How Data Encryption Interacts with the Gaming Industry

Wesley Wang

The gaming industry, in the past decades, has become one of the largest industries around the world. The firms and game developers deal with enormous amounts of gamers' data every day. In today's information age, the information privacy of individuals and firms can be ensured by applying proper and effective data encryption. This article focuses on the application, challenges and significance of data encryption in the gaming industry and the mutual effect of their development.

Game assets are the assets that gamers hold in the video game, typically including virtual currency, characters, accessories and in-game items. These assets are considered personal data for the players. In 2018, 24-year-old security researcher Zammis Clark gained access to Nintendo's highly confidential game development servers and stole 2,365 usernames and passwords, causing up to $1.8 million of damage to Nintendo, right after being bailed out without any restrictions because of stealing Microsoft's confidential files. (Tom Warren, 2019) This case compelled video game companies, including Nintendo, to reinforce data encryption using AES (Advanced Encryption Standard, also known as Rijndael, a variant of Block Cipher, which is an algorithm operating through groups of bits called blocks, widely used in data exchange), symmetric and asymmetric encryption (Encrypting and decrypting using different types of keys).

In multiplayer games, cheating, which means using various methods to gain superiority beyond normal gameplay, is always a problem affecting gamers' experience. Typically, cheating is classified in two ways: modifying original files or using cheating code (sometimes implemented by the game developer) and implanting third-party software. The latter can be avoided to some extent by applying anti-cheating programs in the game which are not related to data encryption. Objectively, the latter can be effectively eliminated by using data encryption for the files, but unexplained leaks of game codes happen, which undermines the usefulness of data encryption. In January 2023, Riot Games stated that the source codes of its popular games League of Legends and Teamfight Tactics were stolen by an unnamed group in a “social engineering attack.” Riots said that the exposure of the codes will increase the possibility of emerging cheats. (Jess Weatherbed, 2023) In the following week of this incident, Riot fixed the bugs that were used in the attack, with the disclosure of the reasons for the attack and the preventions being implemented. Numerous gaming companies have suffered from cyberattacks, and data encryption creates a barrier and fixes the bugs to protect their informative security.

Gaming companies provide closed beta that contains unreleased content. Normally, a contract which aims to prevent illegal leaks of unreleased content will be signed between the company and the testers. However, leaks still happen because of the uncertain sincerity of testers. In July 2024, Shanghai Mihoyo Yingtie Tech Co., a subsidiary of Mihoyo, a Chinese video game company, prosecuted tester Chen for infringing the contract by disclosing the unreleased game content of “Honkai: Star Rail” after recording and photographing secretly in the test room, causing economic loss and negative impact. Even though data leaks cannot be completely avoided, multiple feasible ways are developed as technology advances. Implanting unique “signages” into the game packages and converting them into Moiré patterns generated by computational algorithms, making them optically invisible on the screen by applying data encryption. These methods protect the firms’ rights and properties by providing a feasible and simple way to track the leaker, which can minimize the loss. The increasing significance of information security in the gaming industry promotes the advancement of data encryption.

In conclusion, data encryption plays a significant role in the information age, where information security matters. Video game companies are experiencing millions of attacks every day, and data encryption gives them methods to protect themselves. Conversely, firms and developers keep bringing advancements in data encryption as they are developing safer and more complex cryptographic systems. More breakthroughs are expected to be achieved in this process of mutual development.

References

"Advanced Encryption Standard." *Wikipedia*, Wikimedia Foundation, 28 Sept. 2024, en.wikipedia.org/wiki/Advanced_Encryption_Standard. Accessed 18 Oct. 2024.

"Public-key Cryptography." *Wikipedia*, Wikimedia Foundation, 12 Oct. 2024, en.wikipedia.org/wiki/Public-key_cryptography. Accessed 18 Oct. 2024.

Rodríguez-Vera, Ramón, and J.Apolinar Muñoz-Rodríguez. "Image Encryption Based on Moiré Pattern Performed by Computational Algorithms." *ScienceDirect*, 20 Apr. 2004, www.sciencedirect.com/science/article/abs/pii/S0030401804003803.

"Symmetric-key Algorithm." *Wikipedia*, Wikimedia Foundation, 10 Oct. 2024, en.wikipedia.org/wiki/Symmetric-key_algorithm. Accessed 18 Oct. 2024.

上海市浦东新区人民法院. "上海市浦东新区人民法院（2024）沪 0115 民初 38294 号民事判决书." *Wikisource*, 29 Jul. 2024, zh.wikisource.org/wiki/上海市浦东新区人民法院（2024）沪 0115 民初 38294 号民事判决书.

Warren, Tom. "Security Researcher Pleads Guilty to Hacking into Microsoft and Nintendo." *The Verge*, 28 Mar. 2019, www.theverge.com/2019/3/28/18286027/microsoft-nintendo-vtech-security-hack-breach-researcher-guilty.

Weatherbed, Jess. "Riot Games Warns of New Game Cheats following Security Breach." *The Verge*, 24 Jan. 2023, www.theverge.com/2023/1/24/23569386/riot-games-cyberattack-breach-cheats-code-exposed.