Chapter 18

A Proposed Architecture for Autonomous Mobile Agent Intrusion Prevention and Malware Defense in Heterogeneous Networks

Robert O. Seale
Colorado Technical University, USA

Kathleen M. Hargiss
Colorado Technical University, USA

ABSTRACT

This paper proposes an architecture that can support autonomous mobile agents performing intrusion prevention activities on a heterogeneous network. The division of duties performed by the agents in the system ensures the agents are able to remain distributed throughout the network architecture to eliminate single points of failure. The distributed nature of the architecture reduces the workload on network clients and eliminates duplication of effort wherever possible. The use of virtual machine interfaces between the hardware and the network connection isolates the hardware interface in order to maintain trust and integrity of the connection and reduce the potential for an attacker using a trusted resource to damage network assets. Virtual machine connections allow a potential malware infection that invades the network environment to be safely observed for unusual behavior patterns using heuristic analysis to provide new evidentiary indicators that can be used to identify the malware during future outbreaks.

INTRODUCTION

Network security measures are cumbersome and often interfere with the flow of productivity by consuming device resources (hard drive space, physical memory, bandwidth, and processor time) without contributing anything to the workflow process (Ibrahim, 2010). As security becomes a greater concern among more individuals and organizations, the number and type of security solutions continues to grow. It is common to find that each device on the network is running an anti-
A Proposed Architecture for Autonomous Mobile Agent Intrusion Prevention and Malware Defense

virus application, a malware detection application, a personal firewall, and even possibly a corporate level Intrusion Detection System (IDS) to detect unauthorized behavior on the network all at the same time (Hanjung, Nazereth, & Jain, 2010). All of these types of applications have grown in size and complexity to provide the user with dozens of tools that are mostly unused (code bloat) in order for developers to extol the benefits of their security tool over another in a free market competitive environment (Grossklags & Johnson, 2009). Although many of these all-in-one tools seem to be more effective, they usually only succeed in tying up system resources to the point where the user requirements becomes a secondary consideration after security and the security solution’s overall effectiveness remains a less than perfect solution to the security problem.

Geographically separated and loosely connected heterogeneous networks often connected via the Internet present an additional challenge to security professionals in not only determining which devices to trust, but also in creating and maintaining a standard level of security for all systems associated with that network (Brumley, 2009). Attempting to regulate security policies between associated network resource owners most often results in an uneven and inconsistent application of those policies on the heterogeneous network that are often comprised of several partner or sibling organizations (Pfleeger & Pfleeger, 2007). The solution to this problem requires that security measures are not necessarily device or organization dependent and can dynamically adjust to changing network environments without manual reconfiguration. Autonomous mobile agents are especially well suited for the heterogeneous network environment due to their ability to traverse an entire network while performing specific tasks along the way, communicating and collaborating with other agents, and enforcing network policies on all interconnected devices on the network (Russell & Norvig, 2010).

Mobile agents have one distinct disadvantage in the network environment in that they must be able to operate on different operating system platforms for all systems attempting to connect to the network (Bellavista, Corradi, Federici, Montanari, & Tibaldi, 2003). Although there are numerous platform independent operating environments available as suitable candidates, there is no guarantee that any one environment will be available as a preinstalled option at the time a device is first connected to a network. A device on the network that remains uninitiated and capable of running malicious code represents a threat to the overall security of that network; thus, an important aspect of the mobile agent paradigm is to address the involuntary initiation of a device connecting to the network before network resources are allowed to be shared with that device.

This paper focuses on the overall system architecture, device initiation, agent mobility and transport, agent communication, and agent protection in an autonomous mobile agent intrusion prevention system. The goal is not to limit the choices to a few technologies that may or may not be a suitable architecture; rather, it is to provide a conceptual framework that can lead to the deployment of an operational system. The following sections provide a brief background of previous works involving the use of mobile agents and computer security; introduces the key roles for agent players within the system architecture; discusses system architecture, agent mobility and transport, agent communication; and lastly addresses the protection of mobile agents in transit between hosts.

BACKGROUND

References to the use of mobile agents that can be found in studies conducted as far back as the 1960s where mobile code was used to execute remote job entries (Jansen & Karygiannis, 1999).