Multi-agent System for Security Service

Elhadi Shakshuki, Zhonghai Luo, Jing Gong and Qian Chen

Published at: Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
Qualis: A2
Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1283928
ROADMAP

- Article Introduction
- Article Presentation
- Why Agents?
- Q&A?
The paper proposes a multi-agent security service system architecture.

The main objective of the system is to act as a middleware between users and the network.

There are four types of agents: Interface, Authentication, Authorization, and Service Provider agents.

A prototype was implemented using JADE.

Authentication agents have biometrics authentication capabilities (keystroke dynamics).
The Interface Agent (IA)
The Authentication Agent (ATA)
Authorization Agents (AUA)
The Native Authorization Agent (NAA)
The Foreign Authorization Agent (FAA)
The Foreign Delegation Agent (FDA)
Service Provider Agents (SPA)
The Service Provider Master Agent (SPMA)
The VIP Service Provider Agent (SPA-VIP)
The Normal Service Provider Agent (SPA-NOR)
The Interface Agent (IA)

- the users’ intelligent interface to the system, which allows the user to interact with the security service environment

- Performs the following actions:
  - Receives Login/Password Strings from users and forwards them to the ATA.
  - Receives keystrokes dynamics and forwards them to the ATA.
  - Receives Authentication results from the ATA and returns them to the users.
  - Receives Service Requests from authenticated users and forwards them to the AUA.
  - Receives Authorization results from the AUA and displays them to the user.
  - Receives the service results from service provider agent and display them to the user.
Interface Agent

User

Login/Password Domain
Keystroke Dynamics
Service Request
Access Denied

Request Results

Communications Module

IA

Login/Password Domain
Keystroke Dynamics
Authentication results

Authentication results

Access Denied

Access Granted. Request Forwarded

Access Denied

Authenticated user Data

ATA

AUA

SPMA/SPA

Authenticated user Data
Authentication Agent (ATA)

- Verifies login account and password match
- Produces a biometric template from keystroke dynamics
- Matches the supplied biometric template against the one previously stored in the user’s KB
- Sends authenticated user’s data [account, domain type (local, foreign), user type (VIP, NORMAL) and service level (RBAC, SLA)] to the AUA.

Composed by 3 modules:
- Communications
- Learning/Training
- Validation
Native Authorization Agent (NAA)

- Process local authenticated users’ requests with local ACL rules.
- Forward the request to the SPMA if the access is granted
- Return Access denied messages to the IA if ACL rules fails.
Foreign Authorization Agent (FAA)

- Receives authenticated foreign requests from the authentication agent and validates them.
- Checks if the request service level within the scope of the entitled service range.
- Engages in negotiation with the FDA to determine an appropriate service level.
- If the negotiation succeeds, the FAA informs the SPMA to conduct services in this specific level. Otherwise, the FAA returns the Access Denied message to the IA.
Foreign Delegation Agent (FDA)

- Responsible for delegating foreign users to get the highest level of service quality through negotiation with FAA
- In other words, it recommends the appropriate quality of service for foreign users based in foreign users policies and “distributed trust” which is a contract between domains.
- However, it is the FAA makes the final decision on accept or deny FDA offers and to grant or deny foreign users’ requests
FAA and FDA Architecture
Service Provider Master Agent (SPMA)

- Receives all authorized services requests
- Acts as a dispatching center for SPAs
- Registers SPAs.
- Manages systems resources usage
- Uses service level information, policy rules, KB and the resource usage information to reach a decision (what decision? speculate)
SPMA Architecture
Service Provider Agent (SPA)

- Receives requests from the SPMA
- Processes the request
- Cooperates with other agents (offers help), if registered as a SPA-NOR.
- Asks for help of other SPA-NOR agents if overloaded
- Decides if help requests will be accepted or declined
- Does not offer or accept help requests from other agents, if registered as SPA-VIP
- Return the results to the IA
- Offers encryption services such as symmetric or PKI encryption/decryption
SPA-VIP

- Processes requests for VIP users
- Asks for help from SPA-NOR agents, if overloaded, and keep asking until a non overloaded SPA-NOR accepts the request or until it is no longer overloaded
- Selfish behavior
- Has knowledge of every SPA-NOR agent
SPA-NOR

- Processes requests for Normal or VIP users
- Asks for help from other SPA-NOR agents, if overloaded, and keep asking until a non overloaded SPA-NOR accepts the request or until it is no longer overloaded
- Cooperative behavior. Will always honor help requests, unless it is overloaded.
- Has knowledge of every SPA-NOR agent but does not see SPA-VIP agents
Service Provider Agent (SPA)
Why Agents?

- “The use of this system has shown how the system could be used to increase the flexibility, stability and efficiency of a security service for individuals in distributed systems environments” (from the paper)
- Is it possible to implement the proposed system without agents?
- Would it be more or less complex?
- Is it good or bad, that each agent does not have full knowledge of the entire system?
- What would happen if the system is implemented as a multi-thread system?
Questions or Suggestions?