A Survey of Security issues in Collaborative Virtual Environment

Seunglim Yong, Hyun-Yi Moon, Yuseung Sohn, Miguel Fernandes

Institute for Graphic Interfaces, Seoul, KOREA

Summary

Collaborative virtual environments (CVEs) are computer-enabled distributed systems that allow multiple users to work on different computers which are interconnected through different networks to interact in a shared virtual world. The security of CVE system becomes an important part of the system, because a weakness in CVEs might lead unpleasant results. In this paper, we survey the CVE systems and security issues in CVEs. We also suggest representative applications of CVE and major security requirements extracted from features of those applications and introduce security solutions of those requirements.

Key words:

Collaborative virtual environment, virtual reality, security requirement, security solution

1. Introduction

In recent years, due to the explosive growth of the network and computer technologies, many valuable materials can be shared with each other via networks. There has been much researches done in computer applications for facilitating collaboration among multiple, distributed users.

Collaborative virtual environments (CVEs) are computer-enabled distributed systems that allow multiple users to work on different computers which are interconnected through different networks to interact in a shared virtual world [13]. Like other distributed simulations, CVEs are shared virtual reality spaces where remote users can participate in a simulation.

In CVEs, one of the main research topics for such environments is how to efficiently transmit messages to provide scalability, minimized delay, and reliability. CVEs need to be designed to allow groups of people from a diverse set of organizations and locations to work together easily and securely. However, the security of the CVE system gradually becomes an important part of the system, because a weakness in CVEs might lead unpleasant results, especially when implemented without security considerations.

In this paper, we introduce the collaborative virtual environment and its application. The rest of the paper is organized as follows. We begin by reviewing the CVEs and security requirements in section two. Then from section three to five, we describe the security issued in CVEs application. Finally, we offer conclusions in section five.

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

2. Collaborative Virtual Environment

Collaborative virtual environment (CVE) provides a common space for people to meet and interact with each other. They have their roots in the earlier virtual reality.

2.1 Collaborative Virtual Environment

Virtual reality (VR) is a technology which allows users to interact with a computer-simulated environment as if the users are present in one place of the environment, even when one is physically not situated in that environment. At the time of its occurrence, VR is composed of a single system used by a single user. According to the progress of computer networks along with the development of internet facilitates, the computers are connected over a network and people using those computers are able to interact and collaborate in real-time, sharing the same virtual world.

CVEs are computer-enabled distributed systems that allow multiple users, working on different computers that are interconnected through different networks to communicate in a shared virtual world [13]. CVE can be seen as the result of convergence of computer supported cooperative work (CSCW) and virtual reality. It makes possible to support people working collaboratively in a visual way.

There are two basic foundations of CVEs. At first, 3D virtual worlds provide the three-dimensional view and immersive environment. Second, distributed systems are necessary to offer multi-user and collaborative tools capabilities. CVEs create realistic 3D (virtual reality) displays and provide a rotational capability for views inside, above, beside, or under objects and systems in reduced, normal, or large scale. It makes the significant reduction of the time of new commercial product development and military system operational readiness, and overall development and manufacturing costs [4, 19].

2.2 Architecture

Since CVEs allow geographically distributed participants to collaborate with one another through a synthetic space, network system is essential. CVE systems are various significantly in the ways in which they handle the issues of distribution. There are two types of architectural approaches in the existing CVE systems [5]: Client-server model and decentralized model.

1) Client-server model

This is the classic and most used model, because it is the easiest model to be implemented. In this model, one common server collects all of the data from the different client's machine, stores the changes in some collection of data structures (the centralized database) and then sends the results back out to each participating client's machine. Each participant's application communicates only with a server that is responsible for passing messages to other clients. Although this model has a simple data structure to store and handle the data, it is not scalable. As more processes enter the simulation, they must wait increasingly longer on the bottlenecked, centralized computer.

2) Decentralized model

The alternative, more scalable model is decentralization. The idea is that all components in the distributed system have the same responsibilities acting both as clients and servers. The most wide-known decentralized models are peer-to-peer model. In the peer-to-peer architecture, there is no central server to keep status of the whole system. Each peer maintains its own copy of the virtual environment states and exchanges data directly with other peers. When a program makes changes to its own database, it sends the update data out so that other programs can update their individual databases. There are two types of peer-to-peer architecture. In a peer-to-peer unicast, each individual client program sends information directly to other client programs. Typically, this is the most bandwidth-intensive of the three approaches, but it avoids placing additional load on particular server machines and typically introduces lower network delays. In a peer-to-peer multicast architecture, similar with peer-to-peer unicast, the same information is sent simultaneously and directly to many other client programs. It normally uses a bandwidth-efficient network mechanism such as IP multicast. Multicast is simply a subset of broadcast, where groups of processes can be established, and only those groups receive the message [2, 3, 11, 12, 18].

2.3 Security requirement

For designing the security system, it is necessary to consider information assurance such as confidentiality, integrity, availability, non-repudiation, and authentication. The followings are security requirements based on information assurance in CVE system.

Confidentiality: The data should be encrypted so that the data could not be viewed from outside. And the system needs to protect the channel transmitting the data so that attacker cannot eavesdrop the data. That is, not only the data on storage but also the data in transmission should be protected from attackers [15, 16].

Integrity: The data should not be modified or deleted by unauthorized users or malicious programs. For this, the system has to confirm that there are no erroneous data or unauthenticated modification of data. In addition, the system should inspect virus or backdoor program [16].

Availability: Users should be able to access the system whenever they want to use the system because some applications need a time critical process [16].

Authentication: There should be no extra overhead imposed on users to be authenticated by the system. In addition, we need to build an access control system for server and clients classified by rights [22].

Non-repudiation: When the data of every view are updated or modified, the system must be able to positively identify the source of the data. Therefore, the system should maintain the evidences of the origin of the data and receipt information [23].

For maintaining secure CVE system, every five security requirements should be satisfied. The vulnerabilities of the system, however, are different from each feature of applications. From the next sections, we introduce the main applications fields and security issues from features of applications in CVE.

3. Collaborative work

In CVEs, groupworking is one of the most common and interesting aspects to study. In collaborative work area, there are two applications: military team training and manufacturing system.

1) Military team training

In military environment, CVEs are more than just research tools; they can be used to gain a competitive advantage, generate revenue or reduce operational and developmental costs. For example, development of systems and the training of personnel can be performed without placing humans and the real systems in harm way

(e.g., virtual prototyping and combat flight training). In addition, within a military environment a high degree of early collaboration is imperative for the Army to rapidly develop and make operational a family of complex warfighting assets like the Future Combat Systems (FCS) which is a networked system of system provided by multiple suppliers [15, 16].

2) Manufacturing system

Collaborative design is the process of designing a product by ways of associated groups cooperating throughout the life cycle of the product. This would include people from various departments such as design, manufacturing, assembly, test, quality and purchasing, as well as those from suppliers and customers. Collaborative design environment enables remote designers to work together and to communicate among themselves on a common design project. The objectives of such a collaborative design team might include optimizing the mechanical functions of the product, minimizing the production or assembly costs, or ensuring that the product can be easily and economically serviced and maintained [2, 10, 17].

3.1 Confidentiality

In military team training application, the data are considered very sensitive. If the information of military transmits through the TCP/IP Protocol among the elements of simulation system, the eavesdropping and modification of the network packet is possible.

In manufacturing systems, the system is particularly dangerous because information that has been kept locally on systems presumed to be secure may be loaded across the network, where it is vulnerable to interception and modification. In addition, participants on wireless and wireless environments are easier to be intercepted data than wired ones. Not only the data in transmission but also the data on storage can be attacked by malicious users who want to acquire the data. The data used in the system are made for reviewing and producing the products of corporations. If a competitor can gain an access authorization to the design system without being detected, the competitors can gain and use the important data to develop their products. Therefore, the exposure of the data will generate a lot of financial damages.

Possible solution

There must be some way to identify compromised modules and the presence of malicious users/observers, as well as simple and complex/distributed network attacks. Current design ideas are based on research into both signature-and anomaly-based network intrusion detection systems (IDS).

For secure, stable and fast data communication between server and clients, the system should use VPN (Virtual Private Network). VPN provides secure data tunnels over an insecure network by adding secure protocols to the existing protocols. With VPN, the system can transmit the data safely to the other part of views.

In manufacturing system, the data in the server should be protected against the intruders. Once the data is collected by the manufacturing server, there must be assurance that the persisted data is logically separated by source. For example, if data was collected by tool, the data must be logically separated by equipment manufacturer, tool type and tool. All of the data are stored in the server and the server transmits these data to clients. The data to be stored need to be encrypted with robust encryption algorithms. In addition, the system needs an access control mechanism so that unauthorized user cannot approach the data [2].

3.2 Integrity

The data used in CVE system should not be modified or deleted by unauthorized users or malicious programs. Unexpected change of the data or program can influence the whole CVE system. Therefore, the system has to confirm that there are no erroneous data or unauthenticated modification of data. In addition, the system should confirm every server and client to review same object during reviewing. When the reviewing processes are posed and saved, every party should be assured that they review same object after they resume the processes. The system should assure other clients' data are updated correctly when a client modifies the data. If the data are modified or deleted during reviewing process by malicious users, the unexpected result will be generated and effect the whole reviewing system.

Possible solution

In manufacturing system, the system should assure that every participant review the same object and detect the unexpected change of data during the design phase. For the data integrity of the system, a timestamp and hash functions like one way function should be used to compare new data with old data and find the changes of data. With a timestamp, the system can make sure that every user reviews the same object. With hash functions, the system can find the error of data after transmitting across the network [2].

3.3 Authentication

The biggest problem of the manufacturing system is that users can easily approach to the system without any authentication procedure. Unauthenticated users can approach to the system, modify the data and use resources. Without authentication system, a malicious user could enter into the system and observe and interact with participants. A malicious entity may possess a copy of the application and is able to be accepted as an authorized participant. In addition, the system needs an access control mechanism which should authenticate every user in distributed computing environment and assure only authenticated users can access the computing resources. Similar to risks on confidentiality, without authentication, the corporation who possesses the product gets financial damages and corruption of the whole system in the worst case.

Possible solution

To ensure that data security is not compromised, data originating should be secured from the source. For example, X509 certificate-based strong authentication is required to ensure the manufacturing system is the application actually connecting to the tool. To allow for auditing and ensure that the data can only be read by those authorized, data coming from the tool should be encrypted for transmission. The system can use one factor of biometric data for authentication. The system can authenticate user with camera and microphone attached on the system without additional devices. Therefore, the system can use one method of face or voice, or multimodal biometric identification system by combining face, voice, and lip movement recognition or using face information and audio information can be useful to the system [7].

4. Entertainment

Interactive gaming is becoming more and more one of the dominant application areas for computer graphics. The related industry is growing very fast both in the location based entertainment (LBE) and the PC-game domain. A central aspect of online games is the interaction and collaboration that occurs between gamers. This involves the creation of a social space that includes in-game discussion and collaborative activity and the forming of guilds and groups around specific games. This interaction provides a network of support and assistance to gamers and forms a major part of the appeal of online games. Contemporary multiplayer 3D games can be considered as applications and extensions of virtual reality technologies. In MMORPG (Massive(ly) Online Multiplayer Network role-Playing Game) games or games like Lineage II or World of Warcraft are a good example of the success of these persistent virtual worlds [9, 14, 20].

4.1 Confidentiality

Since all packets exchanged among players and servers, or among peer players are in plaintext, a player can easily cheat by eavesdropping packets and inserting, deleting or modifying game events or commands transmitted over the network. Eavesdropping attacks are difficult to detect since they normally do not leave traces. Unfortunately, sensible information like passwords is still transmitted unencrypted over networks which makes eavesdropping very dangerous. Disclosure of information is more general than eavesdropping since it refers to any information obtained by an unauthorized person.

Possible solution

HTTPS (HTTP over TLS) can be used with server-side certificates to provide an encrypted channel over which a Web-based client can securely send information. For communication involving groups, there is a secure and reliable group protocol (SGL) with properties similar to TLS that X.509 certificates to create an encrypted multicast group.

4.2 Availability

In an online game system, a malicious player may easily block peer players whose IDs are known to him so that they cannot have access to the game or floods an opponent's network connection by launching network DoS attacks, and gets unfair advantages.

Distributed denial of service (DDoS) attack is a severe threat for game hosting. A DDoS attack exploits a number of subverted machines as attack bots to launch a large coordinated packet flood at a target. If the servers are flooded, players will not be able to play the online games at all. So the service availability of game servers is also a critical issue for games.

Possible solution

Technically, a DDoS attack is hard to avoid when using a peer-to-peer topology, however in client-server based games, simply not distributing other players IP addresses will avoid this problem. Attacks on game servers are also possible. This is unlikely to give any specific player an advantage, but it is likely to make the game unplayable for everybody. Using server software that drops non-game packets and technology such as XenoService will help to reduce the effects of such attacks.

5. Education

Many applications have been developed to support the provision of distance learning courses in CVE. CVEs clearly have the potential to enable innovative and effective distance teaching techniques. Students that work in groups need to communicate, argue and give opinions to other group members, encouraging the kind of reflection that leads to learning. Some projects are applied to collaborative virtual environments: MOVE, NICE etc. The MOVE initially designed to recreate collaborative virtual environments in the learning scenario. MOVE distinguishes teacher and student roles and provides interesting tools like professor-guided navigation or moderation capabilities. MOVE was used in medical educational settings and a whole hospital was recreated in the virtual world [6]. NICE is a system where children construct and cultivate simple virtual ecosystems, collaborate with other children remotely located and create stories from their interactions on both real and virtual world [1]. In [8], they suggest the security issues of distance education and possible solutions.

5.1 Integrity

In distance education, on-line exams must be handled. There will not be the physical presence of an instructor to monitor the students during the exam, leaving open. Furthermore, attackers may see, steal, or even modify the students' answers during the transmission or storage of completed exams. To make the outcome of online exams or quizzes more trustable, the data integrity of the results must be preserved.

Possible Solutions

It might be effective is continuous verification of the identity of the student using biometrics. A promising approach is monitoring of student activity. Patterns for activities vary with individuals. Clearly, biometric signatures must be protected from corruption or theft. Protection of data privacy and extent data integrity during transmission of the completed exams may be obtained through the use of SSL. However, the examination agent should sign the examination answers with the student's electronic signature and the signature of the agent. This would assure end-to-end integrity. The exam answers may be protected while in storage through the use of symmetric encryption (e.g. AES or triple DES). However, care must be taken in distributing and safeguarding the keys. Symmetric keys would be protected using asymmetric keys (e.g. using PGP or PKI).

5.2 Confidentiality

In the distance education environment, some data is considered confidential and shouldn't be revealed to others. Applications such as the Course Authoring and Student Assessment needs to collect students' learning performance information and this might be considered an infringement of the student's privacy. Besides, a student should be able to ask the instructor a question in private. The ensuing discussion should also remain private.

Possible Solutions

The learning service provider must have a privacy policy that states: what information it collects, what the information is used for, how long it is kept, whether or not it is shared with others and how it is protected. The provider may also use an electronic policy description language like the Platform for Privacy Preferences (P3P) to express the policy. This is rather limiting since it only states how the learning service operates rather than making adjustments for the individual preferences of students. Ideally, a more flexible policy approach would be used wherein, the privacy policy for each student states what private information the student is willing to share and under what conditions. The university as the provider of the distance education system can then negotiate with the students and come to some agreement on the collection of the learning performance information.

SSL can be used to set up a secure channel between the student and the instructor. All communication flows through this channel would be encrypted, ensuring network privacy.

5.3 Authentication

For both instructors and students, it is important to authenticate them before they can join activities of distance education. The authentication is the basic requirement for the administration function of distance education. The identity of the student and instructors must be authenticated upon logon. Especially, ensuring the identity of the online instructor is very important since the instructor has access to many aspects of the online learning system, including course material, student information, and student performance records.

Possible solution

In case of students, user ID and password authentication should suffice since it is in the student's best interest to attend the online course, and university course content is not generally secret or classified. If more stringent authentication is required, PKI and digital signatures may be used. If this approach makes deployment and the key

management costly, Secure Socket Layer (SSL), without a PKI deployment, can be applied.

As with all user authentications, using SSL can provide a secure connection to the instructor's computer to the e-learning system during username/password authentication. Since the number of instructors is reasonably stable, and low compared to the number of students, organizations may use a public key approach for instructor authentication. As well, role-based access control would be used to maintain the access safeguards, based upon the responsibilities of the instructor.

6. Conclusions

Collaborative virtual environments (CVEs) are defined as any environment used by some number of concurrent users located elsewhere, that perform tasks in cooperation to achieve common goals. CVEs have many applications and their use has resulted in the significant reduction of commercial new product and military system operational, and overall development and manufacturing costs.

In CVEs, the security is important part of the system because a weakness in system might have very unpleasant results, especially when implemented without security considerations. The researches, however, have mainly concerned only access control of architecture of CVE system which is included in five security requirements.

In this paper, we surveyed CVE and security issues in CVE. Especially, we introduced more important security requirements of CVE among five security requirements from features of application and security risks of each application. Then we introduced possible solution against the security risks. More research, however, is still needed in the areas of storage of semi-structured data i.e. XML documents and integration and querying of XML documents originating from different sources.

Acknowledgments

This work was supported by the IT R&D program of MIC(Ministry of Information and Communication)/ IITA(Institute of Information Technology Assessment). [2005-S-604-02, Realistic Virtual Engineering Technology Development]

References

[1] Kawamoto, André L. S., et al. "AVC-MV: Um Ambiente Colaborativo para aplicações Educativas," in Proc. of the 40 SBC Symposium on Virtual Reality, pp. 226-237, 2001.

[2] S. Bu, S. Boehm, M. Portela and H. Jo, "Collaborative Design Review in Virtual Environment," in Proc. of Korea Computer Congress 2007, vol. C, pp.229-232, 2007.

[3] K. Berket, A. Essiari and M. R. Thompson, "Securing Resources in Collaborative Environments: A Peer-to-peer Approach," in Proc. of the 17th IASTED International Conference on Parallel and Distributed Computing and Systems, 2005.

[4] http://www.crg.cs.nott.ac.uk/~sdb/CVEs.html

[5] R. Gossweiler, R. Laferriere, M. Keller, and R. Pausch, "An introductory Tutorial for Developing Multiuser Virtual Environments," PRESENCE, Vol3, No.4, pp. 255-264, 1994.

[6] P. García, O. Montalà, C. Pairot, R. Rallo, and A. Skarmeta, "MOVE: Component Groupware Foundations for Collaborative Virtual Environments". In Proc. of the 4th International Conference on Collaborative Virtual Environments (CVE), pp. 55-62, 2002.

[7] Ferdinand Hommes, Eva Pless, "Networking Support for Collaborative Virtual Reality in National, European and International Context," in Proc. of TERENA Networking Conference, 2004.

[8] N. Lin, L. Korba, G. Yee, T. Shih and H. Lin, "Security and Privacy Technologies for Distance Education Applications," in Proc. of 18th International Conference on Advanced Information Networking and Applications, pp. 580- 585, 2004.

[9] T. Manninen, "Interaction Forms in Multiplayer Desktop Virtual Reality Games," In Proc. of VRIC2002 Conference, pp. 223-232, 2002.

[10] Mackrell J. "Collaboration in product development. Desktop Eng 2000," pp. 8-14, 2000.

[11] Khoury, M. Shen, X. Shirmohammadi and Shervin, "Peer-to-Peer Collaborative Virtual Environment for E-Commerce," CCECE 2007, pp.828-831, 2007.

[12] Y. Pan, Marchese, T. Francis, "A peer-to-peer Collaborative 3D Virtual Environment for Visualization," in Proc. of the SPIE, Vol. 5295, pp.180-188, 2004.

[13] S. Redfern and N. Naughton, "Collaborative Virtual Environments to support communication and community in internet-based distance education," Journal of information technology education, vol. 1, 2002.

[14] Z. Szalavári, E. Eckstein, M. Gervautz, "Collaborative Gaming in Augmented Reality," in Proc. of VRST'98, pp.195-204, 1998.

[15] J. Song, J. Kim, M. Shin and K. Ryu, "Design and Implementation of Security System for Wargame Simulation System," Korea Information Processing Society, vol. 12-3, pp.369-378, 2005.

[16] E. J. Sallés, J. B. Michael, M. Capps, D. McGregor, and A. Kapolka, "Security of Runtime Extensible Virtual Environments," in Proc. the 4th International Conference on Collaborative virtual environments, pp.97-104, 2002.

[17] Saad, M and Maher, M. "Shared Understanding in Computer-Supported Collaborative Design," Comput-Aided Design, pp. 183–92, 1996.

[18] G. Tian and D. Taylor, "Design and Implementation of a Web-based Distributed Collaborative Design Environment," 2001.

[19] http://www.discover.uottawa.ca/

[20] J. Yan et al, "Security Issues in Online Games", *The Electronic Library*, Vol. 20, No.2, 2002.

[21] Z. Zhao, S. Johnson, X. Chen, H. Ren, and D. Hsu, "Research on a Visual Collaborative Design System: A High Performance Solution Based on Web Service," in Proc. of the International Conference on High Performance Computing and Applications, pp.611-615, 2004.

[22] A. Bullock and S. Benford, "An Access Control Framework for Multi-user Collaborative Environments," In Proc. SIGGROUP Conference on Supporting Group Work, pp.140-149, 1999.

[23] J. Onieva, J. Zhou, and J. Lopez, "Non-repudiation Protocols for Multiple Entities," Computer Communi-cations, Elsevier, Vol. 27, pp.1608-1616, 2004.