Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 310 (2015) 113–133

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Model-based Evaluation of Scalability and Security Tradeoffs: a Case Study on a Multi-Service Platform

Leonardo Montecchi[1], Nicola Nostro[1], Andrea Ceccarelli[1], Giuseppe Vella[2], Antonio Caruso[2], Andrea Bondavalli[1]

[1] *Università degli Studi di Firenze, Dipartimento di Matematica e Informatica*
Viale Morgagni 65, I-50134 Firenze, Italy
{leonardo.montecchi,nicola.nostro,andrea.ceccarelli,andrea.bondavalli}@unifi.it

[2] *Engineering Ingegneria Informatica S.p.A.*
Viale Reg. Siciliana 7275, Palermo, Italy
{giuseppe.vella,antonio.caruso}@eng.it

Abstract

Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security issues to be faced arise from exposing applications and data to the Internet, thus requiring an attentive analysis of potential threats and the identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance and scalability properties. The paper presents a model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform, by evaluating how the introduction of security mechanisms may lead to a degradation of performance properties. The evaluation focuses on the OPENNESS platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model, and the evaluation of different configuration by composing them in different ways.

Keywords: Performance evaluation, scalability, web-services, security evaluation, security tradeoffs.

1 Introduction

The increased mobility of devices, pervasive connectivity, and multiple devices per user, produced a shift towards a “thin client” approach, where a large part of the required storage and computational power is demanded to servers [3]. The recent cloud computing paradigm extends this approach with an additional layer of abstraction, which separates physical resources (i.e., hardware) from logical resources (e.g., applications, storage, computational power) which are provided to users.

http://dx.doi.org/10.1016/j.entcs.2014.12.015
1571-0661/© 2015 The Authors. Published by Elsevier B.V.

In the Software-as-a-Service (SaaS) paradigm, software applications are hosted on a central server, and provided to users on-demand. This is often accomplished by means of web-based interfaces, so that clients do not need any other application than a web browser. Social networks and online storage facilities are prominent examples of this paradigm. Due to its advantages in terms of resources, costs, and convenience, this kind of paradigm is often used also within organizations, to provide services to employees or internal users.

However, this approach also introduces several challenges. One of the main problems consists in the scalability of the system with respect to an increasing population of users and applications, so that resources need to be carefully dimensioned. Another challenge consists in the additional security threats originating from exposing applications and data to the Internet, thus requiring stronger security mechanisms to be implemented within the system. Security and performance are often in contrast with each other [17]: mechanisms to improve the security of the system often prescribe constraints on resource usage, or require additional computations to be performed in order to guarantee that security policies defined at design time are actually applied at runtime. Moreover, a large part of security mechanisms relies on cryptography algorithms, which are typically resource-intensive. Therefore, the addition of security mechanisms can produce a negative impact on system performance, which needs to be carefully quantified and evaluated.

In this paper we adopt a stochastic modeling approach in order to evaluate the scalability of a multi-service web-based platform, and the impact of introducing security mechanisms. The evaluation focuses on the OPENNESS platform, a web-based platform providing different services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures.

The model is constructed using the Stochastic Activity Networks (SANs) formalism [16], which can be considered an extension of the well-known Stochastic Petri Nets (SPNs) [5] formalism. The key characteristic of our approach is in the modularity and reusability of the model: the analysis model is defined as a composition of a small set of "template" SAN models, which are then composed to form the overall system model. By composing them in different ways, the same templates can be used to evaluate different system configurations.

The rest of the paper is organized as follows. The OPENNESS framework is described in Section 2, while related work are discussed in Section 3. The stochastic model is described in Section 4, while evaluations and results are described in Section 5. Finally, conclusions are drawn in Section 6.

2 The OPENNESS Platform

The OPENNESS (OPEN Networked Enterprise Social Software suite) platform is the framework conceived within the research project VINCENTE [18], which aims at defining, realizing, and experimenting a technological platform for sustainable entrepreneurship. It optimizes the resources, enhances the sharing of knowledge,