Proceedings of the 2nd International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2023)
DOI: 10.54254/2753-8818/5/20230287

Analysis of security issues in mobile games

Han Liao

SMIC Private School, Shanghai, China

liaohan050713@126.com

Abstract. Mobile games have become a popular form of leisure and entertainment around the world. China's economy is growing as mobile games take a larger share of the country's mobile gaming landscape. Many people's efforts have gone to waste as online scammers steal their game accounts, private information, and virtual property. There are many problems in network security, such as increasing trust in fraudulent accounts; posing as an active party to swindle player information, transmission of Trojan viruses. Therefore, this paper puts forward countermeasures to these network security problems, summarizes the application of encryption technology and identity authentication technology in the transmission of personal privacy information, and proposes the use of part of the RSA encryption algorithm. So as far as it is possible to reduce the network game security problems and improve the network anti-theft system defense ability.

Keywords: cryptology, moblie game, game account, RSA.

1. Introduction

In recent years, with the progress of science and technology, more and more people have access to the Internet and understand many functions, such as online games. Online games have also become a way for people to kill time, and many old players with fancy gear and limited-edition clothes not only spend a lot of money, but also spend a lot of time running their accounts [1]. Some people are even willing to buy an advanced level in real life with their own money in advance to achieve it directly. These phenomena are enough to show that people take games seriously. However, game account theft is currently the most popular network security topic and the most concerning problem for players. There are often players' account passwords, equipment, and other items stolen [2].What's more, some minors use their parents' mobile phones to play games, and some scammers will use corresponding methods to lure minors to charge money. They will send game skin or equipment and other techniques, resulting minors wasting all their parents' hard-earned money [3]. So the network game security guard problem is very important. In this paper, the RSA encryption algorithm will be used to solve the above problems. Its purpose is to improve the security of online games.

2. Security issue

2.1. Trojan virus

It is a virus that is usually hidden as an attachment in an email or a free download file and then transferred to our devices. For example, if we copy something to a friend's thumb drive an then copy it

DOI: 10.54254/2753-8818/5/20230287

to our computer, then a Trojan virus is likely to enter our computer system. Next, the file that some share may also be the Trojan horse virus in disguise. Therefore, once the mobile phone or computer is controlled by the Trojan virus, in other words, it will be controlled by the corresponding client, and the users' daily wechat chat, bank password, game account, and other private information may be recorded and stolen. In addition, Trojan viruses have many functions, some can get users' account passwords through internal scanning. Besides,some can even directly translate the ciphertext to steal users' game passwords, and some can also steal users' personal information through message replication.

The future of esports in China is bright. In other words, China has a huge number of online gamers. The distinction between virtual wealth online and real money is blurring. Therefore, to the network game account password for the purpose of the password virus also appears in people's vision, and the Trojan virus in China is second to none. Whenever a new game is developed, after a week or two, a new Trojan virus will be produced.

2.2. Network cheating

In the network environment, many people will pretend to be game customer service to cheat users' trust and access user accounts and passwords. For example, an unofficial activity that has been released has attracted the attention of many players and they have actively participated in it. As a result, the user accounts involved in the activity will be hacked to steal data and transfer the virtual images. Secondly, there are some crooks in the businesses of selling game accounts to cheat money. When the cheater will get the advanced account or pretend to have been given to the buyer, they will use some excuses to deceive those buyers and sellers, such as the operation error, temporarily unable to deal with the prompt. For example, there is a popular game called PUBG, and some players might as well buy some coins because they think they cost a lot of money. So the author went to some video software like TikTok to search for some videos of people selling Cheecoin, and there would be users commenting on selling Cheecoin under the videos. Sometimes it's true, and sometimes it's just a trick used by scammers. It is usually said that you pay up front, and then you can deliver the car. But when the players handed over the money, the guys just ran away.

As is known to all, esports are becoming more and more popular, both at home and abroad. In other words, people are willing to spend a lot of time and effort to cultivate a single game account, or even multiple accounts. By the time these players receive abnormal accounts, it is too late and all their efforts are wasted.

2.3. Online social threats

In addition to using online activities as bait, there are also some scammers who deliberately register accounts and team up with game players, such as couples, marriage mode, and so on. After establishing trust with the players and reducing the defensive psychology of the players, look for opportunities to log in to the other side's account and obtain the other side's account password at the same time, in order to achieve the purpose of account theft. Internet cafes in China, for example, are equipped with surveillance cameras to help maintain order. But sometimes, on the other side of the security camera, there may be a pair of eyes recording your game account and password.

3. Possible solution

3.1. Strengthen the sense of self protection

It is preferable to make friends online, which enables us to have different sorts of friends. However, friends who meet online have better not bring into our real life. This group of friends can barely help you have a more comfortable environment to play games in and always remember not to randomly give them our passwords and account. People can avoid their losing accounts by increasing their self-protection, installing some applications to resist Trojan viruses in order to protect their virtual property in the game, and changing their account password. Finally, differentiating the ideal world from real life is very crucial. Furthermore, If some people are willing to play inside the net BAR, can

DOI: 10.54254/2753-8818/5/20230287

restart the computer, so that the Trojan virus that new implants cannot be controlled. Secondly, pay attention to observe around the landing game, you can slightly put your hand as a cover block. This protects personal privacy information as much as possible. Thirdly, we should clarify whether some activities are officially released, and do not easily believe the words of anyone we know in the game. Also do not easily believe that the customer service sent the winning message.

3.2. RSA

RSA is an encryption method. It is the representative of modern cryptography, also known as one of the best public key schemes. It is widely used in various Internet protocols to ensure the secure transmission of data [4]. Generally speaking, cryptography is divided into two main categories: secret key cryptography and public key cryptography. Secondly, the RSA encryption algorithm is an asymmetric encryption algorithm. Asymmetry means that different keys are used for encryption and decryption. That is, an encryption key is used for encryption and a decryption is used for decryption [5].

The purpose of passwords is to protect the security of networks and information. It's as big as the nation's finances, and as small as the protection of our private information. When we set the password of the lock screen of the mobile phone, if the setting is too simple, there will be a prompt saying "your password is too simple, please reset" and so on. Or when we log in to a game, sometimes we have our face authenticated so the game knows we're logged in. Even though we have been careful to keep our passwords secret from others, sometimes we can't withstand a phishing campaign. Many players who play King of Glory or Peace Elite will see the benefits of the game in many video apps.Therefore, As a result, some players are led to believe that this is the real situation, will access their game account and password, and then add unofficial fake customer services. These customer services will ask you for your WeChat and WeChat password. Once successfully logged into WeChat, they will go to our WeChat to cheat our virtual property and money in reality [6].

RSA was created to minimize the possibility of stolen numbers. To take the simplest example, one bond is 5,14. 5 is E and N is 14 [7]. So we know that e should go from 0 to fin(N) minus 1, and that's going to give us fin(N) is going to be 6, so e should be between 0 and 5, it could be 0 and 5. Next comes the encryption formula. $(m\text{^}e \equiv c \bmod N)$ c is the resulting ciphertext. So let's say that the encrypted number is equal to 2, and then we plug in, and we get c is equal to 4. Another important formula is the decryption formula, $(C\text{^}d \equiv m \bmod N)$ then substitute into the formula again, $4\text{^}d \bmod 14 \equiv m$, in order to find d you need to combine the two formulas together. 1. $(M\text{^}E \equiv C \bmod N)(C\text{^}d \equiv m \bmod N)$ then we have $m\text{^}Ed = C\text{^}d = m \bmod N$, since GCD (m, N) is 1, the equation has a solution. Divide both and by m, and you get $m\text{^}Ed - 1 = 1 \bmod n$ [8]. According to Euler's theorem, we find that (n) can be divided by Ed -1. So Ed minus $1 = k * fin(N), d = (1/E) * (k * fin(N) + 1)$, which gives us the answer to D, but it depends on the value of k. For example, if we choose k to be 4, then D is equal to 5. We were able to decipher it [9]. In the process, I found that the final answer only depended on the values E and N we chose. On the other hand, the larger the value, the more complex it will be to compute. Based on this, we can say that RSA is a very secure system.

So we set the password as complicated as possible, for example, can match numbers and letters, especially can have uppercase letters. This makes it take more time for hackers to crack our passwords when they break in [10].

4. Conclusion

Cryptology has been developed for many years, or even thousands of years. In the past, there was no good system to protect our privacy, which led some people to lose their treasures and expose their private information. For example, people in the ancient times used hand-writing to express secret messages, sometims with some special signals in order to ensure other people could not decode them. However, it was still compelled by others. Instead, nowadays, we have some changes for mathematical reasons. That is, the semi-prime factorization of RSA for security has made it difficult for us to trust

DOI: 10.54254/2753-8818/5/20230287

math's ability to prevent the loss of our bank information and passwords; In a more mathematically and technologically advanced world, that would be impossible. So the way math protects our privacy online will have to be different, so when it comes to finding harder problems than we already know, maybe the future of encryption will depend on math. While there are some promising new algorithms in development, the extent to which mathematics can protect the future of privacy is uncertain. Yet the beauty of mathematics is that there is always more to explore, always more questions to discover. So the author remain optimistic that a new puzzle that has not been explored before, or a completely new approach to mathematical encryption, will allow mathematics to remain a reliable guardian of our privacy for many years to come. Since there is not enough data to provide as a reference in this paper, the author will use knowledge of number theory and computers as well as real-time data to write and encode in the future research. This would improve the network game security environment and defense system.

References

[1] Analytics Insight. TROJAN MALWARE TAKES ADVANTAGE OF PEOPLE WHO GA ME ONLINE, Online: https://www.analyticsinsight.net/trojan-malware-takes-advantage-of -people-who-game-online/. Accessed 14 Aug. 2022.

[2] Anonymous. 2022. How To Detect Cheaters While Playing Video Games, THISDAYLIVE, Online: https://www.thisdaylive.com/index.php/2022/01/22/how-to-detect-cheaters-while-playing-vi deo-games/. Accessed 14 Aug. 2022.

[3] HealthyChildren.org. 2022. Constantly Connected: How Media Use Can Affect Your Child. Online: <https://www.healthychildren.org/English/family-life/Media/Pages/Adverse-Effects-of-Tele vision-Commercials.aspx> [Accessed 27 August 2022]

[4] Anonymous. What Is the RSA Algorithm. Educative: Interactive Courses for Software Developers, Online: https://www.educative.io/answers/what-is-the-rsa-algorithm. Accessed 15 Aug. 2022.

[5] Lake, Josh. 2018. What Is RSA Encryption and How Does It Work? Comparitech, Online: https://www.comparitech.com/blog/information-security/rsa-encryption/.(RSA)

[6] Anonymous. Privacy Statement. RSA, Online: https://www.rsa.com/privacy/. Accessed 8 Aug. 2022.

[7] Matthew J. Clemente. What Is the Modulus Operator? A Short Guide with Practical Use Cases | What Is the Modulus Operator? A Short Guide with Practical Use Cases. Online: https://blog.mattclemente.com/2019/07/12/modulus-operator-modulo-operation/. Accessed 15 Aug. 2022.

[8] Anonymous. Primes, Modular Arithmetic, and Public Key Cryptography II. Online: http://pi.math.cornell.edu/~mec/2003-2004/cryptography/RSA/RSA.html. Accessed 15 Aug. 2022.

[9] Anonymous. 2017. RSA Algorithm in Cryptography - GeeksforGeeks. GeeksforGeeks, Online: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.

[10] ERIC J. HAYES, Playing it Safe: Avoiding Online Gaming Risks, Online: https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf