Security of Embedded Systems Using "ISO 27002" Standards

Sahar Bukhari, Dr. Muhammad Hasan Islam

Abstract: Embedded Systems are electronic products that contain one or more than one microprocessor and software either programmable or fixed in capability, designed to perform some dedicated function within a large entity. Embedded Systems are increasingly employed in critical sectors such as in Life Critical Systems, Financial Infrastructure, Information Systems, Transportation Systems, Consumer Products and Avionics etc. Their inadvertent and malicious failures can cause dreadful consequences. The situation has become more critical due to rapid change in functional requirements of Embedded Systems particularly in terms of communication and interconnection. High interconnectivity between public networks such as internet and Embedded Devices has become a massive security challenge by which Embedded Systems can be directly attacked. This paper examines the security dimensions of Embedded Systems by means of baseline security intents of Embedded Systems and Information Security standard ISO/IEC 27002 which are basically safeguards to avoid and counteract security risks related to computer software or personal property. It is an Internationally-recognized standard which is cogently designed around a group of interrelated security controls, presented as a proposed solution in this paper to address the aforementioned difficulties of Embedded Systems. This standard is explicitly concerned with the security of all forms of information and equally beneficial for all types and sizes of organizations that handles and be contingent on information.

Keywords: Code of Practice for Information Security Management, ISMS (Information Security Management System), ISO/IEC 27002.

Introduction

Security of an Embedded System can be defined as the ability of an Embedded System to safeguard resources for which it endures protection culpability. Rapid increase in the usage of Embedded products in our daily life has made it crucial to make sure proper security of Embedded Systems. These systems are complex network of components, which are highly configurable and dynamic and their functional requirements are changed over time. Therefore in order to attain the assurance vital for security-critical Embedded Systems it is not enough to meet functional requirements.

Security concerns are actually violated because the security policies and functions claimed by the companies and stake holders are actually not fulfilled. Complex product infrastructure breeds flaws that can be used to break the system security. A secure Embedded Product must be secure for more than 10 years, having safe Machine to Machine Communication (M2M), uphold security despite of increasing intricacy and managing secure software updating during operations. Some of the major roots of Security lapses are: Execution of downloaded software, Complexities of design process, Operations performed in untrusted environments and Network induced vulnerabilities.

Sahar Bukhari is currently pursuing MS degree program in Computer Sciences in National College of Business Administration & Economics, Lahore, Pakistan.
E-mail: sahar.shah7@gmail.com.
Dr. Muhammad Hasan Islam, Professor at Center for Advanced Studies in Engg (CASE), Islamabad, Pakistan.
E-mail: mhasanislam@gmail.com.

A large number of functional security mechanism such as Cryptographic Algorithms, Temper Resistance Mechanism etc. have been introduced in this regard which partially fulfill the security requirements because they are not temper proof so do not provide the far-reaching solutions. For the protection of Information assets, ISO 27002 "Code of Practice" is a good and widespread practice approach which recommends a number of Information security controls that may or may not implement in context of ISMS (Information Security Management System) for the sake of systematically address the risks and satisfy appropriate control objectives. It refers Code of Practice for Information Security Management by determining a common basis and practical guideline for the development for organizational effective management practices and security standards. The major contribution of ISO/IEC 27002 is that, by implementing generally accepted information security controls it develops organization's own information security management strategies. In the following section we will discuss the relevant description in order to clarify the control objectives and their applicability to make Embedded Devices secure enough.

Applicability of ISO/IEC 27002 in Terms of Embedded Security

ISO/IEC 27002 is basically a best practice guide and a generic information security management standard which comprises detailed advice but it is merely advice that can be exploited according to organization's prerequisites for the establishment of a widespread information security management program. It is primarily a "Code of Practice for Information Security Management" recommended by ISO/IEC and each of these practices must be consider for the enhancement of information security management program of an organization.

The major distinction between the ISO/ IEC 27002 and the existed conventional solutions is that it is not mandatory to implement every recommended security practice [1]. It is to be implemented according to the security risk and requirement of the organization. Even though if an organization is not pursuing ISO certification it still can utilize the guidance provided in ISO/IEC 27002 in order to build an information security program. It can be taken as a friendly security expert in order to find out that how things should be done and later on it can be implemented if it found appropriate.

The advice enclosed within 27002 assist to understand the environment in a better way and help to implement a strong information security program [2]. This standard takes a very extensive approach and is all about information that can exist in different forms such as Electronic files, Recordings, Messages, Paper documents, Communications etc. Information is an asset that needs to be sheltered because modern organizations are facing catholic range of security intimidations such as equipment failure to theft, Sabotage, Fraud etc.

For that reason the infrastructure like Networks, Systems and Functions that supports the information must also be secure in order to manage and control the information asset in the best possible way. And then the question arises that how to protect information asset. Here comes ISO 27002 that describes what the companies and organizations can do for the safety of their information assets.

Owing to complexities and interconnectedness of modern organizations, they are threatened by malicious code, Computer hackers and Daniel of Service attacks. Keeping in view all these vulnerabilities ISO 27002 presents a wide variety of controls that can protect the information along with hardware and software function controls which comprises things like Processes, Policies, Organizational Structures and Procedures. For the sake of protection companies need to develop, evaluate, monitor, implement and improve these types of security controls.

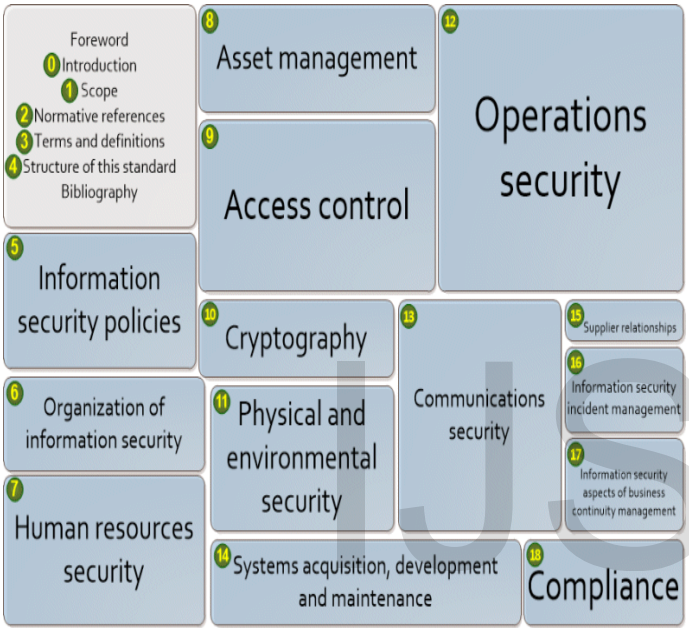

Fig 1. Structure of ISO/IEC 27002

The above structure of ISO 27002 standards presents Security Control Clauses which defines controls and control objectives concerning the necessitate to protect availability, integrity and confidentiality of information. These clauses give recommendations to those who are responsible for selection, management and implementation of information security.

Related Work

A white paper of Information Technology-Security Techniques; ISO 27002: 2013 [3] in which Eric Lachapelle and Mustafe Bislimi called the security controls as safeguard that can be employed as safety measures against computer software risks. According to them ISO 27001 and ISO 27002 are worked side-by side. The main responsibility of ISO 27001 standards is to identify risk in ISMS and control for risk management and then implement, review, monitor and improve these controls through ISO 27002 in the form of policies, procedures, software and hardware functions, organizational structures and processes. They also described some other standards that have somehow same functionalities like ISO/IEC 27002 such as OECD principles, Basel II, PCI-DSS, COBIT and ITIL.

In a Technical Corrigendum1 [4] a clear demonstration is given which is critical for the successful implementation of information security in an organization. It includes establishment of a measurement system for performance evaluation in information security management along with feedback suggestions for enhancement. Moreover commitment and visible support at all levels of management with an appropriate understanding of information risk assessment, security requirements and risk management. It is mandatory to distribute guidance on information security standards and policies to all parties, employees and managers by means of effective marketing. Provision to funds along with proper training, education and awareness in order to maintain a framework of implementing, monitoring and enhancing information security that is consistent to the culture of organization.

A physical and environmental security policy given in an article of Information and communications Technology [5] describes the security areas need to be preventing included damage, unauthorized physical access and interference in the organization's information and premises. Furthermore this policy includes five major areas of security control comprises of Mobile and Portable systems, Interception of data, physical access control, supporting utilities and fire safety. These controls are used to; restrict entry and exit of equipment, media and personal, prevent hardware and data from damage; and provide utilities that are composed of many elements that thwart failures of air conditioning and heating system that may cause a service interruption or damage hardware along with loss of information; prevent three routes of data interception, mobile and portable systems. The implementation of these security controls required some general approaches in order to justify the control selections.

Security Paradigm for a Particular Device

First and foremost step is the selection of compliance that is practically useful for the concern device. The three main compliances are Regulatory, Internal and third party respectively. Regulatory Compliance is the best practice approach which is exploited to handle sensitive data and program overall security. Internal Compliance gives security implementations as a process and integrated part of business. Third party compliance is employed to give proof to partners of good practice around data protection.

The next step will be the identification of the information security requirements and needs of the device and establishment of device's own information security program by choosing security practices recommended by ISO 27002 that comes across the device's security essentials and prerequisite criteria and pay no attention to the ones that don't. Here some of the common best practices are taken into account that are good place to start and must be at the center of information security program according to ISO/IEC[6], [7], [8], [9], [10]. The very first one is allocation of responsibility for information security followed by development of policy document of information security. The next one is to make certain that the processing of information is performed correctly by the applications by means of managing information security improvements and incidents. After that there is need to establish management process of a technical vulnerability by providing security training, awareness and education. Last but not the least is the development of a continuity of management process. Moreover some common legislated practices should also be considered in order to provide a complete protection to the device which leads to respect intellectual property rights, protect organizational records and safeguards the privacy of personal information.

Conclusion

In terms of Embedded security ISO 27002 offers flexible set of controls that can be used in a way an organization wants to secure itself. It is a colossal standard that covers a wide range of Information controls and risks, having so many contents and changes according to the ongoing evolution of Information Security due to which it outstripped the capabilities of other standards. Its major contribution is to prepare and enhance the security framework that controls future information security plans, security controls and compliance activities along with more reliable access to data environment with far-less hindrance and fewer work interruption. It gives the incentive to recognize the positive value of information security control by embedded good practice throughout the organization. Control Objectives and large number of information security controls throughout the standard are high-level, generic statements for business requirements for the safety of information assets. The structure of ISO 27002 is comprehensive and reasonable catalogue in terms of security which is not perfect , perhaps potentially gives incomplete guidance that can be interpreted in the context of organization, but good enough from the existed ones as it covers maximum areas of Embedded Systems which need to be secure.

Acknowledgement

I would like to thanks my father Muhammad Anwar Shah Bukhari for his unflagging belief. I am indebted him for inculcating in me the discipline and dedication to do whatever I understand well.

References

[1].http://www.praxiom.com/iso-27002.htm
http://www.praxiom.com/iso-17799-2005.htm
[2].http://zih.hr/sites/zih.hr/files/cr-collections/3/iso27002.pdf
[3].http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf
[4].http://www.health.wa.gov.au/circularsnew/attachments/871.pdf
[5]. http://www.iso27001security.com/html/27002.html
[6]. www.standards.bz/iso-27002.html
[7]. ISO/IEC 27001:2005. Information Technology - Security Techniques – Information Security Management Systems – Requirements. Known as ISO 27001.
[8]. ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of Practice for Information Security Management. Known as ISO 27002.
[9]. Alan Calder & Steve Watkins (2012). IT Governance: an International Guide to Data Security and ISO27001/ISO27002. 5th edition. Kogan Page Publishing.
[10].http://www.27000.org/iso-27002.htm