



Advancing IoT Security: Exploring the IIC IoT Security Maturity Model



By Mr-IoT & Ranjinni Joshe



Agenda..!

- IoT Security Introduction
- IoT Security Challenges
- How IIC SMM framework Resolves Challenges
- IIC SMM Framework
- References



Ranjinni K Joshe...!

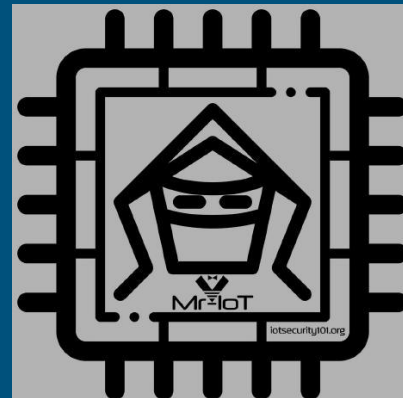
**Senior Cloud Security Specialist, Onward Technologies Pvt. Ltd.
World Wide Women in Cybersecurity Bangalore Leader (W3-CS)**

Social Media :

<https://www.linkedin.com/in/ranjinnijoshe/>

cat /etc/shadow

- Known as Mr-IoT
- Founder of IoTSecurity101 Community
- Null/OWASP Bangalore Chapter Leader
- Published articles in multiple magazines
- Just another guy from IoT World
- Works with crestron electronics as senior product security engineer
- Open Projects IoT-PT OSv1,ICE-Bite
- And many other interesting projects like “commandinwifi” and unpublished one’s



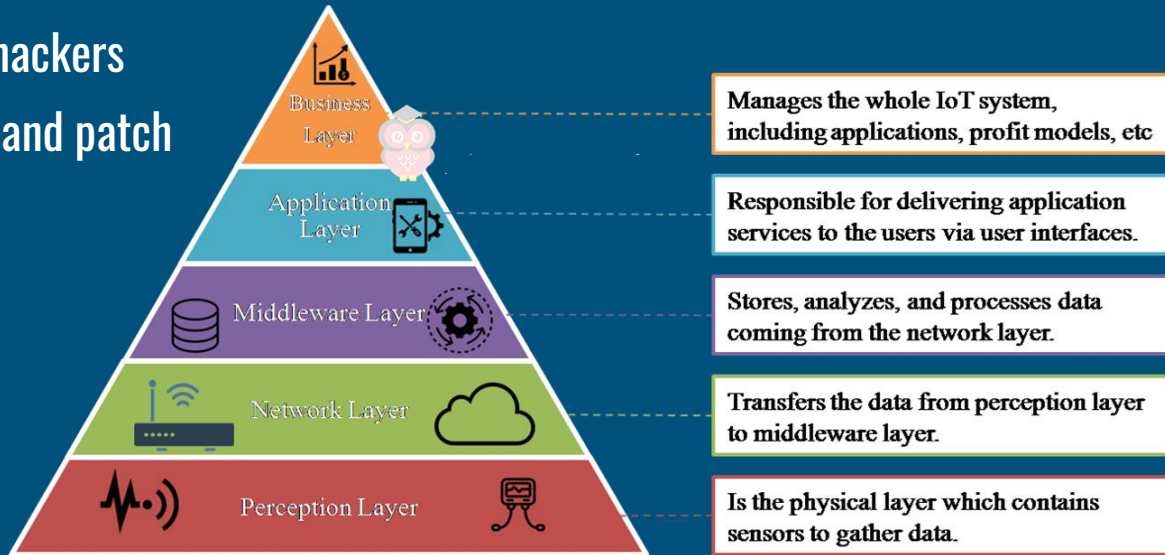
IoT Security

Introduction

- The Internet of Technology (IoT) is a vast network of interconnected physical devices that can exchange data via the internet. These devices could be smaller in size & can have sensors to perform numerous tasks in manufacturing units, factories, and enterprises without human intervention.

Why it is important

- IoT Devices can be access points for hackers
- IoT Devices are important to manage and patch
- Device Integrity and Functionality
- Operational Continuity
- Privacy Preservation



IOT Security Challenges



INTERNET OF THINGS SECURITY CHALLENGES



IOT CHALLENGES FOR DEVICES

ENVIRONMENTAL IOT CHALLENGES

Best Practices:

- Profile Every Device
- Segment Devices
- Implement Zero-Trust Architectures
- Limit Network Endpoints
- Routinely Monitor and Scan
- Risk Assessments
- Communication Channels
- Update Software
- Routines with latest Patch updates
- Change Default Passwords
- User Awareness
- Updated software and firmware
- IAM
- Latest encryption Mechanisms

What is IoT-SMM - Security Mature Model

- It's just another compliance standard
- Confidence in the effectiveness of a security implementation
- GAP analysis in existing model
- Understanding better in security hardening practices and vulnerability patch management

What Exactly SMM Covers..

- **Overview and Relationship:** Introduction to the SMM and its relationship with other IIC documents.
- **Security Maturity Model:** Framework for assessing and improving security maturity.
- **Domains, Subdomains, and Practices:** Detailed explanation of governance, enablement, and hardening domains, and their subdomains and practices.
- **Implementation Process:** Steps for applying the model, including establishing context, setting targets, conducting assessments, gap analysis, and roadmap creation.
- **Case Studies:** Real-world examples demonstrating the application of the SMM.
- **Annexes:** Additional resources such as acronyms, glossary, references, and author information.

How it works

- **Establish Context:** Define the scope and context for security assessment.
- **Set Security Maturity Targets:** Establish desired security levels for different domains.
- **Conduct Assessments:** Evaluate current security practices and compare them to targets.
- **Gap Analysis:** Identify gaps between current and target states.
- **Develop Roadmaps:** Create actionable plans to address gaps and enhance security.
- **Continuous Improvement:** Regularly reassess and update security practices to adapt to new threats and requirements

Security Mature Model

Security Maturity

Governance

Enablement

Hardening

Strategy &
Governance

Threat
Modeling &
Risk
Assessment

Supply Chain
&
Dependencies
Management

Identity &
Access
Management

Asset
Protection

Data
Protection

Vulnerability &
Patch
Management

Situational
Awareness

Event &
Incident
Response,
Continuity of
Operations

Security Mature Model

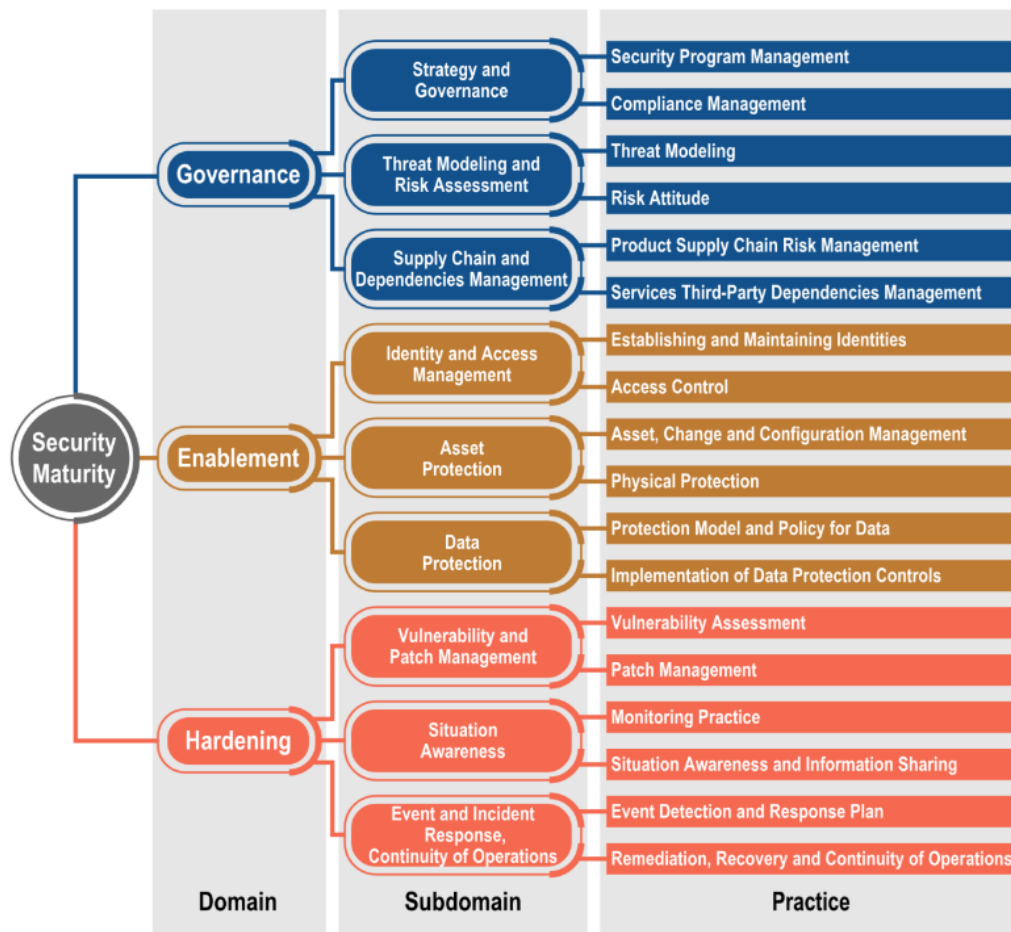


Figure 3-1: IoT Security Maturity Model Hierarchy



Hardening



IoT SMM Comprehensive Levels

Level 0 - none

No Security Practices Applied; no assurance practiced applied

Level 1 - Minimum

Minimum Security Practices Applied; no assurance practiced applied

Level 2 - Ad hoc

Practices cover main use cases and well-known security incidents

Level 3 - Consistent

Practices consider best practices, standards, regulations, etc.

Level 4 - Formalized


Well-established processes for practice implementation; continuous support and enhancements.

Password Management Practice

Level 1 (Minimum):

- Objective: Establish basic password management.
- General Considerations: Use simple password policies.
- What needs to be done: Implement minimum length and complexity requirements.
- Indicators of Accomplishment: Basic password policy documentation.

Practical Implementation:



Password Policy

Minimum Requirements

- Passwords must be at least 8 characters long.

- Passwords must include:

- At least one uppercase letter (A-Z)

- At least one lowercase letter (a-z)

- At least one digit (0-9)

- At least one special character (e.g., !, @, #, \$)

Best Practices

- Avoid using easily guessable information (e.g., names, birthdates).

- Do not reuse passwords across multiple accounts.

- Change passwords regularly (every 90 days).

Enforcement

- Passwords will be checked against these requirements during creation and reset.

Password Management Practice

Level 2 (Ad Hoc):

- Objective: Introduce ad hoc password practices.
- General Considerations: Address common password threats.
- What needs to be done: Educate users on common password security practices and enforce periodic password changes.
- Indicators of Accomplishment: Documented training sessions and records of password changes.

Practical Implementation:



General Considerations

Address Common Password Threats:

- Weak passwords
- Password reuse
- Phishing attacks

Enforce Periodic Password Changes:

Policy Implementation:

- Set a policy requiring password changes every 90 days.
- Communicate this policy to all users through emails and internal communications.

Practical Implementation

r00t@123

Admin@123

P@ssw0rd@123#

Recognized as strong passwords by the policies - because satisfying requirements

But these known strong passwords - leads bruteforce

Password Management Practice

Level 3 (Consistent):

- Objective: Consistently apply password policies.
- General Considerations: Align with best practices and standards.
- What needs to be done: Enforce multi-factor authentication (MFA) and regularly review password policies.
- Indicators of Accomplishment: Regular audits and compliance reports.

Practical Implementation



Design Phase:

Integrate Standards and MFA Requirements: Include these in design documents and conduct threat modeling.

Development Phase:

Implement Policies and MFA in Code: Follow secure coding practices and conduct regular code reviews.

Testing Phase:

Test Policies and MFA Implementations: Conduct penetration testing to identify vulnerabilities.

Deployment Phase:

Ensure Compliance: Monitor deployed devices for compliance with password policies and MFA requirements.

Maintenance Phase:

Regular Audits and Compliance Checks: Update devices and policies based on the latest security findings and standards.

Password Management Practice

- Level 4 (Formalized):
 - Objective: Formalize advanced password management.
 - General Considerations: Use advanced security measures and continuous improvement.
 - What needs to be done: Implement automated password management tools, conduct continuous security awareness training, and integrate with other security systems.
 - Indicators of Accomplishment: Continuous monitoring reports, audit logs, and up-to-date training records.

Practical Implementation.



Limit password attempts to 3 tries.

Automatically unlock blocked IPs or users after 24 hours.

Implement both user-based and IP-based blocking.

Ensure error messages do not lead to user enumeration.

Prevent the device from reusing the last used password or username.

Continuously monitor audit logs and ensure they do not print sensitive information, except for IP addresses.

Detailed Logging: Maintain detailed logs of all password-related activities.

Sensitive Information Handling: Ensure logs do not print sensitive information, except for IP addresses.

Example Log:

[2024-07-26 14:00:00] Password changed for device 12345 by user admin. IP: 192.168.1.100

Monitoring SMM

Level Name	Objective	General Considerations	What Needs to be Done
Level 1 (Minimum)	Occasionally check individual diagnostic logs of components, devices, sensors, and systems.	Basic monitoring of security events using built-in mechanisms.	Follow existing general security guidance on basic security monitoring using existing mechanisms without any specific concerns for the particulars of the specific system.
Level 2 (Ad Hoc)	Obtain status events from devices and check for correct expected operation; detect malware.	Use events generated by individual components, devices, sensors, and systems to detect security issues.	Assign responsibility for analyzing security-related events to the system administrator or other responsible person.
Level 3 (Consistent)	Collect, consolidate, and analyze monitoring information holistically from various sources with human expertise for analysis.	Consolidate information from various monitoring sources and manage holistically.	Use different sources and various additional advanced monitoring systems, involve skilled security personnel or third-party contractors, and protect the monitoring information with secure logging.
Level 4 (Formalized)	Use automation and continuous monitoring with analytics to identify concerns.	Continuous real-time monitoring of all relevant types of security events using appropriate means and automation for analysis.	Automate most of the analysis of security events, conduct required manual reviews where appropriate, perform monitoring at various system levels, implement the whole cycle of monitoring, and continuously improve detection processes.

Q&A