Security Model for Large Scale Content Distribution Applied to Federated Virtual Environments

Adam Wójtowicz

Department of Information Technology, Poznań University of Economics
ul. Mansfelda 4, 60-854 Poznań, Poland
awojtow@kti.ue.poznan.pl

Abstract. In federated multimedia systems new services can be dynamically added or updated, thus a synergy effect related to integration of distributed communities of users and service providers can be observed. However, the inherent security limitation of such systems is implied by malicious host problem, particularly the risk that host software would be modified in order to e.g. violate data confidentiality. In the proposed model the distributed content consumers are provided with encryption scheme securing the confidentiality and integrity of the content roaming with them from host to host e.g. in federated virtual environment. The decryption keys, shared with threshold schemes, are produced in particles that correspond to the subsets of the multimedia content with respect to its structure. The scenes can be reconstructed collectively, but in a selective manner, according to the user privileges. In consequence, the model allows for placing content safely on virtual environment hosts and mitigates the problem of the host code that can be malicious.

Keywords: secure content distribution, secret sharing model, federated system security, multimedia systems.

1 Introduction

Interactive scenes are attractive content form for the modern digital citizens [1], e.g. scenarios based on 3D models of virtual museum objects [2]. Promising container technology for such content is federated virtual environments [3][4] such as Hypergrid [5], for two main reasons. First, they are based on open architecture – new regions on new hosts can be dynamically added to the grid by third parties. Such openness provides a developing market – growing population of active users. Second, they are based on functional, standardized, open, efficient and constantly developing software engines like OpenSim [6], and corresponding client browsers [7].

However, there is a significant obstacle for moving scenes of virtual museums or other content providers to the grid of federated regions (hosts). It is the problem of the data security [8][9], particularly the threat of piracy. In order to participate and contribute to virtual environments, publishers, content creators as well as users need to be sure that their rights to the content will be preserved. It requires assuring confidentiality and integrity of the scenarios that are distributed over the grid, which is hard,

X. Franch and P. Soffer (Eds.): CAiSE 2013 Workshops, LNBIP 148, pp. 502–511, 2013.

mainly because of the malicious host problem [10]. It cannot be assumed that host software has not been modified in order to make illegal copies of digital items that constitute users inventory [11], e.g. for the purposes of illegal pirate distribution. In case of the Hypergrid this is caused by the fact that federated architecture [12] requires user inventory (digital items) to be accessible for target hosts as the user roams from host to host, in order to be properly simulated, rendered or used. The simple authorization mechanism for Hypergrid described in [13] does not solve the problem, since obviously it is assumed that the host visited by the users is an "authorized consumer of the resources". The malicious host problem has been described and it is partially solved only if specific conditions are fulfilled or for specific sub-problems [14].

From the content publisher perspective, the possible partial workaround of malicious host problem in the grid is to set up an own region serving 3D scenes on the own host. However, such theoretically natural solution has a number of practical drawbacks (e.g. for a small or medium virtual museum), which include: uncertainty whether the large enough number of users will be willing to visit the region; lack of third party content that is related to the owner content, constitutes its natural context, and can additionally attract visitors; the time and cost effort related to the region promotion; the time and cost effort related to the region hosting and maintenance. Moreover, using institution-hosted regions protects only the institution's rights to the content. Users rights to the content are still not protected, since they cannot be sure whether confidentiality of their roaming inventories is preserved on remote hosts, unless they fully trust the hosting institutions.

Taking all these factors into account, in this paper the solution to the described problem is proposed. The main idea of the proposed model is providing the distributed community of users with the cryptographic means transparently integrated with virtual environments software, allowing to selectively reconstruct the safely distributed scene subsets. The model enables placing 3D scenes in existing popular regions that attract a large number of visitors and provide rich context for the distributed content, and at the same time mitigates the problem of the host code that controls the region and can be potentially malicious. The software solution design is proposed along with the usage scheme that is based on it.

2 Related Work

Recently, a significant development of the federated virtual environments based on open architectures can be noticed, particularly in open source software communities. Good representatives are platforms based on OpenSimulator [6] engine implementation, such as OSgrid/Hypergrid [15][5], where new regions on new hosts can be dynamically added to the grid. A roaming data processing model and external openness makes federated virtual environments inherently insecure which affects trading of digital goods and their usage control. Their access control mechanism can be bypassed, e.g., by using "copybot" software simulating legitimate applications that

perform uncontrolled operations to copy user assets while a user visits a virtual environment region (host) that is running a malicious code [11].

Open Cobalt [16], another open source platform for constructing, accessing, and sharing virtual environments, makes it possible to hyperlink virtual environments using 3D portals to form a large distributed network of interconnected collaboration spaces. It does not require centralized servers and the processing is distributed in a P2P manner. From the security analysis point of view, interesting element of such approach is reduction of reliance on error-prone server infrastructures by using a peer-based messaging protocol. However, here the problem of untrusted clients appears, which is hard to solve, as the problem of malicious hosts.

One of the other mature open source platforms is Open Wonderland [17] supporting creation of interactive and dynamic content. For access control, any digital object can be associated with an access control list (ACL) to control which users can view or manipulate or edit the object. Here ACLs are hierarchical, so access can be applied to a single object in a space or to all objects within enclosing 3D structure. However, contrary to Open Simulator, Open Wonderland is not based on the paradigm of federalization and distribution, thus it suffers all the limitations of the centralized system.

Solutions grown from the programming platforms for 3D content should be mentioned as well, i.e. X3D-based collaboration servers, such as BS Collaborate [18]. However, they provide only limited security measures and do not enable creating federated environments, but represent traditional, client-server approach.

The techniques that potentially can be used to make grid data confidential, and, at the same time, allowing computation on, or partial access to the data are, respectively, functional encryption [19] (generalization of predicate encryption [20], attribute-based encryption [21], and identity-based encryption [22]) and structured encryption [23][24] (generalization of searchable encryption [25]). These techniques are useful, e.g. in the cloud computing data processing schemes [24], where data remain encrypted on the host after querying or calculating. However, they cannot be applied directly to the multimedia data in federated virtual environment. This is caused by the fact that the dynamically added untrusted hosts are required to have full access to the scenes and user inventories in order to simulate physics and behavior while the users are interacting with each other or are roaming from host to host.

From the wide spectrum of techniques for providing data confidentiality, threshold secret sharing has been chosen in the proposed approach [26][27][28]. Originally it has been designed for the applications where a number of parties, that do not fully trust each other, have to collectively make decisions or gain access to a secret. Since in many applications unanimous decisions or even full presence cannot be assumed, threshold secret sharing schemes allows at least k of n parties to reconstruct secret message. In organizations secret information can be shared between different groups of users (on homogenic layers, e.g. strategic, tactical) in the same way or differently on each layer [29]. In different layers the same or different information can be shared. Reflecting user hierarchies in the secret sharing consists not only in simple providing the users from the higher hierarchy levels with higher number of shares, but also in producing the shares of the different quality for the levels. Moreover, methods allowing the users from higher levels of the hierarchy to delegate the rights to the secrets

have been developed. According to the author's best knowledge the threshold secret sharing has not been used to secure the distribution of the multimedia content in the virtual environments, where it cannot be assumed that users keep acquired data confidential or, even worse, the problem of malicious host appears.

3 Model for Mass Scale Content Distribution

3.1 The Idea

The main idea of the proposed solution is providing the distributed communities of content creators and consumers with the cryptographic means transparently integrated with federated system, allowing for the safely distributed scene subsets to be selectively reconstructed (**Fig. 1**). As an initial step all the elements of the scene and their relations are symmetrically encrypted by the publisher, and the ability to decrypt it is dependent on the submission of the secret keys. The secret keys are split in advance using the threshold secret sharing algorithm for a number of shares. Each shareholder obtains a number of shares proportional to the class of the acquired ticket and corresponding to his or her usage rights to the subsets of the content. In order to start the interactive exhibition, the *k* of *n,* or more, shareholders are needed. The keys are produced in particles that correspond to the subsets of the original scene with respect to its structure, in order to provide the ability to reconstruct the scene in a selective manner. The *k* number of tickets is a parameter of the algorithm (and can be calculated e.g. to create a "critical mass" for which the event is justified for economical reasons). After the shareholders with eligible key shares gather at freely chosen host and decide to start an event, reconstruction of keys is deployed, the scene is decrypted and the exhibition can be run.

Simple scene encryption would not solve the problem since a single ticket holder with the decryption key could illegally distribute the scene. Access control mechanisms designed for the interactive and distributed content, such as proposed in [30][31][32][33][34], also cannot be applied, since they require predefined trusted host, which does not match open grid specificity.

3.2 The Application in Federated Virtual Environments

The proposed concept of the software framework is composed of four main components: a scheme for threshold scenes sharing, layer of integration with virtual environment infrastructure, publisher tools, and a scheme for updating shares.

The first component and the core of the proposed solution is a new scheme for threshold secret sharing adapted to structured and interactive 3D scenes. It is based on existing threshold algorithms, but modified to support specific data structures of the 3D scenes (geometrical models, behaviors/scripts, composability structures). It employs cryptographic keys distribution scheme. The implementation is deployed on the side of virtual museum software (encryption, key splitting), as well as on the side of the region host software (key reconstruction, decryption).

The second component of the solution is a software layer that integrates reconstructing/decrypting algorithms described above with Hypergrid software, or potentially other open virtual environment platform. The integration is transparent (automatic decryption and secret reconstructing on-the-fly) from end-user point of view.

The third component of the solution is a set of publisher tools that allow for selective encryption and sharing of the scene. It integrates splitting/encrypting algorithms with GUI software that enables interactive structuring of the 3D scene. The integration is transparent (automatic encrypting and secret splitting on-the-fly) from the end-user point of view.

The fourth required component is the software implementing scheme of updating shares. It is needed for handling long-term users migration, and is based on proactive threshold secret sharing. The implementation is deployed on the side of the OpenSim-based host software.

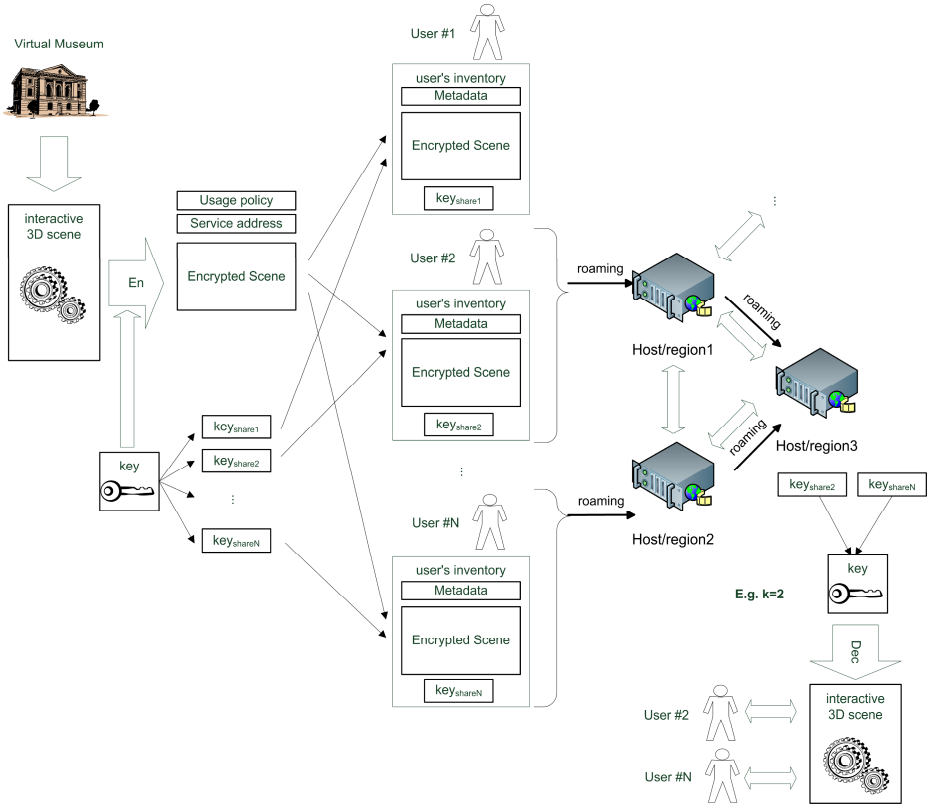

Fig. 1. Scheme for scenes sharing in Hypergrid. Simple example for k=2.

3.3 Structured Content Sharing

In the simplistic example depicted in the **Fig. 1** the whole scene has been shared as a single digital item. However, in the real applications only specific subset of the scenes

is shared among different groups of users (c.f. **Fig. 2**), according to users privileges (or roles when RBAC is applied). These subsets can be composed of elements, i.e. scenes, sub-scenes, geometrical models, scene scripts, behavioral scripts, as well as relations between these elements.

In the example in **Fig. 2** two users have shares in two different subsets of the scene. Since scene subset #2 is the superset of scene subset #1, if k=2, the User #1 and User #2 have right to reconstruct together the decryption keys and decrypt the scene. However, their right is limited only to the range of Scene subset #1. Thus, there is a need for applying cryptographic mechanism for selective scene sharing with respect to scene structure. Therefore, the keys are produced in particles that correspond to the elements of the original scene and to relations between them (there are separate keys for relations). Token-based structured encryption and searchable encryption techniques, having applications in the cloud computing [24] which however differ from the open federated grid, are conceptual inspiration here.

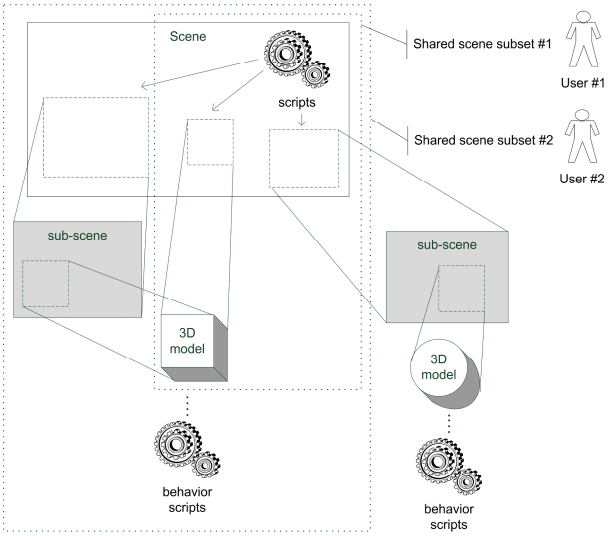

Fig. 2. An example of scene subsets to be shared in case when one scene is the subset of the other

An additional functionality intended to promote the content usage is introduced taking advantage of the features of threshold secret sharing. It assumes that shares are based on variable *k* value for fixed secret, which means that the lowest *k* value is needed to reconstruct scene skeleton (scenes and sub-scenes), the higher *k* value enables reconstructing also geometrical models, and the highest *k* enables reconstructing the behavior scripts and therefore interacting with the complete scene. It encourages the community to gradually populate the host on which the scene is launched, since the "level of details" and the "level of interactivity" of the content increases as the number of content consumers grows.

3.4 Use Case Scenario for Virtual Museums

The solution proposed in the previous sections has been designed as a prerequisite to the new usage scheme for virtual museums that are deployed "in the cloud", particularly on federated hosts constituting 3D virtual environment. Taking advantage of virtual environment functionality, virtual museum staff can build scenes containing multiuser educational scenarios with interactive 3D models. In the analyzed use case this content is secured, distributed and used in three phases: Content Securing Phase, Content Distribution Phase, and Content Reconstruction and Deployment Phase.

In the Content Securing Phase:

- Along with digital ticket to the virtual museum, the participants (not just visitors) obtain shares of scene decryption keys that are generated automatically;
- The scenes are dedicated exclusively for the target population of participants – shareholders;
- The shares generated for the given participant correspond to its credentials (user privileges, role, preferences, ticket class paid, etc);
- The protected scene subsets or models can be reused by content publishers as a building blocks of many different scenes released for distribution;

In the Content Distribution Phase:

- Participants having the shares roam and gather at freely chosen host, and therefore they "support" better hosts through the „wisdom of the crowd";
- Additionally, the chance to have large number of users with their attractive content motivates host providers to assure quality of their service, particularly data security;
- Shareholders have ability to decide about the event context; it allows for decentralizing the content management, which is crucial in federated virtual environments, since their topology is decentralized by design;
- „Malicious host" cannot copy encrypted and shared scenes owned by users that are roaming through it (note that in case of regular Hypergrid model "malicious host" could copy the scene from the inventory of a single user who visited the host).

Finally, in the Content Reconstruction and Deployment Phase:

- Interaction with the scene is possible after virtual exhibition start which requires critical mass of at least k of n simultaneous participants (and additionally e.g. virtual guide with special shares);
- The usage scheme assumes, that even if the content leaks out after the keys are reconstructed and the scene is decrypted on the host, tickets (shares) already have been distributed in the number that makes the content creation cost-effective;
- Moreover, the exhibition with the shared scenes can be launched for a second time and subsequently, provided that k users will gather on any host. Obviously, the k number may include completely different set of users each time, so the content can reach broad range of consumers.

4 Conclusions and Future Work

In this paper the model for large scale content distribution, based on extended threshold secret sharing technique, is proposed, along with usage scheme, that bypasses the "malicious host" problem. Its main practical advantage is protection against illegal distribution of the scenes in federated virtual environment and, at the same time, providing the content consumers with freedom of deciding about the context of the interaction with the 3D scene. It opens the world of the federated virtual environments, its user communities and services, to the content providers such as virtual museums, assuring the desired level of security and cost-effectiveness (no content leaks, no piracy, large populations of users). The support for flexible and selective sub-scene protection is a key factor allowing for applying the proposed solution in practice.

In future the performance of the software implementation will be investigated more in detail. Share size influence the computation and communication efficiency, but since only encryption keys, not whole encrypted scenes, are shared in the proposed solution, splitting and reconstructing algorithms will not add any significant performance costs. However, computational effort related to scenes decryption on-the-fly needs to be tested.

An interesting aspect of secret sharing, that can be taken into account in the future research on the topic, is taking advantage of the knowledge about users rights and, at the same time, about inter-user and inter-role relations, hierarchies, and constraints (e.g. separation of duties), in the key generation process.

References

1. Cellary, W., Walczak, K.: Issues in Creation, Management, Search and Presentation of Interactive 3D Content. In: Interactive 3D Multimedia Content - Models for Creation, Management, Search and Presentation, pp. 37–54. Springer, London (2012)
2. Flotyński, J., Dalkowski, J., Walczak, K.: Building multi-platform 3D virtual museum exhibitions with Flex-VR. In: The 18th International Conference on Virtual Systems and Multimedia, pp. 391–398. IEEE Advancing Technology for Humanity, Milan (2012)
3. Eno, J., Gauch, S., Thompson, C.: Searching for the metaverse. In: Proc. of the 16th ACM Symp. on Virtual Reality Software and Technology, pp. 223–226. ACM, New York (2009)
4. Botev, J., Hohfeld, A., Schloss, H., Scholtes, I., Sturm, P., Esch, M.: The HyperVerse: concepts for a federated and Torrent-based '3D Web'. Int. J. Adv. Media Commun. 2(4), 331–350 (2008)
5. Hypergrid, `http://opensimulator.org/wiki/Hypergrid`
6. OpenSimulator, `http://opensimulator.org/`
7. Kokua/Imprudence, `http://blog.kokuaviewer.org/`
8. Horn, D., Cheslack-Postava, E., Azim, T., Freedman, M.J., Levis, P.: Scaling Virtual Worlds with a Physical Metaphor. IEEE Pervasive Computing 8(3), 50–54 (2009)
9. Alpcan, T., Bauckhage, C., Kotsovinos, E.: Towards 3D Internet: Why, What, and How? In: Proc. of the 2007 Int. Conf. on Cyberworlds, pp. 95–99. IEEE, Washington, DC (2007)
10. Sander, T., Tschudin, C.F.: Protecting Mobile Agents Against Malicious Hosts. In: Vigna, G. (ed.) Mobile Agents and Security. LNCS, vol. 1419, pp. 44–60. Springer, Heidelberg (1998)

11. Hypergrid Security, http://opensimulator.org/wiki/Hypergrid_Security
12. Hypergrid Ref. Guide, http://www.ics.uci.edu/~lopes/opensim/HypergridReferenceGuide.html
13. Lopes, C.: Hypergrid: Architecture and Protocol for Virtual World Interoperability. IEEE Internet Computing 15(5), 22–29 (2011)
14. Bierman, E., Cloete, E.: Classification of malicious host threats in mobile agent computing. In: Proc. SAICSIT, Republic of South Africa, pp. 141–148 (2002)
15. OSgrid, http://www.osgrid.org/
16. Open Cobalt, http://www.opencobalt.org/
17. Open Wonderland, http://openwonderland.org/
18. Bitmanagement BS Collaborate, http://www.bitmanagement.com/products/server/bs-collaborate/
19. Boneh, D., Sahai, A., Waters, B.: Functional encryption: Defnitions and challenges. Technical Report 2010/543, IACR ePrint Cryptography Archive (2010)
20. Shen, E., Shi, E., Waters, B.: Predicate privacy in encryption systems. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 457–473. Springer, Heidelberg (2009)
21. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98. ACM, New York (2006)
22. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
23. Goh, E.J.: Secure indexes. Technical Report 2003/216, IACR ePrint Cryptography Archive (2003)
24. Chase, M., Kamara, S.: Structured Encryption and Controlled Disclosure. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 577–594. Springer, Heidelberg (2010)
25. Song, D., Wagner, D., Perrig, A.: Practical techniques for searching on encrypted data. In: IEEE Symposium on Research in Security and Privacy, pp. 44–55. IEEE Computer Society, Washington, DC (2000)
26. Shamir, A.: How to Share a Secret. Communications of the ACM, 612–613 (1979)
27. Simmons, G.J.: An Introduction to Shared Secret and/or Shared Control Schemes and Their Application in Contemporary Cryptology. In: The Science of Information Integrity, pp. 441–497. IEEE Press (1992)
28. Tang, S.: Simple Secret Sharing and Threshold RSA Signature Schemes. Journal of Information and Computational Science 1, 259–262 (2004)
29. Ogiela, M.R., Ogiela, U.: Information Security Management Based on Grammar Threshold Schemes. In: 1st IEEE/IFIP International Workshop on Knowledge Management for Future Services and Networks, Osaka, pp. 247–250 (2010)
30. Wójtowicz, A.: Secure User-Contributed 3D Virtual Environments. In: Interactive 3D Multimedia Content – Models for Creation, Management, Search and Presentation, pp. 171–193. Springer, London (2012)
31. Wójtowicz, A., Cellary, W.: Representing User Privileges in Object-Oriented Virtual Reality Systems. In: Camarinha-Matos, L.M., Pereira, P., Ribeiro, L. (eds.) DoCEIS 2010. IFIP AICT, vol. 314, pp. 52–61. Springer, Heidelberg (2010)
32. Wójtowicz, A., Cellary, W.: Access Control Model for Dynamic VR Applications. In: Rea, A. (ed.) Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management, pp. 284–305. IGI Global (2011)

33. Wójtowicz, A., Flotyński, J., Rumiński, D., Walczak, K.: Securing Learning Services Accessible with Adaptable User Interfaces. In: Grzech, A., Borzemski, L., Świątek, J., Wilimowska, Z. (eds.) Information Systems Archictecture and Technology. Service Oriented Networked Systems, pp. 109–118. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław (2011)
34. Wójtowicz, A., Walczak, K., Wiza, W., Rumiński, D.: Web Platform with Role-based Security for Decentralized Creation of Web 2.0 Learning Content. In: Proceedings of the 7th International Conference on Next Generation Web Services Practices (NWeSP), pp. 523–529. IEEE, Salamanca (2011)