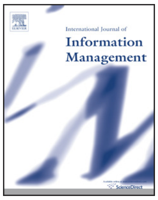
Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



Software security requirements management as an emerging cloud computing service

Muthu Ramachandran

School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds LS6 3QS, UK

ARTICLE INFO

Article history:
Received 15 March 2016
Received in revised form 24 March 2016
Accepted 24 March 2016
Available online 3 April 2016

Keywords:
Emerging cloud services
Software security
Software security requirements engineering
Secured software development
SQUARE method
BSI
Touchpoint
SDL
Requirements engineering and management as an emerging service (SSREMaaES)

ABSTRACT

Emerging cloud applications are growing rapidly and the need for identifying and managing service requirements is also highly important and critical at present. Software Engineering and Information Systems has established techniques, methods and technology over two decades to help achieve cloud service requirements, design, development, and testing. However, due to the lack of understanding of software security vulnerabilities that should have been identified and managed during the requirements engineering phase, we have not been so successful in applying software engineering, information management, and requirements management principles that have been established for the past at least 25 years, when developing secure software systems. Therefore, software security cannot just be added after a system has been built and delivered to customers as seen in today's software applications. This paper provides concise methods, techniques, and best practice requirements engineering and management as an emerging cloud service (SSREMaaES) and also provides guidelines on software security as a service. This paper also discusses an Integrated-Secure SDLC model (IS-SDLC), which will benefit practitioners, researchers, learners, and educators. This paper illustrates our approach for a large cloud system Amazon EC2 service.

1. Introduction

There is no doubt that the cloud computing has revolutionised human lives, communications, digital economy, socialisation, and entertainment. At the same time demands for internet enabled applications grows rapidly. Almost all businesses, applications, entertainment devices, mobile devices, robots, large scale systems (aircrafts, mission control systems), safety-critical systems, medical systems, internet of things devices are internet enabled for various reasons such as online upgrade, distributed applications, team projects, and server connectivity. Therefore, there is ever growing demand for secured applications and trust. Cyber attacks are increasing continuously From spam, phishing, identify theft, and others in much larger scale attacks such as money laundering and cyber terrorism. There is a real possibility that a cyber attack could disable command systems, bring down power grids, open dam floodgates, paralyses communications and transport systems, creating mass hysteria: Any or all of which could be the precursor to terrorist or military attack. These are some of the threats since we (personal, govt. organisations, companies, and business) mostly depend on computers and mobiles for communications and management.

Emerging cloud services are on the increase including eHealth Cloud, E-Learning, E-Manufacturing, etc. Kostoska, Gusev, and Ristov (2014) describe a new cloud protability platform (PaaS) as a service which can accept and exchange from one cloud platform to another platform and installed completely automatically. Han et al., 2016 have proposed an energy-aware VM consolidation based on remaining utilisation-aware algorithm (RUA). Xu (2013) has proposed an interoperable cloud manufacturing system (ICMS) which shares encapsulated resources into a cloud service for manufacturing where manufacturing capabilities and business opportunities are integrated and broadcasted in a larger resource pool. Srivastava et al. (2015) describes how eHealth initiatives and the technology helps to achieve health services at a very low cost by connecting and consulting expertise worldwide for very complicated surgeries, use cloud services, IoT services for collecting and monitoring data, and they also recommend to integrate various technologies. This paper aims to offer software security engineering as an emerging service which aims to offer tools and techniques on security requirements, design for software security, secure software development, vulnerability analysis, security testing, and security metrics.

E-mail addresses: M.Ramachandran@leedsbeckett.ac.uk, muthuuk@yahoo.co.uk

http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.008
0268-4012/© 2016 Elsevier Ltd. All rights reserved.

The cloud vendors include well known businesses such as Amazon EC2, IBM, HP. Google, Microsoft Azure. In addition, there are new cloud businesses on the market such as 2nd Watch which has partnered with AWS (Amazon EC2 Web Service) offers cloud migration, workload management, and has 75,000 instances from hundreds of customers under its management. Similarly, BetterCloud automated management and data security for cloud office platforms, including Google Apps and Microsoft Office 365 (Whiting, 2015), Hsu and Cheng (2015) describe a Semantic Agent as a Service (SAaaS) which collects and discover knowledge from semantic information and works with core cloud services: SaaS, PaaS, and IaaS. All of the cloud vendors agree the strong need for secure cloud services and business migration.

This paper aims to outline the importance of developing secure cloud services using a disciplined approach known as software security engineering and it is also known as secure software development. In particular, this paper identifies key methods and techniques on software security requirements engineering as it is the heart of developing secure cloud services. This paper discusses clear best practice guidelines on software security and discusses our Integrated-Secure SDLC (IS-SDLC) model which overcomes current difficulties in identifying and visually representing security process which have been elaborated From security requirements. In addition, we all enjoy the new technologies based on service computing, such as mobile apps, cloud storages, social media networks, and cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The need for high performance cloud computing and accuracy and precision of big data enforce the need for complete identification of non-functions cloud service requirements and its specification. In addition, security, privacy & trust are the key to the success of cloud computing, which needs to be identified and specified as part of the requirements management process. This paper divided into: section 1 discusses on introduction to our work, section 2 provides the rationale for the subject area, section 3 introduces software security requirements engineering and management, and section 4 introduces an integrated approach to SDLC, and the final section provides a large scale case study using Microsoft Security Development Lifecycle on threat modelling techniques for Amazon EC2 cloud services.

2. Why software security engineering?

Software Engineering (SE) has established techniques, methods, and technology over two decades. SE also provides rich techniques and tools on modelling software requirements, design, development, testing, configuration management, and software metrics. However, security issues are direct attributes of various software such as applications, user interface, networking, distribution, data-intensive transactions, and communication tools, etc. Current applications are being developed and delivered where security has been patched as aftermath. Early commercial developers have tackled security problems using firewalls (at the application level), penetration testing, and patch management.

We are also faced with tackling fast growing information warfare, cybercrime, cyber-terrorism, identify theft, spam, and other various threats. Therefore, it is important to understand the security concerns starting From requirements, design, and testing to help us Build-In Security (BSI) instead of batching security afterwards. McGraw (2006) says *a central and critical aspect of the computer security problem is a software problem*. This paper defines *software security engineering as a discipline which considers capturing and modelling for security, design for security, adopting best practices, testing for security, managing, and educating software security to all stakeholders.*

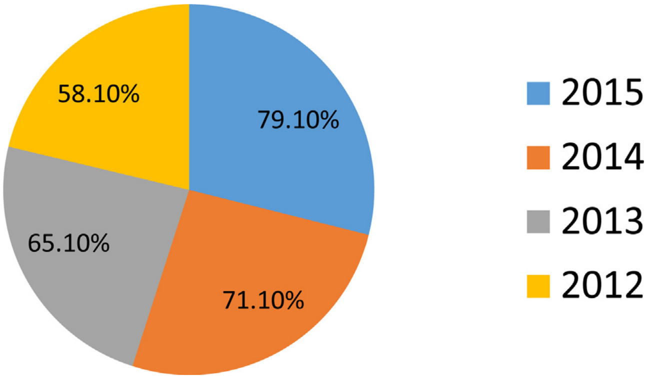


Fig. 1. Annual spending on information security.

Software engineering has well established framework of methods, techniques, rich processes that can address small to very large scale products and organisations (CMM, CMMi, SPICE, etc.), and the associated technology such as modelling (UML), CASE tools, and CAST tools, and others. Software Engineering has also been well established quality models and methods, reuse models and methods, reliability models and methods, and numerous lists of other techniques. The so called—lities of software engineering long has been contributed as part of quality attributes (Quality, Testability, Maintainability, Security, Reliability, Reusability). These attributes cannot be just added on to the system as they have to be built in From early part of the life cycle stages (a typical software development lifecycle include starting From requirements engineering (RE), software specification, software & architectural design, software development (coding), software testing, and maintenance. Security has become highly important attribute since the development of online based applications. Software project management has well established techniques and breadth of knowledge including global development (due to emergence of internet revolution and people skills across the globe), cost reduction techniques, risk management techniques, and others. Nowadays, most of the current systems and devices are web enabled and hence security needs to be achieved right From beginning: need to be identified, captured, designed, developed and tested. Ashford (2009) reports UK business spends 75% of the software development budget on fixing security flaws after delivering the product. This is a huge expenditure and it also creates untrustworthiness amongst customers. Fig. 1 shows the chart for the annual spending on IT security which demonstrated the increase of more than 10% each year (Gartner, 2016).

Due to importance of security driven software development, software security engineering and secure software development disciplines have emerged in recent years (Ramachandran, 2012). Software security engineering deals with rich tools and techniques on software security requirements modelling such as misuse and abuse cases, threat modelling, design for security, vulnerability analysis, secure coding, testing, and metrics. In addition, recent issues with cloud security strategies, techniques are elaborated by Chang and Ramachandran (2015, 2016).

Allen et al. (2008) state that the one of the main goals of Software Security Engineering is to address software security best practices, process, techniques, and tools in every phases and activities of any standard software development life cycle (SDLC). The main goal of building secured software which is defect FSRee and better built with:

- Continue to operate normally in any event of attacks and to tolerate any failure