VirtualLife: Secure Identity Management in Peer-to-Peer Systems

Dan Bogdanov[1,2] and Ilja Livenson[1,3]

[1] University of Tartu, Liivi 2, 50409 Tartu, Estonia
[2] AS Cybernetica, Akadeemia tee 21, 12618 Tallinn, Estonia
[3] NICPB, Akadeemia tee 23, 12618 Tallinn, Estonia
db@ut.ee, ilja@kbfi.ee

Abstract. The popularity of virtual worlds and their increasing economic impact has created a situation where the value of trusted identification has risen substantially. We propose an identity management solution that provides the user with secure credentials and allows to decrease the required trust that the user must have towards the server running the virtual world. Additionally, the identity management system allows the virtual world to incorporate reputation information. This allows the "wisdom of the crowd" to provide more input to users about the reliability of a certain identity. We describe how to use these identities to provide secure services in the virtual world. These include secure communications, digital signatures and secure bindings to external services.

Keywords: identity management, virtual worlds, security, trust and reputation.

1 Introduction

Online virtual worlds are popular among users and organizations. Virtual environments like Second Life and Active Worlds are actively used by companies and organizations to promote their products and services[1]. Establishing a visible presence in such a world has become a marketing strategy. The users are interested in virtual worlds for the social interaction and entertainment possibilities. Building a virtual world to attract both users and service providers requires a strong technical framework and a well-defined focus.

In our work we address the issue of identity verification and trusted service provision. Most of the online worlds currently in active use put little effort on the identification of participants. This is a problem for anyone who has to trust the presented identity of their communication partner. One motivating example is a business transaction, where parties need to identify each other to enter an agreement. Another is a system that verifies the users' age to restrict access to age-specific content or provides age information to communication partners. The last example can be extremely motivating for parents whose children engage in online chats. Also, if a user conducts a criminal act inside the virtual world, then it can be claimed that the responsibility lies on the virtual world provider, because it did not fully identify the user.

Our contribution. We present a holistic solution to identity management and its applications in an online virtual world. We propose a way to handle the assignment

P. Daras and O. Mayora (Eds.): UCMedia 2009, LNICST 40, pp. 181–188, 2010.

and storage of identity information, how to prove identities to other participants and how to build services that use this information. We also describe techniques to make the system more intuitive for users by providing visual indicators of the strength of identity and trust information. The solution has been developed in conjunction with the VirtualLife virtual world [2] and it has been implemented within that world.

The usage of the proposed identity management system relies on the following assumptions: the capability to use X.509 security infrastructure and the capability to establish network connection to any node in the system. Although the solution is generic and can be used in any multi-user system, it was developed and adjusted for use in 3D worlds. It relies on a custom peer-to-peer messaging layer, that is complicated to implement in browser-based virtual worlds.

In this paper we introduce VirtualLife and its identity management system. We discuss how a variety of services can be built using this system and how they benefit from its properties. This is the underlying work for further research that may be conducted once the VirtualLife system is online and actual user experiences can be taken into account.

2 The Architecture of VirtualLife

The design of VirtualLife [2] is based on the idea of a connected network of peers. Every peer can act both as a provider and a user to the services in the virtual world. However, in practice it makes sense to distinguish some more powerful peers that provide additional services. Also, a minimal amount of transactions should rely on a trusted third party, e.g. a server. For these reasons VirtualLife has been designed to use a hybrid peer-to-peer network topology.

Each node runs a selection of services. Based on the services running in a particular node we separate the nodes into *clients*, *zones* and *nations*. The client node is run by a user and it provides the means for connecting to the virtual world and letting the user interact with it. The zone node is responsible for running a part of the virtual world. It maintains the world state, performs the necessary simulations and relays information between nodes. The nation node manages a group of zones and provides them with rules that make all zones in a nation more consistent. The deployment of the VirtualLife network is illustrated on Figure 1.

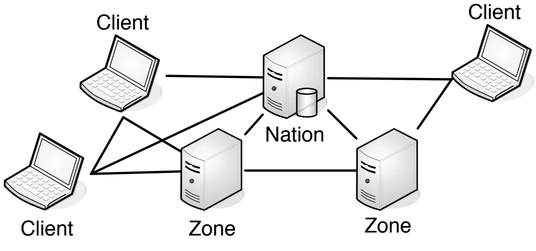


Fig. 1. An example deployment of the VirtualLife network

The security layer of VirtualLife provides a wide range of services that are used by other VirtualLife platform components. These services include data structures and operations for cryptographic primitives, certificate management and authorization. The system is built on top of the X.509 public key infrastructure standard[3], which is widely used for securing access to the sensitive services, for example e-mail accounts and online banks. It defines a hierarchy of trusted third parties called Certification Authorities that issue temporary digital documents binding together a public key and identity information. These digital documents are called *certificates*.

The networking layer of VirtualLife is designed to support the peer-to-peer topology and the identity system. All VirtualLife connections may contain multiple logical streams for different services. For example, chat, world data and user avatar coordinates can use different streams in the same connection. A stream can also be transparently encrypted and authenticated to provide secure transport between peers.

3 VirtualLife Identities

3.1 Identity Information

Every node in the VirtualLife system has an identity that is used for identification in services. The identity is a collection of profile information, security credentials, trust and reputation. VirtualLife uses X.509 key pairs consisting of a public and a private key. The identity is created and managed by every node itself. The key pairs may be added to the identity as needed. In the VirtualLife network, identities are registered at the nation node to simplify lookups during verification procedures. The structure of a VirtualLife identity is shown on Figure 2.

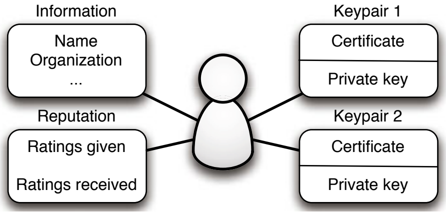


Fig. 2. An example of a VirtualLife identity with two key pairs

The X.509 infrastructure is commonly used for identification and secure transport in existing applications. For example, companies like VeriSign and Thawte are issuing X.509 certificates that can be used for securing websites, e-mail connections and other services. Certification authorities have *certification policies* that describe the procedures taken when issuing a certificate. Some authorities will verify the personal information on the certificate by requiring the user to appear in person or send a copy of a document. Others may issue certificates more freely.

VirtualLife is making use of these established trust relations in VirtualLife to give hints to the users. If it is known that the certification policy of an authority requires certificate holders to prove their identities with a document, VirtualLife can tell its users that if someone who cryptographically proves the ownership of a verified certificate than that someone is more probably who he or she claims to be. This of course holds only to the information in the certificate. All other information provided by the user that has not been verified by the certification authority cannot still be trusted.

We note that the identities contain key pairs that contain private keys. In order for the proposed security measures to work, the private keys must be stored in the client software and not uploaded to the any other node. Any node with access to a private key of an identity can effectively claim to own that identity. If the user wants to use the identity from multiple computers, the key pairs must be transported using a portable storage device.

3.2 Intuitive Identity Verification

There is always a trade-off between the security of the system and its usability. If a system has a strict security policy then the users must perform additional tasks to ensure their security. In the context of identity verification such a task occurs when the user is trying to find out the reliability of a communication partner. In most systems, the only proof of the identity of the other party is the user name provided by the server relaying information. This approach is convenient, but allows an attacker to easily forge an identity as the user gets no proof of identity and has to rely on the information provided by the server.

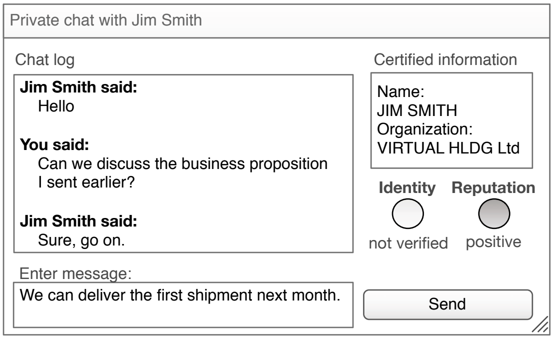
VirtualLife ensures that every authenticated connection between two parties also provides a cryptographic proofs of the parties' identities. However, even when an identity is established, the users still have to decide whether the provided information is reliable. This can be complex due to the amount of associated technical details. To overcome this obstacle, the graphical user interface could display the summary of the identity information.

We propose the inclusion of two "traffic lights" in locations where the user must make a decision whether to trust another user or not. The first traffic light will represent the strength of identity and the second one will represent the reputation. The identity traffic light has three states based on the policy of the certificate authority that issued the user certificate:

1. red (entrusted)—guest or temporary user;
2. yellow (weakly trusted)—certified by an authority that does not verify people's identities using a document and/or physical appearance;
3. green (trusted)—certified by an authority that verifies user identities.

The reputation traffic light has three states as well, depending on whether the user has negative, neutral or good reputation. An example of this design is illustrated in Figure 3.

Clicking on each of the "traffic lights" opens a pop-up with a detailed information. The identity pop-up will include certificate details such as the name of the certification authority, expiration date and certified user information. The reputation pop-up will use visualization to illustrate the reputation status of the user. The identity information must originate from a direct connection with the other user. This is the case in possibly security-critical scenarios such as text or voice chat, file exchange and contract signing.



Private chat with Jim Smith

Chat log

Jim Smith said:
Hello

You said:
Can we discuss the business proposition I sent earlier?

Jim Smith said:
Sure, go on.

Certified information

Name:
JIM SMITH
Organization:
VIRTUAL HLDG Ltd

Identity ○ not verified

Reputation ● positive

Enter message:
We can deliver the first shipment next month.

Fig. 3. Identity verification in a chat. The identity light is yellow and reputation is green.

3.3 Trust and Reputation Management

A strong identification method can be used to improve trust and reputation management. In social networks as well as virtual worlds users can rate each other. While the aspect being rated may differ from system to system, the gathered information can be used by other users to make decisions. Trust and reputation are more important in systems with a commercial component such as auction or sales environments. If many other users consider a seller to be trusted, more users have a reason to trust that seller. On the other hand, a seller with a negative reputation will be avoided by new customers.

In a typical case a seller with a bad reputation will abandon the account and make a new one. This will be impossible if the identity is based on an external source of trust. VirtualLife can restrict the user from creating another identity with the same certificate. We point out that the proposed enhancements are achieved, if the use of outside trust is actively encouraged or strictly required. If the user has a certificate from an authority that issues certificates freely, then any user can create a new identity with a new certificate that has no connection to the previous one. In the latter case the new identity will have no ratings and a default reputation.

The exact algorithms that will be used in VirtualLife for trust and reputation calculations are still being developed.

4 Using Identities in Services

We will now give an overview of services and interactions enabled by the suggested identity and reputation system. We concentrate on the basic secure operations in virtual worlds—authentication, authorization and secure communications. We also describe the use of digitally signed contracts in virtual worlds and linking outside databases to improve in-world services.

4.1 Authenticating Users

Authentication is the process of determining the identity of a user. Virtual worlds authenticate their users to introduce them to other users and look up stored information like profiles and inventory. Usually, the user has to provide a security token, for example, a username and password pair. In VirtualLife, authentication is performed by opening a secure connection between the parties that provides each endpoint with a proof about the identity used for establishing the connection. Since the client machine is the only one with access to the relevant private keys, nobody else can claim to have this identity because nobody can provide the necessary cryptographic proof without the private key.

It must be noted that if a certification authority does not verify the user's identities while issuing certificates, these certificates can still be used to authenticate users if the other party has established the correctness of the certificate using an alternative channel such as a personal meeting, mail message or a phone call.

4.2 Authorization

Authorization is used to verify the user's permission to use a service provided by a peer in the system. For example, nations and zones have to authorize clients before they can join. In a client-server virtual world authorization is essentially a server-side check. This approach does not translate well into a peer-to-peer world, where every node might want to establish its own authorization policy.

In VirtualLife, each node can define its own authorization policy. These policies can be synchronized between nodes that want to behave similarly. For example, in VirtualLife, zones belonging to a nation can ask the nation for its access control list and enforce it also in the zone. VirtualLife has a built-in support for using *whitelists* and *blacklists*. If a whitelist is used, only the users in the list are authorized to use the service and everybody else is denied access. If a blacklist is used, everybody except for the identities in the list are authorized. If we add an identity to a blacklist, we add all the associated certificates too. This way the user cannot circumvent the ban by creating a new identity without losing the chance to use the trusted certification.

4.3 Communication between Users

Interaction between the users of a virtual world must be secure if the world is expected to support business transactions. Textual chat, voice chat, file exchange and other collaborations must be authenticated. When a user is chatting or exchanging files with another user, he or she may not want to disclose private information without verifying the other party's identity. The user interface for all communication services will contain visual indicators for determining the strength of identity as presented in Section 3.

In VirtualLife, private communication channels are implemented using secure streams between the two users. Also, the secure stream is automatically encrypted and verified to prevent eavesdropping or active tampering.

4.4 Electronic Documents

Service providers and clients have to be able to sign contracts to engage in business transactions. The availability of X.509 key pairs allows VirtualLife to provide a digital signature service that conforms to the XML-DSIG[4] and XAdES[5] standards. These standards specify digital documents that can have a number of attached signatures.

A single person may sign a document containing a manifest, a guarantee or an invoice. Two people may sign a contract where one promises to perform some work in the virtual world and the other promises to pay for that work. Any number of people could also sign a declaration and present it to relevant parties. An integrated electronic document system can allow the user to digitally sign the contents of a chat session.

Any contract must state the identity used by each party for signing the contract. This way it is possible to verify that the people who had to sign the contract have indeed done so. A digital contract can be verified as long as at least one copy of the document with signatures exists.

4.5 Binding External Services

It might be the case that the outside certification authority has a database of additional information about the certificate holders. If a service provider in a virtual world has access to that database, it can be used to look up verified user data. For example, a certification authority can store the birth date of the certificate holder. If the certificate holder authenticates to a node with access to this database, this node can use the verified identity to verify the age of the user. Figure 4 illustrates this concept.

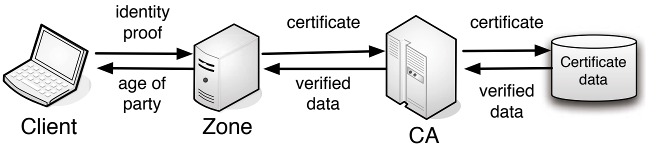


Fig. 4. Using an external certificate authority database for determining age

5 Implementation

In this chapter we give some details of how the proposed identity infrastructure is implemented within the VirtualLife world. VirtualLife has three modules that handle security protocols—**vlsec**, **vlnet** and **vlprotocol**. **vlsec** contains security-related data structures and services. **vlnet** provides the required networking services like stream management and secure communications. **vlprotocol** contains all the application-specific protocols of VirtualLife. Such a distinction is made to have a separation of duties and also allow the re-use of the security and network modules in other software systems.

Figure 5 shows the role of the *Identity* information in the class model. Several instances of *Certificate* and *Keypair* may be bound to a single *Identity*. The *Identity* structure is then used in services to distinguish between the users. In authorization, the *Whitelist* and *Blacklist* contain references to *Identity* instances. Signatures on the *ElectronicDocument* class are identifiable through the *Identity* class. Personal key pairs are encrypted and password-protected. The certificates of other users are cached locally with their trust information to minimize certificate lookup queries to other nodes.

At the time of writing this paper there is no publicly available version of VirtualLife as the system is still in development.

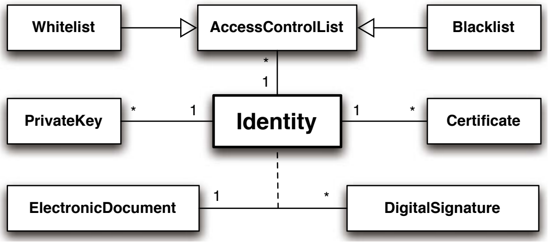


Fig. 5. A selection of identity-related classes

6 Conclusion

In this paper we present an identity management technique for peer-to-peer virtual worlds. The system is based on public key cryptography. Every peer proves its identity when accessing services provided by another peer. The proposed system has been implemented in the VirtualLife virtual world platform. VirtualLife is capable of using already established trust relations in the form of X.509 certificates for notifying its users about the trustworthiness of other users and service providers.

Peers in VirtualLife can have authenticated private channels that allow the users of the virtual world to have secure communication with similar security levels as the one provided in online banking systems. Additionally, built-in support for standardized digital signatures allows users to sign legally binding contracts where the signers can be identified.

References

1. Second Life Work, showcase of the industry usage of the Second Life platform, http://work.secondlife.com (Last checked: 28.09.2009)
2. Secure, Trusted and Legally Ruled Collaboration Environment in Virtual Life, EU FP7 project, http://www.ict-virtuallife.eu (Last checked: 13.07.2009)
3. Housley, R., Polk, W., Ford, W., Solo, D.: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 3280 (2002)
4. Bartel, M., Boyer, J., Fox, B., Lamacchia, B., Simon, E.: XML-Signature Syntax and Processing, IETF/W3C XML Signature Working Group, http://www.w3.org/TR/xmldsig-core/ (retrieved 13.07.2009)
5. Cruellas, J.C., Karlinger, G., Pinkas, D., Ross, J.: XML Advanced Electronic Signatures (XAdES), In: World Wide Web Consortium, Note NOTE-XAdES-20030220 (2003)