Available online at www.sciencedirect.com

SCIENCE DIRECT®

Decision Support Systems 39 (2005) 333–344

Decision Support Systems

www.elsevier.com/locate/dsw

Model checking for design and assurance of e-Business processes

Bonnie Brinton Anderson, James V. Hansen*, Paul Benjamin Lowry, Scott L. Summers

Marriott School of Management and Kevin Rollins Center for e-Business, Brigham Young University, 538 Tanner Building, Provo, UT 84602, USA

Received 29 April 2003; received in revised form 23 July 2003; accepted 22 December 2003

Abstract

Use of the Internet for electronic business has the potential to revolutionize the way many businesses are conducted. Yet, several businesses have fallen victim to problems in information systems that facilitate e-Business. These problems are characterized by uncertainties due to system complexity, rapid development, interconnectivity, and a lack of familiarity with the new technologically based economy. This paper demonstrates how model checking can aid in the design and assurance of e-Business processes in environments characterized by distributed processing, parallelism, concurrency, communication uncertainties, and continuous operations.

Keywords: e-Business; Model checking; Money atomicity; Goods atomicity; Valid receipt; Process and communication protocols

1. Introduction

Electronic business (e-Business) on the Internet has the potential to revolutionize the way many businesses are conducted. Using the Internet as a medium for managing commercial transactions enhances accessibility to a wide variety of information and services, and greatly facilitates remote payments. Consequently, many firms are able to leverage critical business operations through Internet-based electronic processes. That this revolution has already begun is evidenced by the increasing number of resources that are procured, managed, created, and consumed over the Internet, Intranets, and Extranets. Even the world's financial markets, telecommunications, and management of water and power supplies depend on the operations of massive Internet-based information systems [1].

At the same time, many businesses have fallen victim to problems in information systems that facilitate e-Business. Such problems include inadequate security, flawed controls, and poorly designed back-end systems. In the e-Business environment, these issues are compounded by uncertainties that evolve from rapid development, system complexity, increased risk through interconnectivity, and lack of

* Corresponding author. Tel.: +1-801-422-12-15; fax: +1-801-422-06-21.

E-mail addresses: Bonnie_Anderson@BYU.edu (B.B. Anderson), James_Hansen@email.byu.edu (J.V. Hansen), Paul_Lowry@BYU.edu (P.B. Lowry), Scott_Summers@BYU.edu (S.L. Summers).

0167-9236/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2003.12.001

understanding of the new technology and network-based economy [9].

It follows that as firms become progressively more dependent on Internet-based information systems, they are increasingly vulnerable to defects in those systems. These defects can lead to errors, undetected fraud, and a lack of defense against malicious intrusion. For example, an error in an information system designed for stock trading, banking, or air traffic control can be catastrophic; resulting damages can include lost revenue, lost data, lost trust, and increased costs. [9]

Accordingly, effective design of e-Business processes is essential for the avoidance of defects that could otherwise lead to errors, fraud, and intrusion. Carefully designed e-Business protocols can perform well within most expected situations. Yet guaranteeing correct processing under all circumstances is extremely complex and difficult. Hidden flaws and errors that occur only under unexpected, hard-to-anticipate circumstances can lead to subtle mistakes and potentially ruinous failures. Continued growth of e-Business will in large part depend on protocols designed to ensure that the information exchanged between trading parties is protected from unauthorized disclosure and modification. While the model checking we propose cannot guarantee correct processing under all circumstances, given appropriate specifications of system requirements, those specifications can be accurately verified in the implementation. [7]

Verifying that an e-Business protocol is robust against hidden flaws and errors can be a daunting task. Manual methods are slow and error-prone. Even theorem provers, which provide a formal structure for verifying protocol characteristics, may require human intervention and can be time consuming. Moreover, if a failure is found with a theorem prover, it may provide little help in locating the source of the failure. Simulations offer computational power, but they are ad hoc in nature, and there is no guarantee they will explore all important contingencies. [9]

Model checking, on the other hand, is an evolving technology that offers a platform for effective and efficient evaluation of e-Business protocols. Current model checking technology is based on automated techniques that are considerably faster and more robust than other approaches such as simulation or theorem proving. With the best of today's model checkers, very large state spaces can be analyzed in minutes. Additionally, model checkers are able to extend their analysis by supplying counterexamples that indicate the precise location where a protocol failure is discovered. [6]

While still relatively new to the analysis of e-Business processes [3,4,9], model checking has evidenced impressive performance in the practical analysis of complex hardware and software processes [5,8]. In this paper, we define and extend a state-of-the-art e-Business protocol and use it as the basis to demonstrate how model checking can facilitate analysis of e-Business processes. The protocol we use is more sophisticated and complete than those used by Heintze et al. [4] and Wang et al. [9], as discussed in the next section. This protocol is due mainly to the work of Ray and Ray [6], which incorporates processes fundamental to a broad class of e-Business operations. These processes include distributed processing, parallelism, concurrency, communication uncertainties, and continuous operations.

The remainder of the paper is organized as follows: We first discuss related work on model checking, which has provided a foundation and motivation for our research. We then delineate the processes of a state-of-the-art e-Business model. Our application deals solely with procurement of digitized products, which involves slightly more complex processes than those involving physical goods. This delineation is followed by an implementation of the model in the failures/divergence refinement (FDR) model-checking software. We show in some detail how e-process failures are found and how counterexamples are used to identify the location and type of problem. Finally, we review the motivation for the use of model checking for Internet applications and suggest extensions that might be valuable.

2. Related work

Recent studies cf., [6] are finding that e-Business managers, developers, and auditors require robust tools to assure users that e-Business systems are secure and reliable. Designing and implementing highly secure and reliable e-processes is challenging and requires adherence to several specific criteria to be effective.