Chapter 7
Mobile Agents Security Protocols

Raja Al-Jaljouli
Deakin University, Australia

Jemal Abawajy
Deakin University, Australia

ABSTRACT

Mobile agents are expected to run in partially unknown and untrustworthy environments. They transport from one host to another host through insecure channels and may execute on non-trusted hosts. Thus, they are vulnerable to direct security attacks of intruders and non-trusted hosts. The security of information the agents collect is a fundamental requirement for a trusted implementation of electronic business applications and trade negotiations. This chapter discusses the security protocols presented in the literature that aim to secure the data mobile agents gather while searching the Internet, and identifies the security flaws revealed in the protocols. The protocols are analyzed with respect to the security properties, and the security flaws are identified. Two recent promising protocols that fulfill the various security properties are described. The chapter also introduces common notations used in describing security protocols and describes the security properties of the data that mobile agents gather.

INTRODUCTION

Mobile agents are autonomous programs that can run in heterogeneous environments. They act on behalf of users and have some level of intelligence. They have one or more goals and can control where they execute. They traverse the Internet and get executed on various architectures and platforms to access remote resources or even to meet, cooperate and communicate with other programs and agents to accomplish their goals. Hence, their functionality is not affected by the limitations of latency, connectivity, and bandwidth. Also, they support off-line computations and allow the use of distributed resources on the Internet. Agents can be stationary filtering incoming information

DOI: 10.4018/978-1-4666-4707-7.ch007

or migrating searching for particular information across the Internet and analyzing it. The actions of an agent are not entirely pre-established and defined. They are able to take initiative in an autonomous way and exert control over their actions. The agent is able to choose what to do and in which order according to the external environment and user's requests. Mobile agents traverse the Internet and transport from one host to another host. They are expected to transport through insecure channels and execute on partially unknown and untrustworthy environments. Thus, they are vulnerable to various security threats of intruders and non-trusted hosts.

Several cryptographic protocols were presented in the literature asserting the security of data which agents gather while traversing and searching the Internet. Formal verification of the protocols reveals unforeseen security flaws, such as truncation or manipulation of gathered data, breaching the privacy of gathered data, sending others data under the private key of a malicious host, or replacing gathered data with data of similar agents. The detection of a security flaw implies that the protocol is not satisfactorily secure.

The chapter outlines the security requirements of mobile agent applications and analyzes the security flaws in the existing security protocols. It also discusses two recent security protocols that implement new security techniques on top of the existing techniques. The chapter is organized into six sections. The first section presents a background to mobile agents as regards real-world applications, types of data contained within mobile agents, and protocol's common notations. The second section discusses mobile agent security related issues including threats, properties, and techniques. The third section describes various mobile agent security protocols that are presented in the literature and the respective aimed security properties. It then analyzes the detected security problems and identifies the security properties a respective protocol has failed to accomplish. It also proposes an additional set of security techniques that would rectify the detected security problems and establish protocols that are truly free of security flaws. The fourth section presents two recent mobile agent security protocols that implement new security techniques and are proved to be free of the security flaws by formal methods of verification. They are capable of preventing or detecting the security attacks the existing protocols have even failed to detect. The fifth section outlines the fundamental security specifications a security protocol should fulfill. The last section presents a conclusion that summarizes the security problems and the new security techniques that would rectify the security problems. It also emphasizes on the necessity of modeling and verifying security protocols to identify any security problem that might exist using formal methods.

BACKGROUND

Application Domains of Mobile Agents

Mobile agents are deployed in a wide range of real-world applications (Mobach, 2007; Outtagarts, 2009; Chen, Cheng, & Palen, 2009; Kok, Warmer, & Kamphuis, 2005; Paurobally & Jennings, 2005; James, Cohen, Dodier, Platt, & Palmer, 2006; Al-Jaljouli & Abawajy 2010). Several applications as listed below and particular applications are then discussed.

- Forensic management
- Network management
- Traffic management
- Distributed resource management
- Control in electricity infrastructure
- Web service negotiation and agreement
- Stock management
- Mobile healthcare (E-healthcare)
- Transportation planning
- E-commerce