IoT Security Maturity Model: Description and Intended Use

Version 1.1

2019-02-15

The goal of a Security Maturity Model (SMM) is to provide a path for Internet of Things (IoT) providers to know where they need to be and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms. It seeks to help organizations identify the appropriate approach for effective enhancement of these practices where needed. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

As an informed understanding of the risks and threats an organization faces is the foundation of choosing and implementing appropriate security controls, the model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

Not all IoT systems require the same strength of protection mechanisms and the same procedures to be deemed secure enough. The organization determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementation of security mechanisms and processes are considered *mature* if they are expected to be effective in addressing those goals. It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity. Hence, *security maturity* is the degree of confidence that the current security state meets all organizational needs and security-related requirements. *Security maturity* is a measure of the understanding of the current security level, its necessity, benefits and cost of its support. Factors to weigh in such an analysis include the specific threats to an organization's industry vertical, regulatory and compliance requirements, the unique risks present in an environment and the organization's threat profile.

Security level,[1] on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner. The SMM does not say what the appropriate security level should be. Rather, it provides guidance and structure for organizations to identify considerations for different maturity levels appropriate for their industry and system. It provides guidance for defining and taking into account different levels of comprehensiveness and alignment with industry sector and system, including non-industrial systems. Some users of the model will apply its guidance to create industry and system-specific profiles, which can then be used by a broader audience, in concert with the model, to help assess maturity in a specific vertical or use case.

The audience for this document includes owners of IoT systems, decision makers, security leaders in various verticals, business risk managers, system integrators, architects, security assessors, analysts, policy and regulatory authorities, and other stakeholders concerned about the proper strategy for the implementation of mature security practices tailored to the needs and constraints of the specific IoT system

[1] According to the IEC 62443 3-3

Those using this SMM should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements[1] and threat landscape, what is my solution's target maturity state?
- What is my solution's current maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

RELATIONSHIP TO OTHER IIC DOCUMENTS

The Industrial Internet Consortium (IIC) has created the *Industrial Internet Security Framework* (IISF) [IIC-IISF2016] that captures the information technology and operational technology dimensions of Industrial Internet of Things security and describes the security domains and various techniques available to address it. This document builds on the concepts of the *Industrial Internet Reference Architecture* (IIRA) [IIC-IRA2015] and IISF and provides an additional dimension to the security techniques and mechanisms described in those documents. It provides guidance as to which mechanisms are to be used and the maturity required to address specific IoT scenarios.

We rely on the definitions provided in the IIRA [IIC-IRA2015] and the IISF [IIC-IISF2016].

The "*IIC Vocabulary*" [IIC-IIV2017] provides terminology and definitions for this document and other IIC documents. Acronyms are defined in the appendices. Additional terms relevant to this model are also defined in the appendices.

This document, the "IoT Security Maturity Model: Description and Intended Use" is the first of two documents covering the SMM and provides an introduction to the SMM. The second document "IoT Security Maturity Model: Practitioners Guide" will provide the details on the SMM and will be published soon.

[1] Namely, business or mission needs, requirements from regulatory authorities, and other similar factors.

INTENDED USE OF THE MODEL

THE SMM PROCESS

Organizational business stakeholders define goals for the security posture of the organization and the systems it owns or operates. These systems may be brand new or brownfield. These goals should be mapped to objectives that tie to the risks. Technical teams within the organization, or third-party assessment vendors, map these objectives into tangible security techniques and capabilities, identifying the appropriate target security maturity state. Establishing a target maturity state, while taking into account industry and system-specific considerations, facilitates generation of security profiles. These profiles capture target security maturity states of systems and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

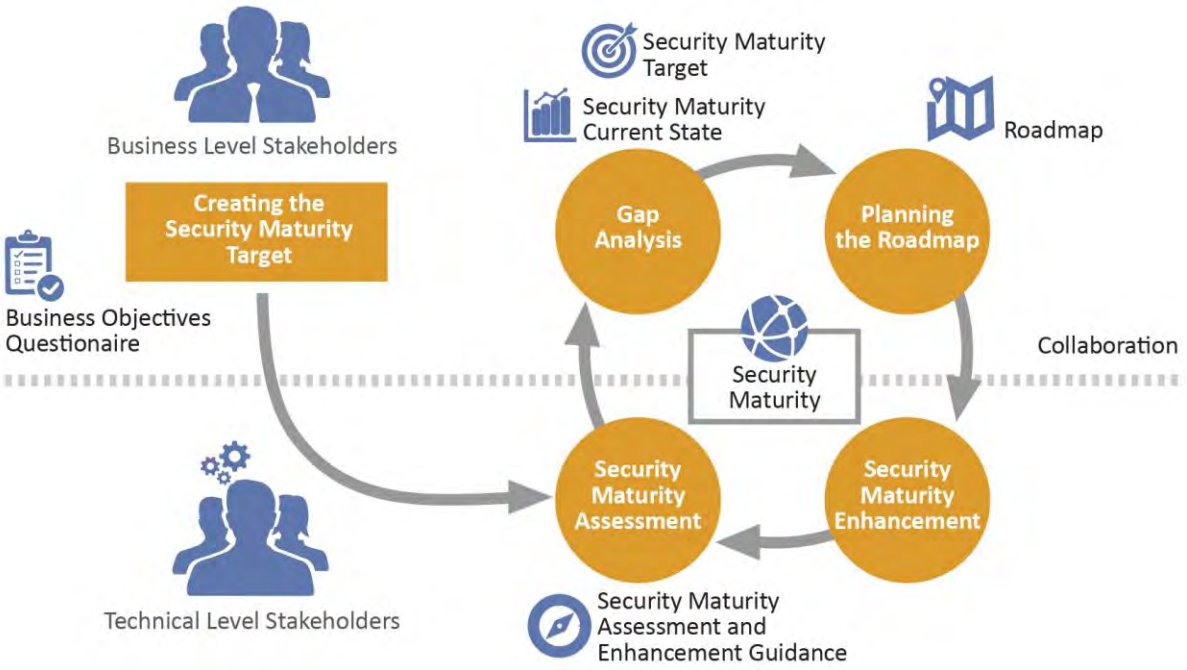


Figure 1 SMM Process

We expect most organizations to follow the SMM process depicted in Figure 1. Once a target has been created or a relevant industry profile identified, organizations would conduct an assessment to capture the current maturity state. The two states are compared and gaps identified so that an improvement roadmap can be established. Once enhancements are implemented, another assessment can be performed. The cycle is repeated to ensure that the appropriate security target is always maintained in an ever-changing threat landscape.

A persistent mature system security state can only be achieved via continued security assessments and improvements, orchestrated over time. Consequently, the maturity model is based on the Plan-Do-Check-Act (PDCA) cycle (Act, in this case, means accepting a new baseline if the check on the result of the improvement step is successful). This cycle begins by establishing the target for security maturity for a specific system. Then an iterative high-level process of security maturity improvement begins, as shown in Figure 2. As security threats and approaches to mitigate them change, organizations should determine how frequently to execute the cycle.

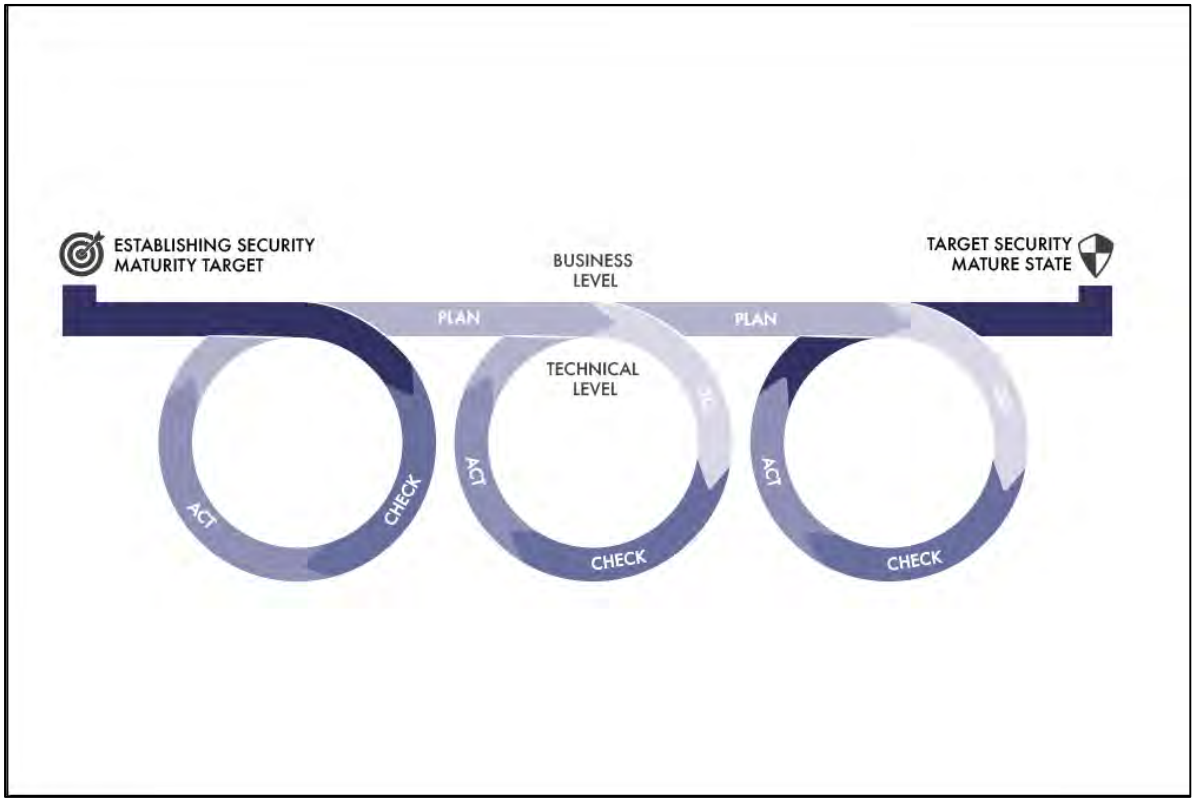


Figure 2 SMM Improvement Cycle

OBJECTIVES

The following are the key objectives for the SMM.

Fostering collaboration among stakeholders: Allow for an efficient and productive collaboration process between:

- business stakeholders (decision makers, business risk managers, owners of IoT systems) concerned about the proper strategy for implementing mature security practices, tailoring the needs and constraints of the particular IoT system, and
- analysts, architects, developers, system integrators and other stakeholders who are responsible for technical implementation.

Identifying security performance indicators: Provide a framework for defining and identifying the security target according to organizational-level demands so that business and technical stakeholders can use it to ascertain what progress should be made.

Guiding the process of achieving the mature state: Provide guidance on the assessment, enhancement and measurement of the current security maturity state in accordance with the defined security maturity target and demonstrate the attainment of all goals set by this target.

REQUIREMENTS

When developing the SMM, the authors were guided by the following requirements.

Real-world applicability: The method for setting the security maturity target must consider functionality, safety, regulatory and legal requirements or guidelines, risk management, security and privacy policies, performance, costs and other business considerations. It must also consider known and emerging threats and affordable ways of countering them. The outcome of the process and the guidance for attaining the target should be directly applicable to the IoT infrastructure in question and therefore be actionable.

Consideration of different perspectives: The SMM facilitates a description of security maturity from different viewpoints including business and implementation views. It helps define security maturity goals from an organizational perspective and security maturity requirements from an implementation perspective. The model helps align these definitions and thus drive collaboration among all stakeholders who are working towards security maturity enhancement.

Appropriate security guidance: The SMM provides guidance for the assessment and further enhancement of security maturity that aligns security capabilities with the use case. Security measures in consumer devices are unlikely to be the same as those in critical infrastructure. Guidance should be practical and actionable.

Adaptable to changing threat environment: As IoT infrastructure and threats evolve, the security maturity target must be adaptable to remain relevant in the long run. It is insufficient to implement security measures only at the system design stage for IoT systems in operation for a long time.

Extensibility: IoT business models, products, guidelines, regulations, technologies and types of organizations will evolve. The SMM needs to be extensible and flexible to accommodate any changes.

UNDERSTANDING THE MODEL

HIERARCHY OF SECURITY MATURITY PRACTICES

Figure 3 illustrates the structure of the SMM and the breakdown of security maturity domains. *Domains* are the high-level views that capture the key aspects of security maturity: governance, enablement and hardening. Each of the domains has different key aspects to it, called *subdomains*. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

This hierarchical approach enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

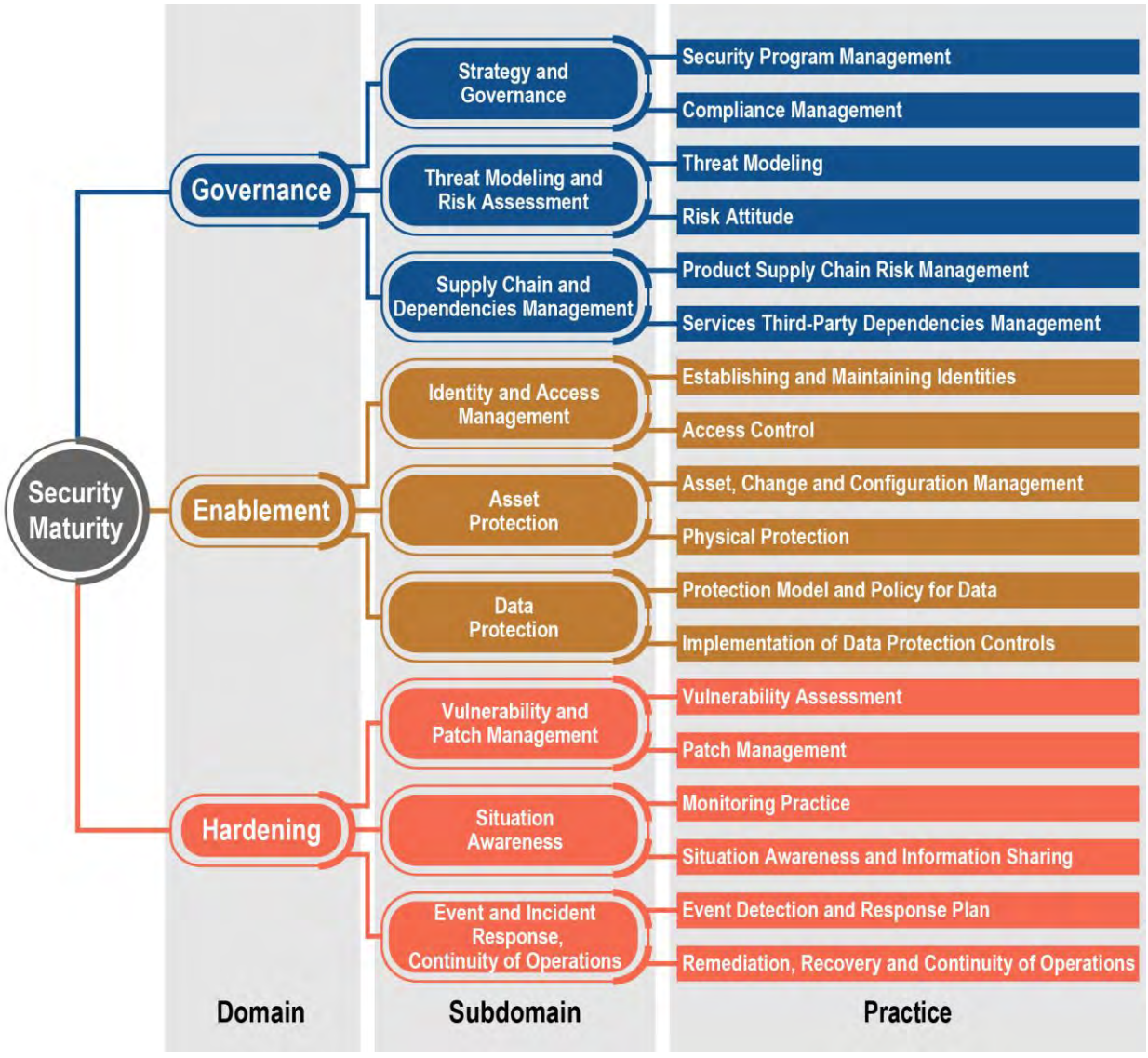


Figure 3 SMM Hierarchy

Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.	At the domains level, the stakeholder determines the priorities of the direction in improving security.
Sub Domains reflect the basic means of obtaining these priorities at the planning level.	At the sub domains level, the stakeholder identifies the typical needs for addressing security concerns.
Practices define typical activities associated with sub domains and identified at the tactical level.	At the practices level, the stakeholder considers the purpose of specific security activities.

SECURITY GOVERNANCE

Figure 4 below describes the elements of the governance domain of the SMM.

The security governance domain is the heart of security. It influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation.

Security strategy and the governance sub domain facilitates organizational drivers along with providing security, compliance with regulations, laws and contractual obligations. This also can relate to customer expectations and reputation management.

Security program management practice is vital to the clear planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.	**Compliance management practice** is necessary when strict requirements for compliance with evolving security standards is needed.

Threat modeling and the risk assessment sub domain identifies gaps in specific configurations, products, scenarios and technologies and prioritize countermeasures accordingly.

Threat modeling practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.	**Risk attitude practice** enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.

Supply chain and the external dependencies management sub domain aims at controlling and minimizing a system's exposure to attacks from third parties that have privileged access and can conceal attacks.

Product Supply chain risk management practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.	**Services Third party dependencies management practice** addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.

Figure 4 Security Governance

SECURITY ENABLEMENT

Figure 5 below describes the elements of the enablement domain of the SMM.

The security enablement domain is based on established security policy and addresses the business risks using the best available means. Security policy and controls are subject to periodic review and assessment.

Identity and access management sub domain aims to protect the organization and control the use of resources by the identified agents to reduce the risk of information leakage, tampering, theft or destruction.

Establishing and maintaining identities practice helps to identify and constrain who may access the system and their privileges.	**Access control practice** policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.

The asset management sub domain is put in place to protect both physical and digital assets. This is an area of strong collaboration between IT and physical security teams.

Asset, Change and Configuration Management practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.	**Physical protection practice** policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.

The data protection sub domain prevents unauthorized data disclosure or manipulation of data, both for data at rest, in transit and in use. This is important for security, privacy, regulatory compliance, legal and intellectual property protection.

The security model and policy for data practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.	**The implementation of data protection controls practice** describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.

Figure 5 Security Enablement

SECURITY HARDENING

Figure 6 below describes the elements of the security hardening domain of the SMM.

The security hardening domain practices support trustworthiness objectives through the assessment, recognition and remediation of risks with both organizational and technical countermeasures.

Vulnerability and the patch management sub domain policies and procedures keep systems up to date and less prone to attacks.

Vulnerability assessment practice helps to identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.	**Patch management practice** policy clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.

The situational awareness sub domain aims at understanding the current security state enabling an organization to prioritize and manage threats more effectively.

Monitoring practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.	**Situational Awareness and Information sharing practice** helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.

Event and incident response, continuity of operations sub domain implemented in a combination of policy and technical preparation allows an organization to respond to incidents swiftly and minimize disruption to the rest of the system.

An event detection and response plan defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.	**Remediation, recovery, and continuity of operations** represent a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.

Figure 6 Security Hardening

APPLYING THE MODEL

Two aspects are essential for measuring the maturation progress of IoT systems and prioritizing associated security practices. The first aspect is the comprehensiveness of the process to assure that security mechanisms work properly. The second is the scope of these mechanisms for the particular IoT sector or system demands.

Comprehensiveness captures the degree of depth, consistency and assurance of security measures that support security maturity domains, sub domains or practices. For example, a higher level of comprehensiveness of threat modeling implies a more automated systematic and extensive approach.

Scope reflects the degree of fit to the industry or system needs. This captures the degree of customization of the security measures that support security maturity domains, sub domains or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

SCORING AND PRIORITIZATION

Any rigorous security self-assessment procedure, including the SMM, needs a scoring and prioritization method to enable evaluation of the current state and the development of a metrics-based security strategy.

Comprehensiveness and scope, which are orthogonal, help score and prioritize security maturity practices. Certain IoT systems may not require the highly sophisticated or narrowly scoped implementation of all security practices. Such implementation may be over-engineered, given the particular system and the threats that it faces. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

COMPREHENSIVENESS LEVELS

There are five comprehensiveness levels for every security domains, sub domain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree of comprehensiveness of security controls. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones.

Level 0, None: There is no common understanding of how the security practice is applied and no related requirements are implemented (As this is null, we shall not discuss it further).

Level 1, Minimum: The minimum requirements of the security practice are implemented. There are no assurance activities for the security practice implementation.

Level 2, Ad hoc: The requirements for the practice cover main use cases and well-known security incidents in similar environments. The requirements increase accuracy and level of granularity for the environment under consideration. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks. For this assurance, application of measures learned through successful references may be applied.

Level 3, Consistent: The requirements consider best practices, standards, regulations, classifications, software and other tools. Using such tools helps to establish a consistent approach to practice deployment. The assurance validates the implementation against security patterns, secure-by-default designs and known protection approaches and mechanisms.

Level 4, Formalized: A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. For this assurance, a more complex approach is applied that uses semi-formal to formal methods.

SCOPE

The scope measurement captures the extent to which the specifics of an application, network or system of interest is taken into account during the implementation of the security facet.

There are three levels of scope for every security facet, from Level 1 to Level 3, with higher numbers indicating a narrower and more specific scope.

Level 1, General: This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific IoT sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

Level 2, Industry specific: The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sector-specific issues, particularly those regarding components and processes that are prone to certain types of attacks, and known vulnerabilities and incidents that took place.

Level 3, System specific: This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes and usage scenarios. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

Visualization helps understand the goals and ongoing progress of security maturity enhancement. Figure 7 shows how comprehensiveness level and scope for security maturity domains may be illustrated on the same diagram. The example describes an IoT system that accepts an ad-hoc approach to threat modeling and security strategy governance. Stricter but still general requirements are applied to asset, change & configuration management, and identity and access management. Incident management and information sharing & communication are specific to the sector because stakeholders want to know about relevant security incidents and track appropriate indicators of compromise. Finally, vulnerability and patch management, as well as the supply chain management and situational awareness are specific for the system because of the need to minimize possible disruptions of supported processes.

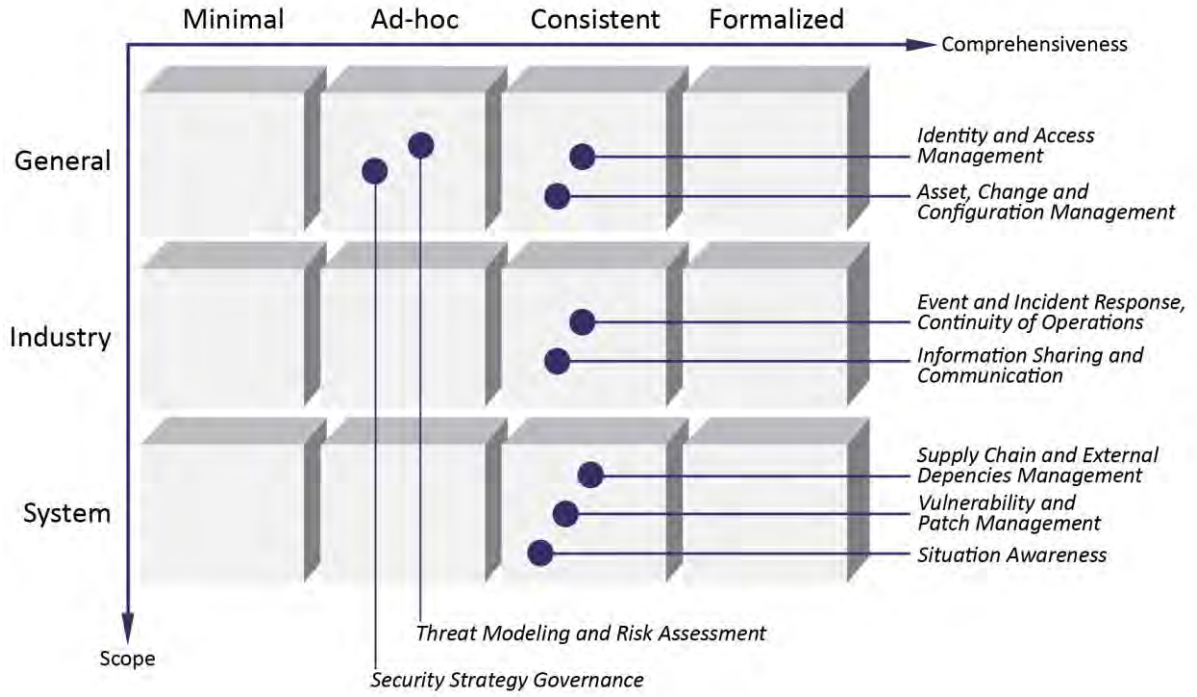


Figure 7 Visualization of two-dimensional approach in measuring security maturity

SMM TEMPLATE

All IoT devices, networks and systems do not require the highest comprehensiveness and scope for all security domains, sub domains or practices. The security maturity target for the system of interest is defined as the set of all desirable values of comprehensiveness and scope characteristics for every security maturity domain, sub domain and practice.

In case of insufficient details about the system-security needs the stakeholders may initially determine the target levels of comprehensiveness and scope just for domains. These levels determine the relative priorities of security governance, enablement and hardening. The levels set for the domains will be inherited by the appropriate sub domains and then by the practices according to the hierarchy. The stakeholders may modify the levels to more closely match the risks. This is helpful for the step-by-step recognition of an uncertain security maturity target.

The security maturity target by default is defined when referring to the comprehensiveness and scope for security maturity practices as seen in Figure 8. Each practice table has four columns, one for each comprehensiveness level. The objective in each level describes the general considerations that should be met. Guidance is provided in the form of general considerations.

	<Practice Name>			
	Comprehensiveness Level 1	***Comprehensiveness Level 2***	***Comprehensiveness Level 3***	***Comprehensiveness Level 4***
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Sector-specific considerations	<List of sector considerations>			
System-specific considerations	<List of system considerations>			

Figure 8 SMM Template

Figure 9 is an example of a partially filled-in threat modeling practice using the above template.

	Practice: Threat Modeling of Medical Devices including a handheld that collects patient telemetry and a base station aggregates patient vitals and shares data across a hospital network.			
	Comprehensiveness Level 1	***Comprehensiveness Level 2***	***Comprehensiveness Level 3***	***Comprehensiveness Level 4***
Objective	Consider general IT security issues as threats	Perform vulnerability analysis to identify threats. Address in an ad-hoc manner	Describe and classify threats in an accurate (optionally formal) way	Reveal and describe IT, OT and IoT factors both known and specific that may put the system at risk
General considerations	At this level, threats are only based on known typical IT security threats. **What needs to be done to achieve this level** Collect the available information about typical IT security vulnerabilities and incidents and recognize those that are relevant as threats. **Indicators of accomplishment** Business-level documents mention general security threats, such as sensitive data disclosure, denial of service attacks, or infiltration with malware.	At this level, the organization performs vulnerability assessments to understand threats as they pertain to the organization. The organization can discern specific IT, OT and IoT threats. **What needs to be done to achieve this level** Perform a vulnerability assessment for IT, OT, and IoT (At this level, they are typically managed separately). Use the generally accepted vulnerability evaluation schemes (such as Common Vulnerability Scoring System) [CVSS].	At this level, accepted formal threat modeling methods are used, and automated tools are used for thread modeling. **What needs to be done to achieve this level** Describe the threats during the analysis using generally accepted classifications like CAPEC or OWASP Top10. Optionally use the tools to describe the architecture of the system to automatically identify threats and possible resolution. Address the IT, OT, and IoT-specific (for example, edge device physical compromise) threats.	At this level, threat modeling is built into business processes and driven by business goals and risk profile. **What needs to be done to achieve this level** Validate the security threats against objectives set according to business needs. Base the threat model upon the set of clearly identified security assumptions about system environment (including physical security), trustworthiness constraints, and key actor's behavior. IT, OT, and IoT threats are integrated.

		Indicators of accomplishment A vulnerability assessment report is available and identifies common and typical threats valid for the identified use cases.	Consider the results of threat modeling and risk assessments as a part of formal processes to address and prevent the identified concerns. **Indicators of accomplishment** Identified tools and documented methods for the threat assessment. An assessment report that consistently describes the classified threats, vulnerable technologies, exploitation method or attack pattern, level of risk and possible resolutions.	Organize the particular threats and attack vectors as a consistent hierarchical structure, including all identified security issues. **Indicators of accomplishment** The accepted methodology for threat analysis and modeling that comprises a part of the rhythm of the business, accounts for business goals and risk, and is performed consistently. The periodic assessment reports demonstrating threat analysis experience and lessons learned over time.
Industry Specific Considerations	**What needs to be done to achieve Level 3** Note: FDA guidance can be interpreted to require that a medical device manufacturer reach or exceed a level 3 comprehensiveness in threat modeling as part of a pre-market submission. The threat model accounts for FDA guidance for post-market management of cybersecurity in medical devices **Industry Guidelines for Level 3** FDA requirements for pre-market submissions related to cybersecurity: *https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf* FDA post-market guidance on managing cybersecurity in medical devices: *https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf* **What needs to be done to achieve Level 4** Threat model includes not only the device in isolation, but the medical environments in which the device will operate. Threat model includes scenarios in which the device could allow its users to violate HIPAA standards (such as by leaking Personally Identifiable Information (PII)) and seeks to mitigate those opportunities.			
Handheld Specific Considerations	The handheld collects only anonymized patient telemetry data. Its exposed attack surfaces are Bluetooth LE, USB, and physical access.			
Base station Specific Considerations	The base station aggregates patient telemetry with PII, making the data it stores and transmits HIPAA relevant. Its exposed attack surfaces include Bluetooth LE, USB, Wi-Fi, Ethernet, and physical access.			

Figure 9 SMM Practice Table Example

SECURITY MATURITY TARGET AND PROFILES

The security maturity target is a goal-setting document that establishes the ultimate security maturity state for a new or brownfield IoT system. The target includes a consistent set of security practices, providing a comprehensiveness view of security to all stakeholders. This view consists of the definition of general security goals and needs and the purpose of every security practice. Establishing what the security maturity target should look like falls to business stakeholders and it should be carried out prior to any investment on enhancing security.

The following procedure is recommended to establish the target and set priorities:

Establish the goal within every security domain according to the global vision of the role of governance, enablement and hardening in the targeted mature state. Define goals for every domain based on the overall goal. The goal chosen from this set determines the comprehensiveness and scope levels for the whole domain. Security maturity sub domains and practices considered within the domain will inherit these levels at this step. This first step provides a rough definition of the security maturity target.

Consider the needs that are covered by the security maturity sub domains defined within every domain. These needs include threats and continuous changes of threat landscape, compliance needs, requirements from regulatory authorities. The previous step provided the initial comprehensiveness and scope levels for the sub domain. Then the stakeholders may further refine the precise levels that address their specific needs. This step specifies whether there are specific security-related needs that require attention beyond the established baseline.

Clarify the purpose of every security practice within the sub domain. As sub domain prioritization emphasizes specific security needs, consideration of security practices for every sub domain clarifies how they contribute in addressing these needs. Some practices may be entirely applicable and some only partially. Target comprehensiveness and scope levels for separate practices reflect the level of assurance in covering sub domain needs by these practices. This step considers the comprehensiveness and scope needed for the implementation of security capabilities, thus providing a greater level of detail to the security maturity target.

Once the security maturity target is available, it may be used in subsequent applications of the SMM, to create a target profile or evaluate a current maturity state assessment, for example.

Security maturity target profile is a typical security maturity target for a specific type of device, organization or system. Using security maturity target profiles simplifies the process of establishing the target for common use cases. Establishing a library of security maturity target profiles for common IoT scenarios is a subject for further development.

CURRENT SECURITY MATURITY STATE

Having a summary of fully or partially implemented security capabilities in a document facilitates establishing a roadmap for focused maturity enhancements. Based on the SMM, the *current security maturity state* document describes the current level of maturity of implemented practices for the given system in a similar format to the security maturity target. Creation of this

document, which implies conducting a security assessment, facilitates identification of gaps between the current state and the target.

The *current security maturity state* is the description of the security maturity state for the specific type of device, organization or system.

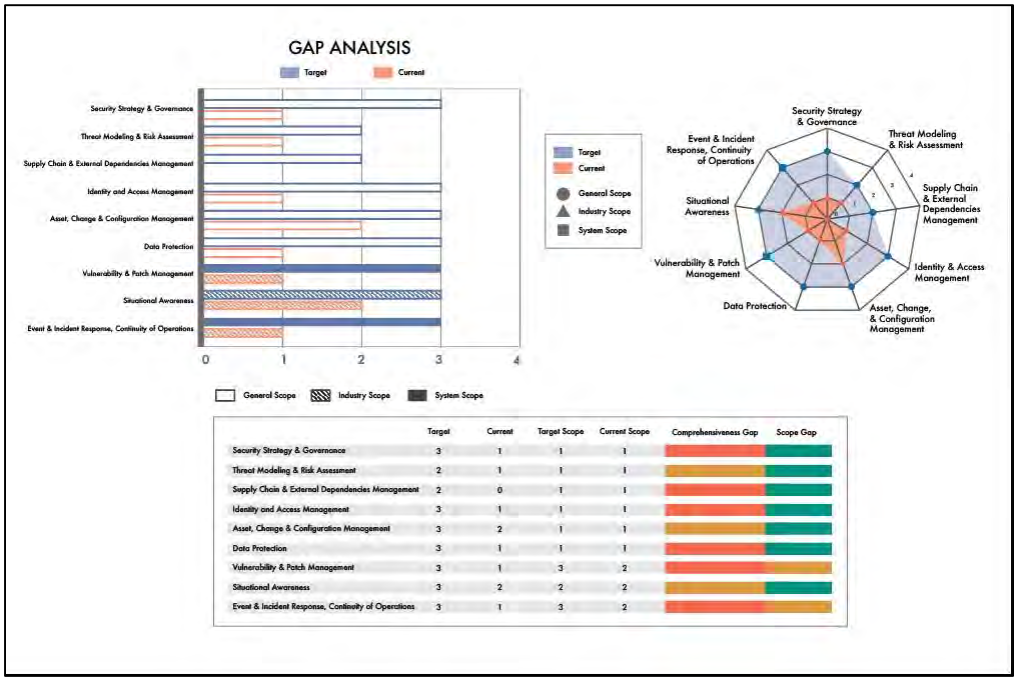
GAP ANALYSIS

The *security maturity* of the target and current state can be compared to identify gaps and opportunities for improvement. As a result of the comparison of the security maturity target and current security maturity state, business and technical stakeholders can measure the progress and negotiate the steps for security maturity enhancement. Three possible visualizations for gap analysis are shown in Figure 10. One is a heat map based on the levels of the target and current comprehensiveness as well as the scope. The heat map displays the gaps for each where red indicates a large gap, yellow small gap and green as no gap.

Similarly, a bar chart can be used to compare the levels of comprehensiveness between the target and current state where the differences between the bars shows the gap, if it exists. The shading of the bars can be used to display and compare the scope (in this example general scope is an empty bar, industry scope is a patterned bar and system scope is a filled bar).

The third visualization is a radar chart showing the current and target comprehensiveness states where the difference between the levels represents the gap, if it exists. In this chart the symbols are used to visualize the scope, with different symbols for the general, industry and system scopes. Where the symbols do not match between current and target this indicates a gap in scope levels.

Gaps in the maturity are determined gaps in the comprehensiveness and scope. If gaps exist for a particular practice, the maturity for that practice is lower than desired and needs to be improved. If no gaps exist (score is even or current state is higher than the target) then the maturity of the organization is sufficient or ahead of the need.



	Target	Current	Target Scope	Current Scope	Comprehensiveness Gap	Scope Gap
Security Strategy & Governance	3	1	1	1		
Threat Modeling & Risk Assessment	2	1	1	1		
Supply Chain & External Dependencies Management	2	0	1	1		
Identity and Access Management	3	1	1	1		
Asset, Change & Configuration Management	3	2	1	1		
Data Protection	3	1	1	1		
Vulnerability & Patch Management	3	1	3	2		
Situational Awareness	3	2	2	2		
Event & Incident Response, Continuity of Operations	3	1	3	2		

Figure 10 Gap Analysis for Security Maturity Target

CONCLUSION AND NEXT STEPS

This document provides an introduction to the Security Maturity Model (SMM). Details on the SMM are in the "IoT Security Maturity Model: Practitioners Guide" which should be read next.

ACRONYMS

CAPEC Common Attack Pattern Enumeration and Classification

IIC Industrial Internet Consortium

IIRA Industrial Internet Reference Architecture

IISF Industrial Internet Security Framework

IoT Internet of Things

IT Information Technology

OT Operational Technology

OWASP Open Web Application Security Project

DEFINITIONS

The following terms, specific to the context of the SMM, are defined here:

Security Level: Security Level is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.

Security Maturity: Security Maturity is a measure of an understanding of the current Security Level, its necessity, benefits, and cost of its support.

Domain: Domains are the strategic level priorities for security maturity. In the SMM, there are three domains: Governance, Enablement, and Hardening.

Sub Domain: Sub Domains refer to the basic means to address a domain at the planning level. Each domain currently defines three sub domains.

Security Practice: Practices are the typical activities performed for a given sub domain; they provide the deeper detail necessary for planning. Each sub domain has a set of practices.

Comprehensiveness: The model defines comprehensiveness levels as a measure of the Comprehensiveness, consistent, and highly assured implementation of measures supporting the security maturity domain, sub domain or practice.

Scope: The model defines scope as a measure for the customized, technically appropriate approach to the implementation of measures supporting the security maturity domain, sub domain or practice, and fitting the needs and constraints of IoT sector or system.

Security Maturity Target: The Security Maturity Target is the desired "end state" Security Maturity for an organization or system. The Security Maturity Target can apply to a new system under development or an existing brownfield system. The Security Maturity Target is determined based upon the business objectives of the organization or group.

REFERENCES

[IIC-IIRA2015] Industrial Internet Consortium: The Industrial Internet Reference Architecture Technical Report, Version 1.7, 2015-June-04 http://www.iiconsortium.org/IIRA.htm

[IIC-IIV2017] Industrial Internet Consortium: The Industrial Internet of Things - Volume G8: Vocabulary Version 2.0, IIC:PUB:G8:V2.00:PB:20170719, 2017-July-17 http://www.iiconsortium.org/vocab/index.htm

[IIC-IISF2016] The Industrial Internet of Things Volume G4: Security Framework Version 1.0, 2016-September-26 http://www.iiconsortium.org/IISF.htm

[RFC 2119] S. Bradner. IETF. "Key Words For Use In RFCs To Indicate Requirement Levels". March 1997. Best Current Practice. https://ietf.org/rfc/rfc2119.txt

AUTHORS AND LEGAL NOTICE

This document is a work product of the Industrial Internet Consortium Security Applicability Contributing Group, co-chaired by Hamed Soroush (Real-Time Innovations) and Ron Zahavi (Microsoft).

Authors: The following persons contributed substantial written content to this document: Sandy Carielli (Entrust Datacard), Ekaterina Rudina (Kaspersky Lab), Hamed Soroush (RTI) and Ron Zahavi (Microsoft).

Editors: Sandy Carielli (Entrust Datacard), Matt Eble (Praetorian Group), Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky Lab), Hamed Soroush (RTI) and Ron Zahavi (Microsoft).

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document: Yoshiaki Adachi (Hitachi), Frederick Hirsch (Fujitsu), Sven Schrecker (Intel) and Arjmand Samuel (Microsoft).

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors, Editors and Contributors into an integrated document.
