Chapter 36
Integrated Security Process Improvement Framework for Systems and Services

Muthu Ramachandran
Leeds Metropolitan University, UK

ABSTRACT

Security of systems and services has been dominant research area in recent years as today's cloud services, big data and networked systems, especially when they provide wireless application access where personal and confidential data to be transmitted across the networked systems. Numerous tools and technologies are available to ensure system's security; however, external threats to computer systems and applications residents thereon, are also becoming more and more sophisticated and on the increase. Therefore, the key aim of this research is to integrate security engineering techniques and process with systems development life-cycle and process improvement frameworks. This paper presents a framework that consists of two components: 1) a security assessment model to looks at the existing security infrastructure of an organisation to determine its security maturity level; and 2) a security improvement maturity model to suggest an improvement mechanism for the organisation to progress from one maturity level to the next higher level. The intention is to provide a scheme to improve the organisation's Systems and network security with the aim that it becomes more efficient and effective than before.

1. INTRODUCTION

In the information society of the 21st century, the information and communication technologies have revolutionised human lives. Wireless telephony, cloud computing, mobile clouds, electronic commerce and online transactions are now common place and within easy reach of general public. All this has become possible through the proliferation of computing technologies and use of the Systems. There is no doubt that World Wide Web, or the Systems, is the binding and enabling force behind all this.

Since the use of the Systems is growing, the demand for the associated products, applications and services is also growing. As a bi-product, the concerns with respect to the security of information, confidentiality of data and reliability of services are also growing. Previously, when the computing systems were used as standalone

DOI: 10.4018/978-1-4666-8111-8.ch036

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

devices, the security concerns amounted to only the physical security (i.e. fear of getting it damaged, getting it stolen, etc). Now, however, because of interconnectivity of computing equipment on a global basis, there are serious concerns with respect to security of networks (including the Systems), theft of data, cyber terrorism and so on. Although, network managers and security experts are doing their best to ensure that transactions are safe, networks are secure and malicious damage to data, services, applications and equipment is eliminated, hackers and cyber terrorists are also becoming more intelligent and finding new ways of breaking and getting into computing systems. The technologies that exist for the benefit of citizens are, ironically, the same technologies that hackers are using for their malicious acts. To ensure the security of Systems applications and the use of Systems, many approaches has been employed including systems such as the following:

- Intrusion detection mechanisms
- Intrusion prevention schemes
- Firewalls and Filters
- Virus detection and removal software
- Build-In security (software security engineering)

However, SecurityFocus (2013) has reported on percentage of vulnerability attacks for operating systems attacks account for 9% vulnerability, web-based software systems attacks account for 61% vulnerability, and other applications attacks account for 30% vulnerability. Similarly, Popović and Hocenski (2010) have reported an analysis of results from IDC ranking of security challenges that 87.5% responded to demand for cloud security against on-demand cloud services. This confirms the importance of cloud security against cloud services.

Cloud computing has emerged to provide a more cost effective solution to businesses and services while making use of inexpensive computing solutions which combines pervasive, internet, and virtualisation technologies. Cloud computing has spread to catch up with another technological evolution as we have witnessed internet technology which has revolutionised communication and information super highway. Cloud computing is emerging rapidly and software as a service paradigm has increasing its demand for more services. However, this new trend needs to be more systematic with respect to software engineering and its related process. For example, current challenges that are faced with cyber security and application security flaws, lessons learned and best practices can be adopted. Similarly, as the demand for cloud services increases and so increased importance sought for security and privacy. The business of cloud technology can only be sustained if we can maintain balance between demand for services in-line with improved cloud security and privacy.

Currently, security related flaws are being found on daily basis are fixed by adding security patches. This is simply unacceptable paradigm for sustainability of cloud computing. Therefore, we need to develop and build cloud services with build in security of services (SaaS, PaaS, IaaS), data centres, and cloud servers. This chapter aims to provide a number techniques and methods for developing cloud services systematically with build in security. It will also cover a range of system security engineering techniques have been adopted as part of a cloud development process. A number of examples of scenarios have chosen from Amazon EC2, to illustrate with, emerging cloud system security engineering principles and paradigm (Ramachandran, 2011; 2012). Similarly, Teodoro and Serrao (2011) have reported web applications security is crucial as they account for a number of malicious attacks and vulnerabilities if not engineered systematically and improved to guarantee security and quality of services.

However, these mechanisms have limitations. In this context, the biggest challenge is to develop and apply appropriate Systems security strategies consistently and uniformly across the entire network and ultimately to individual nodes

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/integrated-security-process-improvement-framework-for-systems-and-services/125320

Related Content

An Exploration of Data Interoperability for GDPR
Harshvardhan J. Pandit, Christophe Debruyne, Declan O'Sullivanand Dave Lewis (2018). *International Journal of Standardization Research (pp. 1-21).*
www.irma-international.org/article/an-exploration-of-data-interoperability-for-gdpr/218518

The Battle Within: An Analysis of Internal Fragmentation in Networked Technologies Based on a Comparison of the DVB-H and T-DMB Mobile Digital Multimedia Broadcasting Standards
Håkon Ursin Steen (2011). *International Journal of IT Standards and Standardization Research (pp. 50-71).*
www.irma-international.org/article/battle-within-analysis-internal-fragmentation/56359

Selected Intellectual Property Issues in Standardization
Martin B.H. Weissand Michael B. Spring (2000). *Information Technology Standards and Standardization: A Global Perspective (pp. 63-79).*
www.irma-international.org/chapter/selected-intellectual-property-issues-standardization/23728

Data Security Legislative as Data Shredding Mill
Jaroslav Kraland Michal Zemlicka (2010). *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues (pp. 240-248).*
www.irma-international.org/chapter/data-security-legislative-data-shredding/43498

Cognitive Cooperation in Wireless Networks
Eng Hwee Ongand Jamil Y. Khan (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 1498-1522).*
www.irma-international.org/chapter/cognitive-cooperation-wireless-networks/75088