Journal of Network Computing and Applications (2016) 1: 42-46
Clausius Scientific Press, Canada

Automatic Security Detection for Access Control Based on Guided Deep Testing

Xiong Dapeng[1, a], Chen Liang[1, b], Wang Peng[1, c], Zou Peng[1, d]

[1] Academy of Equipment, Beijing, China
[a] xiongdapeng@outlook.com, [b] 252958524@qq.com,
[c] 75498437@qq.com, [d] zpeng@nudt.edu.cn

Keywords: security detection, access control, permission leakage.

Abstract: Security detection for access control model by testing whether there is permission leakage, is the key measure to evaluate access control system security. Traditional security verification measure mainly relied on artificial analysis, which is low efficiency and heavy workload. Thus we study on the automatic security detection technology. To avoid the blindness of the test, we propose an improved detection method based on guided deep testing. The novel method improve the test efficiency by reducing the search path.

1. Introduction

Information leakage in access control [1] has become a major problem in the past decades, which lead to a continuous potential threat to the information system. Access control was proposed as a security technology, but its own security is ignored continually, resulting a privilege leak in the access control authorization process, therefor brings great hidden danger to the system security. In order to ensure the security of access control strategy, we need to analyze and verify whether the access control strategy is in the risk of the privilege leakage. The purpose of security analysis is to ensure that the access control strategy is legally executed, not to disclose the authority to unauthorized users, which is the basis for the effective implementation of access control strategy. So it is very meaningful to study the problem of access control security detection.

Security analysis was first proposed by Harrison et al [2], to analyze the information leakage problem in the operating system. They checked out the whole process of the controlled system by executing the command sequence. Then security detection was introduced to access control to detect the permission leakage, to see whether any chance for unauthorized subject of permission to access safe source, which may lead to permission leakage. We use the following example to illustrate the problem of access control strategy and its security analysis.

We explain how permission leakage in access control. As shown in Figure 1(a), an access control matrix specifies the permission of subjects to access the objects. Subject S_1 can read the source of O_1, and Subject S_2 can read the source of O_2, Subject S_2 can write the source of O_2, but Subject S_1 is forbidden to access the source of O_1. While Figure 1(b) simulates the process of a real access case. Source in O_1 was read by S_2, then S_2 write it to O_2, in the end S_1 can read the source of O_1 from O_2. Figure 1(c) show the whole process that how the source O_1 was leaked to S_1, which should be forbidden as claimed in the access control matrix.

	O_1	O_2
S_1	——	r
S_2	r	w

Fig. 1(a) Access Control Matrix

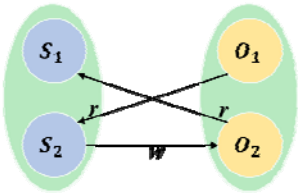

Fig. 1(b) Access Resource

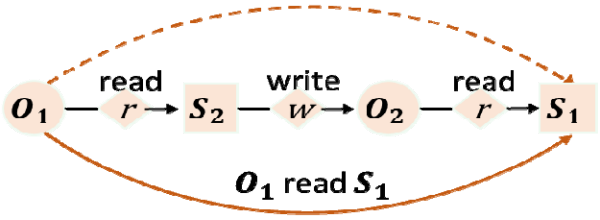

Fig. 1(c) Permission Leakage in Access Control

Automated detection is the primary method of security testing, because it has higher test efficiency and less test cost when compared with common testing method. Access control security testing runs through the entire process of the system, including initial state and operating state. Thus security detection is composed of two parts, system initial state security testing and system transition state security testing. If the system is detected to be safe at the initial state, then test every possible action of access in whole run time, and determine whether the system is still in safe state after each operation.

According to the guiding ideology proposed above, we summary the general access control security detection measures as the following steps:

A. Set up test model. Declare the formal definition of access control subject, object, permission, strategy and other related attribution. Describe the access logic state, decision condition, and authorization rules.

B. Generate test cases. Automated generation of test cases that suitable for the detection based on the model, include a set of test input data, operating conditions and expected results, the goal is to detect the difference between test results and expected results.

C. Security testing in initial state. Traverse the whole access program, form an access control matrix that contain all the subjects and object, and test all possible access control operations combination to check whether there a direct violation of access.

D. Security testing in operating state. Analysis all possible running states by executing every generated operation cases, to see whether the results will violate the access control constraints after each execution.

This paper takes the access control security analysis strategy problems as the goal, aiming at cloud computing RBAC cross domain access control model, through the two aspects of the initial state and the state space to verify the detection and safety evaluation, and carry out specific research from the implementation of the evaluation system.

2. Related Work

2.1 Research Status.

With the continuous expansion of access control model family, serious of access control security monitoring methods have emerged. For specific access control models, logic derivation is usually used. The more common approach is state space reasoning.

1)Logical reasoning based methods. This kind of method [3] proves the root axiom of the access control model is correct by deducing the security axiom. For example, prove the security of BLP model via "Simple safety theorem" and "*- Characteristic theorem" [4]. In fact it is hard to find the root axiom which can represent the security of the model.

2)Mathematical model conversion based methods. This kind of method uses mathematical model (such as "lattice" [5]) instead of access control strategy to prove the security of access control. The defect of this method is that the mathematical model usually can only prove the partial characteristics of security.

3)Quantitative analysis based methods. This method uses information entropy [6] and other quantifiable criteria to measure the security level of access control model, which has strong operability, but cannot fully evaluate the security of the model.

2.2 Problem Analysis.

At present, the security analysis of access control strategy is based on the specific strategy specific analysis, so there is no uniform and universal method. The common security analysis idea is that some security theorems are proved to be customized for specific strategies, which are not generalized. State analysis method based on spatial reasoning, traversal of all security status in the process, there are certain advantages in the proof of completeness and universal methods, and is an important development direction of future access control security analysis.

3. Framework

In this section we promsed a noval detection method for access control security. The security of access control based on state space reasoning is to search the state space of the whole access control strategy to detect the conflict rules. The framework of automatic security detection in access control state space is as shown in Figure 2.

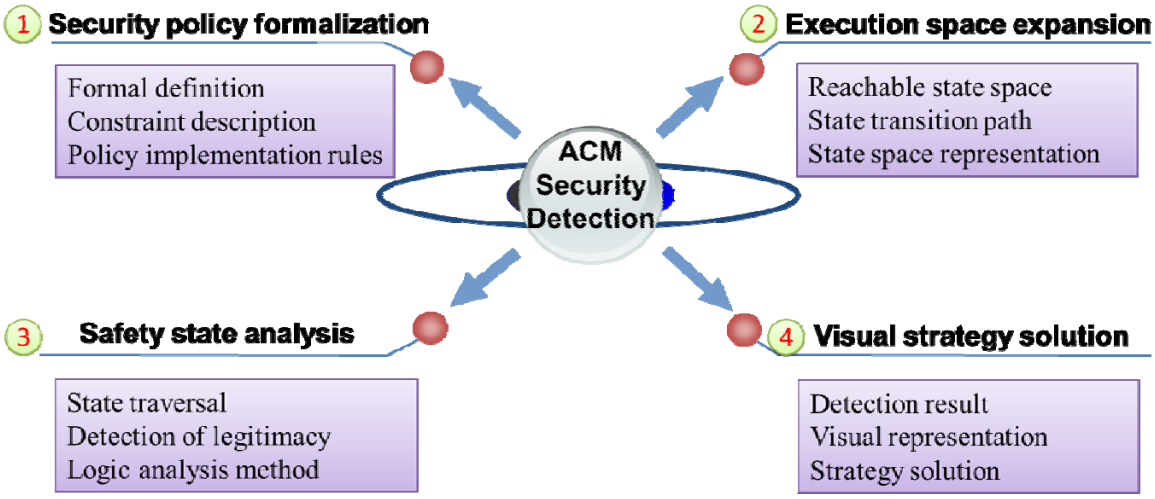

Fig. 2 Framework of Permission Leakage Detection in Access Control State Space

Step 1. Formal definition of execution rules for access control strategies. Express the execution rules of access control strategy with appropriate definitions, representations, and data structures, which will prepare for subsequent analysis.

Step 2. Security state space is used to represent reachable state and path of access strategy. We can get the security space that contains all execution states, by recording the process transfer status of the

user.

Step 3. Verify the security space of access control system based on logic analysis method, to detect each operation state is safe or not. Specifically, hunt out the items that be violating with the constraints of the access rules. Violations of the information dissemination often interrelated with permission leakage.

Step 4. Translate safety state testing results to security conclusion, express the conclusion intuitively, then adjusted security strategies.

4. Algorithm

With the increase of the number of users and resources, the calculation quantity of security state space detection may rise to an unacceptable level. Thus we need to reduce the search space through guide.

Algorithm 1 (Evaluation of a set of testing samples)

Evaluation (M : set of samples,
S : set of subjects, O : set of objects, R : set of strategies) =
$E \leftarrow \varnothing$;
For each $m(s,o,r) \in M \ \wedge \ m(s,o,r) \rightarrow R$ do
if (Operation ($tran(m(s,o) \triangleright m(s',o'))$) $\notin \varnothing$) then do
$E \leftarrow E + m(s,o,r)$ Then
Return *false*;
End For;
Return *true*;
End Evaluation;

Algorithm 2 (Reduce samples of testing)

Reduce (M : set of samples,
S : set of subjects, O : set of objects, E : set of sample evaluation)=
$M_d \leftarrow M$;
While Evaluation (M_d, E) $\neq$ *Fail* do
$M_d \leftarrow App(E, m(s,o,r))$;
End While;
For each $m(s,o,r) \in M_d$ do
if ($m(s,o,r) \in E$) then do
$M_d \leftarrow M_d - m$;
End For;
Return *true*;
End Reduce;

The algorithm determined whether the test sample is a leaf node on the executable chain, and if so, deletes the relevant record from the test state space. So it reduced the amount of computation, and improved the test efficiency.

5. Conclusions

This paper studied on automatic security detection technology for access control model, propose a framework for automatic testing the safety states in the reachable execution space. Then introduced a constraint based reduction algorithm to improve the evaluation efficiency.

Acknowledgements

This work was financially supported by National High Technology Research and Development Application of China (2012AA012902) and "HGJ" National Major Technological Projects (2013ZX01045-004).

References

[1] Morisset C, Oliveira A S D. Automated Detection of Information Leakage in Access Control[J]. Second International Workshop on Security and Rewriting Techniques - SecReT 2007, 2007.

[2] Harrison M A. Protection in operating systems[J]. Acm Sigops Operating Systems Review, 1976, 19(9):14-24.

[3] Li N, Tripunitara M V. Security analysis in role-based access control[J]. Acm Transactions on Information & System Security, 2006, 9(4):391-420.

[4] Si Tiange , Tan Zhiyong , and Dai Yiqi. A Security Proof Method for Multilevel Security Models[J]. Journal of Computer Research and Development,2008,45(10):1711-1717.

[5] LIN Bo-gang. Model analysis of information system security field for Lattice expansion[J]. Journal on Communications, 2009, 30(10):9-14.

[6] Che Tianwei, Wang Chao, Li Na.An theory of access control based on security entropy[J]. Network Security, 2014(5):158-159.