Chapter 22
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 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 todays 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 (Firdhous, 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 recourses. Thus, a distributed system has three primary characteristics: multiple nodes, interconnections, and shared states. This section provides an introduction to the distributed systems and how to characterize them.

Coulouris et al. (2012) have defined a distributed system as "a system where the hardware and software components have been installed in geographically dispersed computers that coordinate and collaborate their actions by passing messages between them". Tanenbaum & Steen (2007) have defined a distributed system as "a collection of systems that appears to the users as a single system". Combining these definitions, it could be stated that a distributed system is an application that communicates with multiple dispersed hardware and software in order to coordinate the actions of multiple processes running on different autonomous computers over a communication network, so that all components (hardware and software) cooperate together to perform a set of related tasks that are targeted towards a common objective (Firdhous, 2011).

Advantages of Distributed Systems

Distributed system has features over a centralized system such as economics, speed, inherent distribution, and incremental growth. Moreover, distributed computing achieves the following advantages (Srinivasa & Muppalla, 2015):

- **Increased Performance:** The existence of multiple nodes in a distributed system allows applications to be processed in parallel and thus improve the application and system performance.

Related Content

Recent Developments in Cryptography: A Survey
Kannan Balasubramanian (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 1272-1293).*
www.irma-international.org/chapter/recent-developments-in-cryptography/203560

Creating an Instrument for the Manual Coding and Exploration of Group Selfies on the Social Web
Shalin Hai-Jew (2021). *Research Anthology on Recent Trends, Tools, and Implications of Computer Programming (pp. 1446-1508).*
www.irma-international.org/chapter/creating-an-instrument-for-the-manual-coding-and-exploration-of-group-selfies-on-the-social-web/261086

Migration Goals and Risk Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners
Shareeful Islam, Stefan Fenz, Edgar Weippland Christos Kalloniatis (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 419-451).*
www.irma-international.org/chapter/migration-goals-and-risk-management-in-cloud-computing/203517

Cloud Computing Adoption: Scale Development, Measurement and Validation
Pragati Priyadarshinee (2020). *Disruptive Technology: Concepts, Methodologies, Tools, and Applications (pp. 837-858).*
www.irma-international.org/chapter/cloud-computing-adoption/231221

The Formalization of CAME Architecture
Ajantha Dahanayake (2001). *Computer-Aided Method Engineering: Designing CASE Repositories for the 21st Century (pp. 59-94).*
www.irma-international.org/chapter/formalization-came-architecture/6875