

Chapter 9

Security Issues in Distributed Computing System Models

Ghada Farouk Elkabbany

Electronics Research Institute, Egypt

Mohamed Rasslan

Electronics Research Institute, Egypt

ABSTRACT

Distributed computing systems allow homogenous/heterogeneous computers and workstations to act as a computing environment. In this environment, users can uniformly access local and remote resources in order to run processes. Users are not aware of which computers their processes are running on. This might pose some complicated security problems. This chapter provides a security review of distributed systems. It begins with a survey about different and diverse definitions of distributed computing systems in the literature. Different systems are discussed with emphasize on the most recent. Finally, different aspects of distributed systems security and prominent research directions are explored.

INTRODUCTION

A distributed system in computer science is an unified system of distributed computers, processors or processes that communicate together through common communication medium or network in order to transmit messages. This distribution could be physical (over a geographical area) or logically (over a virtual space). It is

DOI: 10.4018/978-1-5225-0741-3.ch009

often represented as a connected graph, the nodes are the computers or processes, and the edges are general bidirectional communication channels or links. One of the earliest definitions of a distributed system has been done by Tanenbaum and Steen (2007) who defined a distributed system as “A collection of independent computers that appears to its users as a single coherent system”. Distributed systems have been built with the objective of attaining the following properties: transparency, openness, reliability, performance, and scalability (Coulouris & Kindberg, 2012). In order to achieve the above objectives, security of the system must be given adequate attention as it is one of the fundamental issues in distributed systems (Coulouris & Kindberg, 2012; Alotaibi, Wald & Argles, 2010).

Integration of different distributed components creates new security problems issues. Hence, security is one of the leading concerns in developing distributed systems. Web, clusters, grids and clouds form the backbone of distributed systems. Distributed systems security provides a holistic insight into current security issues, processes, and solutions. Security shapes future directions in the context of today's distributed systems (Belapurkar et al., 2009). In this research, four common distributed systems are considered for detailed analysis with respect to involved technologies, security issues, and proposed solution. This chapter is organized as follows. Next section presented an introduction to distributed systems, its advantages and challenges. Then commonly used distributed systems are described. Different security issues are presented in the following section. Then a thorough description of different distributed systems security methods described in the literatures is represented. Finally, conclusions and future work are discussed.

BACKGROUND

A distributed computing system is the system architecture that makes a collection of heterogeneous computers or workstations act and behave as being one single computing system. In such a computing environment, users can uniformly access local or remote resources, and run processes from anywhere in the system (Firdous, 2011). A distributed system is a collection of (homogenous/heterogeneous) automata interconnected by a network. Its distribution is transparent to the user. So the system appears as one local machine. In a distributed system, the nodes communicate by sending and receiving messages over the network. Various distributed resources (i.e. files and printers) are shared across the network between the nodes in the form of network services that are provided by *servers*. Individual processes, *clients*, direct request the appropriate server in order to access resources. Thus, a

47 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-issues-in-distributed-computing-system-models/164698

Related Content

Healthcare Information Systems (HCIS) Customer Patient Advocacy: Cyber Health Deficiencies in the State of Washington

Eugene J. Lewis and Ramona R. Cruz (2024). *Evolution of Cross-Sector Cyber Intelligent Markets* (pp. 132-157).

www.irma-international.org/chapter/healthcare-information-systems-hcis-customer-patient-advocacy/338608

Behavioral Modeling of Malicious Objects in a Highly Infected Network Under Quarantine Defence

Yerra Shankar Rao, Prasant Kumar Nayak, Hemraj Saini and Tarini Charana Panda (2019). *International Journal of Information Security and Privacy* (pp. 17-29).

www.irma-international.org/article/behavioral-modeling-of-malicious-objects-in-a-highly-infected-network-under-quarantine-defence/218843

Deep Learning-Based Cryptanalysis of a Simplified AES Cipher

Hicham Grari, Khalid Zine-Dine, Khalid Zine-Dine, Ahmed Azouaoui and Siham Lamzabi (2022). *International Journal of Information Security and Privacy* (pp. 1-16).

www.irma-international.org/article/deep-learning-based-cryptanalysis-of-a-simplified-aes-cipher/300325

Is "Privacy" a Means to Protect the Competition or Advance Objectives of Innovation and Consumer Welfare?

Arletta Gorecka (2020). *Personal Data Protection and Legal Developments in the European Union* (pp. 106-124).

www.irma-international.org/chapter/is-privacy-a-means-to-protect-the-competition-or-advance-objectives-of-innovation-and-consumer-welfare/255195

Trustworthy Web Services: An Experience-Based Model for Trustworthiness Evaluation

Stephen J.H. Yang, Blue C.W. Lan, James S.F. Hsieh and Jen-Yao Chung (2007). *International Journal of Information Security and Privacy* (pp. 1-17).

www.irma-international.org/article/trustworthy-web-services/2453