Existing Standards, Tools and Initiatives Working Group (WG1)

Catalog of Existing IoT Security Standards Version 0.01

Draft
September 12, 2017

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:

John F. Banghart
Claude Baudoin
Christopher J Boyer
Ralph Brown
Dan Caprio
Chuck Evanhoe
Ken Figueredo
Katherine Gronberg
Joseph Lorenzo Hall
Deral Heiland
Umair Javed
Kent Landfield
David Logsdon
Ethan Lucarelli
Paul Moroney
Steve Olshansky
Sonal V Patel
Andre Ristaino
Brian Scarpelli
Alex Sneedmiller
Jeff Sorrell
Craig Spiezle
Craig Stermer
Timothy Thatcher
Matt Tooley
Jason Walls

Table of Contents

Table of Contents 4
Introduction 6
Catalog Entry Description 7
Catalog Entries 9
- Alliance for Internet of Things Innovation 9
- Broadband Forum 9
- CableLabs 10
- Cloud Security Alliance 11
- Cloud Standards Customer Council (CSCC): 12
- European Telecommunications Standards Institute (ETSI) 13
- Groupe Spécial Mobile Assocation (GSMA): 13
- IEEE Internet of Things 16
- Industrial Automation and Control System Security 17
- Industrial Internet Consortium (IIC) 17
- International Electrotechnical Commission (IEC) 18
- International Organization for Standardization (ISO) IoT Standards 18
- Internet of Things Consortium: 19
- IoT Security Foundation: 19
- ITU-T SG20 20
- National Institute of Standards and Technology 20
- North American Electric Reliability Corp. 21
- Object Management Group 22
- oneM2M 23
- Online Trust Alliance 23
- Open Connectivity Foundation 24
- Open Mobile Alliance (OMA) 25
- Open Web Application Security Project 25
- OpenFog Consortium 26
- SAFECode 27
- Smart Grid Interoperability Panel (SGIP) 28
- Thread Group 28

TUF 29
U.S. Food and Drug Administration (FDA) 29
US Department of Homeland Security (DHS) 30
Underwriters Laboratories (UL) 31
3rd Generation Partnership Project (3GPP): 31
Appendix A: 33
International Society of Automation (ISA) 33
Internet Engineering Task Force (IETF) 33
ISASecure 34
ISA Security Compliance Institute (ISCI) 34
Appendix B: 35

Introduction

The NTIA IoT Security Upgradability Existing Standards, Tools and Initiatives Working Group (WG) 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 approaches and efforts already underway related to upgrading deployed IoT devices and infrastructure within a variety of stakeholder groups, including primarily industry groups, self-regulatory organizations, and non-governmental organizations . The WG's efforts focused on global efforts, looking at standards initiatives and existing specifications as well as deployed tools vendors or service providers may be using today. 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 in order for readers to avoid duplicating our work in the future.

The WG feels this effort was a key part of the overarching NTIA Upgradeability and Patching multistakholder process, one which will 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 needs 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.

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: Name of the organization hosted the referenced documentation.

Organizational URL: Uniform Resource Locator (URL) of the website of the organization hosting the documentation.

Organizational Summary: Short description of the organization hosting the documentation.

Documents:

Document Title: Title of the document being referenced

Summary: Short description of the document being referenced.

Document URL: Uniform Resource Locator (URL) of the website containing the document.

Published Date: Date of the publication of the referenced document.

Document Version: Version of the document referenced or NA if doesn't not apply.

Domain of applicability: IoT Industry categories, which the document applies to.

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, for example, security technologies or point of sale terminals. 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.

General: Information, which is identified covering multiple domains listed above.

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.

Patchability: The capacity, ability, or proficiency related to the process of patching of software or firmware for security issues or bugs

Remediation: Patch, fix, upgrade, configuration, or documentation change to either remove or mitigate a vulnerability.

Upgradeability: The capacity, ability, or proficiency related to the process of upgrading software or firmware to the lastest supported version..

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.

Catalog Entries

Alliance for Internet of Things Innovation

Organizational URL: https://www.aioti.eu/ http://www.aioti.org/

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, Clinical validation, Security & Privacy, Legislation, Quality of Service
Document URL:

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

Published Date: 2015
Document Version: NA
Domain of applicability: Consumer

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
Document Version: NA
Domain of applicability: Transportation

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 (TR-369)
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.
Document URL:

- https://broadbandforum.github.io/usp/ (Draft release).

Published Date: The 1.0-DRAFT-01 release of USP contains all of the tools necessary for a developer to begin building a rudimentary controller or agent with local point to point communication. The full 1.0 version of the protocol is targeted for Q4 2017.
Document Version: 1.0-DRAFT-01
Domain of applicability: Consumer

CableLabs

Organizational URL: http://www.cablelabs.com/
Organizational Summary: CableLabs is a non-profit Innovation and R&D Lab founded in 1988 by members of the cable television industry. With a strong focus on innovation, CableLabs develops technologies and specifications for the secure delivery of high speed data, video, voice and next generation services. It also provides testing, certification facilities and technical leadership for the industry. CableLabs' mission is to enable cable operators to be the providers of choice to their customers. Cable operators from around the world are members.

Documents:

Document Title: Data-Over-Cable Service Interface Specifications DOCSIS® 3.1 Security Specification

Summary: This specification is part of the DOCSIS family of specifications developed by Cable Television Laboratories (CableLabs). In particular, this specification is part of a series of specifications that define the fifth generation of high-speed data-over-cable systems, commonly referred to as the DOCSIS 3.1 specifications. This specification was developed for the benefit of the cable industry, and includes contributions by operators and vendors from North and South America, Europe, and other regions.

The intent of this specification is to describe security services for DOCSIS communications. It has two main goals:

1. To provide cable modem (CM) users with data privacy across the cable network;
2. To prevent unauthorized users from gaining access to the network's RF MAC services.

This specification provides operators with tools to secure the provisioning process of Cable Modems (CM) and protect Cable Modem users by encrypting traffic flows between the CM and the Cable Modem Termination System (CMTS).

Document URL:

- https://apps.cablelabs.com/specification/CM-SP-SECv3.1

Published Date: January 11, 2017

Document Version: IO7

Domain of applicability: Consumer

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 Title: Security Guidance for Early Adopters of the Internet of Things (IoT)

Summary: The purpose of the document is to give general guidelines for the secure implementation of Internet of Things (IoT) technology. The document acknowledges that "Performing firmware, software and patch updates for IoT devices will require a new approach with considerations given to identifying update provisioning obligations and responsibilities throughout the supply chain." It further recommends: "Organizations procuring IoT assets should also clearly understand and agree on the vendor's model for licensing to ensure that they are able to continue receiving patches and software updates

throughout the course of the IoT asset's life is a broad endorsement of the importance of users' ability to patch and upgrade IOT devices." Under the recommendation "Create a System/Architecture Overview," the document notes the "...[need to] understand the specific types
of vulnerabilities that may eventually be exposed and define processes for how and how often patches and firmware updates should be applied." However, the document does not make specific recommendations for how users of IOT should conduct patching and upgrading, nor does it make specific recommendations for how users should implement such programs.

Document URL:

- https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Published Date: 04/2015

Document Version: NA

Domain of applicability: General

Cloud Standards Customer Council (CSCC):

Organizational URL: http://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:

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

Published Date: 03/2016

Document Version: 1.0

Domain of applicability: General

European Telecommunications Standards Institute (ETSI)

Organizational URL: http://www.etsi.org/

Organizational Summary: ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. Our standards enable the technologies on which business and society rely.

Documents:

Document Title: Multiple documents

Summary: Multiple documents covering 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

Document URL:

- http://www.etsi.org/technologies-clusters/technologies/internet-of-things

Published Date: 06/2017

Document Version: V1.1.1

Domain of applicability: General

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
Domain of applicability: General (Mobile devices)

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
Domain of applicability: General (Mobile devices)

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
Domain of applicability: General (Mobile devices)

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
Domain of applicability: General (Mobile devices)

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
Domain of applicability: General (Mobile devices)

Document Title: **GSMA** IoT Security Guidelines
Summary: Series of guideline documents which promote a methodology for developing secure IoT services to ensure security best practices are implemented throughout the life cycle of the service.
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
Domain of applicability: General (Mobile devices)

IEEE Internet of Things

Organizational URL: http://iot.ieee.org/

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:

Document Title: Internet of Things Related Standards
Summary: Series of documents related to various communication protocols cp,,omly used by IoT technology
Document URL:

- http://standards.ieee.org/innovate/iot/stds.html

Published Date: Various
Document Version: Various
Domain of applicability: General

Document Title: How to Build a Safer Internet of Things
Summary: Blog discussing general IoT security issues and vulnerability and how best to approach those issues
Document URL:

- http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things

Published Date: 02/2015
Document Version: NA
Domain of applicability: Consumer

Document Title: Standard for an Architectural Framework for the Internet of Things (IoT)
Summary: This standard defines an architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.
Document URL:

- http://grouper.ieee.org/groups/2413/

Published Date: Various
Document Version: Various
Domain of applicability: General

Industrial Automation and Control System Security

Organizational URL: http://isa99.isa.org/ISA99 Wiki/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.

Documents:

Document Title: Wiki - public available ISA security documents
Summary: Developing the ISA/IEC 62443 Series of Standards on *Industrial Automation and Control Systems (IACS) Security*
Document URL:
- http://isa99.isa.org/Public/Forms/AllItems.aspx

Published Date: 2015-2017
Document Version: NA
Domain of applicability: Industrial

Industrial Internet Consortium (IIC)

Organizational 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

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

International Organization for Standardization (ISO) IoT Standards

Organizational URL:
http://isotc.iso.org/livelink/livelink/open/jtc1wg10http://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.

Documents: Information technology — Internet of Things Reference Architecture (IoT RA)

Document Title: WG 10 "Internet of Things"

Summary: General Working documents for ISO IoT standards

Document URL:

- http://isotc.iso.org/livelink/livelink/open/jtc1wg10

Published Date: NA

Document Version: NA

Domain of applicability: General

Internet of Things Consortium:

Organizational URL: http://iofthings.org/

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.

Documents:

Document Title:

Summary:

Document URL:

Published Date:

Document Version:

Domain of applicability:

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.

Documents:

Document Title: IOT Security Foundation Best Practice Guidelines
Summary: General best practice guidelines covering the following three categories:

- IOT SECURITY COMPLIANCE FRAMEWORK
- CONNECTED CONSUMER PRODUCTS
- VULNERABILITY DISCLOSURE

Document URL:

- https://iotsecurityfoundation.org/best-practice-guidelines-downloads/

Published Date: 2016
Document Version: NA
Domain of applicability: General

ITU-T SG20

Organizational URL: http://www.itu.int
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."

Documents:

Document Title: Technical papers and reports
Summary: Technical papers and reports covering multiple connectivity topics, from Smart city, M2M to mobile networks.
Document URL:

- http://www.itu.int/pub/T-TUT

Published Date: 2010-2017
Document Version: NA
Domain of applicability: General

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 is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories.

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

Published Date: May 2016

Document Version: 1.0

Domain of applicability: General

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.

Documents:

Document Title: NERC Critical Infrastructure Protection Standards

Summary: The electric industry has long standing security standards for IP-based technology that connects to their networks, and these standards address patching. According to NERC, Bulk Electric Systems (BES) are unique from other systems discussed in this paper because they are generally "air-gapped," or isolated from the internet. The North American Electric Reliability Corp. (NERC) addresses the issue of patching in several communications to its members, first and foremost through its enforceable Critical Infrastructure Protection, or "CIP," standards, including CIP-007-6 Requirement R2 (Security Patch Management) and CIP-010-2 (Cyber Security/Configuration Change Management and Vulnerability Assessments) and CIP-010-2 Section 1.3 (Software Vulnerability Mitigation). NERC's 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity discusses how vulnerability assessments are conducted and how patches and updates are delivered. The document acknowledges that patching is not without its challenges, however, for power generators.

Document URL: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
Published Date: Various
Document Version: Various (note standards listed as "Subject to Enforcement"
Domain of applicability: Industrial

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: General

oneM2M

Organizational URL: http://www.onem2m.org/

Organizational Summary: oneM2M is the global standards for Machine to Machine communications and the Internet of Things. It operates as a global partnership, involving eight of the world's leading ICT standards bodies, six global fora and SDOs, and, over 200 companies from all industrial sectors.

Documents:

Document Title: Published specification
Summary: Multiple documents addressing M2M specification and IoT
Document URL:
Analysis of Security Solutions for the oneM2M System – TR0008, July 2014.

- http://onem2m.org/images/files/deliverables/oneM2M_TR-0008-Security-V1_0_0.doc

Security Solutions (oneM2M Release 1) – TS0003, January 2015 and revised on March 2016.

- http://onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V1_4_2.pdf

Security (oneM2M Release 2) – TR0008, August 2016.

- http://onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf

Published Date: Various
Document Version: NA
Domain of applicability: General

Online Trust Alliance

Organizational 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:

- https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Published Date: January 5, 2017
Document Version: 2.5
Domain of applicability: General

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
Document Version: NA
Domain of applicability: General

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

Domain of applicability: General

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:

Document Title: OWASP Internet of Things Project

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.
Document URL:
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Published Date: NA
Document Version: NA
Domain of applicability: General

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

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

SAFECode

Organizational URL: http://www.safecode.org/publications/

Organizational Summary: The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

Documents:

Document Title: Fundamental Practices for Secure Software Development 2nd Edition
Summary: The Fundamental Practices paper is not meant to be a comprehensive guide to all possible secure development practices. Rather, it provides a foundational set of secure development practices that have been effective in improving software security in real-world implementations by SAFECode members across their diverse development environments. Specific topics include:

- Secure Design Principles
- Secure Coding Practices
- Testing Recommendations
- Technology Recommendations

Document URL:

- https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

Published Date: 2011
Document Version: NA
Domain of applicability: General

Document Title: Guidance for Agile Practitioners
Summary: This paper provides practical software security guidance to Agile practitioners in the form of security-focused stories and security tasks they can easily integrate into their Agile-based development environments. SAFECode has also made available quick reference guides from the paper for download.
Document URL:

- http://www.safecode.org/publication/SAFECode_Agile_Dev_Security0712.pdf

Published Date: 2015
Document Version: NA
Domain of applicability: General

Smart Grid Interoperability Panel (SGIP)

Organizational URL: http://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."

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability: Industrial

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 spec. 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
Domain of applicability: Consumer

TUF

Organizational URL: **https://www.updateframework.com/**

Organizational Summary:

Documents:

Document Title: The Update Framework (TUF)

Summary: The Update Framework (TUF) helps developers to secure new or existing software update systems, which are often found to be vulnerable to many known attacks. TUF addresses this widespread problem by providing a comprehensive, flexible security framework that developers can integrate with any software update system. The framework can be easily integrated (or implemented in the native programming languages of these update systems) due to its concise, self-contained architecture and specification. Developers have so far implemented the framework in the Python, Go,Ruby, and Haskell programming languages. There is a specification that can specification and library that can be universally (and in most cases transparently) used to secure software update systems.

Document URL:

- **https://github.com/theupdateframework/tuf/blob/develop/docs/tuf-spec.md**

Published Date: NA

Document Version: NA

Domain of applicability: General

U.S. Food and Drug Administration (FDA)

Organizational URL: http://www.fda.gov/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
Document Version: NA
Domain of applicability: Medical Devices

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: Strategic Principles for Securing the Internet of Things
Summary: In 2016, the U.S. Department of Homeland Security (DHS) published a document containing high-level principles for IOT security. The principles included, among other recommendations, "Incorporate Security at the Design Phase" and "Advance Security Updates and Vulnerability Management." The document is a broad endorsement of the importance of users' ability to patch and upgrade IOT devices, and notes the then-nascent NTIA multistakeholder process. The document does not make specific recommendations for how users of IOT should conduct patching and upgrading, nor does it make specific recommendations for how users should implement such programs. Noteworthy is the document's endorsement of the concept of defense in depth which, it states, is particularly important as "...patching or updating mechanisms are not

available or insufficient to address a specific vulnerability."
Document URL: https://www.dhs.gov/securingtheIoT
Published Date: 11/15/2016
Document Version:1.0
Domain of applicability: General (enterprise and consumer)

Underwriters Laboratories (UL)

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

Documents:

Document Title:
Summary:
Document URL:
- http://industries.ul.com/mobile/internet-of-things-iot

Published Date:
Document Version:
Domain of applicability:

3rd Generation Partnership Project (3GPP):

Organizational URL:
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.

Documents:

Document Title:

Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

Appendix A:

Resources not fully documented

International Society of Automation (ISA)

Organizational URL: http://www.isa.org/

Organizational Summary:

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

Internet Engineering Task Force (IETF)

Organizational URL:

Organizational Summary:

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

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/https://datatracker.ietf.org/doc/draft-moore-iot-security-bcp/

ISASecure

Organizational URL: http://www.isasecure.org/en-US/

Organizational Summary:

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

ISA Security Compliance Institute (ISCI)

Organizational URL: http://www.isasecure.org/

Organizational Summary:

Documents:

Document Title:
Summary:
Document URL:
Published Date:
Document Version:
Domain of applicability:

Appendix B:

Areas needing further examination

- 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/http://simalliance.org/key-technical-releases/ http://simalliance.org/key-technical-releases/
- Center for Internet Security?
- https://securityintelligence.com/news/industrial-internet-consortium-develops-iot-security-framework/