International Journal of Information Management 36 (2016) 155–166

Contents lists available at ScienceDirect

International Journal of Information Management

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

A resiliency framework for an enterprise cloud

Victor Chang[a,*], Muthu Ramachandran[a], Yulin Yao[b], Yen-Hung Kuo[c], Chung-Sheng Li[d]

[a] School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK
[b] Independent Researcher, Southampton, UK
[c] Data Analytics Technology & Applications, Institute for Information Industry, Taiwan, ROC
[d] IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, USA

ARTICLE INFO

Article history:
Received 17 September 2015
Received in revised form
29 September 2015
Accepted 30 September 2015
Available online 9 October 2015

Keywords:
- Software resiliency
Resilient software for Enterprise Cloud
Cloud computing Adoption Framework (CCAF)
Cloud security and software engineering best practice

ABSTRACT

This paper presents a systematic approach to develop a resilient software system which can be developed as emerging services and analytics for resiliency. While using the resiliency as a good example for enterprise cloud security, all resilient characteristics should be blended together to produce greater impacts. A framework, cloud computing adoption framework (CCAF), is presented in details. CCAF has four major types of emerging services and each one has been explained in details with regard to the individual function and how each one can be integrated. CCAF is an architectural framework that blends software resilience, service components and guidelines together and provides real case studies to produce greater impacts to the organizations adopting cloud computing and security. CCAF provides business alignments and provides agility, efficiency and integration for business competitive edge. In order to validate user requirements and system designs, a large scale survey has been conducted with detailed analysis provided for each major question. We present our discussion and conclude that the use of CCAF framework can illustrate software resilience and security improvement for enterprise security. CCAF framework itself is validated as an emerging service for enterprise cloud computing with analytics showing survey analysis.

1. Introduction

Software engineering has established techniques, methods, and technology over two decades. However, the concept of resiliency has not been exploited well and software security related attacks and how systems are capable of withstanding such an attack remains research challenge. Some of the software security issues are caused by the direct attributes such as applications, user interface, and communication tools. 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 (Curphey & Arawo, 2006; McGraw, 2006). Building resilient software system will help to build trust for users and communities, protect data centres for critical applications such as medical systems and other critical systems (Friedman & West, 2010; Rajkumar, Lee, Sha, & Stankovic, 2010). Software resiliency needs to be defined and identified as we start identifying requirements for software systems. It is relevant to cloud computing as an emerging service that provides data analysis of outputs.

There is a growing demand and pervasiveness for the majority of people to be involved directly or indirectly with fast growing information warfare, cybercrime, cyber-terrorism, identify theft, spam, and other various threats. It is hence important to understand the security concerns starting from requirements, design, and testing. Therefore, we can actually build in security instead of batching security afterwards. McGraw (2006) asserts that a central and critical aspect of the computer security problem is a software problem. This book 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.

Software engineering has well established framework of methods, techniques, rich processes that can address small to very large scale products and organizations (CMM, CMMi, SPICE, etc.), and technologies (UML modeling, CASE tools, and CAST tools, etc.). Software Engineering has also been well established quality, reusability, reliability models, methods and numerous lists of other techniques. The so called "lities" of software engineering has been contributed as part of quality attributes which are known as quality, testability, maintainability, security, reliability and reusability.

* Corresponding author.
E-mail address: V.I.Chang@leedsbeckett.ac.uk (V. Chang).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.09.008
0268-4012/

These attributes cannot be just added on to the system as they have to be built in from early part of the lifecycle stages (Gillies, 2011). It is 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 the emergence of internet revolution and people skills across the globe), cost reduction techniques, risk management techniques, and others. Now a day, most of the current systems are web enabled and hence security needs to be achieved right from beginning: need to be identified, captured, designed, developed and tested (Gillies, 2011; Ramachandran, 2008; Ramachandran, 2012; Ramachandran & de Carvalho, 2010). Hence, a consolidated research is required into interplay between social engineering and software engineering for developing a secured software system, with aims to define and identify software resiliency for a software system to build trust, security, and integrity. All these can help organizations achieve enterprise security since their services are more robust and resilient to hacking, errors and faults. To present our research in developing resilient software systems, a framework is proposed with the rationale and the details of the software components illustrated. Surveys have been conducted with 400 valid samples. Collective user requirements are used as the input for system design and development of the framework, so that the framework can be demonstrated as an emerging service and analytics to validate its resilience and robustness.

The breakdown of this paper is as follows. Section 2 describes the related work for building a resilient software framework. Section 3 presents research methodology with an overview of the framework, cloud computing adoption framework (CCAF) and the resilient component services. Section 4 explains the survey results and how they can be used for the framework development. Section 5 proposes the framework with the four major services and the details in each component of each service. Section 6 explains how CCAF framework can be used as a business resilient framework to provide the competitive edge. Section 7 justifies the collective user requirements for the CCAF development with the rationale explained for summary of comments given by the respondents. Section 8 describes the target met and designed by the CCAF framework to consolidate why CCAF is an emerging service. Section 9 sums up Conclusion and future work.

2. Related work

This section describes the related work with regard to the attack methods, since a comprehensive understanding can help design and improve guidelines for a security framework of cyber security incidents between February and August of 2011 compiled by X-Force of IBM, which include Amazon's loss of data in 2011 and 2012, and the problems with elastic load balancing services in 2013 and RSA's hacked data and services (Li, 2014). Among all security incidents in the previous five years, the most severe incident is the attack on RSA during March 2011. This incident involves what is known as ***Five – layeredofAdvancedPersistentThreat*** (APT), and often includes the following five phases over an extended period of time:

1. Social engineering: initially, spear phishing emails were sent over a two-day period to small groups of employees with RSA. The email subject line read *2011 Recruitment Plan*, was from beyond.com—an HR partner firm of RSA. The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability. One of the RSA employees clicked the attachment from junk mail.
2. Back door: the malware installed a customized remote administration tool known as Poison Ivy RAT to allow external control of the PC or server, and set up the tool in a reverse-connect mode.
3. Moving laterally: the malware first harvested access credentials from the compromised users (user, domain admin, and service accounts), then performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets.
4. Data gathering: attacker behind the malware in the RSA case established access to staging servers at key aggregation points.
5. Exfiltrate: the attacker then used FTP to transfer many password-protected RAR files from the RSA file server to an outside staging server on an external, compromised machine at a hosting provider. Once the transfer completed, the footprints were wiped clean making it impossible to trace back to the attackers.

2.1. Resilient software framework

A resilient software framework is required to ensure that all services are safe, robust and secure. All the components and layers within the emerging services can be useful for organizations to adopt. In exceptional circumstances such as unauthorized access and hacking, the resilient service can withstand all these five commonly attacking approaches. To ensure that a resilient framework is in place, all the essential characteristics in security services are required, which includes the followings:

- Identification is a basic and the first process of establishing and distinguishing amongst person/user and admin ids, a program/process/another computer ids, and data connections and communications.
- Privacy is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and teamwork on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/data/media contents.
- Integrity is defined as a process of maintaining consistency of actions,communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud users' data with honesty, truthfulness and accuracy at all time.
- Durability is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

The other important aspects are as follows.

- Confidentiality, privacy and trust—These are well known basic attributes of digital security such as authentication and authorization of information as well protecting privacy and trust.
- Cloud service security—This includes security on all its services such as SaaS, PaaS, and IaaS. This is the key area of attention needed for achieving cloud security.
- Big data security—This category is again paramount to sustaining cloud technology. This includes protecting and recovering planning for cloud data and service centers. It is also important to secure data in transactions.
- Physical protection of cloud assets—This category belongs to protecting cloud centers and its assets.

2.2. Building in resiliency

This section describes software resiliency and success factors for building resiliency for enterprise security. IT and software engi-