Chapter 111
Secure Software Development of Cyber-Physical and IoT Systems

Muthu Ramachandran
Leeds Metropolitan University, UK

ABSTRACT

This real-world case study has 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 processes presented in this chapter are general systems security principles and are applicable for both a cloud environment and traditional environment (non-cloud environment). The significant contribution of this research is to illustrate the application of the extended system security method known as SysSQUARE to elicit security requirements, 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.

INTRODUCTION

Cyber-Physical Systems (CPS) and Internet of Things (IoT) is on the rapid increase as the demand for such applications is growing exponentially. There is a very strong reason for connecting three technologies such as CPS, IoT and Cloud as the first two are connected to a cloud for receiving and analysing data. 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 superhighway. Cloud computing is emerging rapidly and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to developing secure software engineering and its related processes such as requirements, design, development, and test. For example, current challenges that are faced with cyber security are: application security flaws and lessons

DOI: 10.4018/978-1-5225-7598-6.ch111

learned which can all be applied when developing applications for CPS and IoT systems. 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 expanded or shortened based on service requirements.

Alur (2015) defines CPS as:

"A CPS system is defined as a system consists of computing devices communicating with one another and interacting with the physical world via sensors and actuators." Examples of such systems include from smart buildings to medical devices to automobiles.

McEwen and Cassimally (2014) defines IoT as:

"An IoT system consists of any physical objects contains controllers, sensors, and actuators are connected with Internet." Examples of such system include any devices capable of sending and receiving data through the internet such as internet enabled washing machine, dishwasher, etc.

In other words, IoT can also be defined as the network of physical objects or things that are built or embedded with sensors, actuators, software, and connect via the internet which enables these objects to collect and exchange data. The difference between the CPS and IoT needs to be clarified as the applications being deployed over the years. First of all, let us look at a precursor is known as Embedded systems which have been successfully deployed in wider areas such as aerospace, manufacturing, chemical processes, civil infrastructures, etc. They key difference between the CPS and Embedded system is the inter-connectivity of these networked physical objects, whereas it often not embedded but interact with physical world objects. A wireless sensor networks can be mounted around a river to receive and exchange data amongst them to calculate any abnormal level of river overflow to avoid any natural disasters in the region. Therefore, security of CPS and IoT systems are paramount to our research as well as their data has been secured.

Currently, security related flaws are being found on a daily basis that are fixed by adding security patches. This is simply an 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 & 2014). 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 the extended system 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.