An Authentication Protocol for Agent Platform Security Manager

Gustavo A. Santana Torrellas and Leonid B. Sheremetov

Published at: ETFA-03 IEEE International Conference on Emerging Technologies and Factory Automation
Qualis: B1
Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1247764
ROADMAP

- Article Introduction
- Article Presentation
- Why the Cryptographic Agent?
- Article Conclusions
- How does the paper support our approach?
- Q&A?
Article Introduction

- The paper proposes an authentication platform for MAS.
- The platform is FIPA compliant.
- The security risks of agent-based systems were analyzed.
- Future works addresses the need to prevent malicious agent execution.
- The authors do not propose any solution for malicious agents cooperative attacks.
- No implementation has been made so far.
- The platform requires a cryptographic agent in its architecture.
Article Presentation

- The Security Risks of MAS and how to deal with them?
- The Platform Architecture
- Article conclusions
The Security Risks of MAS and how to deal with them?

❖ “A security service is a software or hardware layer that exports a safe interface out of an unprotected and possibly dangerous primitive service” from the authors

❖ The possible security risks in an Open Agent environment are:
  Misuse of execution environment by mobile agents
  Misuse of agents by other agents
  Misuse of agents by the execution environment
  Misuse by the underlying network infrastructure
Security Threats

- **Alteration**: The unauthorized modification or corruption of an agent, its state, or data
- **Copy and Replay**: An attempt to copy an agent, or a message, and clone or retransmit it
- **Denial of Service**: An attack that attempts to deny resources to the platform or an agent
- **Repudiation**: An agent, or agent platform, denies that it has received or sent a message or taken a specific action
- **Spoofing and Masquerading**: An unauthorized agent, or agent platform, claims the identity of another, authorized or unauthorized, agent or agent platform
Solutions

- **Confidentiality**: “encrypted messages exchanged among agents are difficult to eavesdrop”.

- **Integrity**: one way hash

- **Authentication**: “The identity of an agent must be verified”.

- **Non-Repudiation**: “The agent requests a level of authentication, integrity, and confidentiality to ensure non-repudiation and receives verifying information”
The Platform Architecture

Component Agent Platform

- Agent
- Directory Facilitator
- Agent Management System

- Credential Management
- Policy Manager
- Crypto Agent

Agent Platform Security Manager

Internal Message Transport
The Agent Management System (AMS)

- The AMS is responsible for managing the administrative activities of an agent platform, including creation / deletion of agents, registration of agents at the platform, and control over access to and use of the KCC (Commutation Center Key).

- There is only one AMS for each agent platform.

- The AMS for the platform on which an agent is created is called the home agent platform

- It is responsible for vouching for an agent’s identity.

- Trust must begin with the AMS.

- Probably possesses an PKI pair
Directory Facilitator

- Repository for FIPA parameters
- Repository for agent certificates
- Engages in negotiation with the FDA to determine an appropriate service level.
- Receives queries and returns results of registered agents
Agent Platform Security Manager (APSM)

- The APSM is responsible for maintaining platform and infrastructure security policies, and for run-time activities, such as, communications, providing transport-level security, and creating audit trails.
- The APSM is responsible for negotiating the requested inter and intra-domain security services with other APSM's on behalf of the agents in its domain.
- The APSM is responsible for enforcing the security policy of its domain, and can at its discretion, upgrade the level of security requested by an agent.
- The APSM cannot downgrade the level of services requested by an agent but must inform the agent that the service level requested cannot be provided [FIPA98].
Credential Manager

- Verifies that the agent was created or distributed by the claiming principals
- Verifies that the component hasn't been altered after it has been signed (non-repudiation) need so that the
- Credentials are stored in the credential database.
Policy Manager

- The Policy Manager is responsible for managing the policy schemes stored in the policy database.
- The security policy defines the access each agent has to resources.
- Signed agents can run with different privileges based on the identity of the person who signed it.
Cryptographic Agent

- Provides Encryption and Decryption Services
- Activated by the APMS whenever encryption or decryption is needed
Why the Cryptographic Agent?

““It was decided that cryptographic mechanisms should not be built into the APMS by itself, but rather be modeled as a Service agent.”

“The advantage of this modular design was that other components (even mobile agents) could use the functionality offered by CryptoAgent. Furthermore, the platform could be made unaware of any additions or changes to cryptographic functions offered by this agent”.”
Article Conclusions and Future Works

- “Adding security after the design phase has been shown to be difficult, expensive and inadequate”
- “We have showed that benefits such as simplicity, scalability, flexibility, interoperability, performance and safety have been addressed successfully”
- The architecture tries to prevent code execution of malicious agents
- Implementing “guard” agents. These agents could monitor the environment and terminate agents believed to be harmful
How does the paper support our approach?

- The paper uses an agent exclusively for encryption and decryption services. Our approach uses two instead.
- The Authentication manager provides symmetric key encryption and decryption, session key renegotiation, public key encryption and verification of digital signatures.
- The Private Key Operations Agent is the only software component with knowledge and access to the Private Key, therefore it is responsible to decrypt messages with the Private Key and Generation of Digital Signatures.
- Our approach provides greater security.
Questions or Suggestions?