Toward a Multi-Agent Security System: A Conceptual Model for Internet Security

Lin Zeng  
City University of Hong Kong

Huaiqing Wang  
City University of Hong Kong

Follow this and additional works at: http://aisel.aisnet.org/amcis1998

Recommended Citation
http://aisel.aisnet.org/amcis1998/81

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 1998 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Toward a Multi-Agent Security System: A Conceptual Model for Internet Security

Lin Zeng  
Huaiqing Wang  
Department of Information Systems  
City University of Hong Kong

Introduction

The Internet security has come to be regarded as a critical concern of the survival and success of the burgeoning businesses on the net [1]. Although many security solutions have been introduced to deal with some specific threats, an automated and comprehensive protecting mechanism is still in need. To achieve this end, artificial intelligent techniques are believed to be applicable and promising. Accordingly, a multi-agent Internet security system was proposed [2,3].

It is the goal of this paper to study the means of constructing a formal conceptual model of generic Internet security processes, which would help to understand and analyze the knowledge in the domain of the Internet security, and to facilitate the building of the proposed multi-agent security system.

Modeling Techniques

Our Internet security conceptual model has drawn on accomplishments of the research on knowledge representation (KR) [4,9]. The scheme to be used is based on the KR language Telos [5], a descendant of RML, developed at the University of Toronto. Telos is characterized by the unique features as abstraction mechanisms (classification, aggregation and generalization), treatment of attributes (attributes can be defined in the same manner as entities and have their own attributes), provision of special representational and inferential facilities for temporal knowledge, and an assertional sub language expressing both deductive rules and integrity constraints. Our study uses the Telos KR scheme to represent and model the variety of types of Internet security knowledge within a consistent framework. Each category of knowledge is treated as a class. All the classes are organized hierarchically. Corresponding to the agents in the proposed multi-agent security system, the concept of agent is also used to model the components that are capable to collect, manipulate, and deliver security information [8].

Scenario

Here in this paper, we would illustrate the model with an Internet protection scenario. An Enterprise Software Pool System is an assumed application running on the network, and being protected against IP spoofing attacks.

The Enterprise Software Pool System (ESPS) is assumed to be a multi-user Intranet client-server system providing remote manipulation of software documentation and source codes. Access is authorized to both the internal and external (the Internet) users while access control is needed as one of its security requirements [10].

The ESPS, as an application on an open network, may encounter some kinds of attacks, e.g. IP Spoofing [7]. Many TCP/IP services authorize client based upon a network identity as, for example, IP address in an access control list. The problem is that the source IP address, as well as anything else about a packet, can be changed by the nature of TCP/IP. It is called IP spoofing that the source IP address is forged to impersonate others for unauthorized operations. A number of IP spoofing attacks have been recorded recently.

Although, under some circumstances, IP spoofing can be protected against by means of mutual authentication or traffic filtering, it is a more flexible and active protection to detect the attack based on monitoring and analyzing of audit information. Following are some rules that would be employed for the detection:

- packet transmitting within an internal network, if it is not found at the source address it is claimed, or if it is found in the route that it should not have passed according to the claimed source and destination addresses, should be recognized as counterfeit.
- A packet coming from the Internet that contains the source address of a host inside the private network should be regarded as IP spoofing.
- If a host address on the Internet is known to be sending fraudulent packets, then block all traffic to and from that host.
- Outgoing packet whose source address is not in the internal network should be regarded as IP spoofing.

Ontology

Ontology is specification of conceptualization, which is an abstract, simplified view of the world [6]. Usually, ontological notations are equated with taxonomic hierarchies of classes, objects, relationships, and other entities.
A partial semantic schema for the security conceptual model is given in the figure above, which is sufficient to demonstrate the ontology of the security domain. In the figure, three types of links are used to notate the relationships defined in Telos. They are ISA links (for subclass/class relations), IN links (for instance/parent class relations), and the ATTRIBUTE links. The model consists of three layers, namely, Meta Class, Domain Class, and Token. Objects in the Token Layer correspond to the Internet security domain instances. Classifications of these Token Layer objects are modeled in the Domain Class Layer, where a hierarchy of the classes is also represented for the class generalization. Similarly, by further applying such classification and generalization operations, the hierarchy of the meta classes is represented in Meta Class Layer.

As an example, class MultipleUserApplication in Domain Class Layer inherits attributes (e.g. name, IP address, Application Agent, etc.) from its parent class Application, and is defined as follows:

```
CLASS MultipleUserApplication
ISA Application WITH
ATTRIBUTE
  requirement: set of SecurityRequirement
  session: set of CommunicationSession
RULE
  ExternalIPSpoofingRule:
    (Forall x/session
     (Forall y/requirement
      (Forall z/x.UserAgent.IP
       (y.AccessList.isInternal(z) AND
        x.AuditAgent.fromInternet()))))
    => Warning(IPSpoofing,x))
  InternalIPSpoofingRule:
    (Forall x/session
     (Forall y/requirement
      (Forall z/x.UserAgent.IP
       ((NOT x.UserAgent.Sended(x.packet)) OR
        (NOT z.possibleRoute(x.packetRoute))))))
    => Warning(IPSpoofing,x))
  HistoricalIPSpoofingRule:
    (Forall x/session
     (Forall y/requirement
      (Forall z/x.UserAgent.IP
       (y.AccessList.inSpoofingIP(z) OR
        y.AccessList.inSpoofingName(n))))))
    => Warning(IPSpoofing,x))
CONSTRAINT
  IPConsistenceConstraint:
    (Forall x/session
     (Forall y/requirement
      (Forall z/x.UserAgent.IP
       ((x.AuditAgent.toInternet()) AND
        ...))))
```
y.AccessList.isInternal(z))
OR
(x.AuditAgent.fromInternet() AND
NOT y.AccessList.Internal(z))
OR
(x.AuditAgent.isInternal() AND
z=x.AppAgent.toIP AND
x.UserAgentToIP=x.AppAgent.IP))
END

In the ontology of Telos, rules and constraints are special objects attached as attribute values of propositions. The deductive rules defined above precisely and explicitly model the propositional logic. In this way, reasoning processes are represented formally for proper analyzing and implementation.

Model of Security Processes

The security conceptual model is intended to capture the dynamic evolution of objects, rather than just the latest snapshot provided by conventional conceptual modeling techniques. Four sequential stages in the scenario would be modeled:

Initiating Application

When an Internet application is first installed on the net, its properties such as requirements should be configured at the beginning. Here for the ESPS system, an object ESPS is defined as an instance of class MultipleUserApplication:

TOKEN ESPS
IN MultipleUserApplication
WITH
  Name : ESPS
  IPAddress : 144.214.2.14
  requirement : ESPSAccessControl
  : ...
  AppAgent : ESPSATappAgent
  session : ...
END

Then three attribute objects of the object ESPS, ESPSAccessControl, ESPSAccessFile, and ESPSATappAgent, are declared as instances of class SecurityRequirement, SecurityProfile and ApplicationClass respectively. The four objects defined on this stage are represented in the figure in fill effect of light gray.

Initiating User

Shown in the figure in middle gray, user Zolo is initiated on the Internet. A user agent is also created for Zolo as a communication shell. The attribute IP of the agent is set to Zolo’s login IP address, for example, 144.214.72.99.

Establishing Communication

When Zolo requests access to ESPS, a communication session is set up. Thus ESPS-Zolo, an instance of class CommunicationSession, is created and linked to the object ESPS as an attribute. According to the security requirements of ESPS, other two security agents, AccessControlAgent and AuditAgent are created too (shown in the figure in dark gray).

Detecting IP Spoofing

When, for example, the session ESPS-Zolo gets a packet labeled with Zolo’s address, but Zolo did not send the packet actually,

ESPS-Zolo.packet.IP=144.214.72.99
ESPS-Zolo.UserAgent.Sended(ESPS.packet)=False

it can be deduced that somebody else is trying to masquerade as Zolo by IP spoofing, according to the rule InternalIPSpoofingRule defined in class MultipleUserApplication.

Thus, a formal and dynamic conceptual model for Internet security has been built, by constructing it using Telos and tracking it through stages.

Conclusions

In this paper, we have proposed a framework for constructing ontology of Internet Security, by using a powerful knowledge representation language. Some novel features for modeling security knowledge are worth addressing, e.g. meta level facilities, constraint enforcement, inference mechanisms and temporal dependencies, etc.
By building a rich and precise conceptual model for Internet security, our work provides the basis for both formal study and implementation. In fact, based on the model created, a multi-agent Internet security system is being built in progress.

References