Security Maturity

The Industrial Internet Consortium's (IIC) third-quarter member meeting held virtually from September 28th through October 1st, 2020, was a great success with 190 attendees, 36 working sessions, eleven industry track sessions, nine plenary sessions, six testbed sessions, five webinars, three keynotes and one half-day training course.

Security Maturity Model

The Security Maturity Model (SMM) provides a path for Internet of Things (IoT) providers to know how to invest appropriately in sensible security mechanisms that meet their requirements. It helps organizations identify the appropriate approach for effective enhancement of security practices. 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. It 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, so the mechanisms and procedures fit the organization's goals without going beyond what is necessary. Their implementation is considered *mature* if they are expected to be effective in addressing those goals. The model does not say what the appropriate security level should be; it is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity.

The SMM helps determine and clearly communicate to management answers to:

- What is my solution's current maturity state?
- What is my solution's target maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

The *current security maturity state* describes the current level of maturity of implemented practices for the given system. The *security maturity target* establishes the ultimate security maturity state. The target includes a consistent set of security practices, provides a definition of security goals 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.

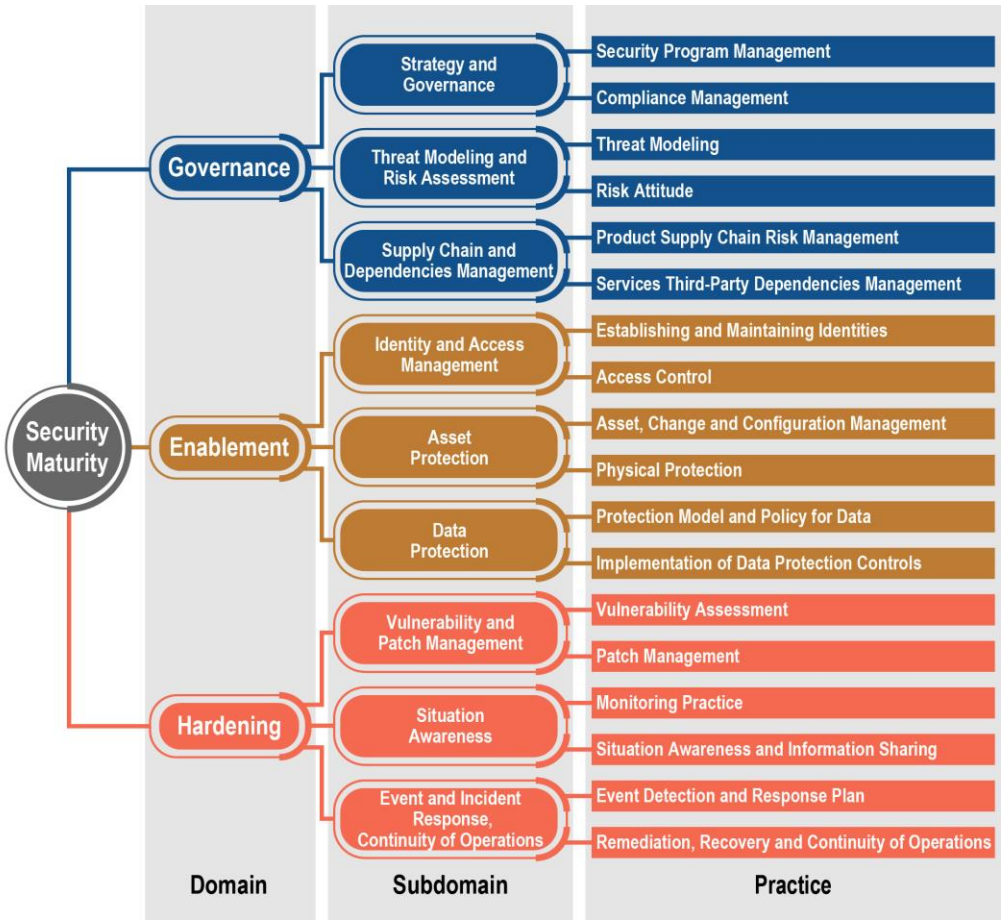

Figure: *IoT Security Maturity Model hierarchy.*

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.
Subdomains reflect the basic means of obtaining these priorities at the planning level.	At the subdomains level, the stakeholder identifies the typical needs for addressing security concerns.
Practices define typical activities associated with subdomains and identified at the tactical level.	At the practices level, the stakeholder considers the purpose of specific security activities.

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.

The hierarchical approach shown in the figure on the previous page enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.[1]

At the prior quarterly meeting, the authors taught (and recorded) a half-day workshop that covered the principles above and a few of the practices. Attendees (or listeners) who passed a knowledge test received a certificate and a badge they could use with their professional profiles.

At this meeting, the authors answered questions after playing the recording, and then taught a hands-on assessment in a workshop format. We now have a full-day class on security maturity that can be taught to technology end users. IIC will extend this kind of help for technology end users over the coming months.

Meanwhile, the SMM can be tailored for specific industries, in a *profile*. The authors, in conjunction with the Retail Task Force at the Object Management Group's standards' development program standardized a profile for the point of sale (POS) retail community because the retail landscape is changing with digital transformation and evolving technologies. The industry is deploying internet-connected devices to serve customers better, ranging from new point-of-sale payment devices such as radio-frequency identification and signature scanners, to audit-logging devices such as printers, lights and cameras.

With the proliferation of mobile devices and other technologies, retailers are intentionally and, perhaps, unintentionally, collecting more and more data about their customers. There are increasing risks associated with greater connectivity and integration and new threats constantly emerge as attackers are becoming more capable and organized. Compliance requirements around data protection and security are becoming more significant. These trends increase the urgency and importance of addressing security and data protection concerns systematically and effectively.

Trust is essential to the customer relationship with the retailer. The challenge is to figure out how much security is needed, how much to invest to fit certain scenarios and which controls to deploy, given the complexity of the retail environment. All aspects must be considered including governance, technology and operations. The SMM helps organize and manage these concerns, enabling various stakeholders to communicate and determine appropriate maturity targets, assess the current status, and create action plans to address gaps.

The SMM defines general considerations for a foundation from which communities can consider their specific concerns and extend the SMM to consider industry and device-specific concerns. The initial SMM publications, IoT Security Maturity Model (SMM) Practitioner's Guide and associated Description and Intended Use white paper, have been updated based on feedback

[1] The above is abridged from IoT Security Maturity Model, written by Sandy Carielli (Entrust Datacard), Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky Lab), Hamed Soroush (RTI) and Ron Zahavi (Microsoft).

and use cases. The clarity and usefulness of the Practitioner's Guide has been improved by adding guidance to the numerous practice tables, clarifying scoring and the case studies, without changing the underlying model. The improvements are based on experience gained in applying the SMM to new assessments, feedback from assessments, training sessions, and profile development. New versions of the two papers are aligned with the published retail profile.

End-User Engagement

Industry Leadership Councils (ILCs) are executive roundtables of innovative strategists representing organizations who meet regularly to set the vision for next generation solutions in their respective industries. The Manufacturing ILC produced the first in a series of technical briefs aimed at help manufacturing leaders keep pace with rapid emergence of new technology. The ILC meets quarterly and includes representatives from major companies; additional end-user companies are welcome. The general criteria for participation in an ILC are a director-level role or higher as well as actively implementing or using an IIoT solution in the corresponding field. The IIC also seeks to form an Energy ILC, focused on utilities and distributed energy management. If you have participant recommendations you may visit the ILC webpage above or contact either Howard Kradjel or Cheryl Rocheleau.

The IIC's vertical task groups, which fall under the Industry Working Group, exist to understand business and technology needs within an industry. They connect industry needs to requirements, testbeds, and guidance that enable technology deployment and digital transformation. There are vertical groups for automotive, energy, healthcare, mining, and smart factory.

Special Interest Groups (SIGs) create customer-validated requirements for the development of holistic solutions for industry, initiate technical validation projects for these requirements, initiate new industry standards to help harmonize the technology landscape and provide an efficient platform for vendors suppliers and industry organizations to shape the future of IIoT solutions jointly. One active SIG topic is the Over-the-Air (OTA) Updates SIG, which is comprised of experts developing and delivering innovative solutions to the automotive sector. For more information, please contact Stephen Mellor.

The Community Forum is an online venue for industry experts to exchange ideas, discuss IIoT problems and network, as well as an IIoT beacon providing helpful, relevant content to technology users, vendors, integrators, technology experts, researchers, government entities and academicians. The Community Forum is a resource for follow-on conversations and webinars.

Industry Programs

The Industry Connect Service helps technology users transform their businesses. Users seeking solutions to large complex problems, to scale existing proofs of concept or to identify requirements for industry standards are invited to submit a problem statement. Both the user

organization (which need not be an IIC member) and IIC member organizations receive direct value through identification and delivery of possible solutions, opportunities for new technology development. If you are interested in submitting a problem statement for consideration by the IIC, please submit one using the link above or contact Howard Kradjel.

IIC Testbeds are where the innovation and opportunities of the industrial internet–new technologies, new applications, new products, new services, new processes, new business can be initiated, thought through and rigorously tested to ascertain their usefulness and viability before coming to market. The testbed program has 26 approved IIC testbeds with more to come.

IIC Test Drives are IIC member solutions that may be deployed as pilots to trial a technology. Test drives enable technology end users to learn about a technology in their facilities. Three test drives have been approved: the Intelligent Video Test Drive, the IoT Sensor Implementation Test Drive, and the Smart Mold, Injection Process Optimization and AI Test Drive.

IoT Challenges aim at solving real problems and validating solutions that address specific end-user-identified pain points. In these challenges, architects and solution providers compete to design industrial internet solutions that address high-profile real-world problems. The Smart Logistics Challenge is seeking principal partners.

Group Activity and Recent Publications

IIC groups made a significant dent on their various activities and deliverables this quarter. Here is a complete list of publications: Technical Papers, Publications and White Papers Webpage.

The *Implementation Aspect: IIoT and Blockchain* white paper was published on 2020-07-22. It provides insight into design principles of a secure distributed ledger. The *Distributed Ledgers in IIoT* white paper was published on 2020-07-27. It addresses the impact of distributed ledger technology on IIoT today and the insight decisionmakers need to soundly conduct a cost-benefit analysis on whether and how this technology should be incorporated in their respective business environments.

The *Digital Transformation in Industry* white paper was published on 2020-07-29. It targets business managers involved in setting the digital transformation strategy factors and overall journey of an organization and technology managers who need to identify and assess how to leverage key technologies to facilitate that journey. Finally, the white paper targets risk, security and safety managers responsible for implementing protection and mitigation strategy factors to minimize the impact of disruptions, attacks, errors along the way.

The IIC and Object Management Group joint *IoT Security Maturity Model: Retail Profile Point-of-Sale Devices* white paper was published on 2020-08-01. It extends the *IoT Security Maturity Model: Practitioner's Guide,* providing details on how to navigate the challenges of how much security is needed, how much to invest to fit certain scenarios and which controls to deploy given the complexity of the retail environment.

Version 2.3 of the *Industrial Internet Vocabulary Technical Report* was published on 2020-09-02. It is a living document defining the latest thinking surrounding key IIoT terminology.

The IIC and Plattform Industrie 4.0 joint *Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0* white paper was published on 2020-09-11. It provides clear definitions of digital twin technologies, standards and use cases, and describes how the Plattform Industrie 4.0 Asset Administration Shell, an implementation of a digital twin for industrial applications, can be used to enable cross-company-interoperability across the complete value stream.

WEBINARS

Visit the IIC Webinars Webpage for access to nine hosted webinars this past quarter as well as a comprehensive list of past and future webinars.

NEW MEMBERS

Please welcome new members this quarter:

- Connected Devices
- MonoM
- RIoT

The Industrial Internet Consortium is the world's leading membership program transforming business and society by accelerating the Industrial Internet of Things. Our mission is to deliver a trustworthy Industrial Internet of Things in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes. Founded March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. The Industrial Internet Consortium is a program of the Object Management Group® (OMG®).

Visit www.iiconsortium.org.

IIC members gain experience they could never have as a non-member. Here are some key benefits of membership:

- ***Networking***—Make the connections; find the needed expertise.
- ***Information & News***—A fast path to newsworthy industry developments.
- ***Competitive edge***—Stay ahead of the competition or take advantage of changes and developments that might otherwise have passed you by.
- ***Create a market***—Join a collective voice supporting a single mission; create the disruption in the market and develop the business opportunities.
- ***Establish a vision*** –Members work to define future architectures and innovate technologies for IIoT.
- ***Success***—Members are building businesses and dedicating their professional lives to IIoT. They want to be successful, and they want others to succeed.
- ***Professional development***—Grow your career, meet mentors and mentees, career prospects.
- ***Solve important problems***—and help your partners and customers.
- ***Events*** – Capitalize on opportunities for continuous exposure to industry developments.