International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 67-72

http://www. irphouse.com /ijict.htm

Trust Model for Hybrid Security Architecture Based on Reputation for Secure Execution of Mobile Agents

Heman Pathak

Dept. of Comp. Sc., GKV, Haridwar, Uttarakhand, India.

Abstract

Mobile Agents (MA) are software programs that live in computer networks, performing their computations and moving from host to host as necessary to fulfill user goals. MA technology has gained popularity in the world of computing for various applications, but securing MAs, as they move from one machine to the other, has been the challenge that hinders full adoption of this technology by organizations. Autonomous behavior of MA and the malicious environment of the internet give rise to various important security issues related with both MA and its host. The major security threats are either threats against the hosts, or threats against the MA. MA security problem is a complex problem and require a multifold solution. This paper presents Hybrid Security Architecture (HAS) inspired by the various existing security techniques including digital signature, encryption, intrusion detections, signed agreement, trust and others. Since all are well studied and experimented techniques, paper does not discuss all in details. This paper explores the trust model based on reputation to provide security to both MA and executing host. Proposed approach divides the network into regions where a centralized component in each region is responsible to compute the Reputation Value (RV) for each incoming and outgoing MAs. Each region maintains a Local Reputation Table for MAs. A Global Reputation Table (GRT) is also maintains which only stores the information about the suspicious or malicious MAs. GRT is concern only when local data are insufficient to make decision about the trust worthiness of MA. Behavior of MA and host are watched during execution and analyzed to update their RV.

Keywords: Mobile Agents (MA), Mobile Agent Systems (MAS), Security, Reputation, Trust Management.

1. Introduction

MA requires an execution environment to get executed on a host. Mobile Agent System (MAS) installed at host provide the execution environment to MA. Execution environment is generally referred as place or platform for MA. Mobile agent technology has gained popularity in the world of computing to enable easiest way of service provisioning, information sharing and service recovery, but securing mobile agents, as they move from one machine to the other, has been the challenge that hinders full adoption of this technology by organizations. Autonomous behavior of MA and the malicious environment of the internet give rise to various important security issues related with both MA and its host (Ahmed 2010). There are various security attacks identified by researchers on Mobile Agent Systems (MAS). The major security threats are either threats against the hosts, or threats against the MA.

Reputation and trust management systems have been useful in situations that involve interaction between mutually distrusting parties to function correctly and to fulfill their purposes (De Capitani 2012). Trust Management System based on reputation gained popularity in recent time for estimating the trustworthiness and predicting the future behavior of nodes and other network entities in a large-scale distributed system where they interact with one another to share resources without prior knowledge or experience. Trust and reputation have gained importance in diverse fields such as economics, evolutionary biology, distributed artificial intelligence, grid computing, and agent technology, among others. Many researchers have proposed different approaches to compute reputation/trust value to evaluate the trust worthiness of the entities involved. Approaches mainly differ based on the system model they have used, entity for which trust worthiness has been computed and area of application where this concept is to be used, as the term trust and reputation can be used anywhere in social, economical and technical domains. M.T. Nkosi has summarizes the work of various researchers in the field of reputation and trust (Habib 2011)(Hoffman 2009)(Nkosi 2007).

2. Hybrid Security Architecture (HSA)

This paper explores the trust model based on reputation to provide security to both MA and executing host. Proposed approach divides the open network like internet into regions and then assigns the responsibility to one of the centralized component within the region to implement security features to protect malicious host and MA from each other. Instead of doing a logical partitioning of the network into regions and then arranging these regions into hierarchy, we use the existing technology to serve our purpose(Pathak 2010, 2011).

Internet is network of networks. Networks are connected with each other via router (Patel 2004). Proposed approach treats each network as a region and router as the centralized component in each region. Router in proposed architecture is not passive but plays an active role. A MA wishes to visit a host within a network, first arrive at the router of the network and then only pass to the designated host. Host in a network offer services and provide an executing environment to the MA to be executed. A host

may be malicious and may tamper the executing MA. Similarly a malicious MA can harm the host in many ways so both need to be protected from each other. Routers are assumed to be fault-free and trustworthy. In each network there is a shared local storage space (LSS), assumed to be fault free and trust worthy. Figure-1 shows the basic architecture and different components of HAS.

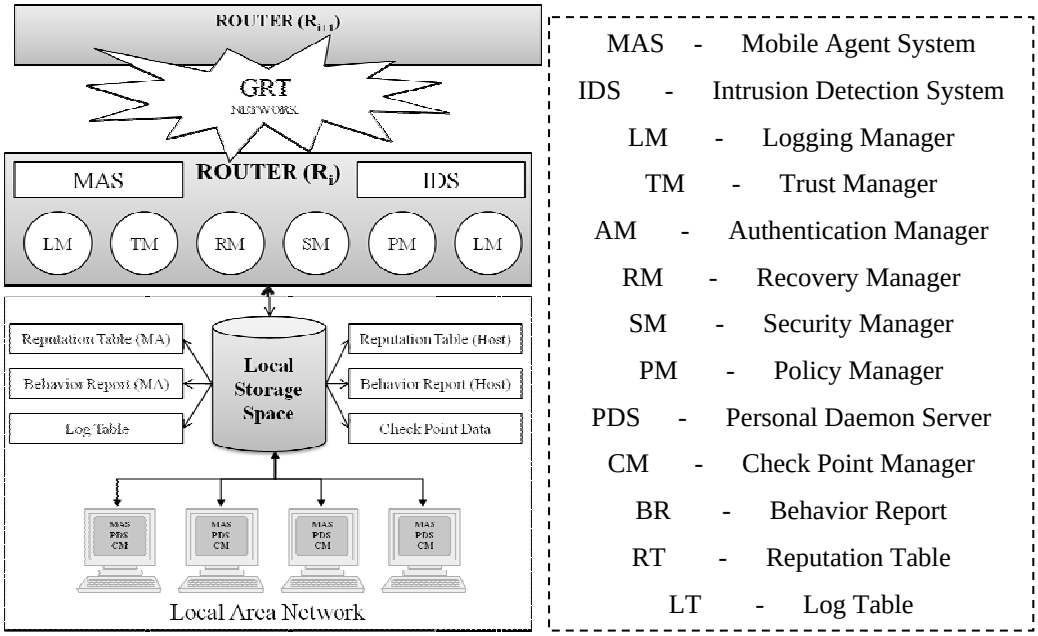

Fig. 1: Trust based Hybrid Security Architecture (HAS) and all its Components.

3. System Components

Hosts are static component of the system and its behavior can be watched locally while MA is a moving entity and its behavior is watched by various components distributed across the network. To compute the reputation value (RV) for the MA, observations of each entity interacted with MA must be compiled. For this I propose to maintain **Global Reputation Table (GRT)**. This table is accessible to all the routers and assumed to fault free and trust worthy. This table is concerned only when information gathered locally or from source router of MA is insufficient to make decision about the RV of the MA.

Internet is network of networks and in each network Hardware components of the system involve in identifying the malicious MA/Host and providing security to them are Router, Agent Server/Host and Local Shared Storage Space (LSS).

3.1 Router

Each MA enters in to a local network or migrates from the network via router. Router is a centralized component within each network. It is responsible to detect a malicious host within the network. It also checks the status of incoming MAs as malicious or not

and block the malicious MA within the network. Software components other than MAS installed at router and their descriptions are discussed in the following section.

3.2 Intrusion Detector System (IDS)
An IDS is installed at the router to detect the behavior of host IDS randomly creates intruder MA and execute it on various hosts and record their behavior. Based on the reports a host is tagged RV is updated in LRT.

3.3. Logging Manager (LM)
This s/w routine is responsible to Log an arrival and departure entry in log table for each MA received and migrated from the network respectively. It is used for tracing the MA path and for recovery from a fault state.

3.4 Trust Manager (TM)
This s/w routine installed on router is responsible for computing reputation value (RV) for all incoming and outgoing MA via router. It also maintains the reputation value of the hosts, part of the network.

3.5 Authentication Manager (AM)
Once a MA is found trustworthy, this s/w component checks access rights of MA and authenticate MA based on digital signature. It also verifies its code and data by using public and private key mechanism.

3.6 Recovery Manager
It is responsible to initiate recovery procedure in case a MA or host is found malicious. Recovery procedure is quite complex and lots of policy and legal issues are involved with it, so not discussed in this paper.

3.7 Host
Host is a computer in the network which offers services to the MA. A MA is passed to be executed on a Host only if both MA and host are found trustworthy. To ensure the trustworthiness of both, some of the security components are installed at the host. Following section discuss these components.

3.8 Personal Domain Server (PDS)
PDS is a proxy server, installed at each Host. It maintains a thread to watch the behavior of the host. When a MA is arrived at a host for execution, it starts threads to record the behavior of MA and executing platform. Executing After the execution of MA, it prepares and store reports for at the local shared storage space.

3.9 Checkpoint Manager (CM)

This is responsible to save the MA and its execution state to LSS periodically and after every successful transaction. This checkpoint data is used to recover the MA and host if attacked by of malicious entity.

3.10 Local Shared Storage Space (LSSS)

Each network is assumed to maintain a fault free storage space. This space is accessible by all hosts and components installed at router. It is used to store Log Table, behavior report of MA and Hosts, reputation table for MA and hosts.

4. Reputation Value Computation

Researchers have proposed various ways to compute RV based on their model and application (Onolaja 2011). Based on the experience gained by the prior work we propose a new way to compute RV. RV assigned to an agent or host is divided into five groups and used to tag them as Malicious, Suspicious, Unknown, Trusted or Highly Trusted.

4.1 Reputation Value Computation for Host

Initial RV for a host is *Unknown*. RV stored in LRT for host is $RV_h(OLD)$. TM analyze the report submitted by the PDS and the executing MA and compute two RV for host as $RV_h(PDS)$ and $RV_h(MA)$. Different weighs are assigned to each W_{oh},W_{ph} and W_{mh} for $RV_h(OLD)$, $RV_h(PDS)$ and $RV_h(MA)$. Maximum weights are assigned to the newly computed values. RV of the MA is used as weight for $RV_h(MA)$. W_{oh} and W_{ph} then selected such that ($W_{ph} > W_{mh} > W_{oh}$). TM then compute $RV_h(NEW)$ as –

$$RV_h(NEW) = W_{oh}*RV_h(OLD) + W_{ph}*RV_h(PDS) + W_{oh}*RV_h(MA)$$

IDS installed at router also observe the behavior of host and compute the $RV_h(IDS)$ as –$RV_h(NEW)=W_{oh}*RV_h(OLD)+W_{ih}*RV_h(IDS)$

4.2 Reputation Value Computation for MA

The RV for a newly created MA is same as the RV of its creator host as $\mathbf{RV_m = RV_h}$. For an incoming MA, TM collects the RV of the MA from the last visited router as $\mathbf{RV_m}(LVR)$. Local Reputation Table (LRT) for MA is also consulted to get the RV of incoming MA as $RV_m(OLD)$. Compute the $RV_m(NEW)$ as average of and $RV_m(LVR)$ and $RV_m(OLD)$. If no old RV_m is found or if data are not sufficient to make decision, GRT is consulted to check if MA suspicious or malicious, RV is then modified accordingly. If MA is found trusted it is passed to AM else to RM. In order to compute final RV different weights are assigned to different RVs.

When a MA get executed at a host and ready to migrate from the network, based on the report submitted by the PDS, $\mathbf{RV_m}(PDS)$ is computed by TM. Weighs W_{om} and W_{pm} are then assigned to $RV_m(OLD)$ and $RV_m(PDS)$. RV of the host has been used as weight for $RV_m(PDS)$ as $W_{pm} = RV_h$. Appropriate values for W_{om} is selected such that ($W_{pm} > W_{om}$). TM then compute $RV_m(NEW)$ as-

$$RV_m(NEW)=W_{om}*RV_m(OLD) + W_{pm}*RV_m(PDS)$$

5. Conclusion

In the proposed architecture, only trusted MAs are transferred to the host and host gets protected from the attack of malicious MA. Also during the execution, behavior of MA is recorded and CM saves the MA and its execution state in the LSS periodically. In case MA attacks the host during execution, this attack can be detected and RM can use the checkpoint data to bring the host in consistent state. Since MA is allowed only to be executed on trusted host, it gets protected from the attack of the malicious host. Even during the execution if it has been attacked, RM can rollback all MA execution and recover it from checkpoint data.

So, the proposed architecture logically secures the MA and Host both from malicious attack. Various components of the system work collectively to provide solution to the said problem. Since the proposed architecture has yet not been implemented or modeled, its practicality is still to be tested. Since most of the approaches used here are well known and has already been implemented successfully so it is quite reasonable to accept that, this architecture once implemented will solve the concern issues successfully. Its efficiency or comparative performance analysis is possible only after the implementation.

References

[1] Ahmed Patel, Wei Qi and Christopher Wills, 2010. A Review and Future Research Directions of Secure and Trustworthy Mobile Agent-based E-marketplace Systems. Information Management and Computer Security, Vol. 18, issue No. 3, pp xx-xx, 2010.

[2] De Capitani di Vimercati, S.Foresti, S.Jajodia et al. Integrating Trust Management and Access Control in Data Intensive Web Applications,ACM Transactions on the Web (TWEB) 6,2, 1-44 (2012).

[3] Habib S., Ries S., Muhlhauser, M., Towards a Trust Management System for Cloud Computing, In Proc. of IEEE 10th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom'11). Changsha, China (2011)

[4] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Computing Surveys 42 (1)(2009) 1–31

[5] Nkosi M.T, Adigun M.O., Emuoyibofarhe J.O., 2007. Agent-To-Agent Reputation-Based Trust Management. IADIS International Conference Applied Computing 2007.

[6] O. Onolaja, G. Theodoropoulos R. Bahsoon,, A Data-Driven Framework for Dynamic Trust Management, Procedia Computer Science Procedia Computer Science 4 (2011) 1751–1760.

[7] Patel, R.B. 2004. Design and implementation of a secure mobile agent platform for distributed computing', PhD Thesis, Department of Electronics and Computer Engineering, IIT Roorkee, India, Aug.

[8] Pathak H., A Novel Hybrid Security Architecture (HSA) to provide security to Mobile Agents and the Executing Host, Proceedings of the International Conference on Communication, Computing & Security Pages 499-502, Rourkela, 2011.

[9] Pathak H., A Novel Flexible and Reliable Hybrid approach to provide Security to Mobile Agents and the Executing Host, Proceedings of the International Conference on Electronics, Information and Communication Systems Engineering (ICEICE-2010),Jodhpur.