# Examining Security Issues in Dolphin Netplay

Austin Taghavi
Department of Computer Science and Engineering
Texas A&M University
College Station, TX
Email: austintaghavi@gmail.com

Philip Van Ruitenbeek
Department of Computer Science and Engineering
Texas A&M University
College Station, TX
Email: philipvr@gmail.com

## I. Introduction

Online gaming is as popular as it has ever been, and only continues to grow. With the advent of eSports, we are seeing competitive video gaming turn into a legitimate industry. Video games are played for fun, but they are also played for sport and, in some cases, as a career. This changes security issues and cheating in online gaming from an annoyance to a serious issue.

One such eSport is the Super Smash Bros franchise, from Nintendo. This is considered by many to be the first eSport, as the competitive Super Smash Bros scene emerged before the game was playable online. While newest installations of Super Smash Bros have online support through Nintendo, older versions do not. In particular, we are concerned with Super Smash Bros Melee, which we will refer to as SSBM throughout this proposal. The competitive community for SSBM began with groups of people meeting in person and holding tournaments. However, in recent years, ways of playing the game online have emerged. Dolphin is a Gamecube emulator for Windows, which provides a system called NetPlay for playing certain Gamecube games online.

We wish to explore the security issues with NetPlay for Dolphin, in particular how they pertain to SSBM. Our analysis will be threefold: (1) Cheating at SSBM through NetPlay for Dolphin, (2) Malicious activity via the connection provided by NetPlay, and (3) possible solutions for the issues we find.

## II. Proposed Technique

To explore the methods of cheating at SSBM via NetPlay, we will first use a network traffic tool such as Wireshark to capture traffic during an SSBM session. This will allow us to analyze the way that data is sent back and forth to establish the game, and enable us to spoof input from one user to cheat.

Next, we will try various known methods of attack using the NetPlay connection, such as buffer overflow. We will note the results and how NetPlay can be used to facilitate malicious behavior.

Finally, we will propose possible solutions to the vulnerabilities that we have found during this project.

## III. Related Work

The online PC gaming in the U.S. is a multi-billion dollar industry [1]. When online gamers encounter cheaters, they may feel that the game is ruined and may give up on playing the game [2].

Online gaming is the most successful software industry in Asia and has led to a rapid increase in cyber-criminal activity in Taiwan [3].

Steam, a popular online game platform, reported that 77,000 accounts are hijacked and pillaged each month [4]. It was later found by [5] that malware had been developed to steal Steam user credentials.

[6] uses a time series based user modeling approach to automatically detect compromised accounts in Massively Multi-player Online Role Playing Games. [7] found that idle time distribution is a representative feature of game players.

## IV. Project Plan

### A. Task 1. Capture and analyze packet data for a SSBM game via NetPlay – Austin and Philip (3 weeks)

This task will require us to play SSBM games via NetPlay and capture the traffic that occurs during the game. We will then analyze this traffic and infer the structure of the packets sent back and forth to establish the game. This will give us a good base for the next task.

### B. Task 2. Design and test out cheating on SSBM via spoofing packets – Austin (4 weeks)

Using what we learned from task 1, we will design and test out methods of cheating in SSBM games by spoofing data.

### C. Task 3. Design and test attacks on victim PC via NetPlay – Philip (4 weeks)

The NetPlay connection could possibly be used to create buffer overflow or other attacks on another PC. We will explore these possibilities.

### D. Task 4. Propose solutions to vulnerabilities found – Austin and Philip (3 weeks)

Finally, we will propose solutions to the vulnerabilities that we found. While we may not be able to implement these solutions, we can certainly design and propose them.

# References

[1] D. Takahashi, "U.S. games industry forecast to grow 30 percent to $19.6b by 2019," Jun 2015. [Online]. Available: http://venturebeat.com/2015/06/02/u-s-games-industry-forecast-to-grow-30-to-19-6b-by-2019/

[2] J. J. Yan and H. Choi, "Security issues in online games," *The Electronic Library*, vol. 20, no. 2, pp. 125–133, 2002. [Online]. Available: http://dx.doi.org/10.1108/02640470210424455

[3] Y.-C. Chen, P. Chen, R. Song, and L. Korba, "Online gaming crime and security issue-cases and countermeasures from taiwan," *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*, 2004.

[4] "Security and trading," Dec 2015. [Online]. Available: http://store.steampowered.com/news/19618/

[5] S. Pontiroli, "All your creds are belong to us," Mar 2016. [Online]. Available: https://securelist.com/blog/research/74137/all-your-creds-are-belong-to-us/

[6] J. Oh, Z. H. Borbora, and J. Srivastava, "Automatic detection of compromised accounts in mmorpgs," in *Social Informatics (SocialInformatics), 2012 International Conference on*, Dec 2012, pp. 222–227.

[7] K.-T. Chen and L.-W. Hong, "User identification based on game-play activity patterns," in *NetGames'07: Proceedings of the 6th ACM SIGCOMM workshop on Network and System Support for Games*. ACM, 2007, pp. 7–12.