Systems Engineering Processes for the Development and Deployment of Secure Cloud Applications

Muthu Ramachandran
School of Computing, Creative Technologies, and Engineering, Leeds Metropolitan University, UK

INTRODUCTION

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. Cloud service providers such as Microsoft, Google, Sales force.com, Amazon, GoGrid are able to leverage cloud technology with pay-per-use business model with on-demand elasticity by which resources can be expended or shortened based on service requirements. They often try to co-locate their servers in order to save cost.

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 article 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, 2013). This real-world case study have been used to demonstrate the best practices on business process modelling and component based design for developing cloud services with Build Security In (BSI). BSI techniques, strategies, and process presented in this article are general systems security principle and are applicable for both in a cloud environment and traditional environment (non-cloud environment). The significant contribution of this research is to illustrate the application of extended systems security method known as SysSQUARE to elicit security requirements, to identify security threats of data as well as integrating build-in security techniques by modelling and simulating business processes upfront in the systems development life cycle.

BACKGROUND

Systems Engineering incorporates systematic and comprehensive approach to modelling, designing, and developing enterprise systems includes software and service based systems. Caminao project (2013) provides a comprehensive framework for systems engineering methods and concepts. The Internet technology has revolutionised the way we live on daily basis. The use of Internet is growing rapidly from devices, appliances and cloud computing which has emerged to address cost-effective solution for businesses. However, security is the most common security concerns of all. Therefore, security for cloud computing is the main aim of this article. The everyday cloud applications and apps can be protected using commonly available anti-security software packages. However, it is harder to protect us

DOI: 10.4018/978-1-4666-5888-2.ch434

from security related attacks which emerges unexpectedly and are often hard to predict. This isn't sufficient for cloud service providers who offer three different types of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Therefore, there is a need for going beyond boundaries of existing security techniques such as password protection, virus checks, secured financial transaction techniques, etc. The following are categories of broad spectrum of security related research that are under taken:

- Application software security which deals with how we can build systems that can automatically protect itself.
- Service-oriented security where issues related to system services such as denial of service attacks, distributed denial of services, and web services.
- Cloud security deals with services security, data security and privacy so that services delivered and assets are protected.
- Open-source software security deals with issues such as trust, certification and qualification models.
- Software components and architecture security which deals with building components and architectures with security can be used as plug-ins.
- Web services security is essential to ensure secured services are delivered with integrity
- Systems & Software security engineering deals with building security in (BSI) right from requirements. This is also considers developing software applications with BSI.

Figure 1 shows a landscape of digital security related areas of research which will dominate most of cloud computing in the forthcoming areas.

Security research is emerging as we discover and learn new forms of threats. Therefore, the research landscape shown in Figure 1 will have to be expanded. Computer security have been classified into a number

Figure 1. Digital security research landscape