Identity and Access Management for the Internet of Things - Summary Guidance

IoT Working Group

Presented by CSA cloud security alliance®

Acknowledgments

Initiative Leads

Arlene Mordeno
Brian Russell

Contributors

K S Abhiraj
Amit Pick
Srinivas Tatipamula
Aaron Guzman
Tom Donahoe
Vinay Bansal
Jay Douglas
Sabri Khemissa
Raghavender D
Mike Flegel
Abhik Chaudhuri
Drew Van Duren
Sudharma Thikkavarapu
Shyam Sundaram
Ayoub Figuigui

CSA Global Staff

John Yeoh
JR Santos

Letter from the Co-Chairs

> The Internet of Things (IoT) is experiencing significant growth in consumer and business environments.

The Internet of Things (IoT) is experiencing significant growth in consumer and business environments. The CSA has established the IoT Working Group (WG) to focus on providing relevant guidance to our stakeholders who are implementing IoT solutions. This document is the first in a series of summary guidance aimed at providing easily understandable recommendations to information technology staff charged with securely implementing and deploying IoT solutions. This document focuses on considerations for IoT Identity and Access Management (IAM).

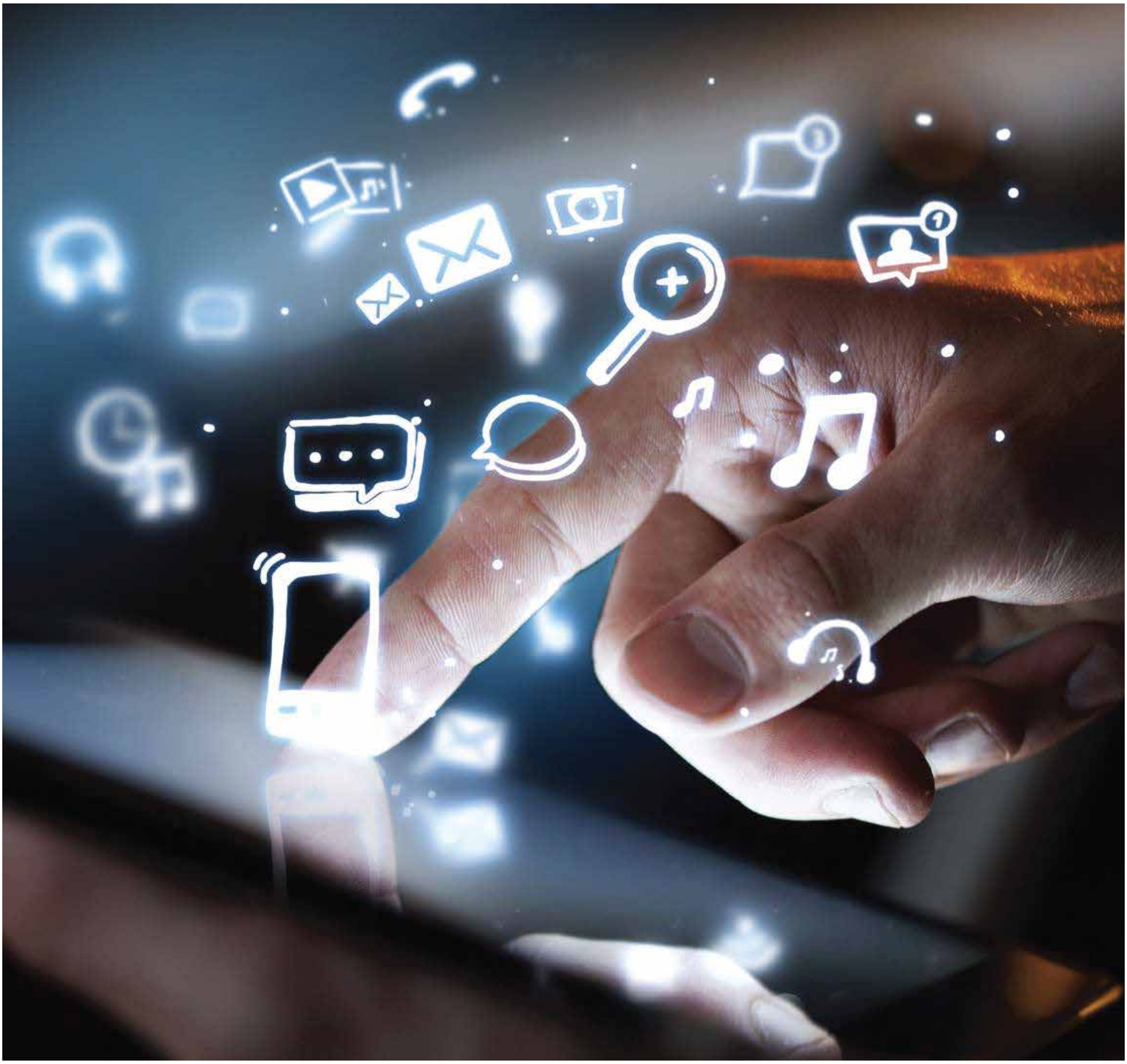
In the CSA IoT WG's April 2015 Report titled Security Guidance for Early Adopters of the IoT, Identity and Access Management (IAM) was discussed, however it was realized that IAM for the IoT is a continually evolving technology area. With this guidance, the CSA IoT WG has attempted to provide information to stakeholders detailing an easy-to-follow set of recommendations for establishing an IAM for IoT program within their organizations.

We realize that there are other organizations that are working towards researching and defining IoT identity management standards and we have referenced those organizations when possible in this document. We will update this document in the future to reflect advances in research and guidance from those organizations as well as our own CSA research.

We want to thank all of the many contributors worldwide who have worked hard to produce this and our other IoT guidance documents. Special thanks go to Arlene Mordeno for volunteering to lead this first summary guidance document and to the peer reviewers who provided substantial and beneficial input into the document's creation.

Sincerely,

Brian Russell
Co-Chair, IoT Working Group



Introduction

The IoT introduces the need to manage exponentially more identities than existing IAM systems are required to support. The security industry is seeing a paradigm shift whereby IAM is no longer solely concerned with managing people but also managing the hundreds of thousands of "things" that may be connected to a network. In many instances these things are connected intermittently and may be required to communicate with other things, mobile devices and the backend infrastructure. Some have begun to refer to this new identity ecosystem as the Identity of Things (IDoT). The IDoT refers to the relationships between devices and humans, devices and devices, devices and application/services or a human and an application/services.

Industry is only now beginning the move towards designing and deploying the IoT,

therefore it is an opportune time to consider how IoT IAM relates to other security services required for an IoT-connected enterprise. This includes services such as asset and cryptographic key management. In some instances, IoT solution vendors have even begun to integrate IAM as a byproduct of connecting IoT assets together.

There is also a move towards Identity Relationship Management (IRM), led by the Kantara Initiative (https://kantarainitiative.org). The Kantara Initiative has defined a set of IRM pillars that focus in part on consumers and things over employees; Internet-scale over Enterprise-scale; and Borderless over perimeter. These pillars are highly applicable to what is needed to support IoT IAM. Organizations should keep apprised of our industry's new IRM offerings.

There are other challenges associated with identity and access management in the IoT. These include the need to re-think what multi-factor authentication (MFA) entails and the need to define naming conventions for an organization's networked assets. According to a European Commission Report on IoT Identities by the Expert Group on the Internet of Things , "the issues of providing non-colliding unique addresses in a global scheme requires an infrastructure in place that supports highly dynamic devices that appear and disappear from the network at any time, move between different local and/or private networks and have the flexibility to either identify their user uniquely or hide his/her identity, thus preserving privacy as needed. Whether managing smart sensors, connected parking meters, automobiles, or connected health devices, each must be addressable within the larger system and the name of the thing should be bound to a credential."

Regarding MFA, it is not always feasible to use traditional MFA methods to support strong authentication of things. The Kantara Initiative and others have pointed to the need to research methods that provide context-based authentication as a new factor in an authentication process. Next-Generation authentication organizations like FIDO (USB-based hardware MFA) and CryptoPhoto (out-of-band smartphone MFA) offer strong authentication with inbuilt mutual authentication, both of which are suitable for IoT devices, even without screens/keyboards.

Because we are in such a new state regarding IoT IAM,

it is also important to stay abreast of standards work in this area. The IETF, for example, is working on a series of efforts under the umbrella of Authentication and Authorization for Constrained Environments (ACE- http://datatracker.ietf.org/wg/ace/documents/). The IETF ACE is working on modifications to existing IoT protocols such as a Delegated CoAP protocol, that "specifies how resource-constrained nodes can delegate defined authentication- and authorization-related tasks to less-constrained devices called Authorization Managers, thus limiting the hardware requirements of the security solution for the constrained devices."

Summary Guidance for Identity and Access Management in the IoT

01

Integrate your IoT implementation into existing IAM and GRC governance frameworks in your organization. Considerations should include the following steps:

a. Define a common namespace for IoT devices.

b. Establish an extensible identity lifecycle that can be applied to things in your organization and can be tailored based on the lifetime of the device and required identifier.

c. Within the identify lifecycle, establish clear registration processes for IoT devices. The rigor of the registration process should be dictated by the sensitivity of the data handled by a particular IoT device.

d. Determine the level of security protections (confidentiality, authentication, authorization) to be applied to unique data flows from sensors and other IoT components.

e. Establish clear authentication and authorization procedures for local access to IoT devices (e.g., administrative local access).

f. Define privacy protections required for different data categories. Establishing a framework reference definition for establishing privacy protections of Personally-identifiable information (PII) will aid in these definitions.

g. Determine and document whether outside organizations have access to certain categories of data.

h. Define how to perform authentication and authorization for IoT devices that are only intermittently connected to the network.

i. Identify access control requirements that apply to IoT according to your organization' access control policies.

Leaders across your business units need to understand all of the above.

02

Do not deploy IoT resources without changing default passwords for administrative access. If possible, do not deploy IoT devices with only local access capabilities. Rather, attempt to integrate all IoT resources into the enterprise IAM system. Note that this guidance does not apply to consumer-based IoT devices that are attached to the enterprise network. New concepts similar to those required for BYOD registration of devices would need to be applied to that segment of IoT devices.

03

Evaluate a move to Identity Relationship Management (IRM) in place of traditional IAM. IRM is more suitable to IoT than traditional IAM and is based on a set of pillars that include a focus on consumers and things over employees, Internet-scale over Enterprise-scale, and Borderless over perimeter. Identify and evaluate IRM vendor solutions as a possible fit for your IoT identity requirements.

04

Design your authentication and authorization schemes based on your system-level threat models. Evaluate each individual manufacturer's IoT implementation and choose vendors that have adhered to applicable standards and/or sought guidance or followed best practices from industry security groups such as BuildItSecure.ly and OWASP. Take into account the vulnerabilities of the system

05

Smartphones for authentication on IoT. Mobile Devices and Telecommunication networks play a major role in the IoT. Smartphones will potentially be used as one means of authentication step to access things surrounding us. The features that makes the smartphone a powerful authentication factor needs to be tightly integrated with other devices. The next generation smartphones would drive different types of authentication mechanisms like facial recognition using the front-facing camera, voice recognition, gesture dynamics and handling dynamics in addition to traditional biometrics such as fingerprints. These smart phones could be used for enterprise level local authentication to IoT devices.

06

Create reference architectures for your IoT implementations using ITU-T Y.2060 as a starting point. IoT reference architectures enable consistent implementation of authentication, authorization and accounting (AAA) services across all IoT devices in the infrastructure and can be used to test the overall accesses of systems at every level, from the individual machine to networks of machines at various layers in the technology stack. Identify the most vulnerable devices within your enterprise and apply MFA whenever possible.

07

Plan for the introduction of IPv6. Organizations have not fully moved to IPV6 as the industry is still in a state of prolonged transition. There are many IoT devices that are designed to use IPv4, so planning now for how a device designed to use IPv4 will talk to a IoT device designed to use IPv6, in a M2M implementation scenario is needed. To make this feasible, consider a Software Defined Networking (SDN) mechanism that can allow these devices to talk to each other to provide the intended service.

08

Consider design updates to your Public Key Infrastructure (PKI) environment to support provisioning of certificates to IoT devices in your organization. Use certificates whenever possible for device authentication and confidentiality during Transport Layer Security (TLS) and other protocol negotiations, as well as to support various other identity bindings when integrating with other access control mechanisms. Ensure that the PKI architecture supports standard services such as revocation checking, trust management, enrollment and registration procedures, and compromise recovery. Evaluate alternative certificate types that are optimized for the IoT, such as the smaller IEEE 1609.2 credential format. Evaluate additional services such as Online Certificate

Status Protocol (OCSP)- stapling or the Domain Name System (DNS) Authentication of Named Entities (DANE) means of supporting an enhanced IoT ecosystem. These technologies can improve security and reduce the burden on the network and sensors as they are not required to communicate with an OCSP server. Ensure that your PKI can scale to issue certificates to the larger quantities of devices that will require them.

09

Establish a plan for sharing IoT-related data with device manufacturers. Device manufacturers will continue to want to have device data access in order to monitor device health, track statistics, and be able to provide support to their customers. This data is collected and stored within various types of databases. Make sure to implement an authorization model for these back-end data stores such that 1) is compliant with relevant privacy regulations and 2) allows the minimal access required by manufacturers and other third parties.

10

Implement an AAA server that allow consumers to define preferences and provide services' consent for access to consumer profile data. An IoT implementation is one such service. This requires management of external identities such as consumers and patients, who are allowed to give their consent preferences for which attributes of their profile information can be shared and to whom. In many cases, this requires the integration of AAA services with third party services that manage consumer and business partner preferences for handling of data.

11

Consider integrating the identity management system with a building's Physical Access Control System (PACS), to enable additional security measures such as selectively provisioning what doors and entrances a person's badge can access. These security enhancements will provide improved physical protection to IoT devices.

12

Implement more restrictive logic in your identity management workflows so that you are proactively restricting access to IoT related systems and devices if a person has not had the necessary prerequisites as specified by your access governance framework. Examples of prerequisites include training and background checks.

13

Implement a privileged user management system to ensure that administrators can access and monitor systems and devices. This includes session monitoring of privileged sessions, protection of passwords to service accounts, and frequent password rotation.

14

Extend where possible the use of your current asset management to inventory and document IoT devices. Categorize them based on risk and assign owners. Modify the access records to support asset ownership, asset deployment, and any required revocation or asset lifecycle workflows. Integrate a service desk system that audits and automates the opening of tickets so that revocation of physical assets occurs in a system of record.

15

Invest in a well-documented plan for how you would respond to failures and breaches when they occur. One example is an Incident Handling or an Incident Response plan. Note that this plan should be made a part of your incident management process and workflows.

16

Establish relationship mappings between people and devices. This includes establishing explicit authorizations for people's authorized behavior on specific data sets. Enforce access management by both users and things. Implement MFA where possible for user access to IoT data.

17

Develop effective AAA mechanisms for sensor nodes based on the context and service security requirements. Wireless sensor nodes can be a key element for IoT implementations, however, AAA of the sensor nodes in a wireless mesh network is not yet fool proof due to limitations in energy and computing power. Consider context as a way to help determine the rigor of the authentication required based on risk introduced by a particular sensor node. Examples include location/coordinates, time-of-day, end-device/system being accessed, or data types being transmitted/received.

Be aware however, that in some attack scenarios, context information is easily stolen, forged, or proxied. Also keep in mind the dangers of context false-negatives and the potential danger that may result when legitimate users are incorrectly blocked (eg: bad device clocks, upgraded endpoints, unexpected but legitimate locations, loss of GPS signal, etc). Perform threat modeling to determine the most appropriate AAA mechanisms for your sensor nodes.

18

Leverage the security controls built into standards-based IoT protocols such as CoAP, DDS and REST to allow for interoperable authentication and authorization transactions between different manufacturers' IoT devices.

The following table shows various, common IoT communication protocols and assertions on what types of authentication are available. Selected protocols, where possible, should employ an integrated authentication approach consistent with the above recommendations.

Example IoT Protocols and Authentication Options

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

Protocol	m2m Authentication Options	Discussion
Zigbee	Pre-shared keys	Zigbee provides both network and application level authentication (and encryption) through the use of Master key (optional), Network (mandatory) and, optionally, Application Link keys
Bluetooth	Shared Key	Bluetooth provides authentication services through two different device pairing options, Standard and Simple Pairing. The Standard pairing method is automatic; the Simply pairing method includes a human-in-loop to verify (following a simple Diffie-Hellman exchange) that the two devices display the same hash of the established key. Bluetooth offers both one-way as well as mutual authentication options. Bluetooth secure simple pairing offers 'Just works', 'Passkey entry' and 'Out of Box' options for device-device authentication
Bluetooth-LE	Unencrypted data authenticated using Connection Signature Resolving Key (CSRK) Device Identity/Privacy is via an Identity ResolvingKey (IRK)	Bluetooth-LE introduces a two-factor authentication system, the LE Secure Connections pairing model which combines – based on device capability – several of the available association models available. In addition, Elliptic-Curve Diffie Hellman is used for key exchange.
HTTP/ REST	Basic Authentication (cleartext) (TLS methods) OAUTH2	HTTP/REST typically requires the support of the TLS protocol for authentication and confidentiality services. Although Basic Authentication (where credentials are passed in the clear) can be used under the cover of TLS, this is not a recommended practice. Instead attempt to stand up a token-based authentication approach such as OAUTH 2

In addition to the above guidance for IoT IAM, consider this additional related guidance to help securely implement IoT within your organization.

20

Mandate “Killswitch” functionality to allow IoT administrators to disable device connectivity to the internet, local area network or bluetooth, in case vulnerabilities have been identified, for which no update/upgrade has been provided yet. Also consider whether auto updates to IoT device firmware/software should be enabled or disabled, based on the unique circumstances of your IoT deployment.

21

Customer education needs to include handling instructions on 1) how to identify that software needs to be updated 2) how to rollback updates in case of errors 3) how security of other devices (smartphone, wireless network, building automation network) can impact the device’s security, 4) how to understand requirements for safeguarding customer data and enabling privacy-related configurations.

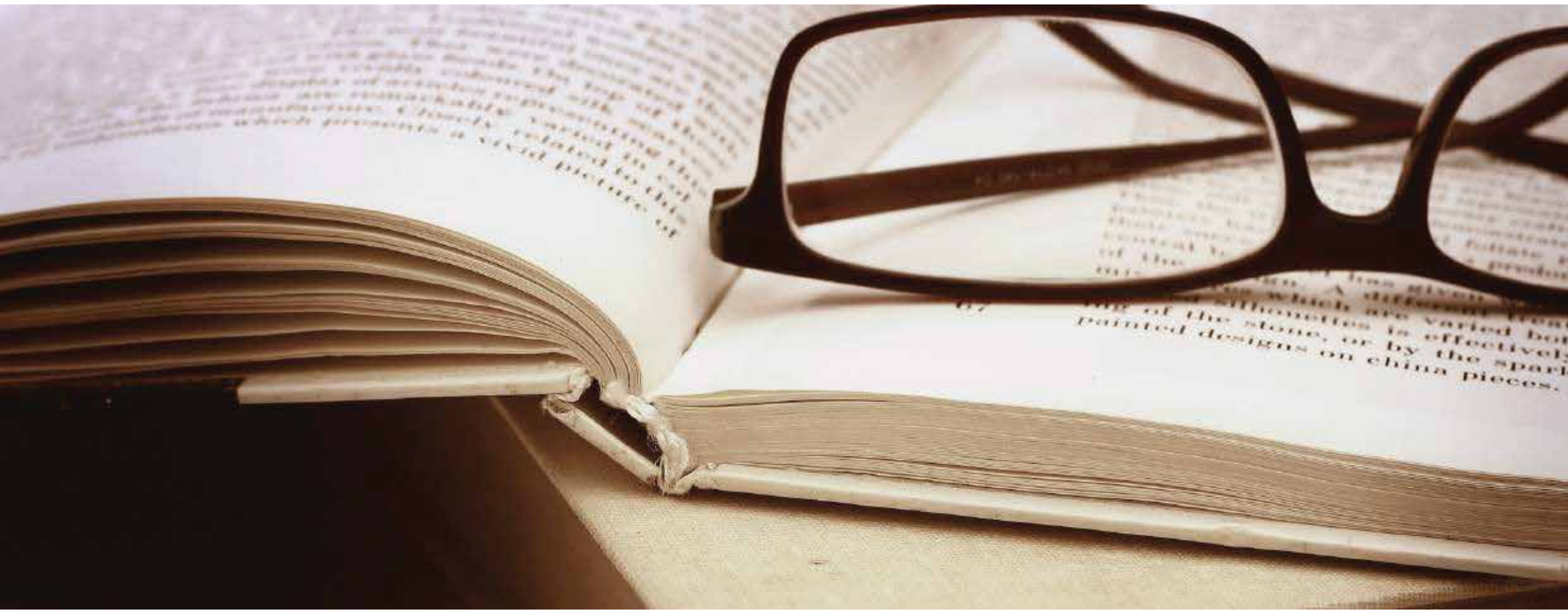
22

Provide a secure default configuration. Security for this broad target audience needs to be as simple as possible. A reset button or functionality should automatically restore the highest level of security. The End Users of IoT devices might not be familiar with minimum security awareness aspects and might not even expect threats associated with new functionality. Instead of making them blacklist undesired functions, they should whitelist functions for which they have understood the impact and appreciate the benefits.

23

Ensure IoT users awareness: needs to explain the impact of IoT use on data CIA (confidentiality, Integrity and Availability) within your organization. Define an awareness sessions to promote best practices related to securing IoT within your organization. These awareness session should :

a. Define a common jargon of IoT security
b. Identify risks related to IoT use
c. Explain techniques deployed to protect IoT
d. Teach users on how to securely use their IoT devices
e. etc.



References

"Things" will force makeover of enterprise ID, access management by John Fontana @ http://www.zdnet.com/article/things-will-force-makeover-of-enterprise-id-access-management/

Deploy360@IETF92, Day 2: DNSSEC, DANE, IPv6, IoT and Homenet @ http://www.internetsociety.org/deploy360/blog/2015/03/deploy360ietf92-day-2/

Challenges from the Identities of Things by Ingo Friese, Jorg Heuer and Ning Kong @ http://kantarainitiative.org/confluence/download/attachments/64389214/PID3057147.pdf

Managing the Authorization to Authorize in the Lifecycle of a Constrained Device @ https://datatracker.ietf.org/doc/draft-gerdes-ace-a2a/?include_text=1

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS (ITU-T Y.2060) @ https://www.itu.int/rec/T-REC-Y.2060-201206-I

10th Meeting of the Internet of Things Expert Group, report by Tom Wachtel @ http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7598&no=6

Expert Group on the Internet of Things (IoT-EG) @ http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752

The shift from IAM to Identity Relationship Management by Joni Brennan, Kantara Initiative @ http://www.scmagazine.com/the-shift-from-iam-to-identity-relationship-management/article/338758/

Gartner Says Managing Identities and Access Will Be Critical to the Success of the Internet of Things @ http://www.gartner.com/newsroom/id/2985717

Bluetooth SIG, FIDO collaboration could bring better security to Internet of Things by Monica Alleven @ http://www.fiercewireless.com/tech/story/bluetooth-sig-fido-collaboration-could-bring-better-security-internet-thing/2015-07-26

Identity Relationship Management by Kantara Initiative @ https://kantarainitiative.org/irmpillars/

The permanent and official location for Cloud Security Alliance Internet of Things research is https://cloudsecurityalliance.org/group/internet-of-things/ .