2013 Sixth International Symposium on Computational Intelligence and Design

Research and Application of Access Control Technique in 3D Virtual Reality System OpenSim

Yun-gang Wei, Yang Lu*, Xiao-yan Hu, Bo Sun
College of Information Science and Technology
Beijing Normal University
Beijing, China
luyang1210@gmail.com

***Abstract*—Access control in 3-D virtual reality systems is a wide and still growing topic. A good access control model is a premise for data security, and makes the whole system play its functions reliably. We compare access control techniques in 3D system OpenSim with that of other virtual reality systems. By using a general extended scheme, we analyze the model and the rule of access control in OpenSim. In this scheme, we provide a method of expanding network services for special proposes. Meanwhile, it verifies the feasibility of developing OpenSim's services on the basis of data security.**

Keywords-Access Control; Capability; Virtual Reality; OpenSim.

I. INTRODUCTION

In recent years, with the growth of virtual reality, various 3D virtual platforms have emerged, and they are always built on distributed systems. Such platforms are able to support thousands of users to interact with each other, sharing information on business, education, social science, news and cutting-edge technology in it [1]. However, these systems are more vulnerable to be attacked in the network because they always run on multiple computers [2]. When it comes to more complicated network environment, a variety of defects in early security techniques may emerge. In this paper, we will give an analysis of access control techniques from 3D virtual reality systems. Then, we take the OpenSim as an example, explaining its advanced access control model with centralized identity authentication and role-based resource management. Based on a well understanding, we design and add an interface of real-time animation import in it, so that prove its scalability and compatibility.

This paper is arranged into 5 sections: in section 2 we present the current research of access control techniques. Through the OpenSim, we summarize common characters of access control in these systems; section 3 analyzes the identity-based Capability in OpenSim, including the initialization, authorization and revocation; in section 4, we design a human-computer interaction function real-time animation import, by extending a new interface in the system. We all think that this work prove it can be compatible with such newly integrated functions; Section 5 draw conclusions and present research directions in future.

II. BACKGROUD

International Standardization Organization (ISO) put forward five security services: authentication, access control, data security, data integrity and non-negation [3]. As one of them, access control stands an irreplaceable position because it can prevent illegal access and malicious tamper to data resources. Therefore, access control should be applied reasonably in network to guarantee system security.

A. Access Control

According to safety strategy, access control falls into Discretionary Access Control (DAC) and Mandatory Access Control (MAC) in early years. Within the MAC, subjects and objects both add with security properties as their respective fixed levels, which would be checked by the system so as to determine whether the access is allowed. Access Control Lists (ACL), Capability, and the Role-based Access Control (RBAC) are basic methods of DAC. ACL is the mode storing Access Control Matrix by column, while as the dual approach, Capability views the matrix by row. In RBAC [4], subjects are categorized as different roles, mapped to different sets of access rights. However, as the collaboration spaces interconnect to form a distributed network, access control techniques are being more fine-grained and hierarchical. Catering to diverse network environments, different models like Trust Based Access Control [5], Attribute Based Access Control [6] and Task Based Access Control [7] have been widely used.

B. Access Control in Virtual Reality Systems

As 3D virtual reality platforms have been used widely, security issues in resource sharing and collaboration should be considered seriously, and they should be handled by access control techniques properly. Platforms like Active Worlds, [8] simplify the work by using "privilege password", which enable object owners to grant access privileges to anyone else; Open Wonderland [9] associates each object with an ACL, which determines who has the right to view, move or modify it; OpenSim use identity-based Capability and RBAC together to solve general security issues in virtual reality systems.

Identity management is a necessary component for each virtual reality system, while most platforms authenticate users by checking their username and password. Through

978-0-7695-5079-4/13 $26.00 © 2013 IEEE
DOI 10.1109/ISCID.2013.130

this technique, system will generate identity-based capabilities to prevent access rights from being stolen. This is a predefined, fixed and coarse-grained access control model. As shown in Fig.1, after authentication, system generates and distributes a set of capabilities for each user, which are formed as identification-based URLs, and serve as access tokens to the content, like "Inventory/Item_move" and "BakedTexture/Upload". This model just classifies users into two groups: the legal and the illegal, without any specified access rights to services.

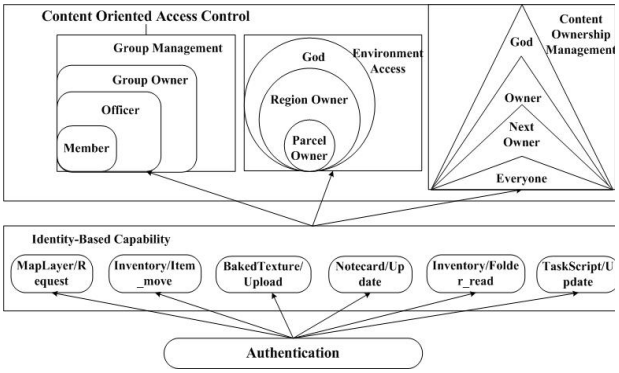

Figure 1. Access control models in OpenSim.

Since User Generated Content (UGC) has been used by 3D world users, developers find content-creation function would be helpful to keep long-term users [10]. However, only by coarse-grained access control is not enough. As shown in Fig. 1, there are three types of management models from RBAC, including content-ownerships management, group management and deal with region management. Through pairing several predefined roles with different capabilities, it simplifies the whole management. Usually, 3D virtual reality systems need to manage a large number of users with different identities and deal with various problems in resource sharing and collaboration. Therefore, access control is seemed to be more significant. In OpenSim, identity-based Capability and RBAC models woke together with different granularities, to solve basic security issues in virtual reality systems.

C. Demands of Access Control

Now we learn that, OpenSim use a coarse-grained access control method to filter users, such as identity-based Capability in OpenSim. Considering the privacy and ownership of the objects in virtual world, it needs to refine data security further. Therefore, methods too coarse will limit users to create new interactive contents or modify existing objects. Principles of 3D virtual reality platforms designing are to promote user creativity and interaction.

III. CAPABILITY IN OPENSIM

A. OpenSim

OpenSim consists of database, server and one or more clients. Server in OpenSim includes two independent sub-servers, Simulator and Robust [11]. Simulator can receive requests from several clients, and then processes them in detail. Afterwards, the information is sent to certain modules in Robust. Robust supports all kind of network services, within the modules of Inventory, Asset and User, while these services are not specified objects, but the interface to memory. Persistent data, such as profiles, motions and outfits of characters need to be stored in database.

B. Capability in OpenSim

Both OpenSim and Second Life use the identity-based Capability. Second Life OGP (Open Grid Protocol, OGP) defines the protocols by which a vast, Internet wide virtual world can operate. It is about a three way interaction between viewer, agent and region providing shared experiences between people [12]. By making extensive use of capabilities, it solves the security issues better.

For the URL-based format, these capabilities are capable of resource location. As shown in Fig. 2, it is composed of protocol, host, port, Capbase and service code. As the root, Capbase is the symbol ensuring itself is the unique during a given session. Service code is typically a four-digit string, which can be used as the code of service and can be mapped into the specific service name afterwards.

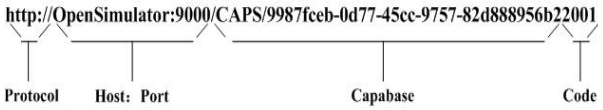

Figure 2. Format of the capability.

1) Authentication and Authorization

Compared with ACLs, Capability has an obvious advantage in distributed resource management, which means users can search capabilities locally. Different network structures use different methods to get capabilities. So, considering network security, only the server has the right to authorize capabilities in OGP.

In the stage of authentication, there is a string of UUID (universally unique identifier, UUID) generating from server, serving as the session token in this period (Fig. 3). It is Capbase, the root of capabilities. Service code here can be defined as '0000', which represents the Seed Service. Both of them will be transmitted to the Capability Server and assembled as Seed Capability, according to the standard format. Finally, the first capability, Seed Capability, will be sent back to the client.

In the stage of capabilities request, clients can request more capabilities by invoking Seed Capability with a two-dimension table full of service names to server. After receiving this, server calls the Seed Service, creating the relevant URLs and loading them into the table. Finally, this table will be sent back again.

2) Revocation

In OGP, capabilities may be either unlimited or one-shot. Unlimited capabilities can be used multiple times, whereas one-shot can be used only once and are automatically revoked on invocation. Additionally, all the capabilities' lifetimes are limited to a given session of user interaction. When a user logs out, system is going to find all the

capabilities and revoke them before shutting down the system.

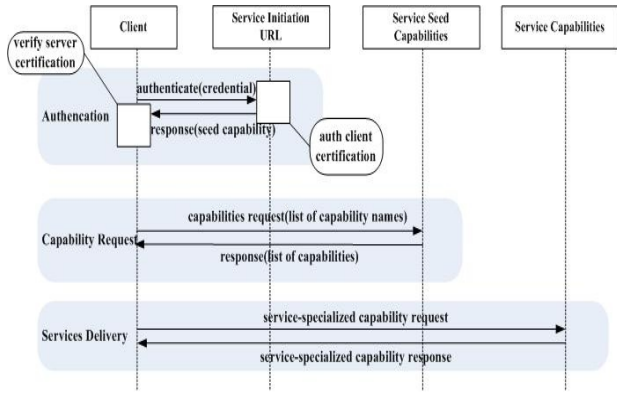

Figure 3. Access control models in OpenSim

C. Advantages of Capability in OGP

There are three advantages of the identity-based Capability.

First, only server has the right to authorize clients in system. Server of distributed system needs to deal with different information, some of which may come from incredible terminals. Therefore, there is a design principle in OGP: only server can create and authorize capabilities. After that, server requests a set of capabilities to legal clients. When users ask network services, they should invoke the corresponding capabilities. This mechanism could avoid illegal diffusion in the classical model.

Second, there is a centralized authentication module in system. Users need to be authenticated before receiving any capability. Only by holding capabilities can they use any basic network services. As OpenSim is composed of multiple modules written in different languages and frameworks, by using the classical way, user may be authenticated for several times. Certainly, this will strain system resources. To solve this problem, OGP adopts a centralized authentication module in server. In this mechanism, security issues could be solved in a central place, Capability Server, which is transparent to any clients. Modules in Robust can receive actual URLs from Capability Server. This centralized module facilitates developers expanding other network services. In next section, we will give a scheme.

Third, system uses a prior authorization mechanism. When sending the same request repeatedly, it usually needs to authorize this client continuously. However, this method no doubt triggers the issue of delay. In OGP, each legal client can hosts a set of capabilities locally. It means that clients can search the token in local, instead of being authorized by the server again and again. This pattern undoubtedly improves the efficiency of the system.

IV. SERVICE EXTENDING

As is introduced above, we have analyzed the identity-based Capability and explored its advantages. Following BSD open source agreement, OpenSim facilitates developers designing and creating their own customized 3D world for their own purposes. In this paper, we have designed and extended a new interface, real-time animation import by adding a new capability and its corresponding functions. Through this work, we can see the access control model could be compatible with new functions, and this can guarantee the data security when doing this work.

A. Real-Time Motion Import

As a new technique, real-time animation can be applied in many fields, such as real-time simulation, distant education, and virtual movement [13]. It is popular to use motion capture devices like 3D mouse, data glove, camera or Kinect to import standard data and execute them instantly through an interface. By implementing this function, quality of human-computer interaction could be improved. Meanwhile, it also verified that expanding OpenSim's services based on the identity-based Capability is feasible.

B. Design and Extending

As is described above, identity-based capabilities manage the basic services in OpenSim, such as the manipulation to inventory, script and content. Also, they are not assigned to the selected object.

There is a file system to read, transmit and store multimedia files in OpenSim. Take "animation upload" as an example. First, such files should be serialized to binary data flows, which are named as "asset", a unified format in system. Then, new assets are stored in database and the item, an interface of data will be generated in the Inventory. For each item, there must be actual data stored in database persistently.

File system usually needs two communications between the client and server: storing data and creating the relation. When a client needs to upload a file, it will send a request to invoke the capability, like

http://OpenSimulator.com/CAPS/4641464353550002

Actually, they are all fake ones, only the visible form with a cryptographically secure path component. Within Capability Server, these URLs can be mapped into the actual internal URLs. In the stage of services delivery, clients may invoke capabilities to perform an HTTP transaction with the capability as the URL. By this step, we can know the operated resource and the access mode.

"0002" is the service code represents Inventory management. After receiving this, server will invoke the function "NewAgentInventory", create an asset unit and a random service code, such as "5968". According to the format, server needs to form a new one corresponding to the function Asset storing, just like

http:// OpenSimulator.com/CAPS/4641464353555896

Again it will be sent back to the client. This time by invoking the newly produced capability, it can store files and generate relations by calling the service "UploadAsset". After that, user could manage multimedia files in the virtual world directly.

Real-time animation import is an interface extended in the next step. It is completely different from the mode of animation uploading. As a function of loading and performing animations instantly, it is unnecessary to store disposable data or create relations, so the work can be finished by one-time communication. Additionally, to assure data security in system, we need to make it meet the identity-based Capability. By defining a new service named "RealTimeAnimation" on both sides and setting the service code "0007", it can be obtained in Seed Service as a basic service. Unlike normal data, the real-time data could be cached in memory instead of disk (Fig. 4), which reduces the amount of disk reads and improves the system performance.

For demonstrating its effect, we add a UI on the client interface as the switch of real-time animation import. In this experiment, we use a buffer for dynamic read-write. Supposed animations are produced from interactive devices and stored in this buffer, we click the switch to invoke an animation every 5 seconds, which includes reading the buffer and rendering on the character.

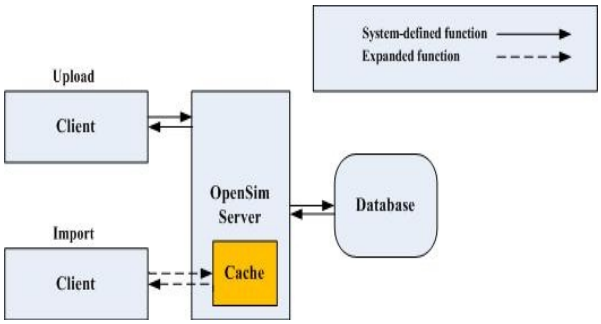

Figure 4. Two storage modes of files management

V. CONCLUSION

We have set up several experiments to confirm the feasibility of the function of real-time animation import. This service will fill the blank 3D system integrates with external devices such as Kinect, a motion sensing input device. What's more, it is of a great significance to build a safe virtual world:

- We extend this service under the identification-based capability mechanism, which greatly ensures data security and verifies the compatibility of the model.
- This work present a guideline for developing new applications in the network based on the data security.

However, we have to admit the shortage in our work: as an independent module, Capability Server is responsible for mapping the URLs to actual ones. Once there is a single point of failure, all the requests won't be processed normally. In the next step, we are planning to address this problem. Besides, aiming at the growth of UGC, we will design a new access control model to support multi-user collaboration.

ACKNOWLEDGMENT

This work was funded by Beijing Natural Science Foundation of China (4102030). Authors would like to thank Ji-yi Xu, Bin Xie, Hao Wu and Shu-ling Zhang for many useful discussions and suggestions.

REFERENCES

[1] Craig, A., Sherman, and W.R., Will, J.D.: Developing Virtual Reality Applications: Foundations of Effective Design. Morgan Kaufmann, San Mateo (2009). pp: 110-112.

[2] Fernandez-Baca, D.: Allocating modules to processors in a distributed system. IEEE Transactions on Software Engineering. vol. 15, 1989, pp. 1427-1436.

[3] Gwo-Ching Chang: A feasible security mechanism for low cost RFID tags. International Conference on Mobile Business. Sydney, Australia (2005).

[4] Zurko, M.E., Simon, R., Sanfilippo, T.: A user-centered, modular authorization service built on an RBAC foundation, IEEE Symposium on Security and Privacy, Orlando, Florida, USA (1999).

[5] Huu Tran, Hitchens, M., Varadharajan, V., Watters, P.: A Trust based Access Control Framework for P2P File-Sharing Systems, Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Hawaii, USA (2005).

[6] Yuan, E., Tong, J.: Attributed based access control (ABAC) for Web services. IEEE International Conference on Web Services, Orlando, Florida, USA (2005).

[7] Sejong Oh, Seog Park (2003), Task–role-based access control model. Information Systems 28(6) 533-562.

[8] Active Worlds. http://www.activeworlds.com(2013). Accessed 5 January 2013.

[9] Open Wonderland. http://openwonderland.org(2013). Accessed 5 January 2013.

[10] Adam Wójtowicz: Secure User-Contributed 3D Virtual. Interactive 3D Multimedia Content. Springer, London (2012).

[11] Open Simulator. http://opensimulator.org/wiki/Main_Page (2013). Accessed 5 January 2013.

[12] OGP. http://wiki.secondlife.com/wiki/Open_Grid_Public_Beta (2013). Accessed 5 January 2013.

[13] Amit Bleiweiss, Dagan Eshar, Gershom Kutliroff, Alon Lerner, Yinon Oshrat, and Yaron Yanai: Enhanced interactive gaming by blending full-body tracking and gesture animation. ACM SIGGRAPH ASIA, New York, USA (2010).