Security Analysis Of Valve's Steam Platform

6.857 Spring 2018

Nitah Onsongo, Michael Sanabria, Abnell Comas, Paul Herold

Table of Contents

Abstract

This paper analyzes the security of Steam, which is mainly a gaming distribution platform that includes an ecosystem of hardware and software products. Beginning with a discussion on the necessity of good security for the purposes of this platform and the user information it contains, this discussion aims to give an overview of its security policy and look at a brief history of Steam's past security incidents. Further analysis is made on the existing security measures across the many features and aspects of the Steam ecosystem. This analysis goes to involve a discussion of the potential existence of a few vulnerabilities found, particularly at the intersection of hardware such as the Steam Link and paired controller with their lesser known functionalities in software. Ultimately, this paper offers recommendations to both users and Valve developers for the mitigation of such attacks, and provides the best route for continued investigation along the path leading possible exploitations to be made from these discoveries further down the line.

1. Introduction

Security considerations are often overlooked and underestimated for a large variety of small or seemingly unimportant applications and services that do not directly interfere with the spaces of highly personal information or of great influence over large amounts of users. However, it is almost always the case that the most clever, unexpected security hacks arise from a series of many exploits to these smaller, often unprotected features and applications that together unlock dangerous breaks in major related systems that would normally be secure on their own. Platforms on such a large scale as Steam, with such a wide variety of different services and huge amounts of users with relatively little awareness of their data, are especially susceptible to such breaks.

The goal of this paper is to offer insight into the many ways that Steam, as a platform, currently protects its users and service, looking into the numerous types of security features that go along with its various components and how they work. This also includes some amount of testing and demonstration, enough to show the existence of potential vulnerabilities. Moreover, discussion is provided on the history of incidents as well as how they occured. The key takeaway is to always take the safe approach of securing even the most secondary features or arbitrary data collections before enabling them, and to never underestimate the dangers of unintended outcomes within these features, especially when these are a component of or are related to a larger product.

1.1 What is Steam?

Steam is a gaming distribution platform created by the Valve Corporation, an American video game developer. Developers can use Steam to make it easy to give potential customers access to their games without having to worry about the distribution themselves. Steam also gives developers a set of tools such as anti-cheat technology, microtransactions for an in-game economy, and cloud storage. Computer games developed at Valve itself are listed exclusively on Steam to great success, attracting millions of concurrent, regular players. The steam platform is the most popular of its kind to date, with

more than 125 million player accounts, thousands of games available and over 3 Terabytes per second of download bandwidth used on peak hours of an average day.

Users of steam benefit from a convenient client for browsing, buying, downloading and running a near-limitless amount of computer games. The steam website also serves as a form of social platform, with customizable profiles where users can showcase the games they've played, the items they own and the achievements they have earned along the way, both within the games and the steam store itself. As of recently, steam has also opened a division in hardware as well, launching a store offering third-party gaming machines running their own operating system, SteamOS, and specialized computer gaming controllers, embedded with trackpads using haptic feedback for mouse control, as well as designer skins, carrying cases and other optional offerings. The hardware store also features the Steam Link, a portable device capable of streaming games over LAN from any device running the Steam client to nearby monitors or display devices.

1.2 Motivation

On the Steam store, games can be bought, traded for something else like another game or bitcoins, and gifted, but not shared. It lies within the interests of both Steam and the developers who submit games that the platform be secure against both theft and piracy. All purchases must happen exactly as designated, for the right game copy, at the right price, for the right region, and for the right account in order for Steam to operate as a proper revenue-generating service. Online sale and distribution of copyrighted digital products makes for a challenging problem of many security-heavy aspects.

The Steam platform also happens to have a massive user base with accounts affiliated to a surprising amount of information. Not only do users submit their own personal information (emails, phone numbers, residency, age, and the like) to account profiles for its social platforming aspect, but it is also a requirement for account activation that users input valid payment information (credit cards, bank account, and even tax information past a certain spending threshold) to fund wallets. Users expect their payment information, (including the account's passwords themselves) to be safe, and often set even basic profile information to private with the expectation that only allowed friends may see it.

Moreover, the Valve corporation publicly uses the Steam platform to collect massive amounts of large-scale data pertaining to usage, demographics and other metadata. If not properly handled, abstract data such as hardware and OS specifications, time and region usage, purchasing behavior and the like can expose a potentially large payload of users to highly specialized attacks and otherwise unwanted outcomes.

2. Responsible Disclosure

Security is crucial to a platform like Steam that holds a lot of a user's private information. Due to this, the Valve Corporation encourages its users to report any issues they find through their designated security input address. Valve was notified thoroughly about the requests, purpose and details of this project through this security address, at security@valvesoftware.com to offer advance knowledge and assume their consent.

3. Security Policy

Valve Corporation's Legal and Privacy Policy (last modified January 23, 2018) from Steam's official website enlists the following as their platform's principals, authorized actions and associated security policies. [1] [2]

3.1 Principals

3.1.1 Valve Corporation

- Collects and processes personally identifiable information (information that can be used to uniquely identify a user such as name, address or credit card number) associated with users' Steam account.
- Allows third party providers such as order or payment processors to access and use users' personally identifiable information
- Communicates directly to its users about Steam updates
- Can use cookies and other technologies such as web beacons and pixel tags to improve users' experience on their sites
- Provides game licenses to users who've purchased game licenses

3.1.2 Steam Users

- Can create a Steam account and set a password for account login purposes
- Can purchase or sell game subscriptions
- Provide personally identifiable information when signing up for a steam account
- Can disable Valve's use of tracking cookies by changing their browser settings
- Can make their personally identifiable information publicly available to third parties
- Can share information such as game scores with other users on chat forums and instant messaging tools provided by Steam
- Can play a game remotely with other Steam users
- Can trade on the Steam platform, for example, a user can exchange a game licence for another game or for bitcoins

3.1.3 Third party Publishers

- Sell and provide legally owned games and other content on Steam
- Can collect personally identifiable information from Steam users who are using their products

3.2 Features and Policies

1. Authorization Keys
   Valve stores a unique authorization key or CD-Key on a user's hard drive, that is either entered by the user or downloaded automatically during product registration. This authorization key is used to identify a user as valid and allow access to Valve's products, services and third party games. This key is necessary for Valve to supply any products and services subscribed by users.
2. User Information Access Authorization

Only parties authorized by a Steam user can access that user's information. However, Valve may release a user's information to comply with court orders or laws that require them to disclose the information.

3. Password Protected User Accounts
   Steam accounts require a username and password for access and authentication. Valve tends to be more rigorous with password strengths than other sites, that is, some passwords that are admissible on other websites are considered weak and unacceptable for use on Steam.
4. Steam Guard
   Steam Guard protects a user's account with two-tier security. If one logs in to their Steam account using their username and password from an unfamiliar device, a code is sent to their email address to verify their identity. Steam reinforces a policy where a user cannot trade on the platform if they don't have Steam Guard activated.
5. Steam Mobile Authenticator
   The Steam Guard Mobile Authenticator is a two-factor authentication feature that provides an additional level of security to a user's Steam account. The authenticator generates a code that a user needs to enter every time they log on to their Steam account. The code changes every 30 seconds, can be used only once, and is unguessable.
6. User Privacy Settings
   Steam has a "privacy settings" tab for Steam users to set their activity status as either private, visible to friends only, or public. Additionally, users can hide their game lists, trading inventory lists, and other profile elements in a similar manner.
7. Trade Holds
   To prevent theft and fraud, Valve recommends that users use their Steam Mobile Authenticator to authenticate secure trades. When users do not use the authenticator, their trades are put on hold for up to three days. In the event of a fraud or theft, the three-day period provides sufficient time to detect and prevent potential scams from succeeding.
8. Game Keys
   Game keys are codes that Steam users purchase and use to activate a game on Steam. One game key can only be used once and for only a specific game. Once a key is used to activate a game, the user can then download and play the game.
9. Steam Wallet
   The Steam Wallet is similar to a bank account within Steam which contains money that a user can spend to purchase games, downloadable content (DLC), and in-game content. This eliminates the need to enter bank details every time a user wants to make a purchase, thereby reducing chances of bank details being exposed to adversaries.

3.3 Security Goals

Valve leverages the security features in section 3.2 to achieve the following goals.

3.3.1 Piracy Prevention

Piracy of games has been a major concern for almost a decade now. Piracy is where a user who hasn't paid to access a game is still able to access the game against Steam's policy. To prevent piracy, Valve uses game keys that are uniquely associated to user accounts who genuinely purchase game licenses. Purchases of game licenses on Steam essentially offer the user an infinite subscription to the game, as this issues a single key to license exactly one copy of the game, which can be opened by the purchaser or gifted to another account. The game key can only be activated on one account, after which point the

game can be played exclusively on that account by running it through the steam client, online or offline. This licensed copy never expires, so long as the Steam platform continues to exist to run the game, maintain your stats, or -if necessary- host servers. Game purchases can only ever be shared with a limited amount of designated "family sharing" accounts, and cannot ever be played online concurrently across multiple family-shared accounts (even concurrently playing entirely different games is disallowed). Moreover, only one computer can ever be online and signed into an account at once, so concurrent online play of games on a single account is also disallowed (concurrent offline play is possible, but will not save progress or achievements to the steam network). At times, the Steam store offers temporary copies of games for free with special events.

3.3.2 User Account and Data Protection

Steam requires sensitive user information for proper functioning of their services. Such sensitive data includes:

- users' identification details such as name, phone number and home address
- login information i.e. email addresses, usernames and passwords
- billing information such as credit card details
- inventory lists, that is, what a user has sold and bought on Steam and for how much
- game lists, that is, game licenses owned by a user, their game scores and other steam users that a user has ever multi-played with

Such information is of interest to criminals who have an interest in misung the data for their own advantages such as making money or making a Steam user look like an adversary when they are not. Valve protects its users from such criminals by use of password-protected accounts, Steam Guard, Steam Mobile Authenticator, User Privacy Settings, Steam Wallet, and enforcement of Trade Holds. For maximum protection, a user should make use of all of them, that is, use of a strong password that is not known to anyone else, activation of Steam Guard and Steam Wallet, and use of the Steam Mobile Authenticator app. Further, a user should set their data to 'private' or 'visible to friends only' so that people unknown to them cannot have access to their information.

3.3.3 Crime Detection and Deterrence

Just like with all other systems, existing Steam security protocols do not guarantee 100% elimination of all potential security risks. To deal with potential criminal activities on the Steam platform, Valve has set up measures that increase chances of detecting crime for examination purposes and for future deterrence of such. The measures include a three-day trade hold where all trades not authenticated using the Steam Mobile Authenticator app are put on hold for about three days. Valve hopes that this is sufficient time for attacked users to identify and report suspicious activity not initiated by them in order for Valve to stop the trades and attempt to identify the criminals. Further, Valve blocks users from trading if they commit any fraud or if they try to perform corrupt trades, for example, by falsely making other users lower their item prices.

4. Related Work

Given the current scale and nature of the Steam platform, there exists, naturally, a significant history of successful attacks as well as reported security vulnerabilities made at the hands of multiple independent parties. A large part of security for such a platform involves reviewing both the existing or known exploitations and handling them in updates both quickly and effectively. The history of major past incidents offers huge insight into the furthest possibilities for exploitation (which, at some point, had not been considered). This provides evident windows for correction and improvement, as well as the possibility of leads into the inevitable security breaches of future actors.

4.1 Known Practices

Steam users can interact on the platform through a multitude of ways, which generously allow a large amount of freedom in the practices that can be used to acquire guarded information or reach unintended outcomes. These tend to take advantage of minor software bugs, and are orchestrated by malicious system players who masquerade as genuine Steam users. Such practices are either of little consideration to Valve in terms of their effect on the platform's revenue and their scale, or they simply are yet to be conclusively corrected within recent updates to the platform. These include, but are not limited to:

1. Cross-site scripting
   A major bug, described in Section 4.2, allowed users to add malicious code to their Steam profile, bypassing Steam's security measures. The trick, discovered by security researcher cra0kalo, was used to redirect victims to a phishing website or a page loaded with malware, among other exploits. [6], [11]. Currently, Steam profiles still allow some inputs of limited amounts HTML or Javascript in various spaces through which similar exploits may still be possible, to a lesser degree.
2. Malicious Steam URLs
   The only official Steam URLs that users should confidently use on their browsers are: *store.steampowered.com* and *steamcommunity.com*. A known and common phishing exploit is where an adversary sends corrupted URLs to potential victims. Malicious URLs used in the past include *steam.steaminstaller.com* and *steamguard.com*, they were fake Steam downloads that caused malware to be downloaded to victims' devices. [4]
3. Impersonator accounts
   These are Steam accounts that change their profiles multiple times in order to trick and attack users by looking similar to their Steam friends' accounts. They change all or some of their Steam avatar, name, location and 'about me' information. Such accounts can be difficult to spot particularly if they are changing their profiles several times within a day. [4]
4. Phishing bots within Steam Chat and Hijacked trading bots
   There are many bots on Steam with that are genuinely used to provide services on the Steam platform such as enabling trading sessions between users. All bots are required to have accounts associated with them, thus it is not always obvious whether an account is a bot or a real user.

Adversaries have been known to take advantage of this and hijack bots for purposes of spreading phishing links within Steam Chat. Further, when trading bts are hijacked they can be used to falsely advertise items that are not genuinely being sold or to advertise false prices that item owners did not publish. Trading scams are frequently heard of on Steam. Users are thus recommended to be very cautious when purchasing items or making trades. [4], [8]

5. Malicious script execution
   Steam users have received official communication multiple times telling them not to open other users' profile pages and their own activity feeds until told otherwise to avoid being attacked. This is because attackers had executed scripts that corrupted many social pages and loaded them with malware. Upon landing on corrupted social pages, users were redirected to non-Steam sites that were malicious. Additionally, some attackers silently bought and traded items with victims' Steam Wallet funds or inventory items. [10]

4.2 Major Past Incidents

In 2016, a group of attackers was able to bypass the security protection offered by Steam Guard. When logging into Steam on a new unknown device that a user hasn't used before, Steam Guard will pop a window asking for a verification code which is sent by Valve to your verified email address. Without this code, a user cannot log in. Attackers came up with a novel way to get around this security measure. They set up a phishing page on Steam where potential victims entered their usernames and passwords. The users would then be greeted by the pop-up box below which looked very similar to the valid Steam Guard pop-up box:

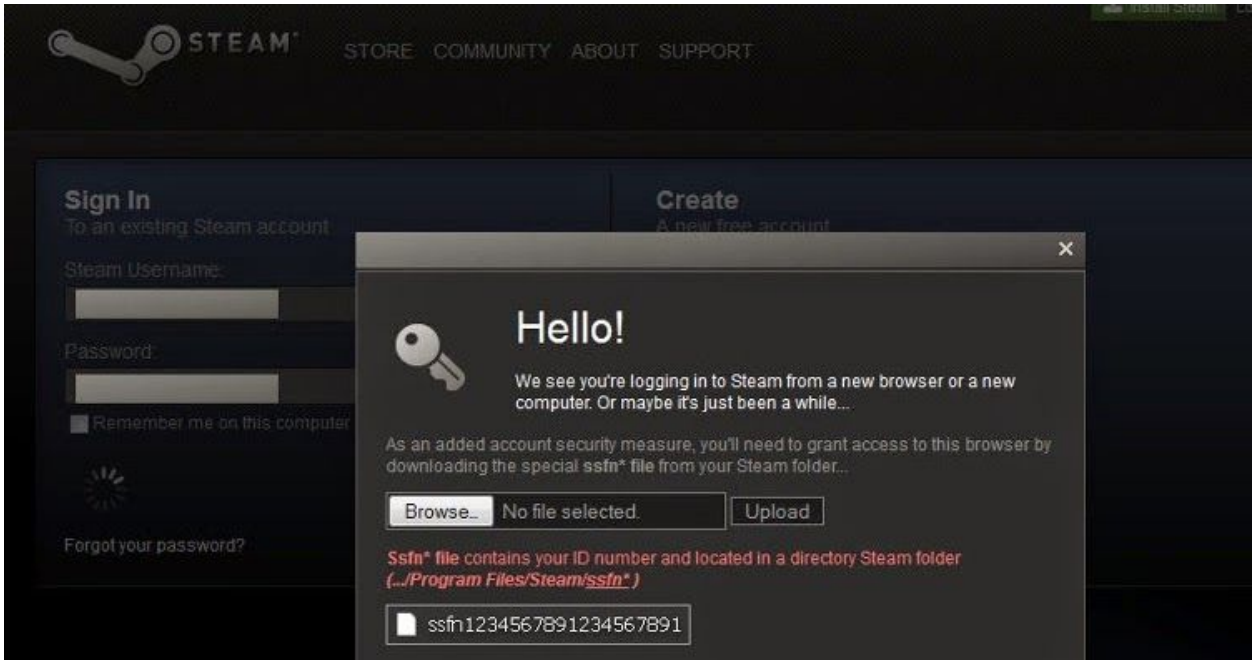

Figure 1. Image of the pop-up box presented during Steam's 2016 phishing attack that was capable of bypassing the Steam Guard security feature provided by Valve.

Users who sent the Ssfn* file to the attackers enabled them to place it into their Steam directory and log in as the victims while avoiding the Steam Guard security prompt requesting for a verification code. This was possible because the lack of a Ssfn* file on a new device is what prompts Steam to verify your identity through Steam Guard. With the Ssfn* file, the attackers essentially avoided being requested for a verification code and thus were able to log in and hijack thousands of user accounts. [5]

On February 2017, Steam was attacked with a Cross Site Scripting Attack (XSS). XSS comes in different types but in essence it's a way for a person to inject his own HTML code into a website so that a victim user will run it and be subjected to malicious intents by the attacker. In the case of steam, the issue was with the Steam Guides titles. Users were able to inject their own code into the guide title, and when another user would open a profile page containing a preview of this guide, the code would run. It would only execute on the preview in a user's profile because Steam developers fixed this issue on the Steam Guides page but not on profile pages. The implications of this vulnerability were vast, they included phishing, hijacking an user's profile, and stealing account funds.

Another big vulnerability was discovered by Ruby Nealon. Steam has a procedure for allowing users to release games into their platform. Many games get denied because they do not follow some set guidelines. Ruby managed to bypass this procedure all together and published his joke game without any review. Users can gain trading cards by playing games on Steam, and Steam has a submission site for users to upload their own trading cards when trying to publish a game. Ruby played around with the source code of this submission site and saw that Steam was tracking his session ID and editor account ID. He played around with it and got back a form that gave him the "Last editor", which was someone from Valve. He then used this information to trick the server into thinking a developer submitted these trading cards and so set their status as released. He then went through the source code for releasing games and called the function ReleaseGame() with his app ID and sessionID from before and his game got released into the store. Luckily enough, his game was just a prank to get Steam's attention to this problem, but an attacker could had used this to publish malicious games that could harm Steam.

5. Potential Exploitations

The Steam platform, including associated hardware, holds a very wide scope of features. Especially in the case of the Steam Link and controller, which are relatively new products with many possible use cases, it is unsurprising that a thorough analysis would reveal a number of significant weaknesses and flaws with the potential for exploitation.

The Steam Link itself is not a product most users intend to modify for purposes other than its advertised streaming capabilities. The unit has a single-core ARMv7 processor running at 1 Ghz, 256 Mb of RAM and 1Gb of flash, so it lies well below a raspberry pi module in computing power. Regardless, Valve offers the Steam Link SDK for the creation of applications and various other small time modification purposes. Popular apps like RetroArch and Kodi currently exist for download onto the Steam Link through a few roundabout methods with full functionality, offering quite invasive customizations to the unit, such as controller input re-mappings and the addition of a channel for downloading and streaming video and other media.

In order to further manage customization of the Steam Link unit and append additional tools, the device offers SSH capabilities. The Steam Link SDK reveals the process to enable the non-default SSH functionality, which involves simply power cycling the device with a FAT32 USB which contains a text file titled enable_ssh.txt in the \steamlink\config\system directory. This will maintain SSH enabled until a complete factory reset is performed. A significant shortcoming in this feature is that, furthermore, it is notably easy to gain root access to a factory-set default Steam Link device. Once SSH is enabled, the default root access password for all Steam Links is set to steamlink123. This password is readily available to the public on the SDK, and while the website recommends that this be changed immediately with the passwd command, the largest part of users will never refer to this knowledge, or even use the Steam Link at all for any other than its original intended purpose, by which this setting would be left entirely unchanged.

Having unintended parties gain root SSH access to a Steam Link device can have many immediately obvious dangers. For one, the SDK denotes specifically under the section for building the kernel a warning about how Steam Link devices will only boot with a kernel signed by Valve. Not much detail is provided on this other than that any attempts to boot an unsigned binary on the device will immediately void the warranty on the device and actually render it unbootable. This does, in fact, imply that even a factory reset would no longer be possible by any conventional means, as these are done exclusively through software. In effect, root SSH access gives a non-benefitting malicious party complete access to the Steam Link's file system, and as such allows them to tamper with kernel code, cause it to fail the secure boot, turn it off and effectively reduce the device to an expensive paperweight. This was shown to be very easily doable on an actual Steam Link device in practice.

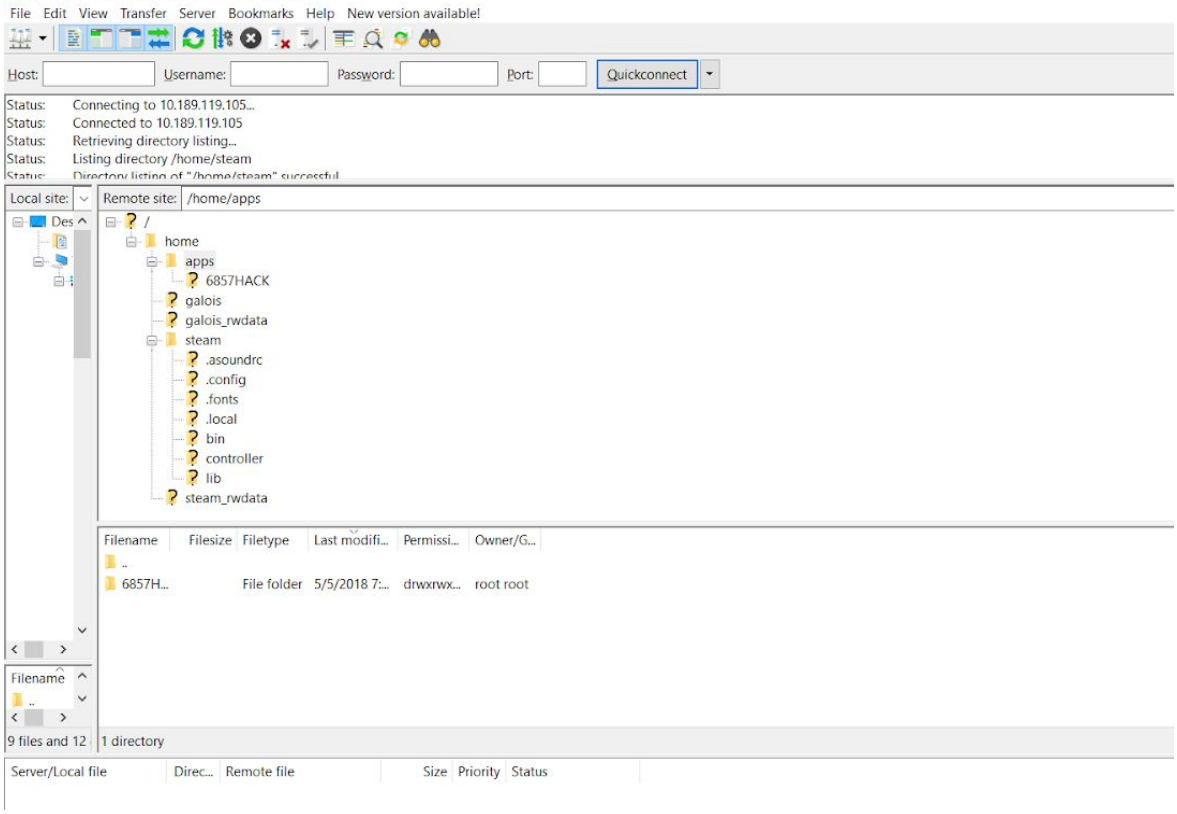

Figure 2. Successful root SSH access to the Steam Link, revealing its entire filesystem, and enabled access to read, modify, and access kernel files. "6857HACK" has been added to the app directory.

Assuming normal conditions, the extent to which this can be exploited is over the Local Area Network through which the Steam Link operates. That said, the limitation comes from the fact that an a malicious party would need the victim's Steam Link's IP address, which was determined to be easily acquirable without the cooperation of the victim from packet sniffing on the Steam Link's operating network. Packets sent out for the device finding protocol are a dead giveaway to provide the device's IP address with packet sniffing software such as WireShark. Given that SSH is enabled on the device (either by the user himself or unknowingly enabled through the aforementioned process by the malicious party), and given the IP address of said device, this attack can potentially be performed from any location on any network.

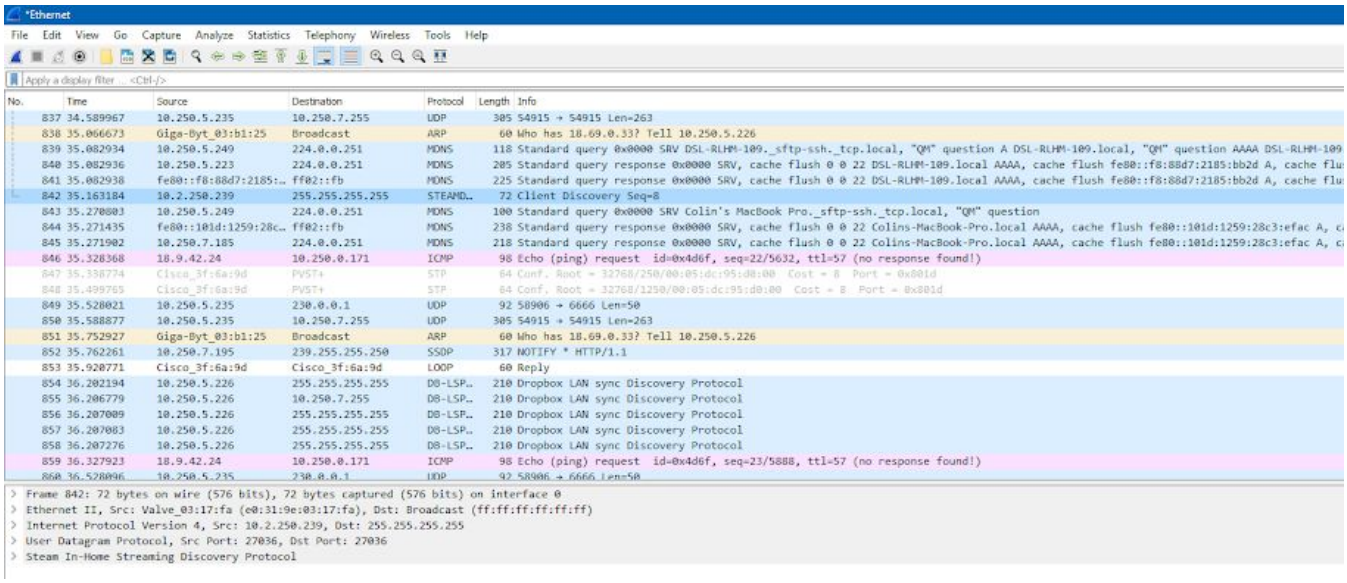

Figure 3. An example of packet sniffing using Wireshark on the Steam Link's operating Local Area Network, revealing, 6 lines down, the Client Discovery Protocol of the device as well as its IP.

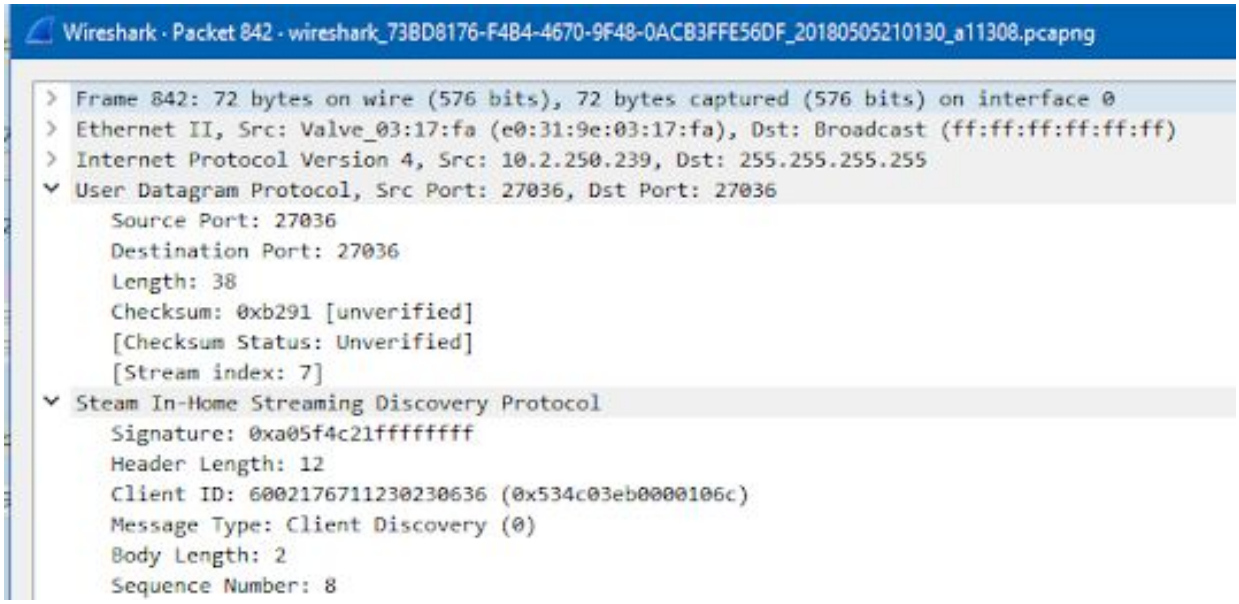

Figure 4. A closer look at the discovered Steam Client Discovery Protocol

There is no benefit to any party simply out of destroying another's Steam Link device. However, there exists potential for further exploitation of the root SSH access, combined with other components of the Steam ecosphere. The Steam controller, when paired with a Steam Link, is used to control the running interface from the Link and play games from the otherwise game input-lacking box. The Steam Link must handle sending data from the connected controller to the device which is loading the streamed content or game. It turns out that the packets sent by the Steam link concerning Steam controller input are actually very easily acquirable and, in fact, completely readable. The inputs are not at all encoded, and they follow a simple scheme which can furthermore be learned and potentially forged. Forging Steam controller input to a streaming Steam Link and into the connected computer would lead to very drastic results. The Steam controller effectively has mouse and keyboard capabilities. Leaving the active steam UI window, big picture mode or client is trivial, and virtually gains the false input controller access to the entirely of the operating system's UI. With a sequence of pre-determined falsified inputs, it would be entirely possible to exit the running steam window, open the command line or browser and wreak havoc on the system without ever actually needing to see any output from the Steam Link or otherwise.

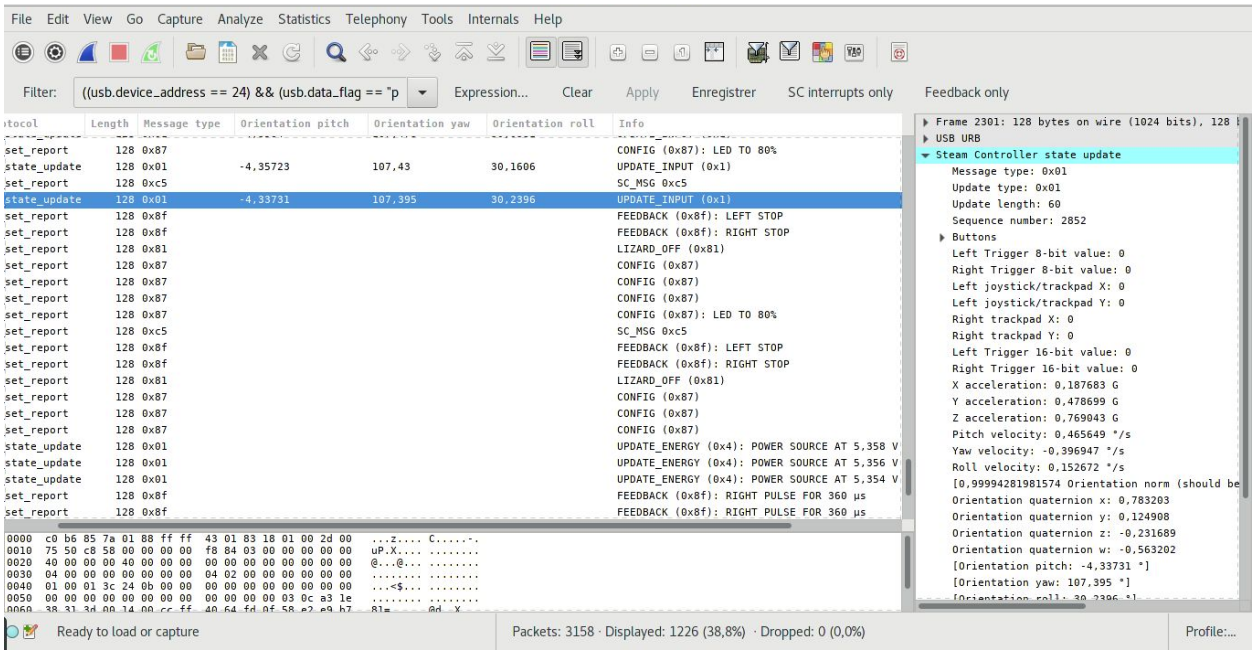

Figure 5. Packet sniffing for Steam Controller input activity reveals button input to be quite readable (right) with very simple, forgeable structure. (Image Credits to user sm-Fifteen on Reddit's /r/SteamController discussion page)

Applications are normally added to the Steam Link in a process similar to how SSH is enabled, using a USB device with the desired application files under a specific directory. By adding an application through a USB through this system as a test, the target location of application data can be determined, and this directory can be accessed through SSH. Using root SSH access, it is actually possible to append to this directory and add custom application files to the system over a power cycle. These applications can encode a large number of functionalities, especially when root access grants the ability to modify kernel code to give an even larger scope of allowances to such custom applications.

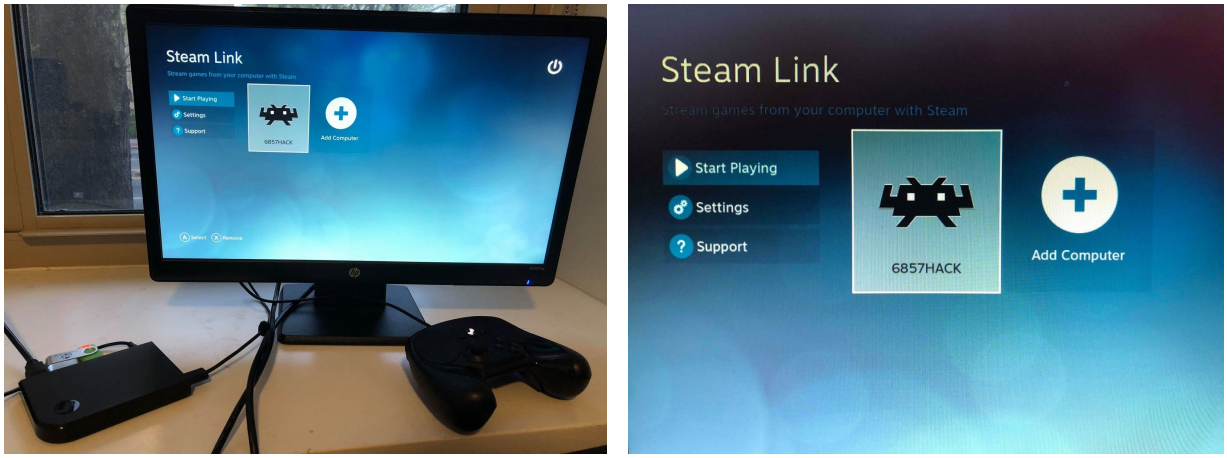

Figure 6. The Steam Link, controller and monitor setup depicted (left) with an inserted custom application titled "6857HACK" shown as selectable and executable in the device discovery menu (right)

The result is that it is quite trivial to add applications to the Steam Link itself which can be pushed on to display normally after a power cycle on the same main menu where nearby discovered devices are selected in the setup process. Such applications can be encoded maliciously, and along with manipulation or abuse of the Steam Link's kernel code, have the potential to serve as a vector for the type of aforementioned attacks with falsified controller input while the device is streaming. Granting the ability to remotely add custom made applications with unspecified functionality that continue to operate under the hood while the Steam Link connects to other devices is quite a major oversight, given the methods described earlier. This serves to show a final, broadening step in a vector of attack with a lot of potential, over a series of small use cases that assume very few specific conditions of the target.

6. Conclusion

This paper was written to provide a detailed analysis of the Steam platform, primarily to increase understanding on how current and possible security breaches that can be performed. It was determined that there potentially exist very large security vulnerabilities in the Steam Link device, pointing out how attackers can gain remote access to the device and the victim's computer. Most users just use Steam Link strictly for its marketed streaming purposes, and by and large SSH access is not a necessity for this audience. As such, there exist many ways that do not degrade functionality to allow the steam ecosystem to be more secure and to protect unaware users. Following this, the ultimate goal of this project is to provide suggestions to further study possible attacks and give recommendations as to how the Steam ecosystem can be designed to be more secure.

6.1 Future Work

The exploit shown in this paper with the most potential for development lies in the creation and installation of malicious applications on the Steam Link. This analysis concludes without completely testing the extent and ability of malicious apps to interfere with the Steam Link itself while streaming or the connected device. It would prove very interesting, for example, if malicious apps could be run in such a way that when a computer starts streaming with the Steam Link, the app could send sensitive

information being sent from the computer to the Steam Link to the attacker. Further developments into the creation of these applications could reveal ways to interfere with this connection without the use of controller input at all, or otherwise steal information and cause damage without obviously visible attacks on the victim computer. The nature of the streaming connection between the Steam Link and operating device leaves many uninvestigated possibilities, especially if applications are made capable of interfering with Steam Link's kernel code and bypassing the secure boot to completely rewrite the functionalities of the Steam Link device from the ground up, while still having it appear trustworthy. Considerations of Steam hardware exploits are not the only space for future exploitation of the Steam network; other aforementioned software functionalities are yet to be fully explored, with a great extent of them being novel services related in various ways to the devices shown to be vulnerable in this paper.

6.2 Recommendations

6.2.1 To Valve

We recommend that Valve force users to choose a SSH password which is set by default as of today. If this small patch were to be implemented, no one could SSH into the device without trying to crack the victim's password. Furthermore, it could be useful if there was some way to physically factory reset the device without the need for software in the case that the device is maliciously broken from the secure boot as mentioned in Section 5. Valve could also choose to restrict some folders in the device so that even if a malicious party had root SSH access to it, they cannot be deleted. Files integral to the integrity of the device should never be modified. Finally, we recommend that Valve analyze how apps can be inserted into the Steam Link and to what extent attackers can use this allowed feature to gain access to a victim computer. Applications and programs should always lie isolated from other functionalities and parts of memory that are not relevant to their usage space. In this way, there is a degree of limitations on what applications can do, especially while streaming, when the device is most vulnerable to exploitation.

6.2.2 To Steam Users

Our executed attack primarily is focused on Steam hardware used to stream PC games purchased on Steam. Most of our recommendations are towards Valve. Nonetheless, we encourage users to minimize potential security risks by:

- Setting a new secure SSH password rather than leaving the password as the default option set by Steam.
- Activating Steam Guard on their settings portal and making use of the Steam Mobile Authenticator App as these minimize chances of an adversary accessing their accounts.
- Setting their profiles to private or at the very least 'visible to friends only'. This prevents adversaries from being able to see your sensitive data such as what games you own.
- Using Steam Chat only to message users that are well known to them. The chat is prone to phishing and malware threats by malicious players and hijacked bots.
- Accessing their Steam accounts only through Steam's official site.
- Using Steam as a gaming platform and not as a communication platform. Users should use other more secure means to message their friends.

7. Acknowledgements

Our team would like to thank the 6.857 professors, Prof. Ronald Rivest and Prof. Yael Kalai, for their profound knowledge on Security and Cryptography as it enabled us to successfully perform this security analysis on Steam. We also acknowledge Valve for allowing academic works like ours that are for the good of the whole Steam community. Lastly, we thank our TA Cheng Chen for his feedback and guidance.

8. Bibliography

1. Valve: *Privacy Policy*. January 18, 2018. URL: https://store.steampowered.com/privacy_agreement/
2. Valve: *Legal*. January 18, 2018. URL: https://store.steampowered.com/legal/
3. Valve: *Bug Bounty Program*. May 10, 2018. URL: https://hackerone.com/valve
4. Jovi Umawing. *Steam Threats: What They Are and What You Can Do to Protect Your Account.* URL: https://blog.malwarebytes.com/101/2014/09/steam-threats-what-they-are-and-what-you-can-do-to-protect-your-account/
5. Christopher Boyd. *Phishers Bypass Steam Guard Protection.* URL: https://blog.malwarebytes.com/cybercrime/2014/04/phishers-bypass-steam-guard-protection/
6. Robert Abela. *Steam Gaming & Entertainment Platform Vulnerable to Cross-site Scripting Vulnerability*. URL: https://www.netsparker.com/blog/web-security/steam-entertainment-platform-gaming-vulnerable-xss/
7. Ruby Nealon. *Watch Paint Dry: How I got a game on the Steam Store without anyone from Valve ever looking at it.* URL: https://medium.com/swlh/watch-paint-dry-how-i-got-a-game-on-the-steam-store-without-anyone-from-valve-ever-looking-at-it-2e476858c753
8. Andy Chalk. *Valve fixes Steam security exploit*. URL: https://www.pcgamer.com/valve-fixes-steam-security-exploitbe-sure-to-update-your-client/
9. Kyle Orland. *Valve patches security hole that enabled takeover of Steam accounts*. URL: https://arstechnica.com/gaming/2015/07/valve-patches-security-hole-that-enabled-takeovers-of-steam-accounts/
10. Alice O'Connor. Warning whistle: beware a possible Steam security hole. URL: https://www.rockpapershotgun.com/2017/02/07/steam-possible-security-hole/
11. John Leyden. XSS marks the spot: Steam vuln dangles potential phishing line. URL: https://www.theregister.co.uk/2017/02/08/steam_vulnerability/
12. sm-Fifteen. Reddit /r/SteamController blog. Trying to figure out the steam controller protocol. https://www.reddit.com/r/SteamController/comments/5zepc8/ive_been_trying_to_figure_out_the_steam/
13. Valve. Steam Link SDK. URL: https://github.com/ValveSoftware/steamlink-sdk