Extending the IIC IoT Security Maturity Model to Trustworthiness

Authors:

Frederick Hirsch
Standards Manager
Fujitsu
frederick.hirsch@us.fujitsu.com

Sandy Carielli
Director of Security Technologies
Entrust Datacard
sandy.carielli@entrustdatacard.com

Matt Eble
Practice Director
Praetorian
matthew.eble@praetorian.com

Ekaterina Rudina
Senior System Analyst
Kaspersky Lab
ekaterina.rudina@kaspersky.com

Ron Zahavi
Chief Strategist for IoT Standards
Microsoft
Ron.Zahavi@microsoft.com

OVERVIEW

Business investment requires decisions that include tradeoffs based on delivering functionality, addressing risks, ensuring business continuity, managing costs and reputation. Addressing risks appropriately by investing in controls and organizational changes when faced with a sea of choices and possibilities can be difficult, especially when considering all the aspects of trustworthiness including safety, security, reliability, resilience and privacy. The Industrial Internet Consortium (IIC) has developed an IoT Security Maturity Model[1] that provides an approach to address risk. This approach initially covers only security issues. This article suggests how this model can be extended and used to consider all the aspects of trustworthiness, enabling organizations to assess their current position with regard to trustworthiness aspects of safety, security, reliability, resilience and privacy against where they need to be, and make appropriate investments taking into account tradeoffs and required investments.

The intent of this article is to raise awareness of the approach, encourage discussion and suggest next steps to raise the bar of trustworthiness in applications by enabling the use of the IoT Security Maturity Model for trustworthiness.

WHAT IS THE IIC IOT SECURITY MATURITY MODEL?

Security maturity is the degree of confidence that the current security state meets all organizational needs and security-related requirements. Security maturity level is a measure of the understanding of the current security level, its necessity, benefits and cost of its support. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape. The IoT Security Maturity Model provides 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.

The IoT Security Maturity Model provides a conceptual framework to help organizations consider the myriad of options and make an informed decision to select and implement appropriate security controls. The framework helps an organization decide what their security maturity target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

The IoT Security Maturity Model allows organizations to determine the priorities that drive security enhancements and the maturity required to achieve differing needs and different strengths of protection mechanisms.

Purpose & Benefits

To drive proper investment and avoid simply applying technologies to a problem, the IoT

[1] IoT Security Maturity Model: Description an Intended Use, IIC:PUB:IN15:V1.0:PB:20180409IoT, http://www.iiconsortium.org/pdf/SMMSecurity Maturity Model_Description_and_Intended_Use_2018-04-09.pdf

Security Maturity Model allows for both organizational and technological considerations. It allows organizations to answer critical questions, including their current maturity level, given their requirements and threat landscape, what their target should be, and what they need to do to move to a higher maturity target state.

Use of the model fosters effective and productive collaboration among stakeholders. Business stakeholders, such as decision makers, business risk managers and owners of IoT systems, concerned about proper strategy for implementing mature security practices, can collaborate with the analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation.

Maturity is about effectiveness, not the arbitrary use of mechanisms. The IoT Security Maturity Model helps by aligning the comprehensiveness and scope of understanding of trustworthiness with the investment in appropriate practices.

Difference from Related Work

The IoT Security Maturity Model is the first model of its kind to address a need in the marketplace to assess the maturity of organizations in relation to their IoT systems and including governance, technologies, and how to manage them. Analysts have noted that the IoT Security Maturity Model is being produced at the right time to address the need and gap in the market.[2] Other existing models may address part of what is addressed by the model, such as within a particular vertical industry, or addressing IoT but not security, or security but not IoT. The IoT Security Maturity Model covers all the related aspects and points to parts of existing models, where appropriate, to recognize existing work and avoid duplication.

Model

The IoT Security Maturity Model is hierarchical and includes Domains, Sub-Domains and Practices.[3]

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.

Domains, Sub-Domains & Practices

The domains of governance, enablement and hardening determine the priorities of security maturity enhancements at the strategic level. Governance influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation. Enablement uses architectural design to address business risks, and hardening defines countermeasures to deal with specific threats before and after the fact. The subdomains reflect the basic means of obtaining the priorities at the tactical level and practices define typical activities associated with subdomains and identified at the planning level.

[2] https://www.iiconsortium.org/press-room/04-09-18.htm

[3] https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

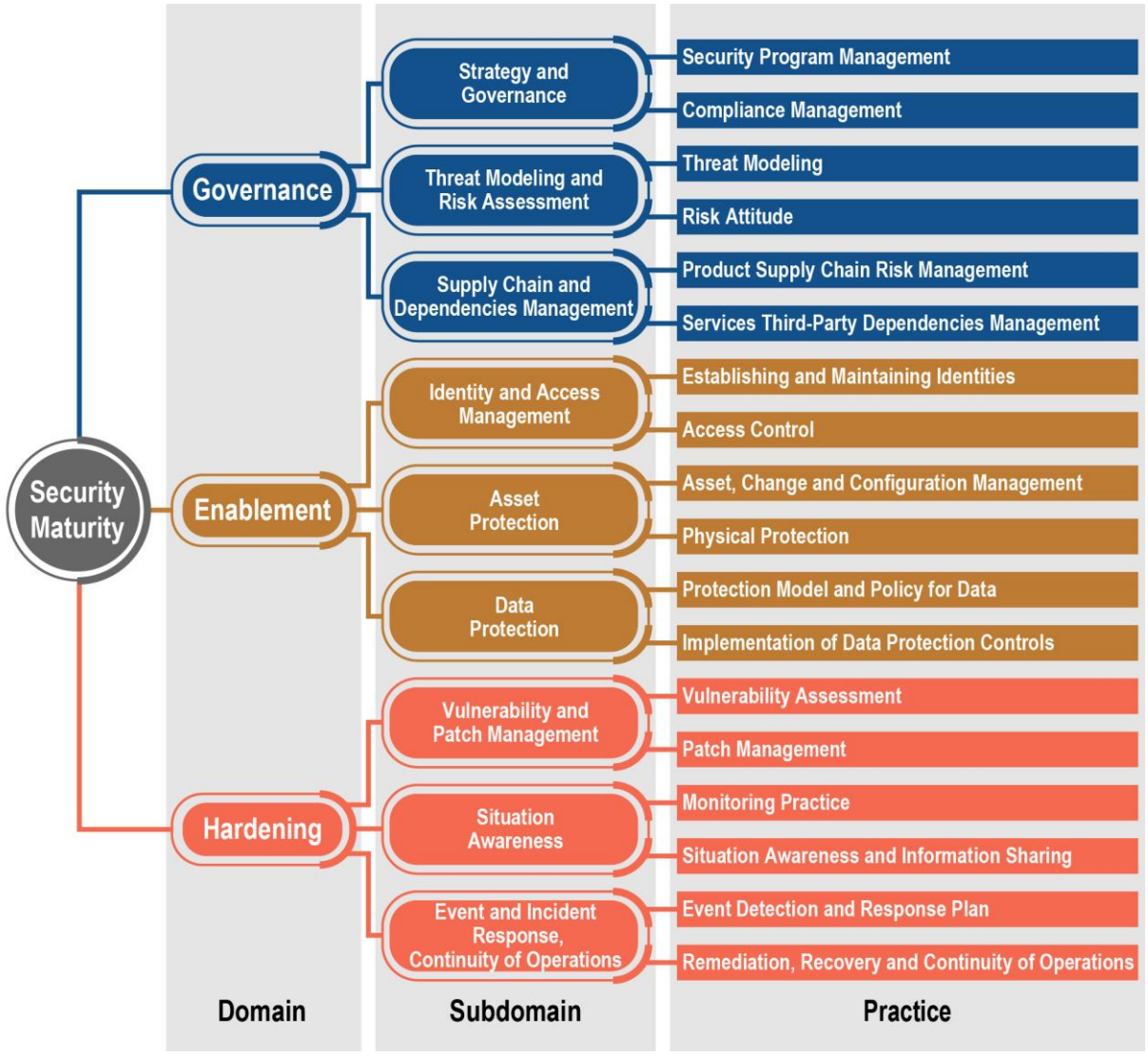

Figure 1: IoT Security Maturity Model Hierarchy

There are two dimensions to the evaluation of the security maturity. They are comprehensiveness and scope.

Comprehensiveness

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

There are five comprehensiveness levels for every security Domain, Sub-Domain and Practice, from Level 0 to Level 4 (None, Minimum, Ad hoc, Consistent and Formalized), with larger numbers indicating a higher degree of comprehensiveness of security controls. Each comprehensiveness level sets out new requirements while also including all of the requirements of the lower levels. The Security Maturity Model describes Levels 1 to 4 but not Level 0 since that level does not set any requirements.

Scope

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 and Practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

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

There are three levels of scope for each security practice: General, Industry Specific and System Specific. The General scope is, as its name indicates, the most general; Industry and System scope are progressively narrower and more specific.

Process and Usage

We expect most organizations to follow the IoT Security Maturity Model process [4] whereby a maturity target is established first. Once a target has been created or a relevant industry profile identified, organizations would conduct an assessment to capture the current maturity state. 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 establish a roadmap, take actions, and measure the progress towards the security maturity target. Once enhancements are

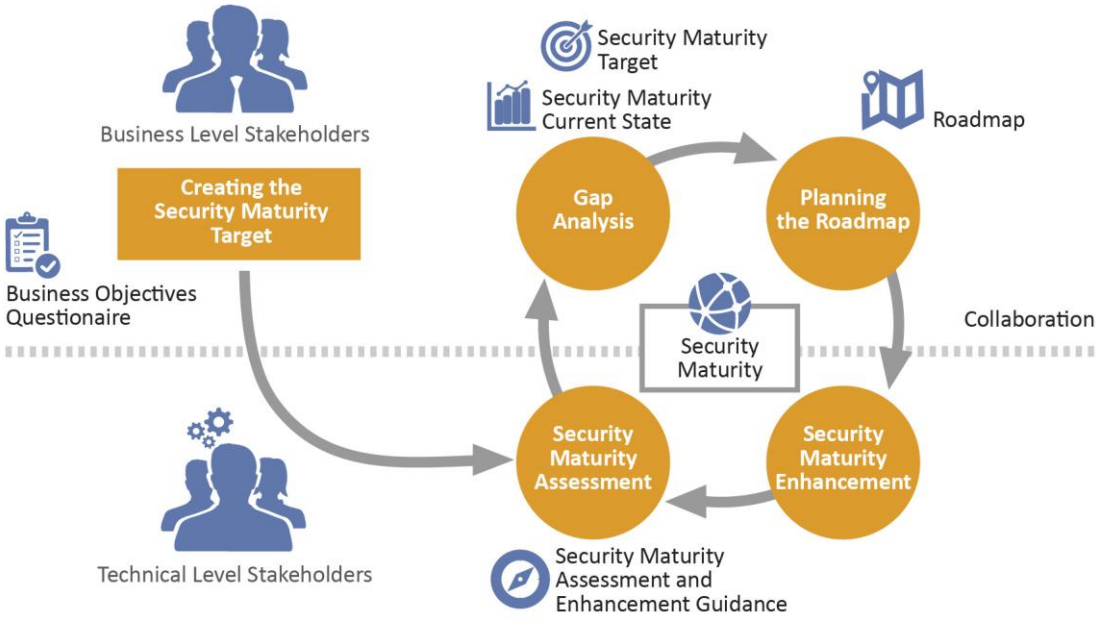

Figure 2: IoT Security Maturity Model Process

[4] https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

implemented, organizations can conduct another assessment to determine the new maturity state. The stakeholders work together to repeat this cycle according to the available resources and timeline set by the established roadmap and ensure that the appropriate security target is always maintained in an ever-changing threat landscape.

Establishing a target maturity level, 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.

Extensibility

The IoT Security Maturity Model is specifically designed to be extensible across a wide array of industries and systems. The initial model addresses the general scope, which looks at common security maturity best practices in the industry. There is an opportunity to add industry specific and system specific scope to any or all of the practices.

The IIC will be collaborating with a wide range of industry groups to encourage development of profiles - practice[5] tables that go beyond general scope and include industry- and/or system-specific requirements for different comprehensiveness levels. For example, a retail group may create profiles of some or all practices that include best practices and regulatory requirements specific to the retail industry; they may also create system-specific profiles for commonly used devices such as card readers or security cameras. A health care profile may include specific guidance related to Health Insurance Portability and Accountability Act (HIPAA), while a system-specific profile could address considerations for, say, US Food and Drug Administration (FDA) pre- and post- market guidance for implanted medical devices.

Note that industry and system profiles need not be created for every practice in the model. An industry may decide that the general scope is sufficient for most of the governance-related practices but that a few of the enablement practices necessitate an industry level point of view. In that case, they may produce industry profiles for only a handful of practices and deem that sufficient for their requirements.

APPLYING THE IOT SECURITY MATURITY MODEL TO TRUSTWORTHINESS

The IIC defines trustworthiness as the "degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human

[5] In terms of the IoT Security Maturity Model, security practices define typical activities associated with the means of obtaining security priorities and identified at the planning level.

errors, system faults and attacks." [6] The confidence that a system "performs as expected" depends on an understanding of the context and requirements of the system with respect to the trustworthiness aspects as well as assurance that the concerns related to the various trustworthiness aspects are addressed. Design and implementation trade-offs and decisions will be necessary since some approaches that impact one trustworthiness aspect may either support or diminish another aspect. As an example, a locked door may enhance security but may reduce safety, as has been evidenced in fires with loss of life (e.g., the New York City 1911 Triangle Shirtwaist Factory fire[7]). Each trustworthiness aspect requires analysis to determine appropriate investment in practices and technologies to meet business requirements and this analysis should consider the interactions of the different aspects.

There are many benefits of applying the IIC IoT Security Maturity Model to trustworthiness, including the benefits of common training and understanding of the maturity model and the possibility for integrated gap analysis and presentation. The model also helps with consistent tooling and a unified and coherent approach enabling consideration of maturity of trustworthiness aspects, not just in isolation but together. Collectively considering the full scope of trustworthiness aspects can enable better prioritization and investments than when evaluated independently. For example, later in this article, we consider a surgically implanted pacemaker where two aspects of trustworthiness, safety and security, need to be considered.

The process outlined in the IIC IoT Security Maturity Model is directly applicable to every trustworthiness aspect, since the generic steps of creating a maturity target, performing a maturity assessment, gap analysis, and planning and executing maturity enhancements are applicable to all aspects of trustworthiness, repeated in a Plan-Do-Check-Act cycle.

The model can be extended to trustworthiness with the concepts of comprehensiveness and scope applied to trustworthiness, as well as extensions to the model hierarchy for trustworthiness.

There are two approaches to extending the IoT Security Maturity Model to trustworthiness. One approach is to create new profiles using the same principles as industry and system specific profiles. Instead of creating a profile to address an existing Security Practice, a trustworthiness profile may define a new practice including the four levels of comprehensiveness, considerations and success indicators for each. We presume that initial trustworthiness profiles would address the General scope, but as with existing practices in the IoT Security Maturity Model, this could also be extended by industry groups to create industry or system specific trustworthiness profiles. Another approach would be to update the core IoT

[6] The Industrial Internet of Things Volume G8: Vocabulary, IIC:PUB:G8:V2.1:PB:20180822, Version 2.1, August 2018, IIC. https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf

[7] Triangle : the fire that changed America / by David Von Drehle. Atlantic Monthly Press, 2003.

Security Maturity Model itself. This would make sense when changes are generally applicable. Both approaches could be followed simultaneously.

APPLYING COMPREHENSIVENESS AND SCOPE TO TRUSTWORTHINESS

Both comprehensiveness and scope are widely applicable maturity model concepts that can be applied to all aspects of trustworthiness. For example, privacy by design and default within an entire organization is a different level of maturity than privacy considered only within a department of an organization. An in-depth privacy program taking into account medical-specific concerns is different than a generic program.

The IoT Security Maturity Model concept of comprehensiveness levels can be enhanced for trustworthiness as follows:

- **Level 1, Minimum.** Trustworthiness can be addressed at this level by noting that general concerns related to trustworthiness aspects beyond security are considered. These aspects represent general concerns such as "we need this equipment to be reliable, safe and to provide enough security features," "we need for this component to be safe and have system resilience in the case of security attacks" and "we have to make the service secure and take care to protect privacy."
- **Level 2, Ad hoc.** Trustworthiness can be considered at this level with separate cases demonstrating how trustworthiness aspects either support or detract from each other.
- **Level 3, Consistent.** Trustworthiness is addressed systematically at this level with the application of methods, best practices and standards. This facilitates a consistent approach toward the implementation of required trustworthiness aspects, taking into account the complexity of the interactions. Metrics are used as appropriate.
- **Level 4, Formalized.** Trustworthiness is supported at this level with assurance cases to establish confidence in the system for organization needs. Support for trustworthiness is continuously evaluated, improved and harmonized among the aspects.

Understanding and managing the interactions of trustworthiness aspects can be difficult. Stakeholders can identify the interactions of trustworthiness aspects by examining use cases. For example, updating the anti-malware databases on a SCADA server affects the continuous control process execution at a production line with a probable negative impact on process safety.

Scope can also be useful to understanding and managing the interaction of trustworthiness aspects, since it is about the industry or system specifics needed to make tradeoffs among trustworthiness aspects. The following considerations may help in revealing the interactions of trustworthiness aspects, to anticipate and mitigate undesirable interactions, and to take advantage of the aspects supporting each other:

1. Consider the definitions of trustworthiness aspects, identify interactions, and consider how industry definitions impact the scope dimension.

   Stakeholders identify the connections between the aspects relying on their definitions. They make assumptions about the situations for which they prioritize one of the aspects over others thus focusing on what is important.

   From the scope perspective, sometimes it makes sense to consider the specific definitions for safety, reliability, etc. as accepted in the industry, thus changing the scope from the General to Industry-specific or even to System-specific according to IoT Security Maturity Model Scope scale.

2. Consider implementation methods for trustworthiness aspects, finding common shared implementation opportunities as well as noting incompatible implementation concerns as well as industry or system-specific implementation concerns.

   Some aspects, such as security and privacy, may have different objectives but the methods for their implementation (such as encryption or access control) might be the same. In some cases, the methods used to implement one of the aspects will weaken the other one. Care must often be taken to ensure aspects support each other when required, for example, that security methods support and do not diminish safety requirements[8].

   From the scope perspective, industry standards may prescribe or restrict the usage of methods and technologies. The specific system may also impose its own constraints. Addressing such constraints will change the scope from General to Industry-specific or to System-specific according to the IoT Security Maturity Model Scope scale.

3. Consider how to apply assurance case approaches to trustworthiness.

   Assurance of system trustworthiness as a whole is one of the more complicated problems for the IIoT. The IIC Industrial Internet Security Framework [9] considers assurance for the separate trustworthiness characteristics. The V-model for the development lifecycle [10] traditionally used for systems requiring safety may be adapted for a concomitant security assurance. Advanced approaches

[8] ITU-T Y.4806 (11/2017). Security capabilities supporting safety of the Internet of things. http://handle.itu.int/11.1002/1000/13391

[9] Industrial Internet of Things. Volume G4: Security Framework https://www.iiconsortium.org/IISF.htm Industrial Internet Consortium, 2016

[10] Kevin Forsberg and Harold Mooz, "The Relationship of System Engineering to the Project Cycle", in Proceedings of the First Annual Symposium of National Council on System Engineering, October 1991: 57–65.

addressing the joint assurance of two or more characteristics for the system in a changing environment are currently being developed[11].

Considering both comprehensiveness levels as well as implementation considerations in the context of the IoT Security Maturity Model should help advance the maturity of trustworthiness in systems by considering all the aspects together with their interactions.

EXTENDING THE MODEL HIERARCHY TO TRUSTWORTHINESS

The previous section outlined how comprehensiveness and scope are applicable to trustworthiness. As trustworthiness includes security, it makes sense to extend the model horizontally rather than vertically. What we mean is that while the existing eighteen practices are sufficient for assessing security maturity, additional practices not relevant to security may make the model more applicable to trustworthiness as well. For example, one might wish to use the structure of the model to define one or more practices around safety. This section outlines potential changes and additions to the model hierarchy to address trustworthiness maturity.

The current model has three Domains: Governance, Enablement and Hardening. In principle, each of these can apply to all aspects of trustworthiness. In some cases, Sub-Domains and Practices are generic enough to cover various trustworthiness aspects, and in other cases, additional Sub-Domains and Practices specific to other trustworthiness aspects may be required by different organizations to address their needs.

Governance - establishing and ensuring the implementation of policies - is appropriate to all aspects of trustworthiness as well as trustworthiness as a whole. The Strategy and Governance subdomain defined in the Governance Domain is relevant to trustworthiness, including program management and compliance management. The Governance Domain also includes Threat Modeling and Risk Assessment as well as Supply Chain and Dependencies Management. If threat modeling is broadened to include hazards, it may also apply to safety as well as security, for example.

Enablement uses architectural design to address business risks, with practices such as access management (and others outlined in the model). Enablement also can apply to policies and practices used to address business risks associated with the other trustworthiness aspects such as safety, privacy, reliability and even resilience (e.g., maintaining adequate financial, technical and social resources).

Finally, Hardening defines countermeasures to deal with specific threats before and after

[11] The CITADEL project, an Innovation Action partly funded by the Horizon 2020 Programme of the European Union under grant agreement no. 700665. citadel-project.org

the fact. This can also apply as mitigations to trustworthiness aspects such as safety hazards, reliability failures, resilience impacts or privacy risks.

Some of the Governance Sub-Domains are generic and can apply to other aspects of trustworthiness, such as supply chain management and program management[12]. A slight naming change can accommodate this by changing the name of "Security Program Management" to "Program Management" and "Product Supply Chain Risk Management" to "Supply Chain Management," for example.

There are also some areas related to trustworthiness that can be added to the model. Trustworthiness generally includes a number of practices that reflect the culture of the organization, especially in the aspects of safety and privacy. A new domain, the "Institutional Domain," could address organizational concerns. This is distinct from the Governance Domain since it is about the culture of the organization and the approach and thinking of people, as opposed to policies and guidance from leadership, though related. This is critical for safety and privacy (also for others, but especially these)[13, 14]. This includes practices related to personal attitudes, organizational prioritization and recognition, management leadership and commitment, accountability, employee involvement and consultation and collaboration.

Another important organizational aspect, especially noted in privacy and safety, is the training and management of staff[15, 16]. This is also part of the Institutional Domain, as the "Training" Sub-Domain. This includes training, coaching and mentoring, competency evaluation, etc.

Continuous improvement and learning contribute to maintaining best capabilities for trustworthiness aspects. This

[12] Using a Reliability Capability Maturity Model to Benchmark Electronics Companies. Article in International Journal of Quality & Reliability Management. May 2007 DOI: 10.1108/02656710710748394. Sanjay Tiku Microsoft, Michael H. Azarian University of Maryland, College Park, Michael Pecht University of Maryland, College Park https://www.researchgate.net/publication/235280160_Using_a_Reliability_Capability_Maturity_Model_to_Benchmark_Electronics_Companies

[13] The Safety Journey: Using a Safety Maturity Model for Safety Planning and Assurance in the UK Coal Mining Industry. Patrick Foster, Stuart Hoult, Minerals 2013, 3, 59-72; doi:10.3390/min3010059 ; https://www.researchgate.net/publication/272661146_The_Safety_Journey_Using_a_Safety_Maturity_Model_for_Safety_Planning_and_Assurance_in_the_UK_Coal_Mining_Industry

[14] Organizing For Reliability – Capability Maturity Model Assessment And Implementation Plans, Executive Summary. May 2015, https://ops.fhwa.dot.gov/docs/cmmexesum/cmmexsum.pdf

[15] Sustaining Operational Resiliency: A Process Improvement Approach to Security Management, Richard A. Caralli April 2006 https://resources.sei.cmu.edu/asset_files/TechnicalNote/2006_004_001_14672.pdf

[16] Introducing the CERT® Resiliency Engineering Framework: Improving the Security and Sustainability Processes May 2007. Richard A. Caralli, James F. Stevens, Charles M. Wallen, David W. White, William R. Wilson, Lisa R. Young https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14876.pdf

organizational initiative is also part of the Institutional Domain, the "Continuous Improvement and Learning" Sub-Domain. This can include organizational, process and technology improvements and is similar in spirit to quality improvement programs such as the Malcolm Baldrige National Quality Award program [17], being institutional in nature. The IoT Security Maturity Model comprehensiveness level 4 maturity levels also emphasize continuous learning. The difference is that the comprehensiveness levels are about the specific practice, while the Sub-Domain is about the organization as a whole. If an organization takes continuous learning as part of its culture, then one can expect the maturity of a number of practices to reflect this.

Another important concept is "trustworthiness by design - "privacy by design" generalized to trustworthiness. Achieving this requires a focus on architecture and design implications for trustworthiness. Thus, the maturity model can add "Analysis and Design" to the Enablement Domain[18].

Another Governance area is performance measurement and metrics related to trustworthiness, used to manage and improve results. Adding "Performance Measurement and Metrics" to the "Governance Domain" reflects this.

Finally, adding "Verification and Validation" to the Hardening Domain reflects the practice in safety and reliability to perform testing and validation.

These changes taken together produce an updated model hierarchy (Figure 3) where new Sub-Domains are shown with dashed lines around the added circles (The diagram reflects name changes as well).

[17] https://www.nist.gov/baldrige

[18] IoT Trustworthiness is a Journey and NOT a Project, in this IIC Journal of Innovation issue.

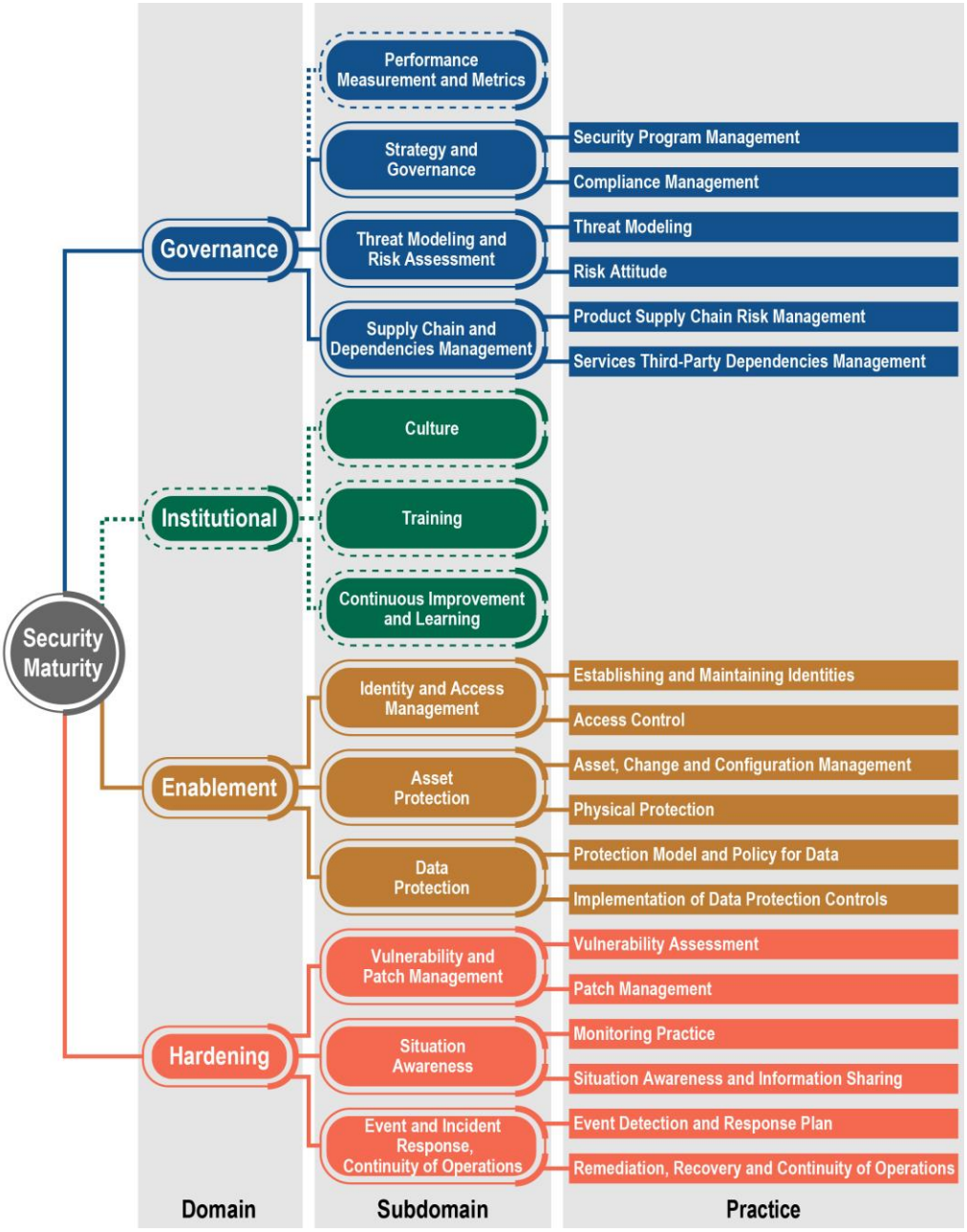

Figure 3: IoT Security Maturity Model Hierarchy Revised and Extended for Trustworthiness

EXAMPLE APPLICATION: PACEMAKER HEALTH CARE CASE STUDY

Manufacturers of implanted medical devices are especially concerned about the trustworthiness of their devices due to the potentially large, possibly life-threatening, impact to patients as well as the high costs of implanting and removing them to correct issues. A specific application of the trustworthiness model to a pacemaker can provide a case study for the applicability of extending the IoT Security Maturity Model to trustworthiness.

The emphasis on medical device safety demonstrates how trustworthiness priorities depend on the context, including the industry application. For medical devices, safety, reliability and security are prioritized in that order. This can lead to reducing the priority of security Sub-Domains that would be unacceptable in many other situations.

Institutional Culture Sub-Domain - For a medical device manufacturer, the institutional dimension includes unique considerations related to attitudes about patient outcomes. There may be a number of nuanced situations in which implanting a device may not be the best course of treatment. A manufacturer needs to be mindful of such edge cases throughout its product lifecycle – design, training, marketing, etc.

Continuous Improvement & Learning Institutional Sub-Domain - In the context of implantable medical devices, a manufacturer's ability to perform continuous improvement of a specific product are limited, but continuous improvement of processes is possible and is valuable. Lengthy requirements for testing, validation and regulatory approval of new product versions increase the costs of incremental improvements over time relative to most other products. Consequently, manufacturers tend to prioritize getting products "right" the first time and incorporating lessons learned into designs for new, upcoming products. There is less of an emphasis on patching and upgrading for small performance or functionality improvements relative to typical consumer products.

The restrictions on product updates for improvement ultimately derive from a regulatory mandate to emphasize safety over other trustworthiness aspects. Incremental improvements to security or reliability must be measured against the potential safety (health) ramifications. For example, if a hardware firmware update to patch a low risk security issue has a 0.01% failure rate, leading to the failure of the device, that security patch will be rejected.

Performance Measurement & Metrics Governance Sub-Domain - This sub-domain is required for regulatory purposes. Extensive testing of performance and failure rates are required as part of a product's development process. Ultimately, the manufacturer must prove to regulators that the failure rates are low enough and the probable health benefits still far outweigh the risks of a surgery.

Training Institutional Sub-Domain - For a medical device manufacturer, staffing considerations extend beyond the immediate organization to the practitioners who will ultimately implant and maintain the devices. The trustworthiness of the device is dependent in part on the competence of those healthcare practitioners to provide the patient care that is specific to that device. This leads to a need to create a training program and certification process for those care providers, to ensure the trustworthiness of the pacemaker when implanted.

Analysis & Design Enablement Sub-Domain - The operating environment in which a pacemaker is deployed (e.g., implanted in a person’s body) means that it is difficult to

impossible to correct problems after a production release. Consequently, the analysis and design processes should be exhaustive and receive greater attention than typical consumer products. Regulatory oversight by the FDA requires that certain design benchmarks be met during the development of an implanted pacemaker. Evidence of those benchmarks must be provided during the submission process. Additionally, importance is given to design considerations that maximize safety and reliability. For example, some wireless protocols and encryption algorithms may be vetoed during the design process due to their high energy requirements and subsequent reduction in the battery's life.

In addition, design must take into account consideration of maintenance when patients use medical facilities lacking advanced equipment to work with implanted devices. Device manufacturers must take into account the fact that patients will travel far from their care providers after receiving an implanted device. Manufacturers need to ensure that those patients have a low barrier to receive care should they suffer an incident while they are traveling. Consequently, designs for implanted pacemakers often make concessions in the practices of authentication and authorization that would be unacceptable in other circumstances. Doing so ensures that medical care providers in less comprehensive medical facilities can still access the implanted device and provide care when needed.

CONCLUSIONS

The IIC IoT Security Maturity Model provides a process and model to enable an organized and effective way to match investments to actual security needs. This can be directly applied to and extended to trustworthiness by using profiles and making necessary changes to the hierarchy model. Key aspects of the model, such as maturity comprehensiveness levels and scope are directly applicable as is the use of a hierarchy of Domains, Sub-Domains and Practices. Many of the items in the model, including the Governance, Enablement and Hardening domains are also applicable. This article reviewed and explained where and why some additions might be appropriate. The Security Applicability Task Group at the IIC continues to work on this.

The addition of an Institutional Domain that includes Organizational Culture, Training and Continuous Improvement and Learning Sub-Domains aligns with existing safety and privacy maturity models and with the concept that support for trustworthiness must become part of the organization's DNA itself. We also recommend the addition of Performance Measurement and Metrics as a Governance Sub-Domain to reflect the need to measure and analyze important aspects of systems to achieve control.

Trustworthiness by design, to reflect the existing concept of Privacy by Design, is important and is reflected by the addition of the "Analysis and Design" Sub-Domain to the Enablement Domain. The Hardening Domain is extended to include "Verification and Validation" which is important in safety, for example.

Although it is possible to use the IoT Security Maturity Model to evaluate trustworthiness aspects individually, using the model to consider trustworthiness holistically can better enable prioritization and investment decisions, especially if the tradeoffs among the trustworthiness aspects are properly evaluated and conflicts are resolved. In this case, the comprehensiveness levels can be used to understand the approach to trustworthiness, ranging from ad hoc approaches to using assurance cases to build trust. Scope is also important. Some trustworthiness aspects may restrict the scope with requirements specific to the industry or system while other aspects may remain general in terms of their required maturity.

We anticipate further work to raise awareness of the IIC IoT Security Maturity Model and invite any ideas and detailed considerations on how to demonstrate its applicability to other trustworthiness aspects.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions.