Trilobyte: Plausibly Deniable Communications Through Single Player Games

Data/Toolset Paper

Yuzhou Feng
Florida International University
Miami, FL, United States
yfeng015@fiu.edu

Sandeep Kiran Pinjala
Stony Brook University
Stony Brook, NY, United States
spinjala@cs.stonybrook.edu

Radu Sion
Stony Brook University
Stony Brook, NY, United States
sion@cs.stonybrook.edu

Bogdan Carbunar
Florida International University
Miami, FL, United States
carbunar@gmail.com

Abstract

Plausibly deniable communication solutions built on services popular in Western countries may invite closer scrutiny into the activities of their users in censored countries. This paper investigates the ability of popular single-player games to provide the medium for plausibly deniable communications. We introduce Trilobyte, a system that hides data in game state generated opportunistically during regular game-playing activities, and shares data-hiding state through accounts on gaming platforms. We show that even in the presence of hypothetical censors that inspect game state, Trilobyte can hide up to 5.3 MB of data in game state saved in a one hour gaming session. We investigate the practicality of Trilobyte through surveys with 285 Chinese gamers, and by renting and purchasing thousands of gaming accounts. We find that most investigated games, including games developed in China, allow users to communicate keywords considered sensitive in China, when compressed, encrypted or hidden in game state or chat channels.

CCS Concepts

• **Security and privacy → Privacy-preserving protocols**.

Keywords

Plausible deniability, covert channel, steganography

ACM Reference Format:
Yuzhou Feng, Sandeep Kiran Pinjala, Radu Sion, and Bogdan Carbunar. 2025. Trilobyte: Plausibly Deniable Communications Through Single Player Games: Data/Toolset Paper. In *Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy (CODASPY '25), June 4–6, 2025, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3714393.3726489

CODASPY '25, Pittsburgh, PA, USA.

ACM ISBN 979-8-4007-1476-4/25/6
https://doi.org/10.1145/3714393.3726489

1 Introduction

Secure and private communication and data sharing tools (e.g., E2EE apps, file sharing sites, social networks) have become almost ubiquitous. However, powerful, state-level censors ban access to such technologies [2] and replace them with approved alternatives, e.g., [4, 5, 8], that monitor and remove communications and content deemed to be sensitive [24, 25]. While a censor may not completely prevent users from acquiring secure communication tools, e.g., WhatsApp, Telegram, Signal apps, the mere use of such services in the censored area is sufficient to invite closer scrutiny of user activities. This leads to a need for covert communication and data sharing solutions. We posit that this can be best achieved by leveraging services that are already tolerated and sometimes even developed in censored regions.

In this paper, we build on findings from [21] about the strategies gamers use to evade age restrictions on gaming platforms operating in China, to investigate the potential of single player games to provide a medium for covert communications. Previous work has used play-time covert channels in online games, embedding data into user commands [22, 23, 26], in-game state [33], avatar movements [31, 33], gaming packets [27], or game locations [13, 29]. However, these approaches often rely on strong adversary assumptions, e.g., the non-collusion of game operators with adversaries and the inability of adversaries to inspect game communications, or require specialized software on game servers.

To address these issues, we introduce Trilobyte, a communication system that leverages covert channels in game state shared through accounts on popular single-player gaming platforms [14], many located in censored countries [12]. The game state is saved to record progress during regular game playing activities, and is synchronized across different devices through storage provided by gaming platforms. Trilobyte assumes an adversary that controls gaming servers and can inspect all gaming communications.

We show that Trilobyte can hide up to 5.3 MB of data during a one hour gaming session (§ 5). We investigate in-game censorship in the gaming ecosystem accessible in China, through experiments between devices in China and US with accounts on 45 different games. We show that single-player games popular in China fail to detect data embedded in uploaded game state, even when containing keywords considered sensitive [1]. While all Baidu API-compliant

games censor plaintext communications containing sensitive keywords, they fail to censor them when compressed, encrypted or steganographically hidden in regular communications (§ 6).

To evaluate the feasibility of acquiring gaming accounts to be used for Trilobyte communications, we acquire thousands of gaming accounts on Chinese gaming platforms (§ 7.1), and conduct surveys with 285 Chinese gamers about their gaming account rental and lending experiences (§ 7.2). We find that gaming accounts rented or purchased in China can be used to communicate and load data, and can be acquired using cryptocurrencies.

2 Related Work

Previous work that used games to evade censorship includes Castle [22], that hides data into play-time user commands of real-time strategy (RTS) games. Castle assumes that the game operators do not collude with the censor, and the censor cannot inspect the game state of users or the content of game communications.

Rook [27] uses the traffic generated by a first-person shooter game to embed hidden data in mutable fields of game packets. Rook assumes that game traffic is unencrypted and can be inspected by the censor, but requires a decentralized game infrastructure, where its software must run on both user devices and private servers.

Telepath [33] substitutes non-disruptive play-time messages in Minecraft network traffic. This ensures that traffic patterns are indistinguishable from regular Minecraft traffic. Similar to Rook [27], Telepath works on a decentralized environment. Similar to Castle [22], Telepath assumes that the adversary can only observe a side channel of times and sizes of encrypted packets.

Trilobyte instead assumes the centralized game infrastructure ubiquitous today, where the game platform does not install additional software, and the censor can inspect all user communications. Trilobyte hides data in state saved during game playing activities on the user device.

3 Model and Background

We consider users located in a censored area, who need to share content with other users who are either in or outside the censored area, see Figure 1. Users consist of both *writers* who hide data and *readers* who access the hidden data. We consider a system that provides such read and write functionality through single-player games accessible in the censored area. Both writers and readers install and run a system client on their devices. This section provides background on the single-player game ecosystem, details the threat model, and specifies the system requirements.

3.1 Single-Player Game Ecosystem

Game Platforms. Gaming platforms like Steam [18], EA App [15], WeGame [19], GOG [17], or Epic Game Store [16], host video games uploaded by game developers, and provide functionality for users to search, access and play video games. Users access gaming platforms through clients, which they install on their devices. The clients provide an interface for users to connect to the platform server.

Game Platforms Accounts. To authenticate to the platform, and then search, purchase, manage, install, and uninstall video games, users need to create accounts on the gaming platform. Creating pseudonymous accounts and using them to communicate is difficult

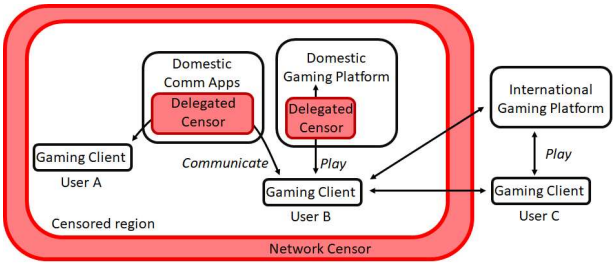

Figure 1: System model. Users install gaming clients, that connect to gaming platforms. Censorship is implemented at the level of the Internet infrastructure, and is also delegated to gaming platforms.

in countries like China where platforms require users to provide government-issued identification. Instead, users can acquire and share gaming accounts by renting or purchasing them, see § 7.2 and § 7.1.

Single-Player Game State. To minimize disruptions during player disconnections, most single-player games provide status-saving functionality, that allows users to save game state on their device. Games store state files in dedicated directories, and each game state is stored in a different file or sub-directory. To enable users to play on multiple devices, major gaming platforms [15–19] provide game state storage services for supported single-player games. Upon game launch and exit events, the gaming client synchronizes saved game state between the user device and platform-provided storage.

Gaming Account Rental Platforms. Dedicated gaming account rental platforms like Zuhaowan [9] enable account owners (or lenders) to list multiple accounts for rent. The listing of any account specifies the purchased games and features accessible from the account, the available renting intervals, e.g., hourly, daily, weekly, and the renting price, which is often only a few cents per hour.

The rental platform provides a client that simplifies the account authentication process and the session management process for renters and lenders. Lenders needs to provide login credentials (account name and password) to the platform. Once the renter pays the requested amount, the rental platform sends the lender's credentials to the client installed on the renter's device. The client uses the credentials to log in at the start of the session, and enforces the account logout at the end of the paid session.

3.2 Adversary Model

We consider an adversary that moderates and censors communications over services hosted in its area of influence. In the following, services hosted within the adversary's area of influence are called *domestic*, those hosted outside are *international*. The adversary can inspect all the Internet traffic of users within its area of influence, and can filter or block any connection where at least one of the endpoints is located in that area, see outer red boundary in Figure 1.

Consistent with previous findings [24, 30], we assume that the adversary *delegates* content moderation and censorship responsibilities to services, e.g., gaming platforms, that operate in its area of influence, see delegated censor blocks in Figure 1. Such services often employ content filters and specialized personnel to monitor

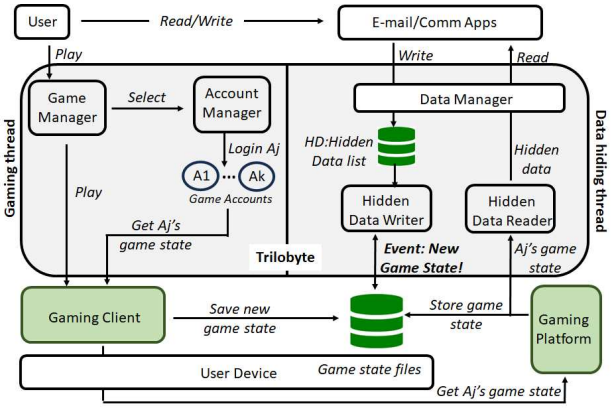

Figure 2: Trilobyte client with independent gaming and data hiding threads. The gaming thread (left) builds on the platform client, and generates the state which is used for cover by the data hiding thread (right).

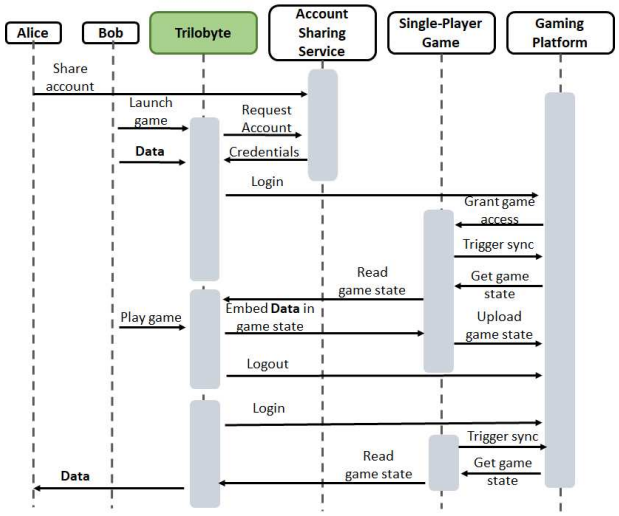

Figure 3: Data communication sequence diagram between Trilobyte clients A and B that share an account owned by A through a rental platform.

and censor user communications and content. This includes removing political messages, discussions of sensitive topics, and the use of certain words or phrases that are considered to be sensitive.

We assume that the adversary can install and use any censorship evasion software on any number of devices. However, it does not have access to the state of software clients installed by other users, has no control over the software they install and execute on their devices, and has no access to game activities they perform on their local devices, and the game state generated and saved locally.

4 Trilobyte

We introduce Trilobyte, a covert communication system for users of single-player games, where communications take place over played games. The Trilobyte architecture is outlined in Figure 2.

Setup. Each user needs to install the Trilobyte client. The client is responsible for embedding and extracting data from game state stored in those accounts. Trilobyte achieves behavioral independence [28] by using independent gaming and data hiding threads. To communicate through Trilobyte, two users need to share key material and information about an account *acc* they share, e.g., an account id on a gaming platform site or with a game developer, or the id of a listing in an account rental site. While outside the scope of this paper, this bootstrapping step could take place over a low-bandwidth out-of-band communication channel. Users share communication-hiding game state through gaming accounts. A user can control and share multiple accounts, see § 7.2.

Embedding Data in Game State. A Trilobyte client embeds data in saved game state, i.e., in the same directories and/or files where the state is written. Several game state fields provide potential cover, e.g., 3D player positions, game play timestamps, and game unit state. However, experiments with the NIST randomness test suite [20] applied to data we collected from hundreds of game states, revealed that none of the evaluated fields pass all the randomness tests. Instead, Trilobyte uses SteganoGAN [32] to hide data in thumbnail images used by popular single-player games to allow users to visually distinguish between saved game states.

Trilobyte organizes data into segments. Each segment is encrypted separately, and stored in a different game state. The length of a segment depends on the size of thumbnail image that is used to hide the data and the threat model. For instance, games from developers that do not collude with the adversary and that encrypt game traffic, offer larger segment sizes than games from colluding or insecure providers.

Communication Protocol. Figure 3 illustrates the Trilobyte communication protocol conducted between a sender (B) and receiver (A) that share a gaming account *acc*, along with data encryption and authentication keys. The keys are shared in an initial setup step, e.g., through out-of-band channels. However, A, the owner of *acc*, shares *acc* with B through a dedicated account rental platform, e.g., Zuhaowan [9] (§ 3.1).

When the sender B launches a game, his Trilobyte client rents the account *acc* from the rental service. Once it logs in to *acc*, the game client downloads any game state stored for *acc*. When user B plays the game, and the user or the game saves state, the Trilobyte client hides encrypted and authenticated communication data into the thumbnail associated with the locally-stored game state. When B logs out of the account, the game platform client uploads all the locally-stored game states to the gaming platform's storage.

Once A is notified by the rental platform about B's logout event, A's Trilobyte client logs back in to *acc*. It then downloads all the newly created game state from the gaming platform. The client uses SteganoGAN [32] to recover the hidden data, and uses the keys shared with B to authenticate the sender, and decrypt the data.

5 Trilobyte Evaluation

We implemented Trilobyte using Python and the SteganoGAN package[32]. We then conducted experiments between two devices, one located in China (i5 2.7 GHz CPU, 8 GB RAM, 200 Mbps downlink, 15 Mbps uplink), and one located in the US (i7 3.6 GHz CPU, 8 GB RAM desktop, 1,200 Mbps downlink, up to 35Mbps uplink). For each investigated game we used two accounts, one accessed from

Game	Hidden Data per State	# of Account Investigated	Max States # in hour	Hidden Data per Session
Balduŕs Gate 3	495KB	5	11	5.31MB
Cyberpunk 2077	62.7KB	5	15	940.5KB
Divinity: Original Sin	92.81KB	2	1	92.81KB
Divinity: Original Sin 2	69.61KB	3	3	208.83KB
Dragon Age Origins	70.4KB	3	6	422.4KB
Loop Hero	25.14KB	3	1	25.14KB
The Witcher 3	15.68KB	2	7	109.73KB
Watch Dogs Legion	62.7KB	3	2	125.4KB
Yakuza: Like a Dragon	15.68KB	3	1	15.68KB

Table 1: Data sharing through single-player game saving file thumbnails. One-hour gaming session in the recent popular game Baldur's Gate 3 can hide up to 5.31MB of data.

Game	Platform	Licensed	Paid	Storage Size	Game State Size	Encrypted Data	Sensitive Plaintext
Minecraft	NetEase	●	○	1GB	≤ 100GB	●	●
Cyberpunk 2077	Steam	○	●	2GB	6MB	●	●
Rimworld	Steam	○	●	92.95GB	16MB	●	●
No Man's Sky	Steam	○	●	210MB	256KB	●	●
Mount & Blade	Steam	○	●	953MB	5MB	●	●
Moncage	Steam CN	●	●	10MB	400KB	●	●
A Perfect Day	WeGame	●	●	100MB	100KB	●	●
Battlefield	Origin	○	●	1GB	2MB	●	●
LoopHero	Epic	○	●	20MB	30KB	●	●
Baldur's Gate 3	Steam	○	●	18.55GB	16MB	●	●
Divinity: Original Sin	Steam/GOG	○	●	200MB	9MB	●	●
Dragon Age Origins	Steam	○	●	100MB	16MB	●	●
The Witcher 3	Steam	○	●	953.67MB	2.5MB	●	●
Watch Dogs Legion	Steam	○	●	1GB	78KB	●	●
Yakuza: Like a Dragon	Steam	○	●	66.18MB	1MB	●	●

Table 2: Data sharing through single-player game snapshots. All evaluated games and platforms allowed uploading and downloading plaintext and encrypted sensitive keywords appended to or replacing game state.

the device in China, the other accessed from the device in the US. Both accounts were used to send and to receive messages.

Ethical Considerations. To minimize risks, all the accounts used for the following experiments were controlled by paper authors. Further, no sensitive data was sent in plaintext over channels accessible to other game users.

Data Hiding Experiments. We evaluated the ability of Trilobyte to hide data in single-player game state, assuming that the censor can inspect all user communications to domestic or international online services. This includes network packets, content of communications taking place through domestic platforms, and data stored on domestic platforms, including game state.

Table 1 shows results from experiments with nine games from the Steam, GOG and Epic platforms, that associate thumbnails to saved game state. While the platforms allow users to upload a total of between 66.18MB and 15.55GB of game state, Table 1 shows the maximum data that Trilobyte can hide per game state thumbnail. Values differ due to different image sizes supported by these games. Table 1 shows that for some games, account renters saved up to 15 states in one hour. Thus, five of the investigated games allow Trilobyte to hide more than 100KB in one hour, with Baldur's Gate 3 exceeding 5.3 MB.

6 Measurements of In-Game Censorship in China

We now present results from an investigation of real-life censors in gaming platforms, to determine if data hiding is currently necessary.

Do Censors Monitor Game State? We first explored the potential to bypass censorship by embedding communications into game state files. We evaluated 15 single-player games from several platforms, both Chinese and international. All evaluated games allow two users to login to the same account, save game state, and download the state created by the other user. Table 2 shows the results. While most games require a one-time purchase, most platforms also host free games that provide storage for game state i.e., Steam (2034 such games), GOG (22) Epic (5), Tencent WeGame (5).

We performed experiments with files containing sensitive keywords sent both in plaintext and encrypted, and with files resulting from the compression of such files and folders. All evaluated games and platforms allowed the injection of such files, in game state directories. In addition, all evaluated games and platforms allowed the injection of plaintext and encrypted sensitive keywords in new fields of existing game state files. They also even allowed completely replacing existing, valid game state files with such content, for all game state file extension types. All platforms allowed uploading such game state from both US and China, and downloading it through the same account in the other country.

Table 2 also shows the average game state size and the per-game limit on total game state size. The average game state size for the evaluated games and platforms ranges from tens of KB to megabytes, with the exception of Minecraft, where maps can take up to 100 GB. However, platforms impose a limit on total game state size that ranges from 10 MB to 2GB. Once the total size of the game state files reaches the limit, the oldest state is removed until there is enough space to store the new one. This reveals the potential single-player games to enable the communication of large sensitive data while evading censorship.

Do Censors Monitor In-Game Communications? We evaluated in-game censorship of keywords considered sensitive in China. For this, we first collected a list of candidate keywords from a public dataset spanning 2004 to 2014 [10], and from online forums and gaming chats. Our evaluation dataset includes 12,858 sensitive keywords. We then employed the Baidu censorship API [1] to detect the keywords filtered by key Chinese game operators such as Baidu, Tencent, and NetEase. The Baidu API identified 3,919 keywords: 1,925 were labeled to be politically sensitive, 723 to be terrorism-related, 1,000 sex-related, 125 curse words, and 41 related to malicious ads.

Table 3 shows results of experiments with sending these keywords on chat channels available on 30 Chinese online games with diverse genres, selected based on Baidu's search index [11]: the 15 highest ranked Chinese online games, 10 randomly selected mid-ranked games, and the 5 lowest ranked games. For each investigated game we used two accounts controlled by paper authors. We logged in one account from a computer in China, and on another account from a computer in the US. We found that no game censored the keywords if they were sent compressed using the Zlib library, encrypted using AES with 256-bit keys, or steganographically hidden in benign cover messages using Unistego [7].

Game Name	Genres	Developer	Licensed	Platform	Paid	Size	Chat Channel	Compressed	Encrypted	Stego-Hidden
Genshin Impact	ARPG	Domestic	●	PC	○	64.5GB	G,P	○	○	○
Honor of Kings	MOBA	Domestic	●	Mobile	○	3.7GB	W,G,P	○	○	○
Sausage Man	Shooter	Domestic	●	Mobile	○	3.5GB	W,G,P	○	○	○
Mini World	Shooter	Domestic	●	Mobile	○	592.3MB	W,G,P	○	○	○
PUBG	Shooter	International	○	PC	○	33.86GB	W,G,P	○	○	○
Cross Fire	Shooter	Domestic	●	PC	○	6.6GB	W,G,P	○	○	○
Game of Peace	Shooter	Domestic	●	Mobile	○	1.89GB	W,G,P	○	○	○
Sanguosha	Card	Domestic	●	PC	○	79MB	W,G,P	○	○	○
League of Legends	MOBA	International	●	PC	○	21.6GB	W,G,P	○	○	○
Fantasy Westward Journey	MMORPG	Domestic	●	PC	○	4.92GB	W,G,P	○	○	○
Naraka: Bladepoint	ARPG	Domestic	●	PC	●	32.33GB	W,G,P	○	○	○
Final Fantasy XIV	MMORPG	International	●	PC	●	35.4GB	W,G,P	○	○	○
Justice	MMORPG	Domestic	●	PC	○	9.61GB	W,G,P	○	○	○
MapleStory	MMORPG	International	●	PC	○	12.9MB	W,G,P	○	○	○
World of Warcraft	MMORPG	International	●	PC	○	75.8GB	W,G,P	○	○	○
Teamfight Tactics	Strategy	International	●	PC	○	2.13GB	W,G,P	○	○	○
Audition Dance Battle Online	Rhythm	Domestic	●	PC	○	1.43GB	W,G,P	○	○	○
AssaultFire	Shooter	Domestic	●	PC	○	21GB	W,G,P	○	○	○
Warframe	ARPG	International	●	PC	○	32.42GB	W,G,P	○	○	○
Hearthstone	Card	International	●	PC	○	2.93GB	W,P	○	○	○
Wulingwaizhuan OL	MMORPG	Domestic	●	PC	○	1.7GB	W,G,P	○	○	○
JX3	MMORPG	Domestic	●	PC	○	7.78GB	W,G,P	○	○	○
Lost Ark	MMORPG	International	○	PC	○	72.47GB	W,G,P	○	○	○
Path of Exile	ARPG	International	●	PC	○	30.01GB	W,G,P	○	○	○
Escape from Tarkov	Shooter	International	○	PC	○	12.1GB	W,G,P	○	○	○
DOTA 2	MOBA	International	●	PC	○	43.6GB	W,G,P	○	○	○
QQ Dance	Rhythm	Domestic	●	PC	○	2.4GB	W,G,P	○	○	○
Honkai Impact 3rd	Action	Domestic	●	Mobile	○	7.6GB	W,G,P	○	○	○
Run Juveniles	Action	Domestic	●	Mobile	○	1.2GB	W,G,P	○	○	○
The Elder Scrolls Online	MMORPG	International	○	PC	●	117.5GB	W,G,P	○	○	○

Table 3: Censorship of communication channels in both domestic (developed in China) and international games, both licensed and unlicensed for operation in China. Empty circles in the last three columns show that Baidu API-labeled sensitive keywords that were either Zlib-compressed, AES256-encrypted or steganographycally hidden in cover text were not censored on any of the available channel types (public, group, world).

7 Account Acquisition Feasibility

Trilobyte users can communicate through their own gaming accounts, or through rented or purchased accounts. We now assess the feasibility of acquiring gaming accounts.

7.1 Account Acquisition Experiments

All the accounts acquired in our experiments were used to estimate capacity and analyze typical user behavior. None of these accounts were used for data hiding experiments.

Renting Accounts. To approximate the amount of data that Trilobyte can hide in a one hour gaming session, we rented 2 to 5 gaming accounts for each game, totaling 29 gaming accounts, and collected their timeline of stored states, see Table 1.

Purchasing Accounts. We found sellers with hundreds of thousands of for-sale, real-name verified gaming accounts, for the Chinese NetEase [3] platforms. We purchased 25 NetEase accounts for 1 CNY (≈ 0.15 USD) each. The sellers accept Tether cryptocurrency payments. We also purchased Battle.net.cn accounts at a rate of 4 CNY (≈ 0.5 USD) per account, and Tencent accounts [6] that come with a linked national ID. We have logged in into and validate each account. To avoid real name verification and the need to provide a phone number valid in China, users can purchase accounts on international game platforms. Such accounts can be found through e-commerce websites, e.g., Taobao; game clients are accessible via domestic search engines. For example, we found Steam accounts registered in Argentina, for sale on Taobao for 1.5 CNY (≈ $0.22).

7.2 Perceptions of Account Acquisition

We further conducted a survey to investigate the perceptions of Chinese users about their experiences with renting, lending and purchasing gaming accounts. The survey, written in Simplified Chinese, was posted on the Wenjuan.com crowdsourcing site. Appendix A includes the English translation of the questions. We recruited participants through the nga.cn forum, a general gaming community for online game video gamers, and WeChat and QQ chat groups dedicated to popular video games.

The survey procedure was scrutinized and was approved by the institutional review board at our university. Participants were presented with a consent form before starting the survey. No personally identifiable information (PII) was collected from participants. The survey did not investigate issues considered to be sensitive in China.

Participants were able to skip any question they were uncomfortable answering. Survey data was stored on a secure university Linux server and accessed via encrypted channels on researchers' password-protected laptops.

Of the 393 survey respondents, 285 were over 18 years old and played video games (127 female, 163 male; 130 employed, 132 students, 17 unemployed, 1 self-employed). All respondents, i.e., 33 account lenders and 114 renters, took at least 30s to complete the survey (M = 36s, SD = 109s). Survey findings include (1) **In-game communications are popular**: Twenty-nine of the 33 account lenders said that renters can use their accounts to communicate; 100 out of 114 account renters have used rented accounts to communicate with others; (2) **Data storage**: Of the 33 account lenders, 30 said that renters are allowed to upload content to their accounts and 71 out of the 114 account renters have uploaded content in accounts they rented; (3) **Cryptocurrency use**: Six lenders accept cryptocurrency payments for their accounts, including Bitcoin (4), Ethereum (2), and Tether (3). Ten renters have used cryptocurrencies to rent accounts, including Bitcoin (all 10), Tether (4), and Ethereum (3).

8 Conclusions

We introduced Trilobyte, a system that hides data with plausible deniability in game state generated opportunistically during regular game-playing activities in single-player games. Trilobyte users communicate data-hiding game state through accounts shared on gaming platforms. Experiments reveal that Trilobyte can embed megabytes of data in state saved for games currently licensed in China with one-hour gaming sessions. We justify the practicality of Trilobyte through surveys with Chinese gamers and through measurements conducted between devices in China and the U.S.

9 Acknowledgments

This work was supported in part through NSF awards 2321649, 2114911, and 2052951.

References

[1] [n. d.]. Baidu Content Censoring Service API. Baidu, https://ai.baidu.com/tech/textcensoring.
[2] [n. d.]. Free privacy and security tools: Blocked In ... Comparitech, https://www.comparitech.com/privacy-security-tools/.
[3] [n. d.]. NetEase Game. http://game.163.com/.
[4] [n. d.]. QQ. https://mail.qq.com/.
[5] [n. d.]. Sina Weibo. https://my.weibo.com/.
[6] [n. d.]. Tencent Online Game Account Selling on Taobao. Taobao, https://item.taobao.com/item.htm?id=669732627265.
[7] [n. d.]. Unistego.
[8] [n. d.]. Weixin/WeChat. https://weixin.qq.com/.
[9] [n. d.]. Zuhaowan. https://www.zuhaowan.com.
[10] 2014. Chinese Keywords GitHub Repository. GitHub, https://github.com/jasonqng/chinese-keywords.
[11] 2022. Most Popular Searched Online Games in China. Baidu, https://lewan.baidu.com/rankland?idfrom=1043&gameSource=client&gameType=0.
[12] 2022. Top 10 Countries/Markets by Game Revenues. newzoo, https://newzoo.com/insights/rankings/top-10-countries-by-game-revenues.
[13] 2023. Finnish newspaper hides Ukraine news reports for Russians in online game. The Guardian, https://www.theguardian.com/world/2023/may/03/finnish-newspaper-hides-news-reports-for-russians-in-online-game.
[14] 2024. How Many Gamers Are There? Exploding Topics, https://prioridata.com/number-of-gamers.
[15] Last accessed 2024. EA App Game Platform. https://www.ea.com/ea-app.
[16] Last accessed 2024. Epic Game Store Platform. https://store.epicgames.com/.
[17] Last accessed 2024. GOG Game Platform. https://www.gog.com/.
[18] Last accessed 2024. Steam Game Platform. https://steampowered.com.
[19] Last accessed 2024. WeGame Game Platform. https://www.wegame.com.cn/.
[20] Lawrence E Bassham III, Andrew L Rukhin, Juan Soto, James R Nechvatal, Miles E Smid, Elaine B Barker, Stefan D Leigh, Mark Levenson, Mark Vangel, David L Banks, et al. 2010. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards & Technology.
[21] Yuzhou Feng, Ruyu Zhai, and Bogdan Carbunar. 2023. A Study of China's Censorship and Its Evasion Through the Lens of Online Gaming. In Proceedings of the 32nd Usenix Security Symposium.
[22] Bridger Hahn, Rishab Nithyanand, Phillipa Gill, and Rob Johnson. 2016. Games without Frontiers: Investigating Video Games as a Covert Channel. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). 63–77.
[23] Julio C Hernandez-Castro, Ignacio Blasco-Lopez, Juan M Estevez-Tapiador, and Arturo Ribagorda-Garnacho. 2006. Steganography in games: A general methodology and its application to the game of Go. computers & security 25, 1 (2006).
[24] Jeffrey Knockel, Lotus Ruan, and Masashi Crete-Nishihata. 2017. Measuring Decentralization of Chinese Keyword Censorship via Mobile Games. In 7th USENIX Workshop on Free and Open Communications on the Internet (FOCI).
[25] Jason Q. Ng Lotus Ruan, Jeffrey Knockel and Masashi Crete-Nishihata. 2016. One App, Two Systems: How Wechat Uses One Censorship Policy in China and Another Internationally. 84 (2016).
[26] Steven J Murdoch and Piotr Zieliński. 2005. Covert channels for collusion in online computer games. In Proceedings of the 6th International Workshop on Information Hiding. Springer, 355–369.
[27] Paul Vines and Tadayoshi Kohno. 2015. Rook: Using Video Games as a Low-Bandwidth Censorship Resistant Communication Platform. In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society. 75–84.
[28] Ryan Wails, Andrew Stange, Eliana Troper, Aylin Caliskan, Roger Dingledine, Rob Jansen, and Micah Sherr. 2022. Learning to Behave: Improving Covert Channel Security with Behavior-Based Designs. Proceedings on Privacy Enhancing Technologies 3 (2022), 179–199.
[29] Abdul Wajid, Nasir Kamal, Muhammad Sharjeel, Raaez Muhammad Sheikh, Huzaifah Bin Wasim, Muhammad Hashir Ali, Wajahat Hussain, Syed Taha Ali, and Latif Anjum. 2021. A First Look at Private Communications in Video Games using Visual Features. Proceedings on Privacy Enhancing Technologies 2021, 3 (2021), 433–452.
[30] Diwen Xue, Benjamin Mixon-Baca, Anna Ablove, Beau Kujath, Jedidiah R Crandall, and Roya Ensafi. 2022. TSPU: Russia's decentralized censorship system. In Proceedings of the 22nd ACM Internet Measurement Conference. 179–194.
[31] Sebastian Zander, Grenville Armitage, and Philip Branch. 2008. Covert channels in multiplayer first person shooter online games. In 2008 33rd IEEE Conference on Local Computer Networks (LCN). IEEE, 215–222.
[32] Kevin Alex Zhang, Alfredo Cuesta-Infante, Lei Xu, and Kalyan Veeramachaneni. 2019. SteganoGAN: High capacity image steganography with GANs. arXiv preprint arXiv:1901.03892 (2019).
[33] Sun Zhen and Shmatikov Vitaly. 2023. TELEPATH: A Minecraft-based Covert Communication System. In Proceedings of the IEEE Symposium on Security and Privacy.

A Survey

1. How old are you now?
2. What is your current occupation?
3. What is your gender?
4. Do you play online video games? If "No" stop the survey.
5. Have you ever rented any game account on an account rental service? (If "No" skip to Q9). (If "Yes", ask) What account renting platforms have you used?
6. Did you ever rent an account that allowed you to communicate with other accounts on the gaming platform?
7. Did you ever rent an account where you were able to upload content to the account?
8. What payment methods do you use to rent accounts?
9. Have you ever advertised and lent any of your own game accounts on an account rental service? (If "No" end the survey).
10. Did you ever lend an account that allow customers to communicate with other accounts on the gaming platform?
11. Did you ever lend an account that allows customers to upload content to the account?
12. What payment methods do you accept to lend accounts?