Protection of Virtual Property in Online Gaming

Song, Ronggong; Korba, Larry; Yee, Georg; Chen, Y.C.

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Protection of Virtual Property in Online Gaming *

Song, R., Korba, L., Yee, G., and Chen, Y.C.
September 2005

* published in the Proceedings of 2005 Conference on Distributed Multimedia Systems. Banff, Alberta, Canada. September 5-7, 2005. NRC 48241.

Canada

Protection of Virtual Property in Online Gaming

Ronggong Song, Larry Korba, George Yee, and Ying-Chieh Chen

Institute for Information Technology
National Research Council of Canada
Ottawa, Ontario K1A 0R6, Canada
{Ronggong.Song, Larry.Korba, George.Yee, Bomy.Chen}@nrc.ca

***Abstract*—Along with the success of the massively multiplayer role-playing gaming industry in Asia, online gaming-related crimes have grown at an amazing rate. Most of the criminal cases are related to virtual properties since markets have developed for the virtual properties giving them real world values. There has been little research and resulting technologies for MMRPG virtual property protection. In order to reduce the crimes and protect online gaming systems, one potential solution is protecting the virtual properties in online gaming systems. In this paper, we propose a virtual property management language to meter the use of virtual property. The language provides a framework for managing the use of virtual properties and recording the history of transactions to trace the life of virtual properties.**

1 Introduction

The Massively Multiplayer Online Role-Playing Gaming (MMORPG) is a popular computer entertainment in Asia. Played by more than one person over the Internet, MMORPG has turned into a successful business. According to the forecast of DataMonitor.com, the global online gaming market will grow to $3.2 billion and 113 million players in 2005 [1]. However, many problems have arisen and greatly influenced our society with the growth of online gaming. For instance, based on the annual criminal statistics report of Taiwan [2], over 30% criminal cases are related to online gaming. In addition, our further research [3, 4] has shown that most of the online gaming crimes are related to misappropriation of virtual properties since some MMORPG virtual properties have very high monetary values for trading in the marketplace. According to the estimation of NewScientist.com, real-world sales of virtual resources gained within MMORPGs has surpassed $100 million worldwide [5]. Another reason is that the systems themselves only have weak protection for virtual properties. Until now there has been little published research or technologies proposed for virtual property protection.

In order to manage and protect the virtual properties in the MMORPGs, we propose a virtual property management language (VPML) in this paper. By investigating the management requirements of virtual properties in MMORPGs, we define the core models for VPML with provisions for security mechanisms. Key entities include: trading agreement entity, history event entity, and security entity. VPML could provide different levels of security protection for virtual properties by choosing different security mechanisms in order to get a balance among required security level, efficiency, and scalability. This makes the systems more flexible, for instance, we could choose a higher level of security protection for the valuable virtual properties, and a lower level of security protection for those virtual properties of less value.

The rest of this paper is organized as follows. Some background research on MMORPG is briefly described in Section 2. In Section 3, the management requirements for virtual property are analyzed and summarized. In Section 4, the Virtual Privacy Management Language is described including VPML models and the requirements of the MMORPG systems. Several VPML XML examples are introduced in Section 5 to demonstrate how VPML works under the different management scenarios. The conclusions are presented in Section 6.

2 MMORPG

MMORPG is one kind of online gaming played over the Internet by many players from geographically diverse locations. The architecture for MMORPGs is based on the client-server technology. Figure 1 depicts the MMORPG network architecture. Currently, most MMORPGs are commercial in which the players must pay a network connection fee for operating their virtual characters and accumulating related virtual properties.

Since the availability of precious virtual properties is limited and some of it requires expenditure of considerable time and energy to develop, players who desire those properties have resorted to trading with players who have already gained desirable virtual property. In fact, the growth of virtual property markets has swollen the dollar value of desirable properties. For instance, a virtual “dragon knife” and a “royally invincible claw” recently received bids of $US 4,800 and $US 4,270 respectively at an online auction [6]. Trading of virtual property has become an extension to entertainment experience and common practice with MMORPGs, commencing with games such as Sony’s EverQuest [7]. For players, using cash to purchase virtual

property can save time and vigor, immediately upgrading their virtual skills or degrees. Some players even run businesses assisting other players in reaching certain higher levels of the game. In Lineage II for example, reaching level 50 requires a fee of $945 within 15 to 20 days [8]. The online gaming industry has evaluated various trading models and methods. It is unlikely that game vendors will revise the rules in order to eliminate trading or exchanging. Players who want to trade virtual property can utilize diverse trading channels to sell, purchase, or exchange. For solving these trading dilemma, ItemBay.com [9] was built to provide a trading platform for players who want to exchange, sell, or purchase virtual properties in Korea and Taiwan since 2001. With this platform, more and more players can earn profits from MMORPGs at a lower risk than previous methods. When virtual properties become valuable to players and attain high real-world values, MMORPG becomes no longer just the entertainment. Within the marketplace for virtual properties, where there is the involvement of real money, conflicts and criminal behaviors can arise.

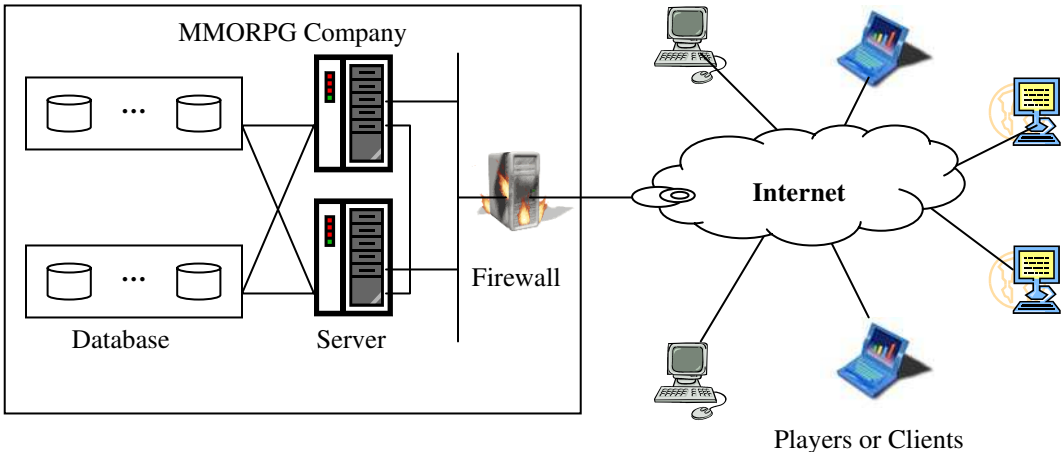

Fig. 1. MMORPG Network Architecture

3 Security Characteristics of Virtual Property

3.1 Security Analysis

In existing MMORPGs, most systems usually use a log file to offer some prospect of virtual property protection. For instance, recording the user's login information and activities provides some security protection for the user's account such that the virtual properties under the account get appropriate protection indirectly. Unfortunately this weak protection creates problems in the protection of virtual properties, especially in cases of fraud and stolen identity [3, 4]. In addition, existing systems have the following disadvantages for the virtual property protection.

- **Hard Tracing:** Since the log file contains a large variety of log messages, it makes the system harder to trace some special events related to the virtual property. The system may require data mining technologies for this purpose. This would often happen when the investigators or court officials require some evidence in the prosecution of online gaming criminal cases. In such cases, many of the other log messages would be useless for this purpose. How to get terse electronics evidence accurately and quickly is a big problem with current MMORPGs.
- **Weak Security Protection:** Current systems do not provide special security protection technologies for virtual properties. Unfortunately, because of this, the log file cannot provide strong evidence for the online gaming criminal cases. For instance, if a player steals another player's virtual property, s/he can claim that s/he has paid for it since the log file usually does not record the trading process, especially the trading agreement. The trading agreement may require some special security functions like a digital signature. Considering privacy issues, some players may want to hide some sensitive information related to the virtual property from other players. Moreover, the log file itself may be attacked and modified. So it is important to incorporate security technologies to protect the virtual properties in the MMORPGs.
- **Little and/or Weak Evidence:** This is caused by the above factors since both hard tracing and weak security protection result in systems in which there is not enough strong evidence for online gaming crime cases.

3.2 Security Requirements

According to our analysis of virtual property security above and our analysis of online gaming security issues [3, 4], there are several basic security requirements for virtual property protection, as follows.

- **Efficiency:** Log event tracing related to the virtual properties should be efficient. This requires efficient, yet accurate message logging.
- **Important Events Recording:** Important events related to the virtual property must be logged in a detailed and accurate fashion. For instance, agreements related to trading or transfer of property, wherein the trading agreement must contain detailed information, such as previous owner and current owner.
- **Signature:** Some important events related to virtual property may require non-repudiation security protection (e.g., a trading or releasing agreement).
- **Encryption:** Some log event records related to the virtual property may contain sensitive personal information (e.g., credit card account). Appropriately applied encryption technologies would provide protection for personal data, as well as resist malicious attempts to alter records in general.

4 Virtual Property Management Language

Virtual property management language is designed to offer efficient management for the virtual property through the recording of important events related to the virtual property with security mechanisms.

4.1 VPML Core Model

Our VPML core model consists of 7 entities: agreement, ownership, offer, event, ownership exchange, signature, and encryption. Figure 2 depicts the core model of VPML and the relationship among the entities.

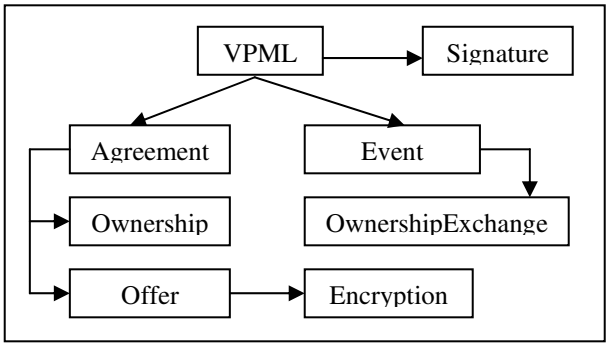

Fig. 2. VPML Core Model

In the VPML core model, the agreement entity expresses the current detailed trading information about the virtual property, for instance, the previous owner and the offer. In order to achieve higher security protection, the agreement message may require digital signatures from both the previous and current owners. The ownership entity contains the virtual property, previous owner, current owner, and ownership exchange method. The offer entity contains the price, trading time, and payment method related to the agreement. Some information like payment method in the offer entity may be sensitive for the customer and thus may require encryption protection. The event entity expresses the key historical events about the virtual property, including the ownership exchange events. In order to make VPML simple and more efficient, the information contained in the ownership exchange entity is the information about the previous agreement. In addition, this also strengthens system security. Detailed information about the core entities are described in the following sections.

4.2 VPML Agreement Model

VPML agreement model expresses the current agreement for the virtual property made by both previous and current owners. The agreement entity is an aggregation of two other entities as follows.

- Ownership – the information about the unique identity, previous owner and current owner of the virtual property, and ownership exchange method. The ownership exchange method could be trading, releasing, pick up, original, and others;
- Offer – the information about the trading related to the virtual property including the price, trading time, and payment method.

The agreement model provides evidence proving the current ownership of the virtual property. The signature entity in VPML, containing both the previous owner's signature and current owner's signature, would offer good security protection for the agreement.

4.3 VPML Offer Model

The VPML offer model expresses the latest trading information of the virtual property contained in the agreement. The offer entity is an aggregation of four other entities as follows.

- Price – the price information of the virtual property in this offer;
- Time – the time that the offer was processed and signed;
- PaymentMethod – the payment method information in the offer (e.g., credit card);
- Encryption – the information related to the encryption including encryption algorithm, key information and cipher data.

The offer entity provides the detailed trading information for an agreement. The use of encryption technology can give a better security protection for the personal data of the owners, especially payment information.

4.4 VPML Event Model

The VPML event model expresses important historical events regarding the virtual property. Currently, the event entity only contains the ownership exchange event. Figure 3 depicts the event model. The ownership exchange entity is an aggregation of three other entities as follows.

- Ownership – unique identity information about the previous owner and current owner of the virtual property in this ownership exchange event;
- Offer – detailed trading information about the virtual property in this ownership exchange event;
- Signature – information about the signature including signature algorithm, key information, and signature value.

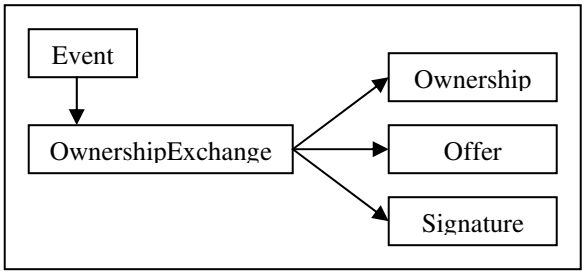

Fig. 3. VPML Event Model

The event model provides extra information for tracing the important events in the life of the virtual property. All information contained in the ownership exchange entity comes from the previous agreement, so the system only needs to put the previous agreement information into the event entity to create event records. This approach requires little extra in the way of computational resources.

4.5 VPML Encryption Model

The VPML core model contains signature and encryption components. We can use the same model as used in Open Digital Rights Language (ODRL) [10] for VPML encryption but we give a simple model for our approach, as follows. The encryption entity is an aggregation of three other entities.

- EncrytionMethod – encryption algorithm used in the encryption entity, e.g. 3DES;
- KeyInfo – key information or value used for the encryption, a session key value may require an encryption with public key system;
- CipherValue – encrypted data with the above encryption algorithm and key.

The encryption entity provides confidentiality protection for the sensitive personal data in VPML such as credit card account. In addition, the agreement signature is only on the cipher data so that the decryption is not required for verification. This makes VPML more efficient and secure since only the seller knows the payment info.

4.6 VPML Signature Model

The VPML signature model is an important model for the virtual property protection. As with VPML encryption, we can use the same model as used in Open Digital Rights Language (ODRL) [10] for VPML signature. We provide a simple model for it here. The signature entity is an aggregation of five other entities as follows.

- DigestMethod – hash algorithm used in the signature entity, e.g. SHA-1, SHA-256;
- DigestValue – hashing result with the hash algorithm;
- SignatureMethod – signature algorithm used in the signature entity, e.g. RSA;
- KeyInfo – public key certificate used for the signature;
- SignatureValue – signature result with the above signature algorithm and key.

The signature entity provides non-repudiation protection for the trading agreements in VPML so that any player can check if the owner is a real owner of the virtual property.

5 VPML XML Examples

In this section, we introduce two scenarios to explain how the XML syntax works for VPML.

5.1 Scenarios

Scenario 1: This scenario describes a general situation that a virtual property "sword of miracles" is distributed to the user named Steve by the system when Steve creates his account. The XML encoding of this scenario is described as follows (See Figure 4). In the coding, vid is the unique identity number of the virtual property, uid_p is the unique identity number of the previous owner of the virtual property, and uid_c is the unique identity number of the current owner.

```
<vpml>
  <agreement>
    <ownership>
      <vid>v8758947389/sword of miracles</vid>
      <uid_c>u8374847294/Steve</uid_c>
      <uid_p>u0000000000/System</uid_p>
      <exchangemethod>original</exchangemethod>
    </ownership>
    <offer>
      <price>0</price>
      <time>8:26/24/03/2003</time>
    </offer>
  </agreement>
  <signature>By System</signature>
</vpml>
```

Fig. 4. Original Agreement of "Sword of Miracles"

In this scenario, the payment method element in the offer entity and the current owner's signature for the agreement is not necessary since the offer price is zero and no reasons for the current owner to deny it. However, the system's signature is important for the current owner since the owner can claim the current ownership by the signature if something happens later, e.g. the virtual property is stolen. In addition, the signature technology is described in the next Section.

Scenario 2: In this scenario, Steve first released his virtual property to the system after playing one month for some reason (for instance, his container does not have enough room for this virtual property). Later, Peter finds the virtual property during his play and picks it up from the system. Peter later sells the virtual property to David for $800 after playing one year. Figure 5 depicts the XML encoding of this scenario. In the scenario, the current agreement is signed by both previous owner, Peter, and current owner, David, during trading. They can show the signature to a court if one of them denies the trading later. Furthermore, in order to make the system more efficient, we only store the previous owner's signature data in each owershipexchange entity of the event entity but this does not reduce the security of the applications since what we want is to trace the previous owner of each ownershipexchange from the event history and provide the evidence (signature) proving that the owner signed the agreement for the ownership exchange.

```
<vpml>
  <agreement>
    <ownership>
      <vid>v8758947389/sword of miracles</vid>
      <uid_c>u7389743894/David</uid_c>
      <uid_p>u3874238974/Peter</uid_p>
      <exchangemethod>trading</excahgnemethod>
    </ownership>
    <offer>
      <price>$800</price>
      <time>13:24/28/06/2004</time>
      <paymentmethod>Encrypted Information
      </paymentmethod>
    </offer>
  </agreement>
  <event>
    <ownershipexchange>
      <ownership>
        <uid_p>u0000000000/System</uid_p>
        <uid_c>u3874238974/Peter</uid_c>
        <excahngemethod>pick up</exchangemethod>
      </ownership>
      <offer>
        <price>0</price>
        <time>11:22/29/04/2003</time>
      </offer>
      <signature>By System</signature>
    </ownershipexchange>
    <ownershipexchange>
      <ownership>
        <uid_p>u8374847294/Steve</uid_p>
        <uid_c>u0000000000/System</uid_c>
        <excahngemethod>releasing</exchangemethod>
      </ownership>
      <offer>
        <price>0</price>
        <time>13:24/28/04/2003</time>
      </offer>
      <signature>By Steve</signature>
    </ownershipexchange>
    <ownershipexchange>
      <ownership>
        <uid_p>u0000000000/System</uid_p>
        <uid_c>u8374847294/Steve</uid_c>
        <excahngemethod>original</exchangemethod>
      </ownership>
      <offer>
        <price>0</price>
        <time>8:26/24/03/2003</time>
      </offer>
      <signature>By System</signature>
    </ownershipexchange>
  </event>
  <signature>By David</signature>
  <signature>By Peter</signature>
</vpml>
```

Fig. 5. History Records of "Sword of Miracles"

5.2 Security Mechanisms

The security technologies used in VPML include symmetrical key encryption technology and public key technology. We don't provide new algorithms for these security technologies but we describe how to embed existing security technologies into VPML to provide the protection for the virtual property and owners.

Symmetrical Key Encryption Mechanism: In VPML, some information like credit card account for payment is sensitive for the buyer. The buyer does not want other people, except the seller, to know it. VPML uses existing symmetrical key encryption technology to protect the buyer's personal data. The protection mechanism is described as follows. The buyer encrypts the sensitive information with a random one-time session key and makes an electronic envelope by encrypting the session key with the seller's public key. Thereafter, the buyer puts the encrypted information into the payment element and makes an offer to the seller. Figure 6 depicts an XML example for detailed encryption information for Scenario 2, above. Upon the reception, the seller decrypts the payment information and signs the agreement to the buyer. At the same time, the seller gets the payment from the buyer and delivers the virtual property to him.

Signature Mechanism: To protect the virtual properties in MMORPGs, VPML bundles the virtual properties with their agreements and event history using the signature mechanism. The signature verification will fail if other players want to change the ownership of the virtual properties illegally. Figure 7 depicts an XML VPML signature example provided by David in Scenario 2, above. The MMORPG system can audit the virtual properties under a player's account by verifying the VPML signature.

Key Management: The VPML security mechanisms include symmetric key technology and public key technology. We use different key management for them in order to make the system more efficient. For symmetric

key technology, we use an electronic envelope for session key management. The detailed information is shown in the above symmetric key encryption mechanism. For the public key technology, we have many choices. One of them uses public key certificate such as X.509 [11]. Another uses the pseudonym technologies [12]. The public key management and pseudonym technology are beyond the scope of this paper.

```
<paymentmethod>Master Card
 <cardinfo>
  <encryption>
   <encryptionmethod> Algorithm= "http://www.w3.org
        /.../xmlenc#tripledes-cbc" </encryptionmethod>
   <keyinfo>
    <encryption>
     <encryptionmethod> Algorithm="http://www.w3.org
                  /.../xmlenc#rsa" </encryptionmethod>
     <keyinfo>
      <X509Data>
       <X509SKI> Seller's Public Key </X509SKI>
      </X509Data>
     </keyinfo>
     <ciphervalue>Encrypted Session Key </ciphervalue>
    </encryption>
   </keyinfo>
   <ciphervalue>EncryptedCreditCardInfo</ciphervalue>
  </encryption>
 </cardinfo>
</paymentmethod>
```

Fig. 6. XML VPML Encryption Example

```
<signature>
  <digestmethod>
    Algorithm="http://www.w3.org/.../smldsig#sha1"
  </digestmethod>
  <digestvalue> Hashed Value </digestvalue>
  <signaturemethod>
   Algorithm="http://www.w3.org /.../xmldsig#rsa-sha1"
  </signaturemethod>
  <keyinfo>
   <X509Data>
     <X509SKI> David's Certificate Info</X509SKI>
   </X509Data>
  </keyinfo>
  <signaturevalue> Signature Value </ciphervalue>
</signature>
```

Fig. 7. XML VPML Signature Example

6 Conclusions

Online gaming crime is becoming a serious issue for our society. In some countries, many criminal cases are related to virtual property according to the latest research and statistics [3, 4]. In order to provide secure, efficient protection and management for virtual properties in the online gaming systems, we propose a virtual property management language. VPML can satisfy some specific requirements of online gaming systems such as efficient tracing and flexible security protection. Some related security problems are not discussed in this paper such as PKI and its development. In this paper we have provided an overview of the VPML model with a description of the different entities and examples of records and agreements for two different scenarios using this model and XML.

For practice, the VPML file can be stored on the distributed client side and implemented in a separate program which has an open interface connect with the gaming software. However, the gaming center can store a copy of the VPML data in its database. This needs a further research.

References

[1] Global online games, Datamonitor Corp. November, 2002.

[2] Annual Criminal Statistics Report, National Police Administration, Taiwan, 2003.

[3] Y. Chen, P. Chen, R. Song, and L. Korba. Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan. In Proceeding of the second annual conference on Privacy, Security, and Trust (PST2004), Fredericton, NB, Canada, October 13-15, 2004. NRC 47401.

[4] Y. Chen, P. Chen, R. Song, G. Yee, and L. Korba. Taxonomy of Online Gaming Crime and Security. In Proceedings of the 16th information resources management association international conference (IRMA2005), San Diego, California, USA, May 15-18, 2005.

[5] Celeste Biever, "Sales in Virtual Goods top $100 Million", NewScientist.com news. Available at "http://www.newscientist.com/news/news.jsp?id=ns99996601". Accessed in October 4, 2004.

[6] A virtual dragon-sky knife is sold on $4800 U.S. dollars in charity bazaar, United Daily, Taiwan, January 29, 2003.

[7] Everquest Online, SONY Corp. Available at "http://www.sony.com".

[8] Lineage II 2 US kain server custom 50 level char. Available at "http://cgi.ebay.com/ws/eBayISPI.dll?ViewItem&category=4596&item=8112795841&rd=1". Accessed in June 10, 2004.

[9] Itembay Taiwan Corp. Available at "http://www.itembay.com.tw". Accessed in June 20, 2004.

[10] Open Digital Rights Language (ODRL). Available at "http://www.odrl.net/".

[11] CCITT Rec. X.509 (03/00) | ISO/IEC 9594-8: 2001, Information Technology – Open Systems Interconnecion – The Directory: Public-key and Attribute Certificate Frameworks.

[12] Lysyanskaya, A., Rivest, R. L., Sahai, A., & Wolf, S. Pseudonym Systems. In Howard Heys and Carlisle Adams (Ads.), SAC'99, LNCS 1758, pp. 184-199, 2000.