review of existing standards and initiatives as they apply to Security Patching and Upgradability. The intent of the working group was to research and analyze efforts already underway in the industry related to upgrading deployed IoT devices and infrastructure. The WG effort's focused on global efforts, looking at standards initiatives and existing specifications as well as deployed tools that vendors or service providers may be using today. The WG searched for what exists from a standards and best practices perspective. As an outgrowth of the research, the WG decided it would be beneficial to create a catalog of existing IoT-related security standards and guidelines since there are a great deal of work going on and no one should have to duplicate the work we did.

This is an effort that can have a very positive impact on the community and the security management of emerging technologies moving forward. Consumers of these new types of devices and capabilities need to be protected from vulnerabilities and security related exposures. This working group is trying to assure we are not reinventing the wheel but leveraging what is on-going today globally and properly documenting the best practices we encounter during our research.

The ultimate objective is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT requires common definitions so that manufacturers and solution providers have shared visions for security, and consumers know what they are purchasing. Currently, no such common, widely accepted definitions exist, so many manufacturers struggle to effectively communicate to consumers the security features of their devices.

The goal of this process will be to develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers. One initial step will be to explore and map out the many dimensions of security upgradability and patching for the relevant systems and applications. A goal will be to design and explore definitions that are easily understandable, while being backed by technical specifications and organizational practices and processes. A final step will be to develop a strategy to share these definitions throughout the broader development community, and ultimately with consumers.

2. Catalog Entry Description

NOTE: This section will describe the individual components of each of the catalog entries. It will also provide more specificity on the use and parameters of the document attributes that are not readily obvious. This too is a work in progress.

Organization:
Organizational URL:
Organizational Summary:
Documents:

- **Document Title:**
- **Summary:**
- **Document URL:**
- **Published Date:**
- **Document Version:**
- **Domain of applicability:**
- **Reference Category:**
- **Useful sections:**
- **Related Organizations:**
- **Additional Notes:**
- **NTIA WG Relevance**
- **NTIA WG owner:**

3. Definitions

Disclosure: Act of initially providing vulnerability information to a party that was not believed to be previously aware. The overall disclosure process typically includes multiple disclosure events.
Exposure: Time between the discovery of a vulnerability and the time a vulnerability can no longer be exploited.
Mitigations: Actions that reduce the likelihood of a vulnerability being exploited or the impact of exploitation.
Remediation: Patch, fix, upgrade, configuration, or documentation change to either remove or mitigate a vulnerability.
Vendor: Individual or organization that developed the product or service or is responsible for maintaining it.
Vulnerability: Weakness in software, hardware, or a service that can be exploited.

Domain of applicability:
This applies to documents identified, which concern IoT technologies designed, created, deployed and or marketed to a particular sector

- **Transportation:** Sector directly related to physical vehicles designed for the purpose of conveying people, goods or conducting other mobile functional purposes. This would include automobiles, trucks, farm vehicles, planes, trains, drones, and ships. This list is not all-inclusive.

- **Medical:** Medical instruments, apparatus, implement and or machine, which is used for the medical diagnosis, and treatment, and is regulated by the Food and Drug Administration (FDA).

- **Industrial:** Sector where the technology is directly related to the manufacturing of goods, energy and management of typical city services including water, sewer, lighting and traffic control

- **Enterprise:** Sector where the technology is used within the business environment but is not directly associated with manufacturing and industrial processes. This would include such areas as building heating, ventilation, security systems and lighting. This would also include technology used for day-to-day business activities. Enterprise sector technology would typically be higher scale products not normally marketed to home consumers.

- **Consumer:** Sector where the product is produced for sale to a consumer for personal use.

The Industrial Internet Consortium published the following two-level taxonomy in March 2016:

Sector	Verticals

Academia and research	Higher education, research
Agriculture	Farming, ranching, fishing, weather
Building	Building/construction, smart home, office, building security, building maintenance
Business services	Business consulting, business process management, marketing services, product lifecycle management, engineering product development and testing, media
Consumer and home	Consumer products, home products, cooking (commercial), entertainment, phone and network services, sporting events, travel, tourism
Defense/aerospace	Defense, military, aerospace
Energy	Energy, utilities, mining, Oil & Gas, smart grid
Finance and banking	Banking, commerce, financing
Healthcare	Connected medical devices, hospitals, medical offices, pharmacies, medical therapy, home healthcare, disease diagnosis, continuous patient monitoring, clinical trials, assisted care, dentistry
IT & networks	Communications, media, services, software, computers, networks, asset management, security, development tools, testing tools
Manufacturing	Factory, industrial automation, smart products
Public sector	Education, environment, water, transportation, waste management, civil administration
Public security and public safety	Public safety, public security, surveillance, disaster prevention, law enforcement/police, fire, emergency and crisis response, military
Retail	Big-box, online, brick and mortar, hospitality, food and beverage distribution
Transportation	Mobility, transportation, public transport, vehicle, traffic infrastructure, logistics, freight management, pipelines, shipping, aeronautics

4. Online Trust Alliance

URL: https://otalliance.org/resources/iot-industry-resources

Organizational Summary: OTA is convener of a multi-stakeholder initiative to address public policy and technology issues impacting IoT devices. Through this effort OTA released the IoT Trust Framework, a strategic set of foundational principles providing guidance for developers, device manufacturers, and service providers to help enhance the privacy, security, and life-cycle of their products. To-date over 100 organizations including industry leaders, consumer and privacy advocates, testing organizations, academia, government agencies, and others have contributed to this effort. The working group's goal is to help promote best practices, embrace a self-regulatory code of conduct and help educate policy makers worldwide.

Documents:

Document Title: IoT Trust Framework

Summary: The IoT Trust Framework includes a set strategic principles to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, key principles have been identified for connected home, work and wearable technologies including toys and fitness devices. The Framework outlines mandatory requirements including comprehensive and security patching post warranty.

Document URL: http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT Trust Framework.pdf
Published Date: January 5, 2017
Document Version: 2.0
Reference Category: Framework
Useful sections: #3, #4, #5, #6, #16

5. Industrial Internet Consortium (IIC)

URL: http://www.iiconsortium.org/

Organizational Summary: The Industrial Internet describes a world in which physical manufacturing and other machinery connects with sensors and software that gather data, analyze it, and use it to adjust the machinery—essentially, the non-consumer IoT. The IIC was created to make sure that products from different companies can easily share data; its members will be building security protections into its reference architectures. 25 organizations contributing to this new IoT security framework. Industrial Internet of Things, E2E Architecture, Testbeds

Documents:

Document Title: Industrial Internet of Things, Volume G4: Security Framework

Summary: The purpose of this document, 'Industrial Internet of Things, Volume G4: Security Framework' (IISF) is to identify, explain and position security-related architectures, designs and technologies, as well as identify procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. It describes their security characteristics, technologies and techniques that should be applied, methods for addressing security, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations.

Document URL: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

Published Date: September 19, 2016

Document Version: 1.0

Domain of applicability: Industrial

Reference Category: Guideline

Useful sections: 7.3, 8.1, 8.10, 11.5.1 (see notes below)

Related Organizations: Object Management Group (OMG)

Additional Notes:

Because this is a security document, its applicability is related to the possibility that an upgrade or patch may be submitted by a malicious actor, which is attempting to disable or subvert a part of an IoT system under the guise of submitting a legitimate change.

Several early sections of the document "miss the opportunity" to specifically mention upgrading and patching among the concerns and measures listed:

- Section 3 on "Key System Characteristics Enabling Trustworthiness."
- Section 3.1 on assurance cases, abuse cases and the threat model.
- Section 3.2, in its mention of code signing as an integrity control.
- Section 5.2.2, which focuses on the STRIDE model, in which spoofing identity (S) and tampering with data (D) are the first two of the six elements and clearly apply to security of the upgrade/patch process.
- Section 5.4, "Ongoing Business Attention" on areas requiring continuous management.
- Section 5.6, "Management Considerations."

Section 7.3, "Endpoint Protection" states that "Endpoint secure configuration and management controls updates of security policy and configuration at the endpoint, **including upgrades and patches of known vulnerabilities"** (emphasis added) but without any specifics. Section 7.6 refers to endpoint configuration and management again, and this time fails to mention upgrades and patches.

Section 8.1, "Security Threats and Vulnerabilities on Endpoints" is a logical place to mention the risk of malicious updates -- or of not correcting an existing vulnerability through the lack of an update. Updates are alluded to, but very lightly, in the bulleted paragraphs named "illicit changes to application software," "vulnerabilities of the deployment process," and "vulnerabilities in configuration and management." But Section 8.2.1, "Endpoint Security Lifecycle," omits the issue completely.

Section 8.10 states **"All updates and changes should be signed, their payload encrypted, and actions logged for subsequent auditing and recovery of the endpoint"** (emphasis added). The next sections provide some details on encryption and endpoint protection, but not on code signing.

Section 11.1 mentions an API that allows the updating of a policy -- not the updating of the endpoint software or firmware. That is also the focus of Section 11.4.3 on "policy assignment and delivery."

Section 11.5.1, **"Secure software patching and firmware update,"** addresses the crux of the matter. It references IEC TR 62443-2-3:2015 'Patch Management in the IACS Environment.' This document must be purchased (about $350), but appears to contain more defined information on ICS security and patching. *A preview containing the full table of contents is available at* *https://infostore.saiglobal.com/store/PreviewDoc.aspx?saleItemID=2843060*

NTIA WG Relevance: Shows that IoT device upgrading and patching is also a concern in the industrial domain. Provides a reference to the IEC's Technical Report on patch management.

6. Open Connectivity Foundation

Organizational URL: https://openconnectivity.org

Organizational Summary: The Open Connectivity Foundation (OCF) is a group of over 300 technology companies, including Cisco, Intel, and Samsung, and is developing interoperability standards for the IoT and sponsoring an open source project to make this possible. OCF will unlock the massive opportunity in the IoT market, accelerate industry innovation and help developers and companies create solutions that map to a single open specification. OCF will help ensure secure interoperability for consumers, business, and industry.

Documents:

Document Title: OCF Security FAQ, and
OCF 1.1.1 Security Specification
Brief summary: Overview and full recent security spec.
Document URL: https://openconnectivity.org/resources/ocf-security/ocf-security-faq
https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf

Published Date: 2017 for Security Spec
Useful sections: Section 15, but software updates still in work
Related Organizations: ***OCF, AllSeen Alliance and IoTivity combined as a single org***
Additional Notes: *Must have membership to access current work items

AllSeen Alliance (Note, OIC and the AllSeen Alliance merged in Q4 2016 to form OCF):

This consortium counted about 185 members and promoted the open-source AllJoyn

Framework, managed by the Linux Foundation, which aims to allow devices to discover and communicate with one another and to give developers tools to create compliant IoT applications.

https://allseenalliance.org

IoTivity – Open Source IoT Framework sponsored by OCF:

IoTivity is an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the Internet of Things. Each day more and more devices are coming online, adding to the ever-growing Internet of Things (IoT). Analysts agree the IoT will grow to many billions of devices over the next decade. The challenge for the IoT ecosystem is to ensure these emerging IoT devices can connect securely and reliably to the Internet and to each other. The IoTivity project was created to bring together the open source community to accelerate the development of the framework and services required to connect these billions of devices. The IoTivity project is sponsored by the Open Connectivity Foundation (OCF), a group of industry leaders who will be developing a standard specification and certification program to address these challenges. IoTivity will deliver an open source reference implementation of the OCF standard specifications, yet will not be limited to those requirements.

https://www.iotivity.org/
https://wiki.iotivity.org

7. National Institute of Standards and Technology

Organizational URL: https://www.nist.gov/

Organizational Summary: The National Institute of Standards and Technology (NIST) was founded in 1901 and now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

Documents:

Document Title: CPS PWG Cyber-Physical Systems (CPS) Framework

Summary: Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. CPS and related systems (including the Internet of Things (IoT) and the Industrial Internet) are widely recognized as having great potential to enable innovative applications and impact multiple economic sectors in the worldwide economy. The objective of the CPS PWG is to develop a shared understanding of CPS and its foundational concepts and unique dimensions (as described in this “CPS Framework”) to promote progress through exchanging ideas and integrating research across sectors and to support development of CPS with new functionalities.

Document URL: https://pages.nist.gov/cpspwg/

Published Date: May 2016
Document Version: 1.0

8. IEEE Internet of Things

Organizational URL: http://www.ieee.org/index.html

Organizational Summary: A number of IEEE standards address elements of security that can be applied to the Internet of Things, including IEEE P1363, a standard for public-key cryptography; IEEE P1619, which addresses encryption of data on storage devices; IEEE P2600, a standard that addresses the security of printers and copiers; and IEEE 802.1AE and IEEE 802.1X, which address media access control security. P2413 - Standard for an Architectural Framework for the Internet of Things (IoT) is the umbrella for IEEE IoT efforts.

Documents:

http://iot.ieee.org/
http://standards.ieee.org/innovate/iot/stds.html
http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things
https://standards.ieee.org/develop/project/2413.html

9. Alliance for Internet of Things Innovation

Organizational URL: http://www.aioti.org/resources/

Organizational Summary: The Alliance for Internet of Things Innovation was initiated by the European Commission in 2015. Their mission is to contribute to a dynamic European IoT ecosystem. Group appears to have a main focus on business enablement for IoT

Documents:

Document Title: AIOTI WG07 Report on Wearables
Summary: For the "Wearables" working group (WG07) the wearable technology. This report focuses on wearable technology market in Europe and associated emerging market covering general subject matter in the following categories:

- Future Vision
- User Adoption
- Xlinical validation
- Security & Privacy
- Legislation
- Quality of Service

Document URL: https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG07Report2015-Wearables.pdf

Published Date: 2015
Domain of applicability: Consumer
Reference Category: Report
Useful sections: Pg 10 Privacy and security "The pilot should address how security is to

be monitored and upgraded or dynamically adapted as necessary; how security updates and patches can be implemented as needed in a simple way for users"

Document Title: AIOTI WG09 Report on Smart Mobility
Summary: The report defines the scope and focus of the WG 09 and in particular considers applications of the Internet of Things to the mobility domain (Internet of Vehicles) as next step for future smart transportation and mobility applications with short-termed European wide economic potential and applicability."
Document URL: **https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG09Report2015-Smart-Mobility.pdf**
Published Date: 2015
Domain of applicability: Transportation
Reference Category: Report
Useful sections: The document make basic references to Security and safety throughout its content

10. Broadband Forum

Organizational URL: http://www.broadband-forum.org
Organizational Summary: The Broadband Forum (in their own words) defines best practices for global networks; enables new revenue-generating service and content delivery; establishes technology migration strategies and engineers critical device, service & development management tools, in the home and business IP networking infrastructure. They develop multi-service broadband packet networking specifications addressing architecture, device and service management, software data model interoperability, and certification in the Broadband market.

Draft work is available only to members or through liaison. Finished work is publicly available mostly at: https://www.broadband-forum.org/standards-and-software/technical-specifications/technical-reports

Documents:

Document Title: User Services Platform (Working Text #, WT-369, will become TR-369 when published) https://www.broadband-forum.org/standards-and-software/major-projects/user-services-platform
Summary: This document describes the architecture, protocol, and data model that builds an intelligent User Service Platform. It is targeted towards application developers, application service providers, CPE vendors, consumer electronics manufacturers, and broadband and mobile network providers who want to expand the value of the end user's network connection and their connected devices. It includes:

- The overall architecture of USP Agents, Controllers, and service elements
- The proxy mechanisms for addressing non-USP service elements
- Requirements for the transport protocol used to handle USP messages, and defined bindings for specific protocols.

- The various USP messages, their requirements, and expected behavior patterns, along with on-the-wire encoding of USP messages
- The protocol requirements for discovery, end-to-end security, authentication, and authorization
- An explanation of the data model and how it is used to enable USP, service elements, proxying, and object defined operations

The objects necessary to implement USP are described in the Device:2 data model of the CPE WAN Management Protocol, (CWMP) (version Device:2.12, which will be published alongside USP).

Document URL: BBF Members can access WT-369 through the BBF document management system. Ongoing discussion is tracked at https://wiki.broadband-forum.org/display/BBF/User+Services+Platform+Project+Stream
(also private - though there will publicly available resources after May).

Published Date: The BETA release of USP will contain all of the tools necessary for a developer to begin building a rudimentary controller or agent with local point to point communication (i.e., not across proxies or through NAT or firewalls), and is targeted for August 2017. This version is for development purposes only and shouldn't be used in deployments. The full 1.0 version of the protocol is targeted for Q4 2017.
Document Version: Working text is currently in revision 10 (BETA version will likely be 0.11), but the final publication will be version 1.0 of the protocol.
Domain of applicability: USP is designed for consumer electronics/IoT, home network/gateways, smart Wi-Fi systems, and virtual services (though could theoretically be used for any connected device in many different verticals). It is targeted towards developers, application providers, and network service providers looking to deploy those products. The User Services Platform allows service providers, consumer electronics manufacturers, and end users to:

- Perform lifecycle management of consumer connected devices
- Enable IoT and consumer electronics upgradability for critical security patches
- Bootstrap and configure newly installed or purchased devices and virtual services
- Let customer support monitor and troubleshoot connected devices, services, and home network links
- Easily map the home network for controlling service quality and monitoring threats
- Securely control IoT, smart home, and smart networking devices and systems locally or from the Cloud
- Enable multi-tenant management and control

11. International Electrotechnical Commission (IEC)

Organizational URL: www.iec.ch

Organizational Summary: International Standards and Conformity Assessment for all electrical, electronic and related technologies

Documents:

Document Title: IEC/TR 62443-2-3, "Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment."

Summary: Describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. This Technical Report recommends a defined format for the distribution of information about security patches from asset owners to IACS product suppliers, a definition of some of the activities associated with the development of the patch information by IACS product suppliers and deployment and installation of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however, it may also be applicable for non-security related patches or updates.

Document URL: https://webstore.iec.ch/publication/22811

Published Date: 30 June 2015

Document Version: 1.0

Domain of applicability: Industrial Automation

Additional Notes: The document needs to be purchased for about $350. A preview, containing the full table of contents but nothing more, is available online.

WG Relevance: Very relevant in the industrial context, and is presumably applicable with few changes to the commercial IoT context.

12. Open Web Application Security Project

Organizational URL: https://www.owasp.org/index.php/Main_Page

Organizational Summary: The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. The project looks to define a structure for various IoT sub-projects such as Attack Surface Areas, Testing Guides and Top Vulnerabilities.

Documents:

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

13. Cloud Security Alliance

Organizational URL: https://cloudsecurityalliance.org/

Organizational Summary: To promote the use of best practices for providing security

assurance within Cloud Computing and provide education on the users of Cloud Computing to help secure all other forms of computing.

Documents:

Document URL:
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

14. Object Management Group

Organizational URL: www.omg.org

Organizational Summary: OMG, founded in 1989, is a membership-based not-for-profit consortium. It is the home of software and system modeling standards such as UML and SysML, business standards such as BPMN, middleware standards such as CORBA and DDS, the Data Distribution Service, and many others.

Documents:

Document Title: DDS-Security

Summary: This specification adds several new "DDS Security Support" compliance points ("profile") to the DDS Specification. The use of SPIs allows DDS users to customize the behavior and technologies that the DDS implementations use for Information Assurance, specifically customization of Authentication, Access Control, Encryption, Message Authentication, Digital Signing, Logging and Data Tagging.

Document URL: http://www.omg.org/spec/DDS-SECURITY/

Published Date: August 2016

Document Version: 1.0

Domain of applicability: All IoT solutions that use the Data Distribution Service (DDS) to communicate between components. DDS is an OMG standard used in a number of industrial and smart city applications.

Useful sections: None specifically. All sections are relevant to an implementer. This standard helps secure real-time communication in general (below the application level), and therefore does not specifically address updates or patches.

WG Relevance: DDS-Security addresses issues of authentication, access control, encryption and logging of operations that are key to establishing a secure upgrading or patching service. DDS is mostly being applied to large-scale real-time IoT installations, and may therefore be of limited applicability to low-end consumer IoT deployments. One might argue, on the other hand, that the adoption of DDS in the commercial world (including its streamlined version for resource-constrained environments) would precisely help solve upgrading/patching security by allowing the use of DDS-Security.

15. Internet Engineering Task Force (IETF)

Organizational URL: http://ietf.org/

Organizational Summary: The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

Documents:

https://www.ietf.org/id/draft-pei-opentrustprotocol-01.txt
https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons
https://datatracker.ietf.org/doc/draft-moore-iot-security-bcp/

16. Thread Group

Organizational URL: https://www.threadgroup.org

Organizational Summary: Thread was designed with one goal in mind: To create the very best way to connect and control products in the home.

- DESIGNED FOR THE HOME: Securely and reliably connect products around the home
- BUILT-IN SECURITY: Provides security at the network layer
- BATTERY FRIENDLY: Based on the power-efficient IEEE 802.15.4 MAC/PHY
- OPEN IPv6 BASED PROTOCOL: Provides device-to-device and device-to-cloud connections
- ROBUST MESH NETWORK: Devices can route messages with no single point of failure
- SIMPLE TO SET UP AND USE: Install using a smartphone, tablet, or computer. Intended to run variety of application layers.

Documents:

Document Title: Thread 1.1 Specification
Summary: Public release of most recent Thread specification. Current work items confidential to the group until complete.
Document URL: http://threadgroup.org/ThreadSpec
Published Date: 2/13/2017
Document Version: 1.1.1
Useful sections: Chapter 7
Additional Notes: Many public white papers are available on the Thread Group site.

17. Cloud Standards Customer Council (CSCC):

Organizational URL: www.cloud-council.org

Organizational Summary: "The Cloud Standards Customer Council™ is an end user advocacy group dedicated to accelerating the cloud's successful adoption. Join the CSCC™ to discover best practices and to learn about cloud standards and open source initiatives within one organization."

Documents:

Document Title: Cloud Customer Architecture for IoT

Summary: "... it is important for IoT systems to have architectures, systems principles, and operations that can accommodate the interesting scale, safety, reliability, and privacy requirements." This is not a standard, but a guide for customers of IoT systems that use the cloud for part of their functionality.

Document URL: www.cloud-council.org/deliverables/cloud-customer-architecture-for-iot.htm

Published Date: March 2016

Document Version: 1.0

Domain of applicability: IoT applications that have a cloud component (e.g., for storage and/or analysis of data collected from devices)

Useful sections:

Under "Cloud Customer Reference Architecture for IoT," "Provider Cloud," the 8th element is "Device management" (page 11), which "contains device provisioning, remote administration, **software updating,** remote control of devices, monitoring devices. Device management may communicate with management agents on devices using management protocols as well as communicate with management systems for the IoT solutions" (emphasis added).

Under the "System, Application, and Solution Lifecycle Management" (pages 14-15), the guide says that attention to security must cover, among others, "the supply chain, application and software development, through to system operations and **change management of deployed and in-service systems."** It also warns against "attacks ranging from malicious code insertion to inappropriate firmware/software deployment." "Code, key material, and even physical components must be verified as they flow from procurement and creation through to their installation into the devices, IoT gateways, and systems that make up the IoT system. The IoT system should also provide the capability to **update individual components in a secure way, both to address vulnerabilities and also to address functional enhancements over the lifetime of the system**" (emphasis added).

The next section, "IoT Governance," suggests that "IoT systems must be designed and deployed with **change/update/modification** in mind along with strong governance of these systems to **ensure that such change is done appropriately, safely, reliably, and securely.** Indeed, IoT system change is likely to be needed long after device warranty periods have expired, as it is well known that physical systems are often used for very long periods of time." This is one of the most clear existing recognitions of the importance of upgradability and patching of installed IoT devices.

Additional Notes: This "cloud architecture for IoT" was developed in parallel and independently of the IIC's Industrial Internet Reference Architecture (IIRA) and is not related to it, which is arguably a shortcoming since the two organizations are part of the "family" of consortia spun off by the Object Management Group.

18. Groupe Spécial Mobile Assocation (GSMA):

Organizational URL: http://www.gsma.com/

Organizational Summary: Connecting everyone and everything to a better future is the common purpose shared by every mobile operator across the planet. One common purpose illustrates our industry's commitment to remain the leading contributor in creating a world where we are all connected and where the way we work and live together continues to transform and improve. The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 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.

Documents:

Document Title: **GSMA Embedded SIM Remote Provisioning Architecture**
Summary: This document describes an architecture which, when implemented, will enable remote Provisioning and Subscription management, while at the same time maintaining at least the same level of security both for network operators and Customers as present solutions. This includes the safe keeping of MNO Network Access Credentials, such as keys for cryptographic functions, and identifiers such as IMSI and other Customer identities used.
Document URL: http://www.gsma.com/connectedliving/wp-content/uploads/2014/01/1.-GSMA-Embedded-SIM-Remote-Provisioning-Architecture-Version-1.1.pdf
Published Date: December 17, 2013
Document Version: 1.1

Document Title: **GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification**
Summary: The aim of this document is to define a technical solution for the remote provisioning and management of the Embedded UICC (eUICC) in machine-to-machine Devices which are not easily reachable. The adoption of this technical solution will provide the basis for ensuring global interoperability between potentially different MNO deployment scenarios, different makes of network equipment (for example SM-DP, SM-SR) and different makes of eUICC platforms.
Document URL: http://www.gsma.com/newsroom/wp-content/uploads//SGP.02_v3.1.pdf
Published Date: May 2016
Document Version: 3.1

Document Title: **GSMA SAS Standard for Subscription Manager Roles**
Summary: The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which Subscription Manager – Secure Routing (SM-SR) and Subscription Manager – Data Preparation (SM-DP) suppliers subject their operational sites to a comprehensive security audit to ensure that adequate security

measures to protect the interests of mobile network operators (MNO) have been implemented.
Document URL: http://www.gsma.com/aboutus/wp-content/uploads/2015/01/FS08-SAS_SM-Standard-v2_0.pdf
Published Date: May 13, 2015
Document Version: 2.0

Document Title: **GSMA SAS Methodology for Subscription Manager Roles**
Summary: The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which Subscription Manager – Secure Routing (SM-SR) and Subscription Manager – Data Preparation (SM-DP) solution providers subject their operational sites to a comprehensive security audit. The purpose of the audit is to ensure that SM-SRs and SMDPs have implemented adequate security measures to protect the interests of mobile network operators (MNO).
Document URL: http://www.gsma.com/connectedliving/wp-content/uploads/2014/10/SGP-09-GSMA-SAS-Methodology-for-Subscription-Manager-Roles.pdf
Published Date: October 13, 2014
Document Version: 1.0

Document Title: **GSMA Remote Provisioning Architecture for Embedded UICC Test Specification**
Summary: The main aim of the GSMA Embedded SIM Remote Provisioning Architecture [1] & [2] is to provide a technical description of the 'over the air' remote provisioning mechanism for machine-to-machine Devices. This Test Plan provides a set of test cases to be used for testing the implementations of the GSMA Embedded SIM Remote Provisioning Architecture [1] & [2]. This document offers stakeholders a unified test strategy and ensures interoperability between different implementations.
Document URL: http://www.gsma.com/newsroom/wp-content/uploads//SGP11_Remote_Provisioning_Architecture_for_Embedded_UICC_Test_Specification_v2_0.pdf
Published Date: November 02, 2015
Document Version: 2.0

19. Open Mobile Alliance (OMA)

Organizational URL: http://openmobilealliance.org

Organizational Summary: OMA is the wireless industry's focal point for the development of mobile service enabler specifications, which support the creation of interoperable end-to-end mobile services. OMA drives service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms and that work across devices, service providers, operators, networks, and geographies.

Documents:

Document Title: OMA Device Management Security
Summary: This OMA document describes general security requirements, and provides description of transport layer security, application layer security, etc. It also describes security mechanisms that are used to provide for integrity, confidentiality and authentication
Document URL: http://www.openmobilealliance.org/release/DM/V1_3-20160524-A/OMA-TS-DM_Security-V1_3-20160524-A.pdf
Published Date: 24 May 2016
Document Version: 1.3
Reference Category: Guideline
Additional Notes: This document describes OMA-DM security requirements in general, and provides description of transport layer security, application layer security, etc. It also describes security mechanisms that are used to provide for integrity, confidentiality and authentication.

20. U.S. Food and Drug Administration (FDA)

Organizational URL: http://www.fda.gov/

Organizational Summary: The Food and Drug Administration is responsible for protecting the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; and by ensuring the safety of our nation's food supply, cosmetics, and products that emit radiation.

FDA also has responsibility for regulating the manufacturing, marketing, and distribution of tobacco products to protect the public health and to reduce tobacco use by minors.

FDA is responsible for advancing the public health by helping to speed innovations that make medical products more effective, safer, and more affordable and by helping the public get the accurate, science-based information they need to use medical products and foods to maintain and improve their health.

Documents:

Document Title: **Postmarket Management of Cybersecurity in Medical Devices**
Summary: The Food and Drug Administration (FDA) is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device1 . A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the

overall risk to health.
Document URL:
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf
Published Date: December 28, 2016
Domain of applicability: Medical Devices
Reference Category: Guideline

21. US Department of Homeland Security (DHS)

Organizational URL: https://www.dhs.gov
Organizational Summary: The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector.

Documents:

Document Title: Securing the Internet of Things
Document URL: https://www.dhs.gov/securingtheIoT

22. Continuing Investigation

The following organizations and initiatives are still under research.

22.1. European Telecommunications Standards Institute (ETSI)

Organizational URL: **http://www.etsi.org/technologies-clusters/technologies/internet-of-things**
Organizational Summary: A wide range of technologies work together to connect things in the Internet of Things (IoT). ETSI is involved in standardizing many of these technologies. M2M, IoT Applications, Security, Embedded communications, eHealth, etc.

22.2. Industrial Automation and Control System Security

Organizational URL: http://isa99.isa.org/ISA99%20Wiki/Home.aspx
Organizational Summary: IEC 62443/ISA99, Industrial Automation and Control System Security Committee develops security standards and technical reports that define procedures for implementing secure industrial automation and control systems.

22.3. International Organization for Standardization (ISO) IoT Standards

Organizational URL: http://isotc.iso.org/livelink/livelink/open/jtc1wg10

Organizational Summary: The International Standards Organization's (ISO) Special Working Group on the Internet of Things is assessing existing standards that might apply to the IoT along with current efforts to develop standards; it plans to help guide their evolution to better account for security.

22.4. Internet of Things Consortium:

Organizational URL: http://iofthings.org/#home

Organizational Summary: Founded in 2012, the IoTC is a non-profit member-based organization connecting a global ecosystem of leading companies building the Internet of Things -- spanning across areas including home automation, industrial IoT, smart cities, connected cars, connected retail and more. Our mission is to ignite the growth of the IoT movement and aid the development of thriving businesses for this industry. Through facilitating partnerships, promoting knowledge sharing plus education, and ultimately driving adoption of IoT products and services, the IoTC strives to help the Internet of Things reach its great promise and potential.

22.5. IoT Security Foundation:

Organizational URL: https://iotsecurityfoundation.org/

Organizational Summary: IoTSF is a collaborative, non-profit, international response to the complex challenges posed by security in the expansive hyper-connected world. As such, IoTSF is the natural destination for IoT security professionals, IoT hardware and software product vendors, network providers, system specifiers, integrators, distributors, retailers, insurers, local authorities, government agencies and others who seek security. Our aim is to raise the quality bar, and drive the pervasiveness of security in IoT.

22.6. ITU-T SG20

Organizational URL: http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx

Organizational Summary: Established in June 2015, the International Telecommunication Union has an emerging standard that is designed not only to cover the IoT but also "smart cities and communities (SC&C)." The SG20 standard "is responsible for international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks."

22.7. oneM2M

Organizational URL: http://www.onem2m.org/technical/published-documents

Organizational Summary: Standards for Machine to Machine communications and the Internet of Things.

22.8. North American Electric Reliability Corp.

Organizational URL: http://www.nerc.com/Pages/default.aspx

Organizational Summary: The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people.

22.9. Industrie 4.0

Organizational URL:
https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/industrie-4-0

Organizational Summary: Industrie 4.0 is the German vision for the future of manufacturing, one where smart factories use information and communications technologies to digitize their processes and reap huge benefits in the form of improved quality, lower costs, and increased efficiency.

22.10. OpenFog Consortium

Organizational URL: https://www.openfogconsortium.org

Organizational Summary: Enabling advanced IoT, 5G and AI with Fog Computing

Fog computing is a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things. It is a:

- Horizontal architecture: Support multiple industry verticals and application domains, delivering intelligence and services to users and business
- Cloud-to-Thing continuum of services: Enable services and applications to be distributed closer to Things, and anywhere

along the continuum between Cloud and Things
- System-level: Extend from the Things, over the network edges, through the Cloud, and across multiple protocol layers – not just radio systems, not just a specific protocol layer, not just at one part of an end-to-end system, but a system spanning between the Things and the Cloud
- Fog Architecture, Operational Models

22.11. Smart Grid Interoperability Panel (SGIP)

Organizational URL: www.sgip.org

Organizational Summary: SGIP is an industry consortium representing a cross-section of the energy ecosystem focusing on accelerating grid modernization and the energy Internet of Things through policy, education, and promotion of interoperability and standards to empower customers and enable a sustainable energy future."

22.12. Underwriters Laboratories (UL)

Organizational URL: http://www.ul.com (http://industries.ul.com/mobile/internet-of-things-iot)

Organizational Summary: UL is a global independent safety science company with more than a century of expertise innovating safety solutions from the public adoption of electricity to new breakthroughs in sustainability, renewable energy and nanotechnology. Dedicated to promoting safe living and working environments, UL helps safeguard people, products and places in important ways, facilitating trade and providing peace of mind.

22.13. 3rd Generation Partnership Project (3GPP):

Organizational URL: http://www.3gpp.org/

Organizational Summary: A global initiative that unites seven telecommunications standards development organizations (known as "organizational partners"), the 3GPP develops specifications covering cellular network technologies, including radio access standards. Launched in 1998, the 3GPP is now moving to address the telecommunications issues, including security, that relate to the proliferation of IoT devices.

22.14. Other Places to Investigate:

- Apple Homekit / Home automation standardization efforts
- Vulnerability Management - The intent here is to potentially look at traditional security upgradability and patching best practices that could apply to IoT.

- SimAlliance - eUICC Profile Package: Interoperable Format Technical Specification http://simalliance.org/key-technical-releases/