IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4540

An XML-based Security Protocol for Semi-Autonomous Agents

Allen Johnston and Merrill Warkentin
Computer Systems Administrator, Management & Information Systems
Engineering Research Center, College of Business & Industry
Mississippi State University, Box 9627, P.O. Box 9581
MS STATE, MS 39762-9627, MS STATE, MS 39762-9581
Phone: (662) 325-4900, Phone: (662) 325-1955
Fax: (662) 325-7692, Fax: (662) 325-8651

ABSTRACT

Future inter-networking environments will be characterized by extensive interactions between multiple servers and their agents. This hyper-interactive environment will expose all parties to significant new risks and liabilities. It will be imperative that intelligent agent behavior be guided by the prescribed intentions of the agent owners who develop and introduce them. The XML-based protocol presented in this paper, if widely adopted by agent developers, provides a practical method for ensuring such compliance. Agents embedded with these protocols will exhibit behavior consistent with the predetermined security position of the owner along several key continua, while still enabling independent autonomous control. A proposal for this XML protocol is presented, along with suggestions for future research.

AGENTS AND MULTI-AGENT SYSTEMS

Modern systems architectures are highly interconnected – the TCP/IP protocol enables nearly all network systems to be inter-operable. In this environment, many organizations are deploying intelligent software agents, which can act on behalf of the agents' owners in various ways (Chan et al., 1999; Gannon, 1998; Grimes, 1998). Agents can automate various activities and act on behalf of their owner in problem solving and decision making activities, repetitive tasks, finding and filtering information, and intelligently summarizing complex data. Just like their human counterparts, intelligent agents have the capability to identify patterns in their environment, to learn from their owners, and even to make recommendations to their owners regarding a particular course of action.

Consideration of the dynamics of an agent-based system requires the recognition of three basic components: external environment, internal environment, and information structure among autonomous agents (Szczerbicki, 1996b). An information structure is formed by the exchange of messages between external and internal agents and facilitates various forms of collaboration among agents (Lashkari et al., 1994). However, communicating agents must share a common syntax and protocol regardless of the origin of the agents.

Multi-agent systems (MAS), and agent communications in particular, lack explicit design regulations. Inherent in the design goals of the Extensible Markup Language (XML) is its extensibility, flexibility and ease of use. Because it is extensible, XML can be applied to a variety of applications for which data do not have a standardized structure. Therefore, XML provides a useful method for creating meaningful semantics that can easily be expressed and understood by software agents (Shiau et al., 2000) during agent communications.

SECURITY CONSIDERATIONS

Early research into security considerations theorized two methods for agent development and trust measurement (Maes, 1994). Applying a semi-autonomous approach to software agent development provides an increased level of trust. However, this method requires a high skill level on behalf of the programmer, as well as a high level of insight of the domain in which the agent will exist. A "knowledge-based approach" would allow the agent to use programmed knowledge to adapt and contribute to an objective. However, this approach provides a lesser degree of trust to the user due to its higher degree of autonomy. Although the intelligent agent can perceive its domain and respond proactively, the manner in which it responds may not be consistent with the security posture desired by the agent deployer.

To facilitate the process of secure agent development, the characteristics of agent information exchange must be identified. The characteristics must be considered in a broad sense because of the dynamic nature of risk identification. Consider the risk associated with an electronic commerce (e-commerce) transaction. Personal information is often required by business entities prior to a sale, service, or license activation. When dealing with the dissemination of personal identity information, a certain amount of risk of identity manipulation can be expected. Additionally, the risk associated with the knowledge of an agent's history is significant. An agent's deployer may not want to provide a history of previous agent destinations or communications. If considered from a "brick and mortar" perspective, a potential customer of an establishment might not want to provide the details of where he or she had shopped prior to this visit. Finally, agent task information provides the details of the operating goals of the agent. This information consists of domain search goals, price strategies, and other product search criteria. This type of information, if intercepted unbeknownst to the deployer, can be used in a manner that negatively impacts the ability of the agent to perform its tasks.

Based upon these risks, three categories of information involved in agent communications are proposed. The categories are Personal Information, Agent and Host Information, and Agent Task Information (see Table 1).

Within each broad category, there are subcategories that contain the actual information objects, or risk objects, such as name, address, and telephone number. Within any particular agent, each instance of such objects may have a current value. This approach is intended to provide flexibility for the addition or deletion of risk objects depending

Table 1. Categorized Agent Information

Personal Information

- Identification data such as name, address, social security number
- Financial data such as credit history, income, account balances
- Medical data such as insurance coverage, medical history
- Legal data such as legal history, parole status

Agent and Host Information

- Agent source address
- Agent destination address history
- Agent communication history with hosts or agents
- Host address
- Host communication history with agents

Agent Task Information

- Agent task goals
- Task data such as host domain goals (.com, .edu, etc.), price considerations

upon their applicability to various domains. The value assigned to a particular risk object represents an agent’s desire for relative openness in information exchange. The proposed logic that drives the agent’s intelligence will assume a risk object that does not contain a value to be private and not available for disclosure.

SECURITY SOLUTION

One primary goal of any security system implementation is to increase the level of user confidence in the system. XML statements within multi-agent systems can be used as a method for providing a secure structure within which to define security protocols. The protocols, or rule structures developed to dictate the actions of the agents, will derive from insight into the security aspects of agent-to-agent, agent-to-host, and host-to-host communications.

The information exchange that occurs in agent communications can be defined or limited by an established set of protocols that promote the security posture desired by the deploying host. This posture is unique to the mission of the agent and may vary depending on a multitude of circumstances and influences. Examples of agent delimitations based on deployer preference include restricting the range of hosts and agents with which it can interact and limiting the types of information it can retrieve and provide in agent-to-agent or agent-to-host communications. A rule-based system (RBS) approach can be employed to generate a risk assessment conclusion based on tacit knowledge of the risks involved in information exchange. The conclusion can be any action or stance such as to close communications or to proceed with a financial data exchange.

A rule set can be established for risk assessment prior to, and separate from, any knowledge of the specific risk objects defined for an agent. The RBS approach also allows layers of rules to be established, whereby each layer is specific to a particular type of knowledge. This layered approach allows knowledge to be applied in a modular fashion, pseudo-independent from additional layers (Dhar et al., 1997). Following an RBS model, a series of “if-then” statements can be constructed that will comprise the lowest layer. These rules will form the logic necessary to meet a conclusion that accurately reflects the desired security posture of the agent owner based on the risk parameters and values provided by the agent. When an agent, populated with a desired set of risk object-value pairs, encounters another agent or host, the unknown agent or host must be able to provide an adequate set of object-value pairs for rule instantiation. If the communicating party cannot supply the required data for first level rule instantiation, the communication must be aborted.

The required object-value pairs will be determined by either agent or host involved in the communication. This process of evaluating minimum trust requirements is referred to as intent evaluation. An agent must be able to assess the communicating device’s intent for information sharing; therefore, rules must be formed to guarantee a break in communications if the situation warrants. Therefore, agents must also be equipped with the necessary logic for negotiating a restricted message exchange, and the message format must be flexible enough to provide agents the ability to vary the amount of information obtained or gathered. Assuming the intent evaluation was successful, an agent must be able to assess the security posture of another agent or host, even if some object-value pairs are unavailable.

In order to implement a rule-based agent messaging architecture, a flexible format for representing risk object-value pairs must be established. The format must allow an interfaced user the opportunity to relate a risk tolerance posture that can be interpreted consistently and correctly. The language of the message must also be flexible enough to allow a user to add or remove risk parameters without disrupting the ability of the agent to communicate with other agents or hosts; therefore, risk object-value pairs will be expressed in XML format. Consider the following example of an XML structured agent design.

```
<?xml version=’1.0’ encoding=’utf=8’?>
<AgentData>
    <Personal>
        <Identification>
            <Name>John Doe</Name>
            <Address>1 Home Rd.</Address>
            <Email>doe@hostname.org</Email>
            <SSN/>
        </Identification>
        <Financial>
            <Credit>Citibank</Credit>
            <CardNum/>
        </Financial>
        </Personal>
        <Agent>
            <HostIP>192.168.1.1</HostIP>
            <HostName>homepc.domain.net</HostName>
            <History>130.10.1.20</History>
        </Agent>
        <Task>
            <Quantity>2</Quantity>
            <ItemNum>3874490</ItemNum>
<HighPrice>$120.00</HighPrice>
        </Task>
    </AgentData>
```

The XML element names are descriptive of their respective contents, and some of the elements are empty. In this case, the logic states that the missing information is withheld intentionally. This knowledge, in conjunction with other element contents, forms a picture of the security posture of the agent deployer.

DISCUSSION AND SUMMARY

In order to ensure that agents can be used by their owners effectively without exposing the owners to undesired risk, it is imperative that agent developers adopt XML-based standards for representing various security attributes and attribute values (Warkentin et al., 2001). Interorganizational systems cannot have a significant impact unless a standard data representation scheme is used for data of mutual value. The true potential of intelligent agents to efficiently exchange information will not be unlocked unless and until there is a common standard for the representation of all product and service attributes which can be easily transferred and interpreted by all economic players across the Internet. An international standardized data representation scheme for product and service attributes would extend the capabilities of agent-based data mining processes, thus further improving the efficiency of all marketspaces throughout the World Wide Web.

REFERENCES

CHAN PK FAN W PRODROMIDIS AL and STOLFO SJ (1999) Distributed Data Mining in Credit Card Fraud Detection. *IEEE Intelligent Systems and their Applications* **14**(6), pp. 67-74.

DHAR V and STEIN R (1997) Seven Methods for Transforming Corporate Data into Business Intelligence.

GANNON T and BRAGGER D (1998) Data Warehousing with Intelligent Agents. *Intelligent Enterprise* **1**(1), pp. 28-37.

GRIMES S (1998) Agents Come in From the Cold. *Database Programming and Design* **11**(4), pp. 48-53.

LASHKARI Y METRAL M and MAES P (1994) Collaborative Interface Agents. *Proceedings of the National Conference on Artificial Intelligence*.

MAES P (1994) Agents that Reduce Work and Information Overload. *Communications of the ACM* **37**, pp 31-40.

MAES P GUTTMAN RH and MOUKAS AG (1999) Agents that Buy and Sell. *Communications of ACM* **42**(3), pp 81-87, 90-91.

SHIAU J RATCHEV M and VALTCHANOV G (2000) Distributed Collaborative Design and Manufacturability Assessment for Extended Enterprise in XML-Based Agent System. *Proceedings of the 9th IEEE International Workshop*, pp 260-265.

SZCZERBICKI E (1996) Signed Directed Graphs and Reasoning for Agents and Multi-Agent Systems. *International Journal of Systems Science* **27**, pp 1009-1015.

WARKENTIN M SUGUMARAN V and BAPNA R (2001) Intelligent Agents for Electronic Commerce: Trends and Future Impact on Business Models and Markets. *Internet Commerce and Software Agents: Cases Technologies and Opportunities*, pp 101-120.