

# Secure Mobile Agents for Network Vulnerability Scanning

Jeffrey W. Humphries and Udo W. Pooch  
{jeffhump, pooch} @cs.tamu.edu  
Texas A&M University

## Purpose

The rapid increase in attacks on computer systems has made security concerns increasingly important in academic, corporate, and government networks. The ability to constantly monitor an organization's networks for both old and new vulnerabilities is critical to securing a system before it is attacked. While vulnerability scanning is not a new technology, mobile agents offer many advantages to traditional implementations. The most significant contribution is the increased ability for system administrators to quickly and easily add distributed components to an existing system which can look for newly published vulnerabilities. Service customization is a major asset provided by code mobility because it requires little work to alter an agent to perform a new function. Mobile agents, however, can be a major disadvantage if they are not secure, because they offer a tempting target to would-be attackers. Therefore, a vulnerability scanning system has been designed using secure mobile agents that is easy to customize and is also resistant to attack.

## Method

We suggest a methodology and architecture for building vulnerability scanning systems using secure mobile agents. This architecture supports the defense of computer systems through secure, mobile agent-based distributed components. The architecture ensures agent confidentiality, integrity, and availability through the use of cryptographic methods. The confidentiality of mobile agent code and data is protected during transit between hosts. The integrity of mobile agent code is monitored so that any changes to an agent are detected. The integrity and confidentiality of vulnerability data collected during an agent's lifetime is ensured so that subsequent hosts cannot view this data or make changes without detection. Unauthorized changes to an agent's path itinerary are also detected. The system can also protect mobile agents from denial-of-service attacks in that malicious or malfunctioning hosts that attempt to remove or suspend agents will be detected. Finally, the system provides authentication of both agents and hosts to prevent spoofing and other attacks.

## Results

The requirements for building a vulnerability scanning system using mobile agents have been developed. A prototype to implement the basic features of such a system and to build hosts for its mobile agents has also been designed. This design addresses the following issues. Servers must be built to handle the creation, transportation, and execution of mobile agents traversing the system. Servers assume access to a public key infrastructure in order to decrypt, encrypt, sign, and authenticate components of mobile agents. A prototype to demonstrate the principles of securing these mobile agents is currently being implemented. The results will demonstrate the system's ability to protect the confidentiality of mobile agents as they travel between hosts, to protect the availability of mobile agents by ensuring that the system is resilient against unintentional or malicious denial of service attacks, and to protect the integrity of mobile agent code and data. Several useful mobile agents are being developed to demonstrate their ability to be protected while performing vulnerability scanning activities.

## Novel Contribution

The principle contribution of this paper is to introduce a methodology and architecture for the use of security mechanisms to protect mobile agents while performing vulnerability analysis. To date, no other vulnerability analysis tool has attempted to use secure mobile agents as the core component in its implementation.

## Conclusions

Secure mobile agents offer significant contributions in network vulnerability scanning. Because they are easily customizable, agents can be quickly built to scan for new vulnerabilities as they are published. In addition, this system scales well to larger networks because more agents can be easily added to increase host coverage. Securing the agents ensures that an intruder does not get access to information on system vulnerabilities and cannot modify these agents for malicious purposes.