Advanced Science and Technology Letters
Vol.111 (NGCIT 2015), pp.74-78
http://dx.doi.org/10.14257/astl.2015.111.15

The Study of Access Control Model

Huanming Zhang [#], Quanlong Guan [#], Weiqi Luo

etwork and Education Technology Center, 510632, Jinan University, China
[#] These authors are co-first authors, who contributed equally to this work,
E-mail address: Huanming96965@163.com

Abstract. XML, the Extensible Markup Language, had become an important tool for both storage and exchange of data. In this paper, we would first made a brief introduction of access control using XML, and some requirements of XML access control would be included. Finally, we analyzed the direction and difficulty in the study of access control using XML, and then illustrate the practical significance of the study.

Keywords: XML, authority, access control, security, XML schemas

1 Introduction

XML was an open standard of data representation, along with lots of advantages: concepts of elements, extensible, separation of display and content, complex structure presentable, and etc. XML had played an important role in almost all E-commerce systems and Web applications. As XML was just a language, security of its application could not be guarantee by itself. Hence, there was a need to build secure application platform as the precondition and foundation of its applications.

Generally, security threats faced by E-commerce with such following classification [1, 2]: illegal access, illegal tempering, counterfeiting, repudiation, denial of service. And to force those mentioned secure threats, the E-commerce application system must fulfil the following needs: data confidentiality, access control, authorized identity identification, data integrity, and denial-anti. There some new work about this area. E Damiani et al[9] propose five basic requirements for standardizing XML access control at the tag level. Venkatasubramanian et al. [10] proposed an Adaptive and proactive Access Control Approach for Emergencies in Smart Infrastructures.

2 Requirements of XML to access control

Protection could not be guaranteed while using traditional access control uniquely because of some special features of XML documents, hence there was a need to declare a special access model using XML. By analyzing existing models, we found that those model were all based on the declarations of a group of authorities, and these authorities must at least contain the subject of their application, protected object, and

ISSN: 2287-1233 ASTL

the upcoming execution. Difference of recent XML access control models were mainly presented by different implementation of the access to subject, and object.
We would discuss the basic features of existing access control model [5] using XML:

Better access control granularity: Access control would support different levels of granularity of access control, from documents set, single document, elements set, single element, to particular elementary content.

Support levels of authority [6]: In many instances of access control, mono-concentration authority could not adopt to the multi-level request from application environment. Good access control system should support global and local (or even more levels) authority.

Support for Web technique: With the use of Web site, XML document would always usable. Without using existing API and development tool, XML access control should be convenient and Web technique integrated.

Transparency: Access control operation should be as transparent as possible to the requester. Requester should not able to notify message hidden by access control system in a document. Moreover, access control should guarantee the effectiveness of document to its DTD

Good compatibility and interoperability [7]: Access control should conveniently interoperate with other system

Integration with existing user authorization technique: Access control should easily integrate other user authorization technique.

3 Access Control Model using XML

The following would be an introduction of an access control model using XML, access control of XML schemas or instance documents needs the declaration of subjects and objects, and the access control rules especially for subjects and objects.

The xml subject which mean a user or a group of users. Each user had a notification symbol, which could be used as the user login name also. Each user or user group described by user features document. Then safety administrator could define the system safety rules according to the user features document. The XML document shown in figure 3.1 was a simple user characteristic document.

```
< userProfile>
   < users>
      < user id= " tang" name= "Tang" />
      < user id= "ma" name= "Ma" />
      < user id= " liu" name= "Liu" />
      < user id= "huang" name= "Huang" />
      < user id= " lee" name= "Lee" />
   < /users>
   < groups>
      < group id= "professor" >
         < member uidref= " tang" />
         < member uidref= "huang" />
      < /group>
      < group id= " researchAssistant" >
         < member uidref= " liu" />
         < member uidref= " lee" />
      </group>
      < group id= " financial">
         < member uidref= "ma" />
      < /group>
   < /groups>
</userProfile>
```

Fig. 1. User features document in XML format (UserProfile.xml)

For simplifying definition of authority, some access control model allowed the authority specification defining subject into following three categories:
User group: statically defined a group of user, which could be nested and overlapped
Position mode: a group of position set, acquired by adding the character * in front of the physical or symbolic address
Role: according to authority set, users could determine their role dynamically.
Our access control models using XML mentioned above were with following features:

(1) Support authorization with fine and coarse granularity: That model support model-level and instance-level authorization; model-level authorization was to fulfil a certain authorization to all instance of DTD; instance-level authorization was to authorized a certain particular XML document, where the authorization could be refined to certain part, certain element or attribute of the document

(2) Take two different transmission strategy: transmission strategy of authorization basically separated into local and recursive; local meant the authorization of certain element was only applied to all attributes; recursive meant the authorization of certain element would be applied to its attributes and sub-elements. Generally, “grand” could be “local” or “recursive” authorization, and “deny” would be “recursive” authorization.

(3) Provide support to abnormal condition: XML access control model was facing two kinds of abnormal condition: authorization collision, and incompletion problem. We could use the higher priority principle to authorization collision;

and for incompletion problem, as “grand ” and “deny” had not be clearly invested, a “open” or “close” strategy would be used by default generally, which meant accept “grand” or “deny” authority.

4 Evaluation

In this paper, our experiments using SUNXACML, JDOM parser and Java language. SUNXACML developed by Sun Java-based XACML API, which provides the PDP and PEP implementation. The simulation is carried out in the following environments: Intel Core i3-2120 3.3GHZ CPU processor, 8GB of memory, Windows 7 operating system. JDOM version is 2.0.5 and Java is SE 7.0 (1.7.0). Testing with DTD and XML documents by XMark obtained authorization rules set XPath formula based on the DTD is generated by YFilter The XPath tool, query the artificial setting.

The proposed model are proof of concept level, the benchmark index is used to obtain the differences in performance. Since our sample XML data is generally small, and provide experimental file type size were 2KB, 5KB, 8KB, 10KB, 15KB, 20KB, not likely to reflect the efficiency of the model, the experimental results produced are not comparable. To properly measure the results, we take 1024 iterations of experimental data obtained 2M, 5M, 8M, 10M, the amount of data 15M, 20M of. Disposable minimize overhead, XML input completed 1024 iterative resolution files of different sizes. Benchmarking tests were repeated six different types of files, to see how to deal with six different models in size. This means that the first iteration of six different sizes of file 1024, and then measure. Before parsing and calculation, the file is completely loaded into memory. This does not include the loading time consuming to resolve. 1024 iterations estimates are carried out in its own process. This means that, for each file in a separate process for resolution. A process running again. Each file is estimated that three times. 1000 file parsing process start and stop three times, the final calculation of the average value of their time. Processes are performed sequentially, not in parallel.

5 Conclusion

By its advantages, XML was becoming a general media for data exchange and representation, widely used in E-commerce, became the core while constructing Web Services. These application domain required some safety requirements for certain level, but XML was just a kind of markup language which was not able to guarantee the safety for those applications using XML as their base. Design and implementation of access control model using XML would like to be an important tool to guarantee the application safety. Recently, there were three directions for the study of XML access control:

(1) Access control method based on XML: ACT (access condition table), SMT (strategy matching tree), static analysis and etc.

(2) Access control strategy language based on XML: Recently, some expressive and functional strategic standard language like XACL, XACML and WS-Policy had been designed to implement standard manual of safety strategy using XML. As semantics and syntactic of those language were still complex, hence, developed an expressive XML access control strategy language with easy semantics and syntactic was an important direction for the recent study of XML access control
(3) Design of XML access control model: in recent years, kinds of access control models had been proposed, like model based on safety view or fine granularity.

Acknowledgments. Huanming Zhang and Quanlong Guan are co-first authors, who contributed equally to this work. This work was supported by Major Program of National Natural Science Foundation of China(No.61133014, No.61272415, No.61272413), the CEEUSRO project of Guangdong province,China (No.2012A080102007, No.2011B090400324, No.2010A011200038, No.2012B040305008), Science and Technology Planning Project of Guangzhou city(No.11A12070544, No.2013Y2-00071),the Project for Engineering Research Center of Guangdong Province(No.GCZX-A1103), and the Fundamental Research Funds for the Central Universities(No. 21613336).

References

1. LIU Yun-sheng, ZHONG Hao, WANG Yi. XML Access Control Model and its Application . Journal of Chinese Computer Systems.2005.(05)
2. Fan Feng, Xueqiang Zhou, Xuebin Feng, Bo Ye. The XML fine-grained access control model based on priority [J]. Journal of Computer Applications.2006,(S2)
3. TANG Shao-hua. Methods on XML Authorization and Access Control [J]. MINI- MICRO SYSTEMS.2005.(03)
4. WANG Zhan-min,CUI Du-wu. Access control strategy based on RBAC for XML security. [J]. Computer Engineering and Applications.2007,43(17)
5. LI Lan, HE Yong-Zhong, FENG Deng-Guo. A Fine-Grained Mandatory Access Control Model for XML Documents [J] Journal of Software , 2004,(10)
6. FU Haiying, LI Hui, WANG Yumin. An Overview of XML and XML-Related Security [J]. Application Research of Computers.2004,(02)
7. S. De Capitani di Vimercati1, S. Foresti1, S. Para boschi2.Access Control Models for XML.http://www.springerlink.com/content/

