International Journal of Digital Crime and Forensics
Volume 10 • Issue 1 • January-March 2018

Trust Evaluation Strategy for Single Sign-on Solution in Cloud

Guangxuan Chen, Zhejiang Police College, Institute of Software Application Technology, CAS, Guangzhou, China
Liping Ding, Digital Forensics Lab, Institute of Software Application Technology, CAS, Guangzhou, China
Jin Du, Digital Forensics Lab, Institute of Software Application Technology, CAS, Guangzhou, China
Guomin Zhou, Zhejiang Police College, Guangzhou, China
Panke Qin, Henan Polytechnic University, Jiaozuo, China
Guangxiao Chen, Universidad Carlos III de Madrid, Madrid, Spain
Qiang Liu, Zhejiang Police College, Guangzhou, China

ABSTRACT

In order to solve the security problems like single point failure, maliciously access or even destruction of the authorizing node that was caused by the lack of knowledge of trust evaluation of interactional nodes, this article proposes a trust evaluation strategy for single sign-on solutions in the cloud. The strategy improved the D-S evidence theory to verify the security of the peer nodes in cloud, including the calculation, combination and transfer of the direct trust and recommended trust. This solved the security problems brought on by evidence conflicts in trust combination and provides security insurance for single sign-on solutions in the cloud.

KEYWORDS

Evidence Conflict, Single Sign-On, Trust Combination, Trust Transfer

INTRODUCTION

Single sign-on solution is commonly adopted in cloud as the user accessing various resource and service in multiple nodes to accomplish a specific task (Chen, Du & Qin, 2013; Dai & Wang, 2014; Kumar, Abhishek, Singh & Kumar, 2015). Trust is the basis of single sign-on mechanism. Trust also is a natural attribute of human society. Some expanded the definition of trust by adding the concept of predictability. Some defined the trust in the context of network environment. These definitions and research all contain the evaluation to the entity behavior and is adopted in the research of node behavior and authentication in cloud (Noor, Sheng & Bouguettaya, 2014; Wierzbicki, 2011).

In the cloud, the authorizing nodes have to make access control decisions to the requesting nodes when different nodes visiting each other. Sometimes, the decision was made when there is little information about the required nodes. This will lead to the situation that the requesting node maliciously access or even destroy the authorizing node. So, it's necessary to conduct trust evaluation to the requested node before the authorization.

So, this paper proposed a trust evaluation strategy for single sign-on solution in cloud. The strategy improved the D-S evidence theory to calculate, combine and transfer the trust of the peer node so as to verify the security and behavior of the peer nodes in cloud. The strategy can help solve the security problems like single point failure, maliciously access or even destroy the authorizing node that caused by the lack of knowledge of trust evaluation of interactional nodes.

DOI: 10.4018/IJDCF.2018010101

DESIGN OF TRUST EVALUATION MODEL OF NODE

In this paper, each cloud server node is regarded as a unified entity of SP (Service Provider) and IDP (Identity Provider) and as a peer node N_i for single sign-on in cloud. The distributed and dynamic characteristics of the cloud resources determine that SP adopted the policy of "fully trust" or "totally do not trust" to the verification certificate provided by the IDP. As for the previous centralized single sign-on model, the credibility and determinacy will decrease with the increase of the number of the entities. Usually, for a certain peer node in the group which contains a large number of peer nodes often can't obtain the whole information of the other peer nodes. Therefore, this paper proposed a trust evaluation model for the peer node N_i.

Each peer node N_i has a list that records trust evaluation value of the other peer nodes. The trust value of the peer node can be represented by triples $T_{tuple}(\alpha, \beta, \gamma)$, and $0 \le \alpha, \beta, \gamma \le 1$, $\alpha+\beta+\gamma=1$. Here, α refers to the probability of "can trust" of the peer node; β means to the probability of "can't trust" of the peer node; γ represents the probability of uncertainty of the peer node. According to the different understandings of the trust of the peer node (for example, peer node N_i considers it is trustable only when $\alpha > 0.9$, while N_j thinks it is fully trustable as long as $\alpha > 0.7$), the values of α, β and γ are continuous rather than discrete. According to the role and function, there're four types of trust: trust of SP, trust of IDP, recommended trust of the SP and recommended trust of the IDP.

Suppose the trust evaluation value of source peer node N_s to destination peer node N_d is $(\alpha_1, \beta_1, \gamma_1)$ and trust evaluation value of the other peer nodes to N_d is $(\alpha_2, \beta_2, \gamma_2)$, the finally trust value of N_s to N_d can be calculated through:

$$t(\alpha, \beta, \lambda) = (\alpha_1, \beta_1, \lambda_1) * t_1 + (\alpha_2, \beta_2, \lambda_2) * t_2 \quad (1)$$

Here, t_1 and t_2 are empirical coefficients which determined by each peer node according to their own situation, and $t_1 + t_2 = 1$, $t_1 > t_2$. Generally, the peer node has greater trust value over their own judgment than that over external judgment. So, for the last two types of trust, $t_1 = 1$, $t_2 = 0$.

CALCULATION, COMBINATION, AND TRANSFER OF TRUST

Direct Trust Calculation

Direct trust means one entity (here refers to node) obtains the trust value over another entity according to the direct interactions in the given context.

The direct trust in the trust evaluation strategy includes three types: direct trust of IDP, direct trust of SP, the direct evaluation to the recommended trust of IDP and SP. As for the calculation of the direct trust of IDP, a variety of factors are taken into consideration, e.g., authentication technology, the quality of the service that provided by the IDP to the SP (response time, rejection probability, online time, and so on), the behavioral level in the SP of the identity information provided by IDP, the last time that IDP provides identity information, and so on. Similarly, the quality of service provided by the SP, whether there exists malicious behavior when the SP requires IDP for service, whether the SP legally use the node information provided by the IDP, the last time the SP requires for service, and other factors are taken into consideration when evaluating the direct trust of SP.

Here, each node N_i will associate a direct trust list L_{dir}, which records the interaction number between the service node and other nodes in cloud, the latest interaction time and the latest evaluation from the accessing node. The direct trust value L_{dir} of destination node N_d over accessing node N_s can be calculated through:

$$T_{dir} = (m_s(T, t_s), m(F, t_s), m(T, F, t_s)) \quad (2)$$