Towards Automation for Pervasive Network Security Management Using an Integration of Ontology-based and Policy-based Approaches

Hui Xu, *Student Member*, *IEEE*, Xue Xia, Debao Xiao and Xuejiao Liu
Institute of Computer Network and Communication
Huazhong Normal University
Wuhan, P.R.China, 430079
xuhui_1004@hotmail.com

Abstract

With the popularity of heterogeneous network devices and security products, pervasive network security management has been a fashion. However, a chief problem lies in how to characterize various attack scenarios from the viewpoint of both security information and security policies for automation. This paper discusses the potential of applying an integration of ontology-based and policy-based approaches to automate pervasive network security management, and then proposes a model in order to validate the feasibility of this integrated approach.

1. Introduction

Computer networks usually produce large amount of event-based data, including alerts from Intrusion Detection Systems (IDSs), log files of firewalls and various security-related software, routing information from the network, general information from network devices, etc, and all these collected data need to be involved for pervasive network security management. The critical challenge becomes how to use all these data to not only verify the success of an attack, but also detect and track various attack scenarios, in order to meet increasing requirements of network users for intelligent security management.

Our prior work adopted the form of framework described by XML to represent network security information, since a lot of XML-related tools are available nowadays. However, when taking automation into consideration, the XML-based approach is still far from satisfactory.

These days, ontology has been emerging as a widely used technology and it is currently under review in automatic management scope, while policy-based management has been used for several years, though policy isn't widely deployed since there are few similarities between policy-aware components and systems. It seems that the integration of ontology-based and policy-based approaches may be a promising way towards automation for pervasive network security management, since ontologies may provide the formalism needed by the policy-based approach while the use of policies may enhance the automation of ontology-based approach. The aim of this paper is then to discuss the potential of an integrated approach and propose a model based on it for validation.

The remainder of this paper is organized as follows. Section 2 discusses related work. And the potential of applying an integration of ontology-based and policy-based approaches to pervasive network security management for automation is demonstrated in Section 3. Sequentially in Section 4, for the purpose of validation, a model is proposed based on the integrated approach and a possible scenario is also provided. We conclude our work in Section 5.

2. Related work

The need for ontology-based approach applied to security management has been proposed [1], and Reference [2] defines a standards-based security ontology, which extends the CIM model with ontological semantics. However, this approach is still under development, calling for further research.

Additionally, policy-based management has attracted significant interest from both the academia and industry for many years, and the term "policy" means rule governing the choice in the behavior of the managed element. Policy-based approach, such as the design of policy ontology [3] [4], has been used in security management, connecting policies to ontology. However, these work lack a mechanism for seamless integration with ontology-based approach.

3. Potential of an integrated approach

It is not enough to use single event-based data as the signature to detect attacks, which always leads to

The 3rd Intetnational Conference on Innovative Computing Information and Control (ICICIC'08)
978-0-7695-3161-8/08 $25.00 © 2008 IEEE

high false alarm rate. Networks are dynamic in nature and at each time interval their components produce large numbers of security data. Theoretically, various network security products can collect all these event-based data, and the trace of an attack is often scattered in these extraordinary data. Thus instead of using single data as the signature, we can use a joint scenario signature combined with casual, spatial and temporal patterns to characterize and distinguish various attacks. Therefore, one main problem becomes how to characterize various attack scenarios from the viewpoint of both security information and security policies for the automation of pervasive network security management.

3.1. Ontology-based approach

Ontology plays an important role in Semantic Web, for it is much more powerful than XML in expressing semantics. In brief, ontology aims in defining a set of concepts, properties, and their axioms that provide rules that govern them. Ontology languages have been in a rapid development and the recently developed Web Ontology Language (OWL, not an acronym) [5], is a very complete ontology language.

OWL can directly be used to specify security management information because it has most of the constructions included in management information languages and even those facets, which are not included, can be defined by extending OWL and RDFS [6]. Note that, only an OWL ontology is not enough for the automation of pervasive network security management. The OWL ontology can achieve the integration of management information from a semantic viewpoint, along with the definition of management behaviors and services respectively expressed in SWRL [7] and OWL-S [8], both of which facilitate the integration of network security management information expressed in OWL. Fig. 1 demonstrates the coordination of these three ontology-related languages to automate security management.

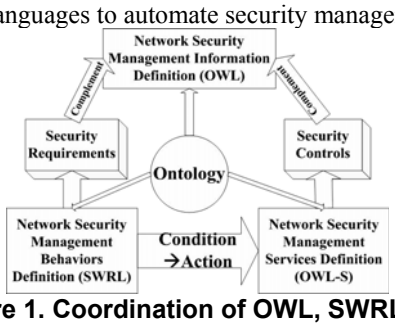

Figure 1. Coordination of OWL, SWRL and OWL-S for the automation of pervasive network security management

As is indicated in Fig. 1, the ontology described by terms of OWL+SWRL is enough to a security management information definition, and OWL-S then specifies security management actions invoked by the behaviors defined in SWRL. When a particular condition defined in the management OWL ontology occurs, the manager invokes one network security management service according to the rule defined by SWRL, and the corresponding service will then be executed to those selected security products or network devices. In this way, the automation of pervasive network security management can be partially implemented from the information point of view.

3.2. Policy-based management

It seems that, policies may act as the language for controlling autonomic systems or the guidance for decision-making. The Common Open Policy Service (COPS) [9] and its extension for policy provisioning (COPS-PR) [10] are currently being developed as the protocols to implement policy-based management.

The COPS protocol is a simple query and response protocol that can be used to exchange policy information between a policy server, Policy Decision Point (PDP) and its clients, Policy Enforcement Points (PEPs). Each PEP may support one or more clients of different client-types, which exist for different policing areas. COPS-PR is one of those client-types. In COPS-PR, policy requests describe the PEP and its configurable parameters. If a change occurs in these basic parameters, an updated request is sent. Decisions are not necessarily mapped directly to requests, and are issued mostly when the PDP responds to external events or PDP events.

Several policy languages, such as Ponder, have been designed for policy-based management. However, the use of different policy languages may lead to the difficulties for implementation of the management system, let alone to automate pervasive network security management. Since ontology is formally defined and thus enhances semantic expressiveness, it can be used as an alternative to management information, as demonstrated above. Hence, we argue that, by the use of OWL ontologies, network security management policies may be combined in the same model with network security management information, which directs a prospective way to automate pervasive network security management.

3.3. Integrated approach

978-0-7695-3161-8/08 $25.00 © 2008 IEEE

Ontology-based management is a new technology in security management scope, especially for semantic management. It has been a promising way to automate pervasive network security management, but it is not a complete one. One quick way to widely use the ontology-based approach may be to integrate it with existing management framework and technology. Policy-based management has attracted significant interest for several years. To some extent, it aims in the automation by means of policies. Unfortunately, it fails to be feasible enough to implement, since formalizing security policies is a complex task. It seems that the integration of ontology-based and policy-based approaches may be a prospective approach to promote automation for network security management.

As for pervasive network security management, ontologies seem to be one formal way to express the security policies. However, it is still not enough to describe network security management policies only by the OWL ontology. Note that, when applying ontologies to define security management information, we complement the OWL definition by SWRL behavior definitions and OWL-S service definitions, since SWRL provides a way to express those implicit restrictions on management information in a formal explicit way while OWL-S defines services corresponding to security management actions, which are invoked if the given condition defined in SWRL occurs.

Thus in the same way, we can describe policies acquired from requirement with deployable security controls by SWRL, which defines the implicit behavior of management implementations in a formal way. Then we can get the unified ontology for automation of pervasive network security management, using OWL+SWRL to define not only collected security management information but also defined security management policies. Additionally, OWL-S is extended to express those actions invoked by the policies when the conditions contained in the integrated security management ontology happen. Fig. 2 presents application of the integrated approach.

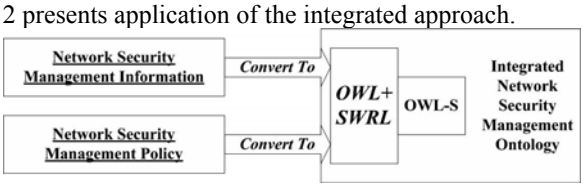

Figure 2. Application of the integrated approach to describe both information and policies for network security management

As is implied in Fig. 2, applying ontology languages (OWL+SWRL and OWL-S) to describe both network security management information and network security management policies in an integrated way will be a basis of implementing automation for pervasive network security management.

4. Validation

It seems that the integration of ontology-based and policy-based approaches becomes feasible by means of OWL+SWRL and OWL-S, and it is also an effective step forward the automation of pervasive network security management. On the one hand, ontologies provide a formal way to express security policies for the implementation of policy-based approach. On the other hand, the use of policies can facilitate ontology-based security management for automation.

4.1. Proposed model

Considering these three OWL-relate languages defined by W3C and the architecture for policy-based management provided by IETF, a common model for the integration of ontology-based and policy-based pervasive network security management is then presented in Fig. 3 by using them properly for the purpose of automation.

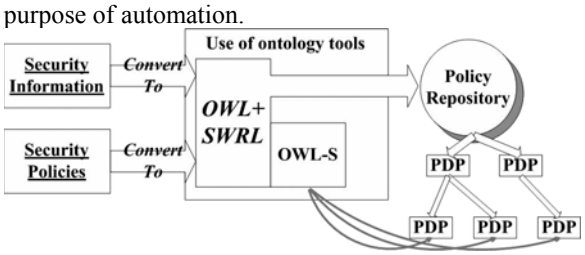

Figure 3. A common model for the integration of ontology-based and policy-based automatic network security management

As is demonstrated in Fig. 3, there are at least three steps to implement pervasive network security management for automation based on the integrated approach.

Step 1: Use an ontology tool, such as Protégé-OWL editor [11], to convert security information and security policies to OWL+SWRL network security management ontology manually, semi-automatically or automatically, depending on the capability of the chosen tool.

Step 2: According to the behaviors defined in SWRL for both network security management information and policies, corresponding actions can then be defined in the form of network security management services described by OWL-S, still with an ontology tool. When invoking the behavior defined in this integrated ontology as security policies, a corresponding control action is performed according to the OWL-S definition.

978-0-7695-3161-8/08 $25.00 © 2008 IEEE

Step 3: Put all the polices contained in the ontology for pervasive network security management to the policy repository, which is used to store the policies generated by network management tools, so that they can be used by the IETF architecture for policy-based management.

4.2. A possible scenario

Here we take the following formula for risk assessment taken from Open Source Security Information Management (OSSIM) [12] as an example.

Risk = (*Priority* * *Reliability* * *Asset*) / 25,

where *Priority* means the threat level represented by the event, *Reliability* means the probability that the event will occur, and *Asset* means the value of the assets associated with the event.

Since *Priority* is leveled as integral from 0 to 5, *Reliability* is marked as integral from 0 to 10, and *Asset* is identified integral from 0 to 5, *Risk* is then between 0 and 10, also defined as integral.

Security information mainly includes *Priority*, *Reliability*, *Asset* and *Risk*, while security policies consist of different treatments to different risk assessment result classified by the value of *Risk*. Using the proposed model in Section 4.1, we can make full use of the integrated approach, as is shown in Fig. 4.

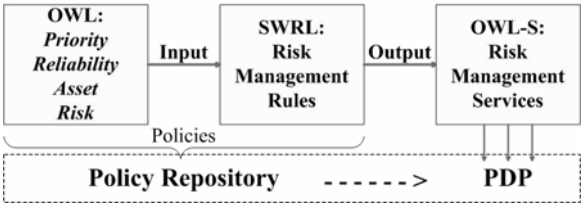

Figure 4. A possible scenario using the proposed model

5. Conclusions and future work

In summary, this paper aims at introducing the integration of ontology-based and policy-based approaches to automate pervasive network security management and proposing a security management model based on this integrated approach for validation.

As is implied in this paper, pervasive network security management has developed in a way that integration is widely used. Thus we argue that the integration task plays a significant role in the evolution of automation for pervasive network security management, since automation is a goal that one technology alone may not be essential to achieve.

Future work mainly includes implementation issues on application of the proposed model to automate pervasive network security management.

6. Acknowledgement

This work is supported by the Scientific and Technological Planning Project of Wuhan City, P. R. China under Grant No. 200710421130.

7. References

[1] M. Donner, "Towards a Security Ontology", *IEEE Security and Privacy*, 2003, 1(3), pp.6-7.

[2] B. Tsoumas and D. Gritzalis, "Towards an Ontology-based Security Management", Proceedings of the 20th International Conference on Advanced Information Networking and Applicaion, 2006, 1, pp.985-992.

[3] A. Uszok, et al., "KAoS: A policy and Domain Services Framework for Grid Computing and Semantic Web Services", Proceeding of 2nd International Conference on Trust Management, 2004, pp. 16-26.

[4] H. Chen, et al., "SOUPA: Standard ontology for ubiquitous and pervasive applications", Proceeding of the 1st International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004, pp. 258-267.

[5] P. F. Patel-Schneider, P. Hayes and I. Horrocks, "OWL Web Ontology Language Semantics and Abstract Syntax", *W3C Recommendation*, February 2004.

[6] J. E. López, V. A. Villagra and J. Berrocal, "Applying the Web Ontology Language to management information definitions", *IEEE Communications Magazine*, 2004, 42(7), pp. 68-74.

[7] I. Horrocks et al., "SWRL: A Semantic Web Rule Language Combining OWL and RuleML", *W3C Member Submission*, May 2004.

[8] D. Martin, "OWL-S: Semantic Markup for Web Services", *W3C Member Submission*, November 2004.

[9] J. Boyle et al., "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[10] K. Chan et al., "COPS Usage for Policy Provisionning (COPS-PR)", RFC 3084, January 2000.

[11] Stanford Medical Informatics, Protégé-OWL editor, http://protege.stanford.edu/overview/protege-owl.html.

[12] Open Source Security Information Management, http://www.ossim.net/.