Jash Popat (z5611818)

COMP6441 – Security Engineering

25 July 2025

The Revival of Retro Gaming: Assessing Player Security and Decentralized Cybersecurity in Unofficial Online Communities for Nintendo Wii and Wii U Consoles

** If you don't know what a term or name is, refer to the "A Gamer's Guide to Nintendo Hacks" in Appendix A*

Deliverables (on GitHub): https://github.com/JashPopat/The-Revival-of-Retro-Gaming

Results:

The main outcome of this project was to analyze the unofficial decentralized servers set up for the Wii and Wii U, namely Wiimmfi (for Nintendo Wii) and the Pretendo Network (for Nintendo Wii U), and perform a comprehensive cybersecurity investigation on their services using packet capture techniques on Wireshark, along with decryption of packet information with the help of learned algorithms and written code to test out their strength against attacks from outside.

Using the information found in the Wireshark traces and from within individual packets themselves, communications between the console and the severs revealed several workarounds and methods used to implement the online functionality of the games, like Pretendo redirecting queries to its own servers vs. Wiimmfi spoofing Nintendo's original routes.

Wiimmfi's traces helped reveal that on the Wii side of things, security was not a priority when implementing the unofficial connections. Transmissions were done using cleartext HTTP (not HTTPS) for transmitting sensitive data like game tokens, passwords, MAC Addresses and more; and when extracting the data from the traces, it was observed that Base64 encoding was used to obfuscate the data being sent over. This measure was clearly not enough as extracting this data and running it through some code I wrote helped decode it and provide actual values (very harmful!).

Pretendo's traces displayed that the developers of this network learned from the past, as this time, proper protocol was followed with the use of TLS (v1.0 or v1.2 based on compatibility). Not only did the developers implement TLS, but also added in an extra layer

of security as TLS1.2 wasn't initially supported by the Wii U. Only once Pretendo got added as a server option did connections move from TLS1.0 to TLS1.2 when confidential information was being sent over to Pretendo's own servers and back. Using new connections each time a TLS1.2 connection was needed, Pretendo not only ensured confidentiality and integrity but also availability and stability as these connections tended to me much more consistent compared that of Wiimmfi (and even Nintendo's original servers, but that is a bit of stretch). The only downside of this was that when receiving both legacy and newer content, the console would need to initialize new connections each time standards had to be changed to TLS1.2, leading to strained connections and frequent timeouts (observed each time software and games were started), as the TLS1.2 connections would often be initiated and then shut soon after due to a constant need to load legacy content. Yet, despite the fact that Pretendo implemented such rigorous measures to ensure safety and security, they were only able to use TLS1.2, which as per today's standards is outdated and insecure. The developers have largely been focused on getting more game to be supported on the service and hence, have not been able to update the security standards for their connections (but could also be the case since such obsolete hardware just isn't capable of handling such standards).

What I Did:

The process began with the modding of my personal Wii U (which is capable of running Wii U games and is backwards compatible with the Wii via its own dedicated "Wii Mode"). This involved:

1. Homebrew environments Aroma and Tiramisu (For Wii U) along with the Homebrew Channel (For Wii) were installed using the Wii U Browser Exploit.
2. Internet Sharing was initialized from my laptop and connected to the Wii U to route all the traffic through the laptop.
3. DNS settings were changed on the Wii U/Wii to redirect traffic to Pretendo and Wiimmfi.
4. Live traffic was captured on my laptop via Wireshark while playing online-enabled games like Super Smash Bros Brawl (Wii), Super Mario Maker (Wii U) and Super

Smash Bros for Wii U; and Miiverse-equivalent services like Nintendo Land (Wii U) and Juxtaposition (Pretendo's own take on Miiverse).

5. Traces of Wii U traffic were analyzed using Wireshark and Python scripts (used for Base64 decoding)

How I Was Challenged:

I was faced with several challenges along the way, all the way from setup to initialization and execution. They are:

Setup: – The major challenge was modifying the NAND of the Wii U as any change would be permanent and any mistake could lead to the console becoming unusable. This, on top of the fact that I had never modded a Wii U before, made this a very unnerving experience as each segment had to be done with incredible caution. This is where I learned how to format hardware the right way, take a NAND backup, load foreign files onto the console, use system vulnerabilities to access internal data and a lot more, all for the very first time.

Initialization: – After loading the mod files onto the console, I had to go through system documentation, Nintendo support pages and helpful YouTube videos to figure out what settings needed further changes, especially in the case of the Wii. The Wii U modding completed a lot of things for me in the GUI, but due to the Wii being a much older console, its modding wasn't coded in as intuitively. I had to manually go through several CLIs to install further add-ons, followed by Wii System settings to input a very particular DNS server to route my connections and finally do a system test to ensure nothing else got unknowingly modified in the process.

Execution: – After capturing the files over the course of a few days, I observed that the most annoying phenomenon that took place was outside packets being detected in Wireshark as well. For example, along with my Pretendo server traffic, Spotify packets from my laptop were also picked up, which lead to some confusion, although it could easily be identified and

avoided from the research. Apart from that, interpreting raw network traffic was the most interesting challenge I faced, especially when the payloads were encrypted or encoded. Understanding TLS handshakes in Pretendo's encrypted sessions and decoding Base64 POST payloads in Wiimmfi's cleartext transmissions were probably the highlight of the challenges, as this was a real life implementation of what I have learned previously, thus motivating me to develop better network debugging habits in the form of noise filtering and TCP segment tracking.

If I had to repeat this project, I would try to mitigate these issues by streamlining my analysis with Wireshark Scripting, broaden the scope to also include the Nintendo DS and 3DS (as they are also supported by Wiimmfi and Pretendo resp.) and even add games like Mario kart Wii and Mario kart 8 to the mix. One more thing I missed out was on gaining the insights of the developers themselves, which would have aided in my research a lot; but sadly, they didn't respond to my requests.

Appendix A - Glossary: *A Gamer's Guide to Nintendo Hacks*

Homebrew – Software created by independent developers that runs on consoles not intended by the manufacturer.

Pretendo – A community-developed online service created by fans to replicate and replace Nintendo's discontinued Wii U and 3DS online features.

Wiimmfi – A fan-made server network created by developers Wiimm and Leseratte to revive online play for Nintendo Wii games after official support for Nintendo WFC (Wi-Fi Connection) ended.

Wireshark – A network packet analyser used to capture and inspect data sent over networks.

Miiverse – A social platform for Wii U.

Juxtaposition – Pretendo's custom implementation of Nintendo's Miiverse

Nintendo Wii – A home video game console released by Nintendo in 2006, known for motion controls and online play.

Nintendo Wii U – The successor to the Wii, released in 2012 with a unique GamePad controller and backward compatibility with the Wii.

Nintendo DS – A handheld gaming console with dual screens released in 2004.

Nintendo 3DS – A successor to the DS, released in 2011, featuring 3D visuals and enhanced online functionality.

NAND – Flash memory used to store the console's system software and data; dangerous to modify without backup.

Base64 Encoding – A method to encode binary data into ASCII string format; often used in transmission but not secure.

DNS Spoofing – Redirecting domain name requests to a different server to simulate or intercept traffic.

TCP Retransmission – When a TCP packet is lost or not acknowledged, it is re-sent to ensure data integrity.

Modding – Altering a console's hardware or software to enable functionality not intended by the original manufacturer.

Bricking – Rendering a device unusable (like a brick) due to firmware or hardware failure.

Appendix B - References

Wiimmfi Project Overview – https://wiimmfi.de/about

Pretendo Network Documentation – https://pretendo.network/

Base64 Encoding Explained – https://datatracker.ietf.org/doc/html/rfc4648

Wii U Homebrew Guide – https://wiiu.hacks.guide/

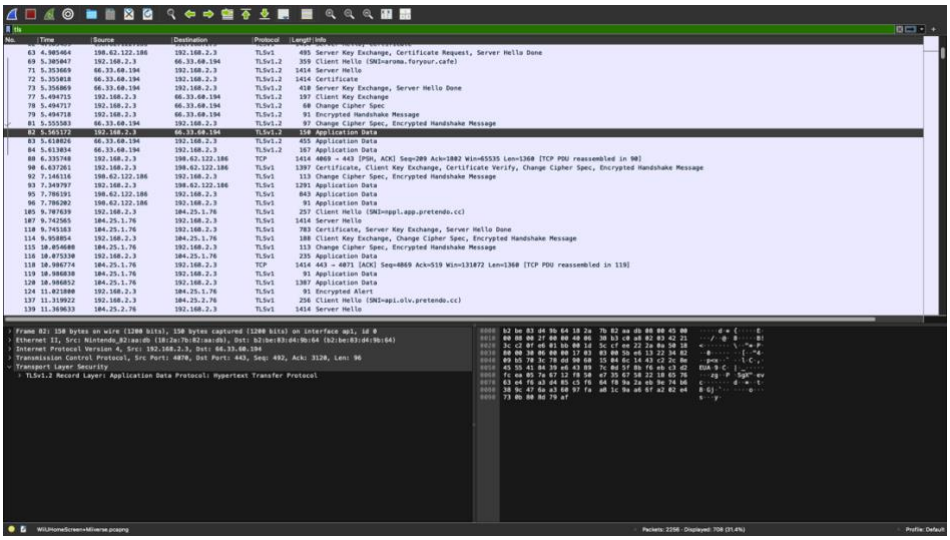
vWii Homebrew Guide - https://wii.hacks.guide/vwii-homebrew-channel.html

Aroma Documentation - https://aroma.foryour.cafe/

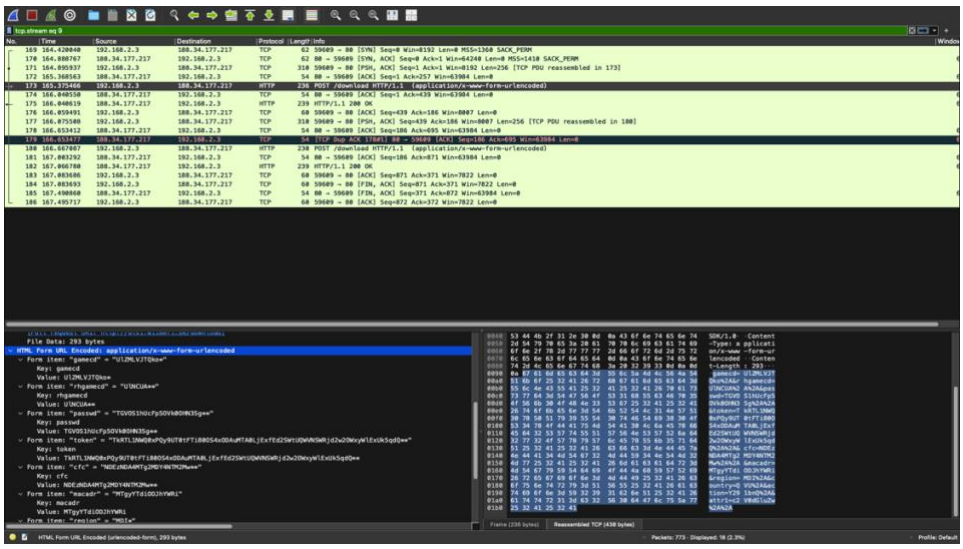
Nintendo Homebrew Channel – https://wiibrew.org/wiki/Homebrew_Channel

Wii U Homebrew Tutorial - https://www.youtube.com/watch?v=XFjFcGJA8ec

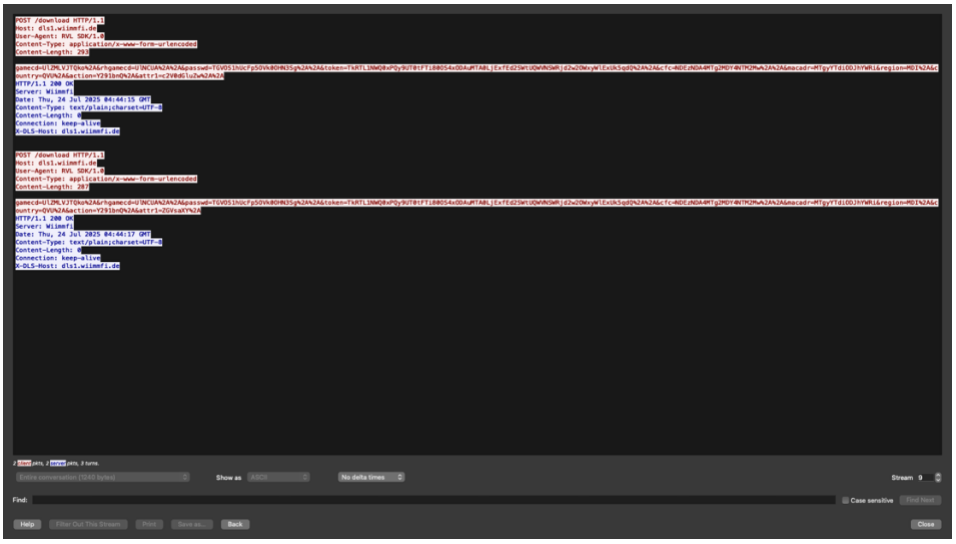
Appendix C – Screenshots (More provided in the deliverables files)



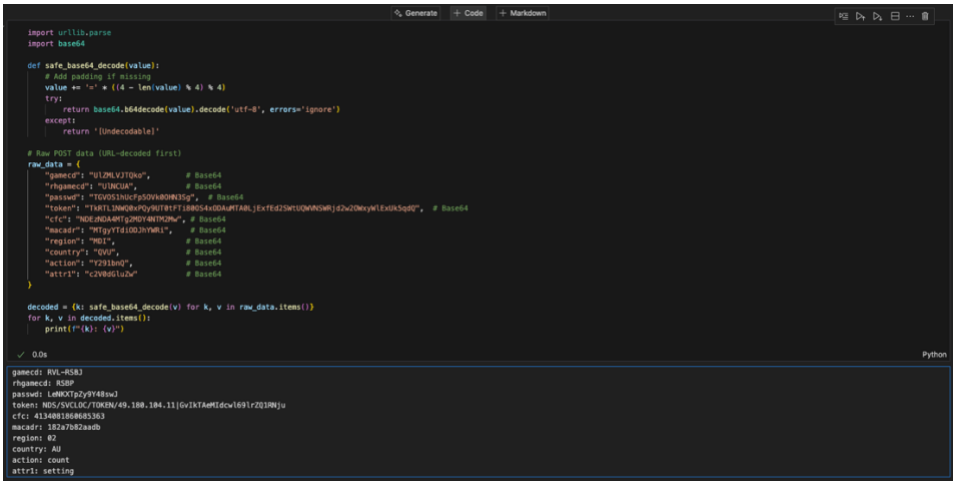
Screenshot A: Wireshark trace showing TLSv1 and v1.2 handshakes with Pretendo Network



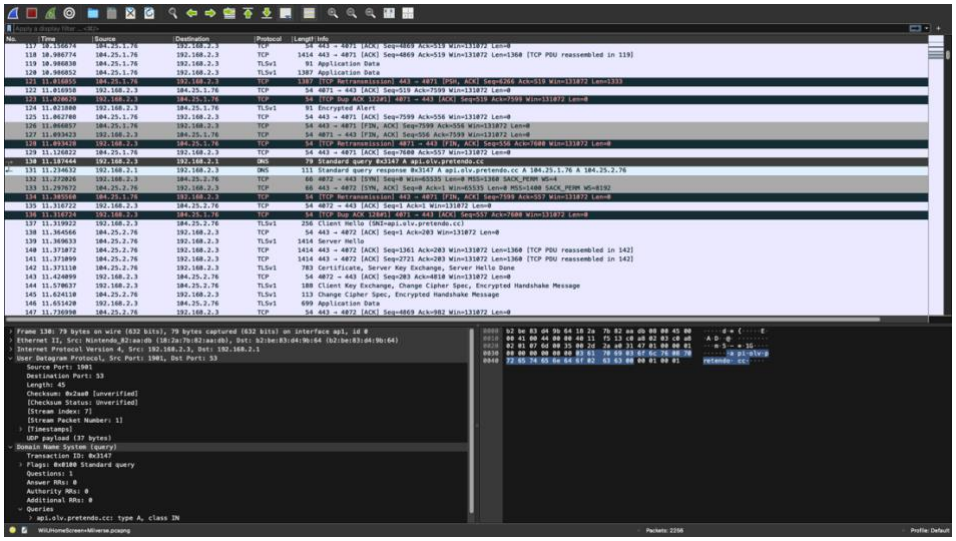
Screenshot B: Wireshark capture showing cleartext POST to Wiimmfi



Screenshot C: Wireshark capture of Follow HTTP Stream for a Wiimmfi Packet



Screenshot C: Base64-decoded token payload from Wiimmfi



Screenshot D: DNS query and response logs for api.olv.pretendo.cc