Security Model of Mobile Online Games

LIU Jia
School of Humanities
Jiangxi University of Finance and Economics
Nanchang, China
wishbaibai@126.com

***Abstract*—This paper made a detailed analysis on the characteristics of mobile online games and pointed that security is one of the most important things which the games operators should focus on. There are several fields of the security problems, the communicate security would be the most important one. In the authors' opinion, the communicate security could be effectively improved through crypto system, then the benefit of the players could be protected and also the justification of the game. In order to achieve security, a data crypto communication mechanism is developed through the symmetric secret key algorithm and asymmetric secret key algorithm collaborative approach. The authors also designed a model of security games. Be convenient to design, refresh, maintain and high reusability are the advantages of this model.**

Keywords- Mobile Online Games; Communication Security; Crypto System; Model

I. Introduction

The number of cell phone users in China has got half a billion and this number is keeping increasing with a high speed these years. It brings a huge commercial opportunity to the mobile operators, value-added services providers, mobile commerce providers and mobile equipment providers.

In the sight of value-added service providers, the number of them is big, so they have to face the drastic competition. All the SP want to get more profits by providing applications and services which could attract more mobile users.

The mobile online games has got a field in the entire mobile network applications these years, it will also develop fast in the coming times.

The online game is a kind of recreational games with the interactive form. The online games provide integrated function to the players, including user registering, interaction, instantaneity, long-term data preserving and other kinds of value-added services. The traditional online games generally base on Internet and PC. The bandwidth of the Internet and function of PC today could ensure the users to get virtual and aural shock through online gaming.

Which is different from Internet and PC online games, the client of mobile online games is planted in the cell phones or PDA and also other mobile equipments. Mobile users could do interaction with other players at any time and place with their mobile equipment.

The development of mobile online game is in a primary step phase now. Under the condition of GPRS or CDMA mobile network nowadays, the speed of data transporting has been a main problem which limiting the development of mobile online games. However, with the application of 3G networks and the refreshment and development of equipments, these limitations would be removed at last.

After all, it is a huge market, for the number of mobile users is much bigger than that of PC owners. The huge market is worth to research and quest for SP and scholars.

II. Characteristics of Mobile Online Games

A. Characteristics of Online Games

Mobile online games have some features same with traditional online games which are different from stand-alone games. They are interaction, value-adding, security and operation.

Interaction is the most important difference between stand-alone games and online games. In the stand-alone games, there is only one player who participates the game, what the players play with are programs which were programmed beforehand, the game model cannot be changed and also the things would happen during the game. There is no random thing, so the players may feel lonely. However, in the online games, due to the interaction, the communication between players is inevitable, one player is always affected by other players, then the unpredictability is improved and also the interesting. In addition, the interaction between players is similar with the interaction between human beings. Men are animals with social, we need interaction, and online games provide it.

Value-Adding is another difference between the two kinds of games. Game sellers do not provide other service but sell the game software in one time in traditional stand-alone games. But the online games are different. Value-Adding, which means the game operators gain profits through providing several kinds of value-added services. There are a lot of games who announcing they are free of charge, which get large profits by the value-added services. Players who buy the services gain more advantage and dominances compared with other players.

Security is the communication security, privacy security, service security and fair gaming which should be provided in the online games. Most of the online games put security system in the progress of data transmission between the client and server, like encryption mechanism, accessing controls and so on, due to the online games are using the insecure Internet. Although the security is the thing should

978-1-61284-840-2/11/$26.00 ©2011 IEEE

be insured by the operators, not all the operators do enough in this place. Traditional stand-alone games do not use networks, so they do not need security service either.

Operation means that the online games call for the operating system. Dealing with stand-alone games, you can get profits just by developing the game and selling the software copy. However, an online game calls for long time operating by a operating organization, responsible for the publicizing, marketing, operating management, maintaining, upgrading and value-added managements after the game developed.

B. *Advantages of Mobile Online Games*

Compared to the PC online games, mobile online games have the advantages of mobility, free of installing and fairness.

Mobility means that players are free of the limitation of time and space, and they can join the mobile network and play with others anywhere. This is much more convenient than the PC online games. Most online games which based on Internet using PC client generally can not be movable.

Free of installation is another advantage of mobile online games. After the game software is downloaded through the mobile network, then the game runs without installation. Especially the games developed by J2ME technique, which is free of installation and also has the strong advantage of cross-platform, because of the huge market share of cell phones using JAVA.

The fairness means the players could gain more fairness form mobile online games than the Internet games. Internet games are mature today, but for the popularity of the hacking software, fairness has been exiled in most online games, players are harmed and operators lose profits. However, there are fewer people know the techniques of games based on mobile network, hacking programs against a mobile game would be hard to achieve. Certainly, the situation may change with the mobile online games developing. Therefore, operators should concern about the cheating and anti-cheating.

C. *Disadvantages of Mobile Online Games*

Certainly, disadvantages exist in the mobile online games: the small clients' screens, discommodious to handle, clients' low managing capability and poor security.

One of the disadvantages limiting the development of mobile online games is the clients' screen are small. Although screens of mobile phones are larger and larger, compared to the 17 or 19 inches PC screens, they are too small. People who have born in the 1970s always dislike these small screen games.

Discommodious to handle is also a complication. The handle of mobile online games mostly rely on the cell phone keyboard, but most of cell phones' press are small and compact arranged, makes the cell phones cannot suit games with high instant.

The clients' lower capability is a problem which cannot be ignored. The data processing capability of cell phones is not worth mentioning comparing with PC. Due to the lower capability, most mobile online games cannot be as large and luxuriance as PC games. And the data calculation in the games should also simple as possible, which also limits the interesting.

Poor security is a severe problem in the mobile online games' operating [1]. Because data transmission is processed through mobile network, player may lose their trust in the game if no safety mechanism is provided. Player gains no benefits without fair gaming. From this point, mobile online games' developers and operators should insure the security of the games.

III. MOBILE ONLINE GAMES SECURITY PROBLEMS

Security problems in mobile online games, which are also called cheating problems, are not common nowadays, but can be severer with the increasing number of people who know the technology of mobile online games.

In practice, that players' data is deciphered and that virtual items is stolen have appeared. Operators should pay attention to these problems.

Most security problems could be specified to these species:

First: plug-in software using. Using a program, which can send dictates substituting players while playing mobile online games to gain better outcome in the games. Although not all the cell phones could run paralleled programs, there are more and more phones can do it.

Second: BUG attack. Sometimes players can get improper benefits using bugs of the game program.

Third: cooperation cheating. These problems commonly happen in the chess online games. For example, one man who has two cell phones could take part in one chess game with his two phones, gain double information, and then get a higher winning rate.

Fourth: passwords stealing. While logging on the games, players type the passwords first. One can steal others' virtual items by stealing passwords.

Certainly, there are still other security issues. These problems' appearing calls for countermeasures form operators.

Common countermeasures include anti-cheating mechanisms, security detection mechanisms and security management mechanisms.

Setting up anti-cheating mechanisms is to nip in the bud. For example, checking users' identity and doing data transmission in crypto manners could do some effects.

Setting up security detection mechanisms may help operators monitor the behavior of players and detect whether there is abnormity in the games. If there is abnormity, operators will take countermeasures according to the information of abnormity.

Mechanism of security management includes users' security management and the operators' security management [2]. On the one hand, players' awareness on security and anti-stealing should be improved. On the other hand, to avoid stealing and message missing, the operators' interior data management systems should also be improved.

Here the authors focus on the anti-cheating mechanisms. This paper tries to get data transmission security and fair-gaming by ensuring safe transmission between users and server with crypto mechanisms [3].

IV. Working Flow of Crypto Mechanism

Encrypting is a good way to ensure the data transmission security [4]. Common crypto mechanisms include symmetry secret key encryption and asymmetry secret key encryption [5]. The symmetry secret key crypto mechanism has higher operation speed. However, the key security cannot be ignored, for the secret key is easy to be stolen in the process of transmission. The asymmetry secret key encryption, which has a better security with its double secret key [6], however, gets a low operation speed, especially in the condition of large amount of data need to be encrypted, whose operation time would be terrible.

A relatively effective answer would make the best use of these two mechanisms and overcome their defects [7]. That is, transfer a symmetry secret key using asymmetry algorithm before the communicate data transferred with the algorithm of symmetry [8].

With this idea, a crypto mechanism can be used in mobile online games could be developed, which has two phases, called handshake phase and communication phase.

A. Handshake Phase

The main purpose of handshake phase is setting up connection between sever and client, affirming each other's identity, and confirming the symmetry secret key which would be used in communication phase [9] [10].

Steps of handshake phased may like this:

- Secret key producing program and encrypting /decryption program start up with a player starts mobile online games in his phone.
- Cell phone sends request for communication and sets up communication channels.
- Server receives the request.
- Server produces a pair of secret keys randomly. These keys are corresponding to a certain asymmetry secret key algorithm's private key and public key. The authors name them Sprivate-S and SPublic-S.
- Server sends Public-S to the client.
- Client receives Public-S.
- Client produces a pair of secret keys randomly, these keys are used as a certain asymmetry algorithm's private key and public key, here named as CPravite-S and CPublic-S.
- CPublic-S is encrypted by the client using asymmetry algorithm and corresponding server public key SPublic-S, then is sent to server.
- Information received is decrypted by the server using SPrivate-S, then the client public key CPublic-S is obtained by server.
- A symmetry secret key called Sym-S that would be used for symmetry secret key algorithm is randomly generated by server.
- Server encrypts its identity certification with SPrivate-S, then encrypts the encrypted information, Sym-S and certification with CPublic-S, and then sends them to Client.
- After client receives information from server, the information is decrypted by CPrivate-S. Then the encrypted certification information is decrypted by SPublic-S. By comparing the two decrypted certificated information, server identity is recognized and Sym-S is saved.
- Client encrypts username and passwords entered by user with Sym-S. The encrypted information is transferred to server.
- After the encrypted username and passwords are received, sever decrypts them with Sym-S, then check username and passwords with its user list. User will be allowed to log on the game once identity checked.

Description of these steps can be found in Figure 1.

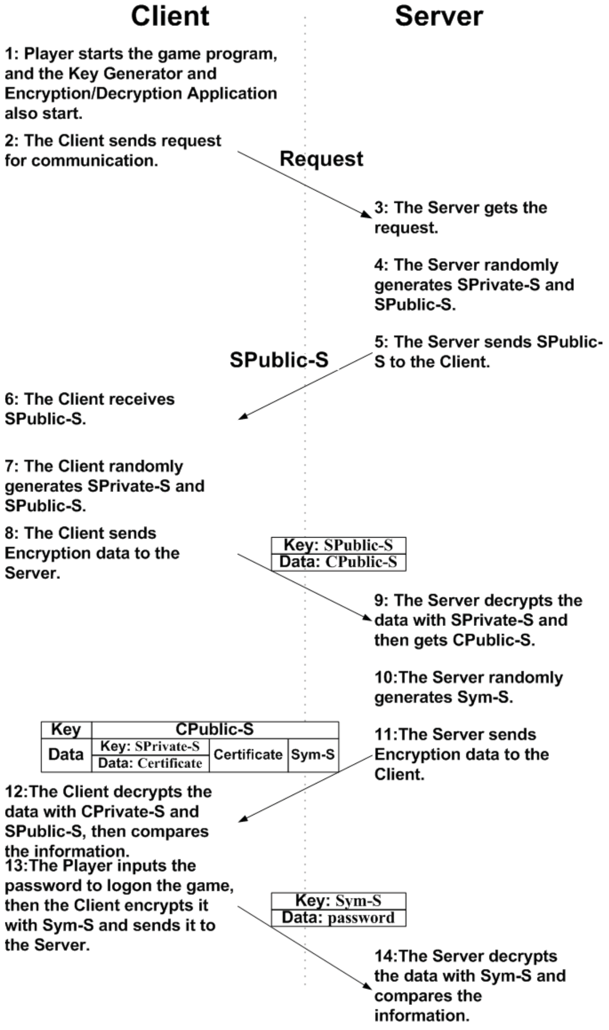
Client
Server
1: Player starts the game program, and the Key Generator and Encryption/Decryption Application also start.
2: The Client sends request for communication.
Request
3: The Server gets the request.
4: The Server randomly generates SPrivate-S and SPublic-S.
5: The Server sends SPublic-S to the Client.
SPublic-S
6: The Client receives SPublic-S.
7: The Client randomly generates SPrivate-S and SPublic-S.
8: The Client sends Encryption data to the Server.
Key: SPublic-S
Data: CPublic-S
9: The Server decrypts the data with SPrivate-S and then gets CPublic-S.
10:The Server randomly generates Sym-S.
Key
CPublic-S
Data
Key: SPrivate-S
Data: Certificate
Certificate
Sym-S
11:The Server sends Encryption data to the Client.
12:The Client decrypts the data with CPrivate-S and SPublic-S, then compares the information.
13:The Player inputs the password to logon the game, then the Client encrypts it with Sym-S and sends it to the Server.
Key: Sym-S
Data: password
14:The Server decrypts the data with Sym-S and compares the information.

Figure 1. Process of Handshake phase between client and server

This encrypting method checking both server's and client's identity, ensures the security transmission of symmetry secret key during communication phase. In addition, the amount of information encrypted and transferred in this phase is small, so just to select the appropriate algorithm will help this phase complete within the tolerant time.

Certainly, concerning the capability of clients, the length of the asymmetry key used in the algorithm should be smaller than that of the asymmetry key used in PC games. Therefore, these keys are relatively easy to be deciphered. But actually it can't be a real big problem. The asymmetry secret key is generated randomly every time the player logs on game, then players' online time cannot as long as the PC games do. Even though somebody could decipher the keys, players may have logged out when he got the keys.

B. Communication Phase

The main task of this phase is transferring encrypted data between server and clients using secret key Sym-S generated in handshake phase.

Using of symmetric secret key encryption algorithm to encrypt data ensures the efficiency of data transmission and game running smoothly. At the same time, using of symmetric secret key encryption /decryption algorithm has no higher demand on the operating capacity of mobile phones.

Clearly, the use of asymmetric key encryption algorithm to transfer symmetric key and the use of symmetric key encryption algorithm to transfer game data, not only ensure the security but also the game running speed.

V. DESIGN OF MOBILE ONLINE GAMES SECURITY MODEL

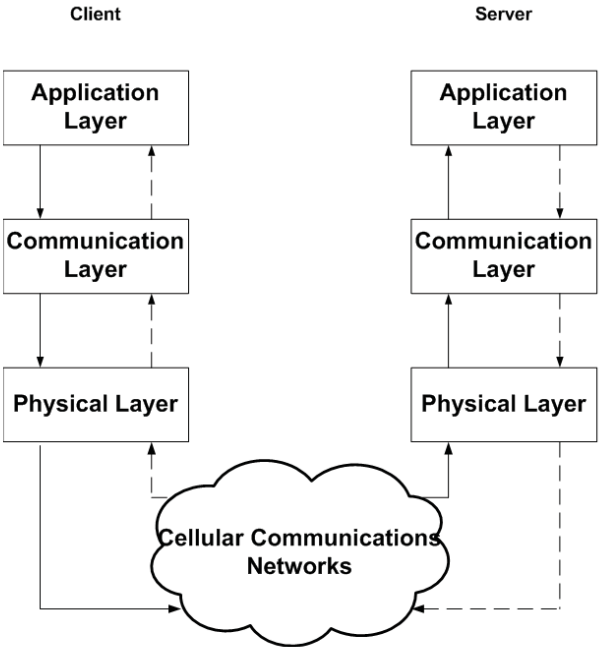

Figure 2. Model of secure game.

The crypto mechanism discussed above can enhance the security of mobile online games. But how this mechanism should be integrated into the mobile online games? One possible approach is to separate logically the encryption mechanism from the game running process and take the crypto mechanism as a component of the whole mobile online game system. Through logical separation, the encryption mechanism part and the game running process part can be developed separately, which makes it easier for developers to design a online game. According to this idea, a possible security can be designed as Figure 2.

In fact, it is a hierarchical model.

The Physical Layer in Figure 2 actually is not the part of mobile online games. This layer is in the mobile communication devices (such as a cell phone), which is responsible for the data form upper layer to provide communication support.

The main function of Communication Layer is to make identity authentication and provide secure data communication between the server and the client with the encryption mechanism described in Fig.1. Data form the upper layer will be encrypted in this layer and sent to the lower layer. Data from the lower layer will be decrypted and sent to the upper layer. Because of the existence of this layer, the secure communication between the server and the client can be ensured and the real information transferred is difficult to access by others.

The top layer in Figure 2 is Application Layer, in which the game running process is implemented in this layer. Of course, for the client, the main function of this layer is to conduct a small number of local computing, refresh images, send data to the lower layer and respond to the data from the lower layer. For the server, the main function of this layer is to conduct a large number of computing, forward messages among multiple users, send data to the lower layer and respond to the data from the lower layer.

Such a communication model has many advantages:

First, it is easy to achieve. It has been discussed that the separation between the security mechanism and game running process can facilitate the development of the online games.

Second, it is easy to maintain and update. If the game process (Application Layer) needs to update or a lot of changes, the operators could only update the Application Layer and leave the Communication Layer alone.

Third, it can ensure security. The Communication Layer provides the encryption mechanism discussed in Fig.1, which can ensure the secure communication, prevent the leakage of personal information, protect the user passwords and safeguard the virtual goods in the games.

Fourth, it can protect the fairness of the online games. For the games without encryption mechanism, it is easier for somebody to develop a cheating program to simulate information from games client [11]. But in this model, if a person wants to develop some plug-in software, then he has to overcome the obstacles of encryption mechanism. So, this model can prevent cheating to a certain extent.

Clearly, it is a good model. It can be extended and have a high reusability. In addition, this model is easy to manage, user-friendly, and able to provide secure communication.

VI. CONCLUSIONS AND FUTURE WORK

Through analyzing features of mobile online games and its security problems, this paper designed a model, which can be used on safety mobile online games by using encryption technology. The technology of encryption and decryption are the kernel of the model. Using asymmetry secret key algorithm transfers symmetry secret key, so that secure data communication is provided by using symmetry secret key and its algorithm.

This model is convenient to achieve and easy to manage and maintain. In addition users' communication security in online games can be ensured by it. Certainly, during the initial stages of research, the authors did not bring entity system suitable to the model. Therefore, the achievement of the system, what disadvantages will be discovered while the system runs and how to perfect it will be the research focus in the future.

[1] Anderson. R. "How to cheat at the lottery," Proceedings of Annual Computer Security Applications Conference. 1999.

[2] Yan, J.J., Blackwell. "The memorability and security of passwords – some empirical results," Computer Laboratory, University of Cambridge, Cambridge, Technical Report No.500. 2000.

[3] Bruce Schneier. "Applied Cryptograghy, Second edtion: Protocols, Algorithms, and Source Code in C (cloth)," John Wiley & Sons inc. 1996.

[4] Apostolopoulos, George, Peris, Vinod, Saha, Debanjan. "Transport Layer Security: How Much Does It Really Cost," Proceedings - IEEE INFOCOM. No2, pp: 717-725. 1999.

[5] Chou, Wesley. "Inside SSL: The Secure Sockets Layer Protocol," IT Professional. vol4, pp: 47-52. 2002.

[6] Gutmann, Peter. "Simplifying Public Key Management," Computer, vol37, pp: 101-103, 2004.

[7] Singh, Kehar. "Optical Encryption Techniques For Data Security," Proceedings of SPIE - The International Society for Optical Engineering, vol4829, pp: 419-420, 2003.

[8] Gertner, Yael, Kannan, Sampath, Malkin, Tal, Reingold, Omer, Viswanathan, Mahesh. "Relationship Between Public Key Encryption And Oblivious Transfer," Annual Symposium on Foundations of Computer Science – Proceedings, pp: 325-335, 2000.

[9] Fujisaki, Eiichiro, Okamoto, Tatsuaki. "How To Enhance The Security Of Public-key Encryption At Minimum Cost," Communications and Computer Sciences, vol E83-A(1), pp: 24-32, 2000.

[10] Perlman, Radia. "Overview Of PKI Trust Models," IEEE Network, vol13, pp: 38-43, 1999.

[11] Yong Gyu Joo, So Young Sohn. "Structural equation model for effective CRM of digital content industry," Expert Systems with Applications, vol34, pp: 63-71, 2008.