Research on Control Technology of Cloud-based Security for Mobile Terminal

Chong Li

Information Engineering School Chongqing Vocational Institute of Engineering,Chongqing 402260,China

lizong@sohu.com

Keywords: Mobile Internet, mobile terminal, cloud security, control technology.

Abstract. According to the researches on the safety status and security products in mobile terminals, this paper analyzes the security issues faced by mobile terminals and pointed out the deficiencies of the existing security products and security researches. By using a proxy server and cloud security technology, this paper proposes the use of the cloud to solve the current difficulties faced by mobile terminals and then propose cloud-based mobile terminal security architecture. According to the proposed security architecture and the system architecture, this paper designs and implements a cloud-based security system for mobile terminals. This paper confirms that the system is able to enhance the safety of mobile terminals through solving the current problems faced by mobile terminal.

Introduction

In recent years, the mobile Internet is developing rapidly. Three aspects of intelligent mobile terminals including hardware, software and bandwidth are improved. With mobile terminals becoming more and more powerful, more and more users use mobile terminals processing and transmitting data. [1] The security problems of mobile terminals will become increasingly prominent. Mobile terminal operating system is facing the most serious challenges due to its openness market share. Mobile terminal has its own characteristics compared with the PC. [2] Due to its slow processing speed, small storage space, limited battery power and easily lost, the security measures to protect PC are generally not able to directly migrate to the mobile terminal. There are some limitations on the existing security products and researches for mobile terminals. This paper designs and implements a cloud-based Mobile terminal mobile terminal security system to improve the defects and shortcomings of existing security products and security researches.

Related work and technology

As the development of Cloud Computing and the popularization of Intelligent Mobile Terminal, providing cloud service has become one of the most important applications of Cloud Computing. Because of the distributed and dynamic characteristics, resource sharing between different domains faces new security challenges. This paper researches resource access control under mobile and cloud environment. [3] The model uses access control to achieve cross-domain resource protection.

From the security requirements on cross-domain resource, combining with the current situation of the access control model in existed system, the paper proposes a new cross-domain access control model with risk mechanism. [4] This model imports risk management to RBAC model. The model not only uses cursor in the required domain, but also extends it to the domain which starts the requirement.

We assume $x=\{x_1,x_2,...,x_n\}$ express the entity domain. The indicator set is expressed as Y.

The risk Is defined as follows:

$$Y(x)=\begin{cases}1-\dfrac{S}{\sum(S+F)} & \sum(S+F)!=0\\ 1 & \sum(S+F)=0\end{cases}$$

Where, *S* and *F* express respectively the number of success and failure in the system.

This risk cursor mechanism enhances the security of cross domain requirement. In addition, the model also imports timeline in each domain which involved in the requirement. The timeline binds with the risk level in order to realize the granule of the cross-domain access control. It is determined by the human beings according to the experience. The nodes which require longer time may involve higher risk. [5] With risk and timeline mechanism, a fine-grained authorization mechanism is enabled. This new model also set threshold of visiting time to limit the frequency of the requirement, in order to restrict the frequency of the requirement. It will avoid the happening of the centralized malicious behavior. Use 0 or 1 to mark which resource the management node can see. Through the method of restrictions on history records management node visit, this model realizes privacy protection on the historical records. The level of entity risk is followed as Table 1.

Table 1 The entity level of risk

1	0-0.2	Very low
2	0.2-0.4	Low
3	0.4-0.6	Risk
4	0.6-0.8	Higer risk
5	0.8-1.0	Higest risk

We can seen from Table 1 that the risk level 0.8-1.0 is the highest risk, while the risk level 0-0.2 has the lowest risk.

Design and implementation of mobile terminal system

Considering the frequent migration characteristic of mobile terminal and the research actuality of existing delegation based RBAC access control, the delegation based cross-domain access control model in cloud computing of the mobile terminal is presented. By introducing the delegation mechanism, this model can effectively solve the problems which due to the frequent migration of mobile terminal.

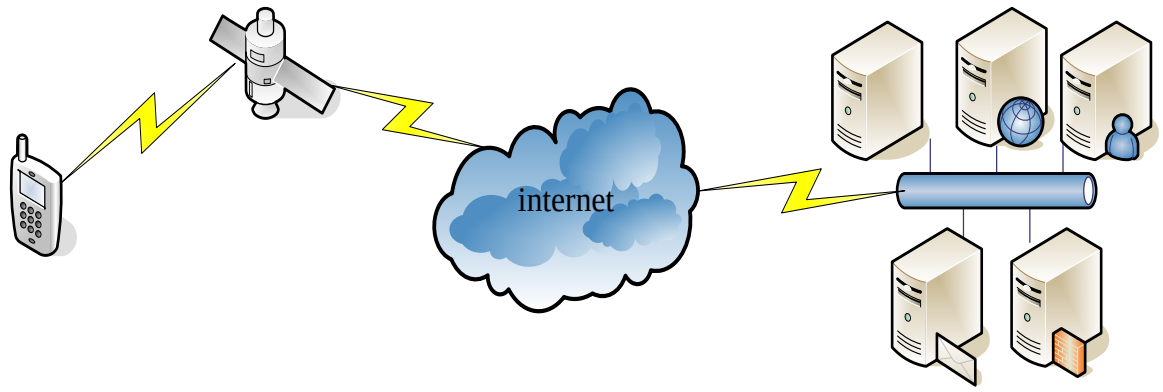

Fig. 1 System network topology

When the mobile terminal moves to another domain which is not the start domain of the cross-domain requirement, it will bring new problems to the interaction. This model makes the management node of each domain maintain a dynamic routing table. When the node leaves the domain, the management node will add a new record to the routing table. This dynamic routing table solves the localization of nodes. The model defines two kinds of mapping roles which named local mapping role and role based requirement. Also, we propose a synthetic method to obtain synthetic mapping role. Combining the quantified-role method, the delegated node obtains the final mapping role of this cross-domain requirement. This model can effectively solve the problem of permission hidden ascension in the process of the mapping. The requirement frequency threshold will avoid the risk which is caused by the malicious node's excessive operation. Analysis shows that the model has better security. The network system topological graph is shown in Fig. 1.

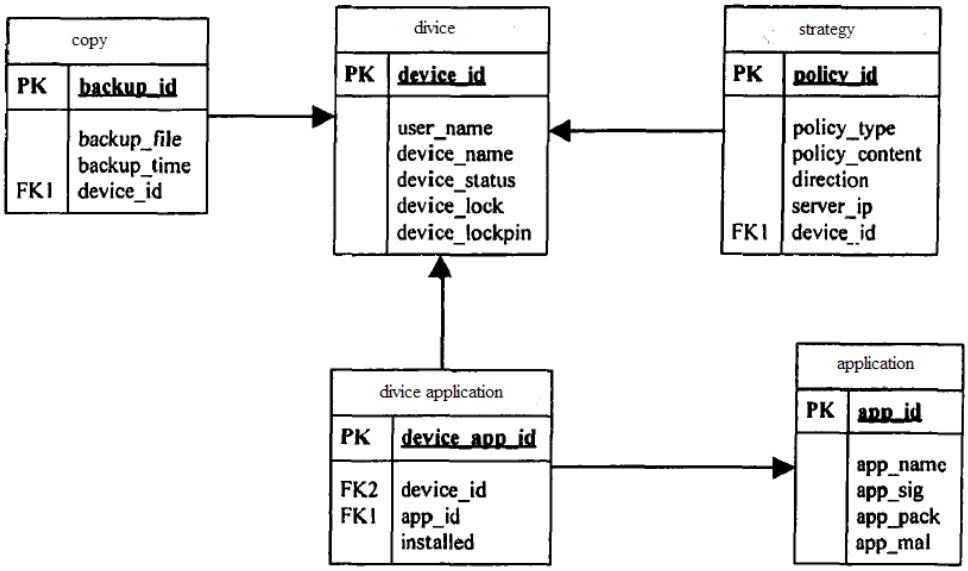

Fig. 2 The structure of management server database

We can seen from Fig. 2, three are five aspects in the structure of management server database, that are copy, device, strategy, device application and application.

Authentication of cloud security

Authentication of cloud security, as the basis of cloud security, is the guarantee of other security strategy, if other security strategies can take their effect. In the present way of cloud security authentication, most of cloud products take the certificate based traditional authentication, in which certificate is the most important part. However, traditional certificate-based authentication, due to its inherent certificate operation of certificate request, certificate verification, certificate sending and so on, has lower efficiency in computational and communicating cost, which increases cloud terminal's load and makes cloud terminal have a poor scalability. In addition, certificate management of certificate granting, revocation, issuing etc also is a fussy work. In allusion to the character above, in this paper, we propose an identity-based cloud security authentication scheme which regards the hashing value of some user's legal identity as the user's public key, vivificating the user's public key only by the user's identity and the hash function, and has the characters of non-certificate, shorter key size and less interaction etc.

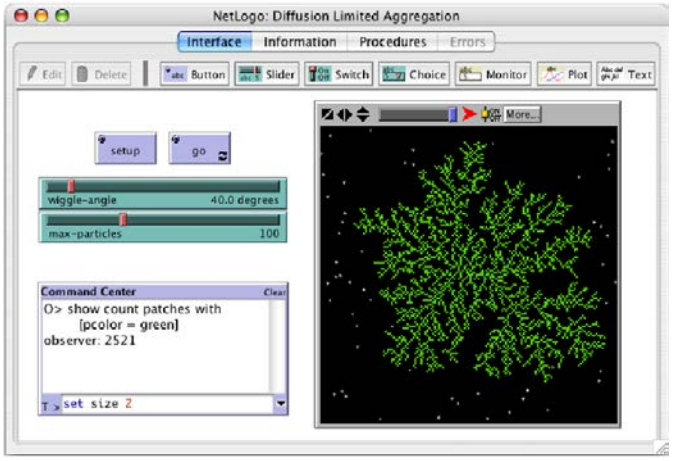

Fig. 3 Control interface

Control interface is shown in Fig. 3. This scheme is implemented by bilinear function, an emerging cryptographic technique, and its security is ensured by BDHP (Bilinear Diffie-Hellman Problem), in addition, in this scheme, we use exclusive or, a less cost operation, when constructs conversational key, instead of public operation in traditional authentication. By the result of the simulating experiment, we can find that the efficiency of authentication is improved much. And

farther, we also analyze the reason why the SAP (SSL Authentication Protocol) has lower efficiency in computational and communicating. Longer key size，using digital certificate，interaction for many times contribute to the lower emergency of SAP, which also displays the excellence characters of short key size, non-certificate, less interaction of Identity-based Authentication.

Furthermore, this paper proposes a solution for the secure transmission of cloud user data. Firstly, set up a cloud computing system according to the existing cloud computing system structure. It analyzes the data transfer process of cloud computing that build, learns that there are two aspects to the threat of data: 1) security threat, private information may be intercepted by hackers; 2) integrity threat, data may be tampered by hackers. In response to the above threats, the paper proposes the use of double encryption and message validation technology to ensure the security and effective transmission of user data. The specific implementation plan is that, different users use different symmetric key to encrypt the users' sensitive data with symmetric encryption algorithm, and generate a message digest. The distribution of symmetric key is using asymmetric encryption algorithm. Secondly, The paper designs and implements a cloud computing security transmission system. The system consists of six modules: the client module, the main server module, the block server module, symmetric encryption module, asymmetric encryption module and information check module. The cfient uses the MDS algorithm of the hash function to generate a message digest, then encrypts and transmits the extensible message with DES symmetric encryption algorithm. For the symmetric key distribution between a particular client and sub-nodes, it uses RSA asymmetric encryption algorithm. Finally, testing and validating the cloud computing security transmission system. The experiment shows that the system is safe, both can safety and completely transmission the user' sensitive data and can safely distribute user keys.

Conclusions

Terminal security system framework is proposed for mobile cloud. The key technology of framework is introduced first in this paper, including system, proxy server and cloud security technology. Then study on cloud security and cloud-based thought, combined with mobile terminal system and proxy technology understanding, this paper proposes the use of proxy implementation of mobile terminal security framework based on cloud.

Acknowledgements

This work was supported in part by a grant from Yunyang Teachers’ College in 2014 for the scientific research project “The key technology and application of large data reliable storage based on Internet” (No. 2014C18)

References

[1] Information on http://www.gartner.com/idpage.jsp?id=22373 l5

[2] D. Ferraiolo, R. Sandhu, S. Gawila, et.al. A Proposed Standard for Role Based Access Control. ACM Transactions on Information and System Security, 2011, 4(3):224-274.

[3] James B. D. Joshi, E. Bertino. A Generalized Temporal Role-Based Access Control Model. IEEE Transaction on Knowledge and data engineering, 2005.

[4] P McDaniel. On Context in Authorization Policy. ACM Symposium on Access Control Models and Technologies, 2013.

[5] Liu Peng, Shi Yao, Li San-li. Computing Pool:A Simplified and Practical Computational Grid Model. Shanghai, China:Grid and Cooperative Computing, Second International Workshop, 2013, 661-668.