Computers and Electrical Engineering 36 (2010) 874–885

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

# Vulnerability analysis of networks to detect multiphase attacks using the actor-based language Rebeca

Hamid Reza Shahriari [a,*], Mohammad Sadegh Makarem [a], Marjan Sirjani [b,c], Rasool Jalili [a], Ali Movaghar [a]

[a] Department of Computer Engineering, Sharif University of Technology, Azadi Avenue, Tehran, Iran
[b] Department of Electrical and Computer Engineering, University of Tehran, Kargar Street, Tehran, Iran
[c] School of Computer Science, Institute for Studies in Theoretical Physics and Mathematics, Niavaran Square, Tehran, Iran

ARTICLE INFO

*Article history:*
Available online 26 June 2008

*Keywords:*
Security analysis
Vulnerability analysis
Actor
Model checking
Rebeca language

ABSTRACT

Increasing use of networks and their complexity make the task of security analysis more and more complicated. Accordingly, automatic verification approaches have received more attention recently. In this paper, we investigate applying of an actor-based language based on reactive objects for analyzing a network environment communicating via Transport Protocol Layer (TCP). The formal foundation of the language and available tools for model checking provide us with formal verification support. Having the model of a typical network including client and server, we show how an attacker may combine simple attacks to construct a complex multiphase attack. We use Rebeca language to model the network of hosts and its model checker to find counter-examples as violations of security of the system. Some simple attacks have been modeled in previous works in this area, here we detect these simple attacks in our model and then verify the model to find more complex attacks which may include simpler attacks as their steps. We choose Rebeca because of its powerful yet simple actor-based paradigm in modeling concurrent and distributed systems. As the real network environment is asynchronous and event-based, Rebeca can be utilized to specify and verify the asynchronous systems, including network protocols.



## 1. Introduction

As computer networks grow in size and complexity, their security analysis becomes more complicated. The evolution of computer networks on one hand and their distributed nature on the other hand, creates opportunities for insiders and outsiders to violate the system security. Many services are perfectly secure when offered in isolation, but when combined with other services, result in an exploitable vulnerability. For example, the file transfer protocol (ftp) and the hypertext transfer protocol (http) offered simultaneously in the same host, may allow the attacker to write in a web directory using the ftp service which causes the web server to execute a program written by the attacker.

Accordingly, security evaluation has become an important requirement in design and management of computer networks. When evaluating the security of a network, it is not enough to consider the single vulnerabilities without considering the other hosts, their relationships, and interactions as well as their network infrastructure. Many of the attacks exploit the global weaknesses in network introduced by interconnections. Nevertheless, the analysis of network security is a complex

* Corresponding author. Present address: Department of Computer Engineering and IT, Amir-Kabir University of Technology, Tehran, Iran. Tel.: + 98 21 64542716; fax: +98 21 66495521.
*E-mail addresses:* shahriari@aut.ac.ir (H.R. Shahriari), makarem@ce.sharif.edu (M.S. Makarem), msirjani@ut.ac.ir (M. Sirjani), jalili@sharif.edu (R. Jalili), movaghar@sharif.edu (A. Movaghar).

0045-7906/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2008.04.009

and error prone task by hand. Thus, the automatic analysis has been considered. Some people have modeled the network in order to analyze and detect different attacks [1–13]. They could analyze the network model to show some simple attacks. Because of the lack of expressive and simple modeling languages, the complex and distributed attacks have not been considered widely.

In this paper, we use a model based approach to show that how an attacker may use simple attacks to construct a complex attack and reach her/his goals, which were not possible using simple attack methods. We use an abstract model of a network in order to find the complex multiphased attack, named Mitnick attack. To the best of our knowledge, this attack has not been modeled.

Multiphase attacks usually are performed using interaction of different network agents. Such environment is well fitted in actor-based computation paradigm. We use Rebeca [14–16] to model a system consisting of a server, a client, an attacker and their TCP protocol stack layer.

Rebeca (*Reactive Objects Language*) is an actor-based language with a formal foundation, presented in [14–16]. A model in Rebeca consists of a set of reactive objects (called rebecs) which are concurrently executing and asynchronously communicating. Rebeca can be considered as a reference model for concurrent computation, based on an operational interpretation of the actor model [20–22]. It is also a platform for developing object-based concurrent systems in practice. Formal verification approaches are used to ensure correctness of concurrent and distributed systems. The Rebeca Verifier tool, as a front-end tool, translates Rebeca code into languages of existing model checkers, allowing verification of their properties[23,24]. There is also an ongoing project on developing a direct model checker for Rebeca using state space reduction techniques [25–27].

We choose Rebeca because of its powerful yet simple actor-based paradigm in modeling concurrent and distributed systems, and easy to use Java-like syntax for software engineers in modeling, and also the naturally decomposable model and independent modules which is exploited in formal verification and model checking as well as in modeling. The network environment is asynchronous and thus is well fitted in fully asynchronous model of Rebeca. Moreover, the object-oriented nature of Rebeca facilitates the modeling in comparison to other languages such as Promela [31].

The next section surveys the related works that have been done in this field; the third section briefly describes Rebeca. Section 4 presents the model, and its analysis is shown in Section 5 and finally we conclude in Section 6.

## 2. Related work

The works published on related topics include a set of works which focus on using model checking to verify and analyze the security of systems and other approaches to analyze network vulnerabilities. The CSP process algebra and its model checker FDR have been widely used to verify the security protocols [10]. It belongs to class of formalisms which combine programming languages and finite state machines. Shahriari and Jalili [1] used CSP to model and analyze the Transmission Control Protocol vulnerabilities in presence of a malicious attacker. They used model checker FDR to find some attack scenarios to TCP in broadcast network. They focused on simple attacks, such as connection reset and connection hijack. In [6] CSP is used to discover de-synchronization attacks on intrusion detection systems. Such attacks occur when the state of the intrusion detection system (IDS) becomes desynchronized from that of the system it aims to protect. In [7] the same authors showed that their analysis is data-independent.

Security analysis has been paid more attention recently in two aspects, the individual host and the network vulnerability analysis. Several tools are proposed for detecting individual host vulnerabilities. These include Nessus vulnerability scanner [28], which scans the hosts to detect vulnerabilities. Similar tools such as System Scanner by ISS [29], and CyberCop by Network Associates [30] scan hosts attempting to discover vulnerabilities in the host configuration. However, they do not attempt to investigate how a combination of configurations on the same host or among hosts on the same network can contribute to the vulnerabilities of a network.

The NetKuang system [11] tries to assess beyond host vulnerability. The system is an extension to its authors' previous work on building a rule-based expert system, named Kuang. They extended the Kuang's rule-set to include certain UNIX network security issues, which are undetectable when searching a single host. NetKuang uses a backtrack search algorithm to accomplish the identification of vulnerabilities.

Dacier and Deswarte [12] proposed the concept of privilege graphs. Each node in a privilege graph represents a set of privileges owned by the user, and edges represent vulnerabilities. Privilege graphs are then explored to construct an attack state graph, which represents different ways in which an intruder may reach a certain goal, such as root access on a host. Ritchey and Ammann [13] used model checking for vulnerability analysis of networks via the model checker SMV [17]. They could obtain one attack corresponding to an unsafe state. The experiment was restricted to specific vulnerabilities. However the model checking approach has been used in some other research to analyze network vulnerabilities by Sheyner et al. in [18]. The expressiveness of the language of the model checker has limited their model.

Ramakrishnan and Sekar [4] used a model checker to analyze a single host system with respect to combinations of unknown vulnerabilities. They presented an abstract model of a simple UNIX system. The key issue in their research is checking of infinite space model using model abstraction. However their approach was limited to the configuration vulnerabilities.

In [19] Bellovin has described some implementation independent flaws in Transmission Control Protocol (TCP). He also presented a variety of attacks based on these flaws. The flaws are specified informally and also the single step attacks have been regarded. In this paper we find multiphase attacks on TCP using actor-based model checking.