Hacking Networked Games

Matthew Ward and Paul Jennas II

Abstract

With the explosion of the game of poker came an explosion of on-line poker. The popularity of on-line poker boosted the popularity of on-line gambling in general. Even with the passage of the *Unlawful Internet Gambling Enforcement Act of 2006*, which prohibited banks and other financial institutions from allowing transactions with on-line gambling sites, on-line gambling worldwide remains a $30 billion dollar per year industry [2]. That kind of popularity and money often attract people who are willing to take the money by immoral or even illegal means. This paper will explore the various methods of cheating that threaten on-line gambling games.

1 Introduction

The on-line gaming industry as a whole has taken the world by storm with games such as World of Warcraft, Second Life, and Final Fantasy each amassing millions of monthly subscribers. Along with their success has also come a variety of techniques contrived by cheaters to gain an unfair advantage. In non-gambling games, new markets have been created where gamers are able to purchase virtual items from one another for real money. These virtual items might be virtual money, weapons, clothes, etc. The involvement of real money has led to increased focus on preventing cheating. On the other hand, one could argue that because these markets are outside of the realm of the game and even in many cases against the will of the game companies themselves, these markets should not have an impact on a gaming company's motivation to prevent cheating. This implies that it is the company's desire to provide an enjoyable experience for the gamer that should be the sole motivation. According to Ralph Koster, creative designer for *Star Wars Galaxies*, "any behaviour that hurts business is bad behaviour." [13] However in the world of on-line gambling, the exchange of money is at the heart of the game. It is therefore clear that the involvement of money in on-line gambling provides the driving force for protecting the integrity of the game.

Today many of the techniques employed in non-gambling games are now a threat to these on-line casino games. Through the process of generating the attack tree in Figure 1, which consist of these various methods, a somewhat natural grouping of the various methods resulted. While others would likely have variances in their attack tree upon completing the same exercise, it is clear that the different cheats have a definite relation and similarities to other cheats such that they can be grouped based on these similarities. In this paper we will discuss the major categories of cheating in on-line gambling games. In particular we will show each type of cheat, including information about known countermeasures and historical examples. Section 3 details the controversial use of bots. The different forms of DoS attacks are discussed in Section 4. Sections 5 and 6 cover collusion and software exploits. The paper then concludes in Section 7.

1.1 Poker Basics

This report focuses on exploiting on-line poker. The techniques described can be applied to any on-line game, but the financial importance of on-line poker make its an excellent candidate to study.

With this is mind a short tutorial on the basics of poker is required. Poker is a card game where card ranks (e.g Ace, King, Queen) and forming ”hands” is used to determine a winner. A hand is a pre-defined combination of cards. For example, ”three of a kind” is a hand where a player has three cards of the same rank. The rarer the odds of obtaining a hand the higher the rank of that hand. This makes poker a game of statistics. However, there is also a human element, as players can pretend to have certain hands (called a bluff) and good players must be able to tell what hand a player really has. There are many variations of poker (Texas Hold'em, Omaha, Stud, etc.), but the hand definitions are fairly standard across most variations. The differences lie in how the hands are formed. In Texas Hold'em each player is dealt two hole cards which only that player can see. Then there are 5 community cards that all players can see and use to form their hands. Typically community cards are revealed one at a time and after each card is dealt players take turn performing game actions. Typical actions include Bet, Check, Fold, Call, Raise. Players often make these decisions based on a concept called pot odds.

Pot odds essentially determine whether or not making a particular bet is profitable. To make this determination, a player will first calculate the ratio w of their chances of losing to their chances of winning. They will then compare this to the ratio p of the size of the pot to the size of the bet. If p is greater than w then this is a profitable bet, otherwise it is a losing bet. For example, let us imagine a situation where a player has a 20% chance of getting a card that will give them the winning hand but they are faced with needing to make a $10 bet to see the next card. In this case, w is 4:1 (i.e. 80%:20%). Thus the pot size needs to be greater than $40 in order for p to be greater than 4:1 (i.e. $40/$10). On average, for every 5 times the player is in this situation with a large enough p they will lose $10 four times but win more than $40 one time so they are said to be ”getting odds” to place the bet as the law of averages will work in their favor over time.

2 Bots

One controversy that has long existed in the game of on-line poker is the use of bots. Bots are pieces of software that are typically used by on-line gamers to automate the process of providing some form of input for he user. In on-line poker, bots can range from simple hotkey scripts that employ a simple and standard strategy to much more sophisticated programs that employ an intelligent AI. A simple strategy based solely on hand probabilities and pot sizes may only result in a small amount of money earned per hour. However, multiple bots can be run at different tables around the clock. Unlike its human counterpart, a bot is also not subject to its play degrading due to fatigue nor emotions. Thus the average amount that it is capable of winning per hour will be fairly consistent.

2.1 Artificial Intelligence

Skilled players will rely heavily on their memory to collect information on how each player at the table plays. Keeping track of each players' habits to learn for example how often each player bluffs in a given situation can be used as input to factor into calculating pot odds. However, a bot can far exceed the limits of a human player in both the amount of data that can be readily retrieved and processed within a set amount of time. Therefore, a more sophisticated bot with a complex AI can be far more profitable than a bot playing a simple strategy. This is evidenced by the 2008 Man vs. Machine Poker Championship in which a bot named the Polaris Bot defeated its human competitors and won the entire event [6]. The fact that developing the Polaris Bot required a team of researchers at the University of Alberta over a 17-year period might suggest that players will

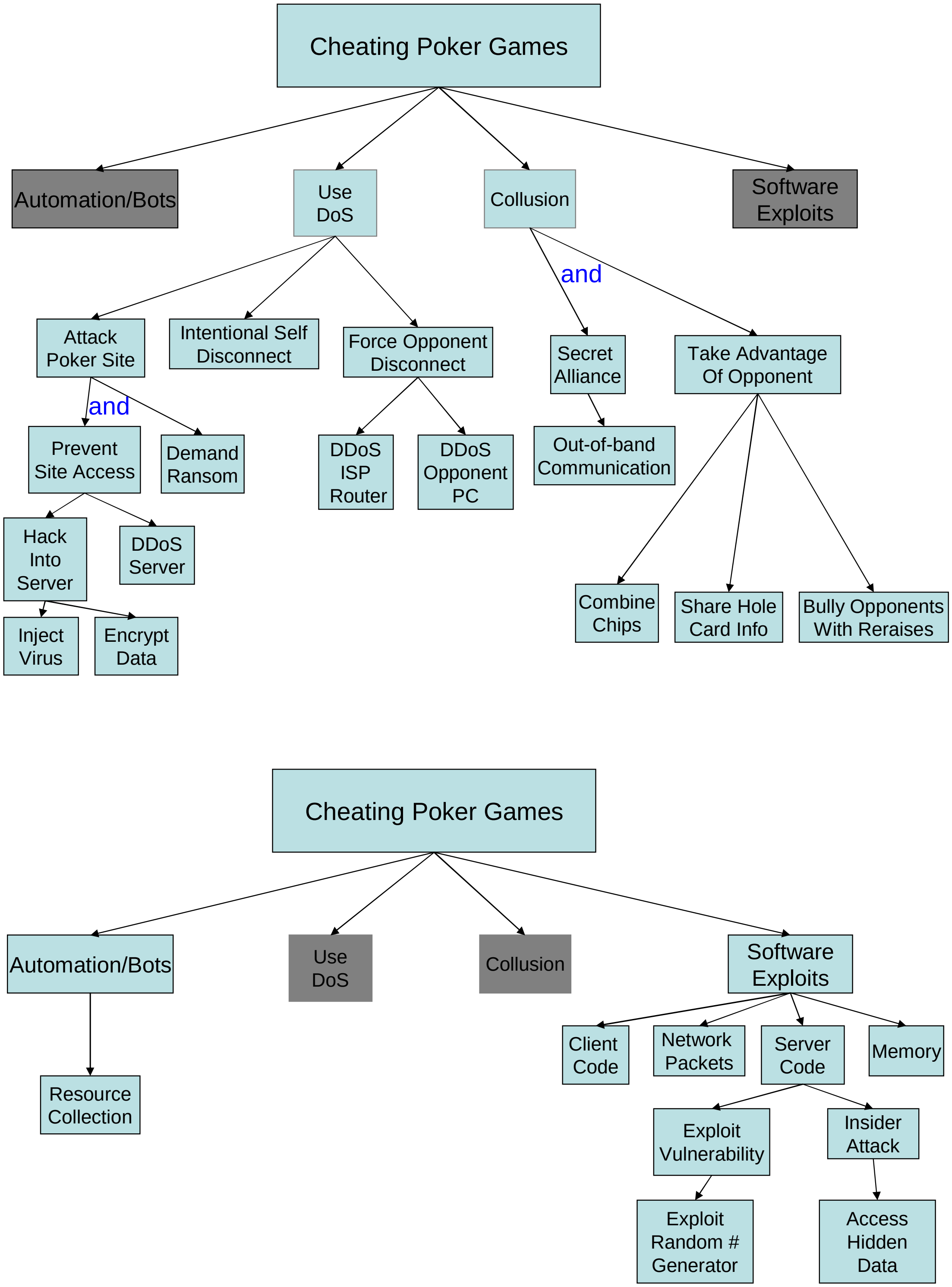


Figure 1: Attack tree for cheating on-line gambling

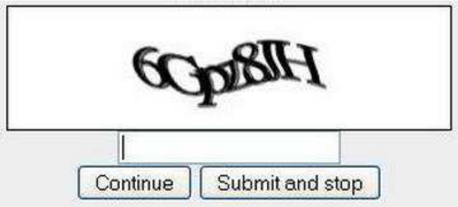


Figure 2: Example of a CAPTCHA

likely not need to fear the presence of any bot in the typical on-line poker room with this level of sophistication. However, Polaris was playing against poker professionals so the potential for less sophisticated poker bots with enough complexity to play a winning game against average players cannot be ruled out.

2.2 Bot Countermeasures

Some players welcome the use of bots because of their view that they are essentially playing against their human designers. However, many poker sites still consider the use of bots to constitute cheating. To combat the use of bots, some sites will periodically prompt their players with CAPTCHAs. This mechanism prevents bots from interfacing with their clients. Figure 2 shows an example of a CAPTCHA.

Still others have even tried to use detection schemes to identify common bots on their players' systems. A similar method was used by Blizzard Entertainment when they introduced the "Warden" [10]. The Warden software monitors and scans the computers of World of Warcraft players to search for bots or other software enabling the player to cheat. Given the controversy that the Warden caused, employing this countermeasure in poker may be even more controversial than the original problem that it is intended to defend against.

Players themselves will often also try to detect bots by using the in-band chat feature of the poker software since a bot is essentially unable to respond. However, in a game where deception is fundamental to the strategy, some players will refuse to respond as they may be perfectly content to have opponents believe that they are bots.

3 Denial of Service Attacks

Denial of service (DoS) attacks are another form of cheating in on-line gambling. There are two traditional forms of DoS attacks that have been used to exploit online gambling sites: a malicious player can attack the site itself to stop its business or they can attack an opponent to prevent communication between their computer and the server. In addition, there is a non-traditional DoS exploit that malicious players can use in certain situations: an intentional disconnect.

3.1 DoS Against Poker Sites

On-line gambling company Grafix Softech suffered an attack from hackers in Russia [15]. The hackers were able to launch a virus within the production servers used for on-line games. As a result, the data on the servers was encrypted by the virus. The hackers demanded a ransom, the amount of which remains undisclosed to the public, in exchange for the decryption key.

Upon receiving the decryption key, the company was able to decrypt data on all but 1 of its servers. However, on that system the problem became worse once the decryption key was used. The system lost all of its data which was key to their operations. It is unknown if the loss of data was due to some other mechanism put in place by the hackers or human error on the part of Grafix Softech's IT team in trying to decrypt the data. Grafix ultimately turned to CBL Data Recover Technologies Inc. to recover the data. Only the metadata pointing to the locations of real data was removed during the deletion as is typical for most operating systems during a deletion operation. They were able to manually reconstruct the data and get Grafix back up and running.

3.2 DoS Against Opponents

In on-line poker, players are given a set amount of time to make their decision when the "action" gets to them (i.e. when it is their turn to bet). At many sites, if the player does not make their choice within that time then the server automatically folds their hand. Depending upon the information provided by the server about the other players, a given player may have his or her opponents' IP addresses. Alternatively, a user could determine the ISP to which a poker site is connected (by running traceroute for example). In either case, when a cheater is involved in a large hand, he or she can launch a DoS attack either against the opponent when it is his or her time to bet or launch a brief attack against the ISP thereby preventing communication between the opponent and the server.

The challenge here is that the attack has to last just long enough for the opponent to be auto-folded but short enough that communication can resume with the cheater's system so that they can win the pot. Since there are likely a number of variables involved that are outside the control of the cheater, they may not be able to always successfully execute the attack. Therefore, any given attempt could actually cost the cheater money. However, through trial-and-error the cheater can determine the probability of successfully executing the attack. This can be useful in a situation where they are heads up against an opponent for a large pot. "Heads up" means that there are only two players left in a hand. They can simply compare the probability of a successful DoS attack on the opponent against their probability of winning the pot outright. If the chances of a successful attack is higher then executing the attack will still prove profitable in the long run. The cheater may want to limit their use of this cheat so as not to have other players discover their intent which is why they may choose to use this attack only when a large pot is at stake.

3.3 Intentional Disconnects

An alternative policy that some on-line poker sites employ for players who get disconnected is to place them all-in with their current bet and remove the remaining chips in their stack from play. In an all-in scenario, the player will remain in the hand until the end. Whatever money is in the pot at that point is placed to the side as the "main pot". A side pot is created for future bets between the remaining players at the table. The disconnected player is still eligible to win the main pot if their hand beats all of the remaining players at the end.

With this policy, if a player is in a situation where a large pot is at stake and they feel they only have a small chance to win but do not want to pay the remaining bets to get to the end, they can simply disconnect their client by killing the application or causing a network disconnect. The site should take countermeasures by tracking the frequency of disconnects by each player during a hand and the number of times that the disconnects were advantageous to the player i.e. when the disconnect came during a large pot with continued aggressive betting. Suspected players can then be warned or more severe actions can be taken.

4 Collusion

Collusion is any secret collaboration by two or more players at a table. This form of cheating has always been a problem in the game of poker and is difficult to detect even at a live table on a casino floor. Collusion requires some means of hidden communication being available to players. At live tables, players have developed very advanced means of communication with subtle signals and speaking in code that appears to be legitimate conversation about another subject. However, with the action being moved to on-line virtual tables where players sit privately in a location where they can no longer be monitored, solving this problem becomes many times more difficult. The requirement for secret communication is easily met in an on-line environment and once players have established their communication vehicle, there are a number of actions they can take to gain an advantage.

4.1 Combining Chip Stacks

Players may choose to combine chip stacks by having one player purposely lose all of his or her chips to another player with which he or she is collaborating in order to gain an advantage. This technique is also known as "chip dumping". In poker tournaments, the difference between the sizes of two opposing players' chip stacks can in some cases have an even bigger impact on the outcome of the game than the difference between their playing abilities. Two or more players using this technique will then split up the winnings after the game.

4.2 Sharing Hold Card Information

Players can share what the values of their hole cards are with one another to gain a significant advantage in decision-making as the hand plays out. Experienced players are often calculating pot odds with each bet that they place. Knowing the values of two additional cards has a significant impact on the result of these calculations.

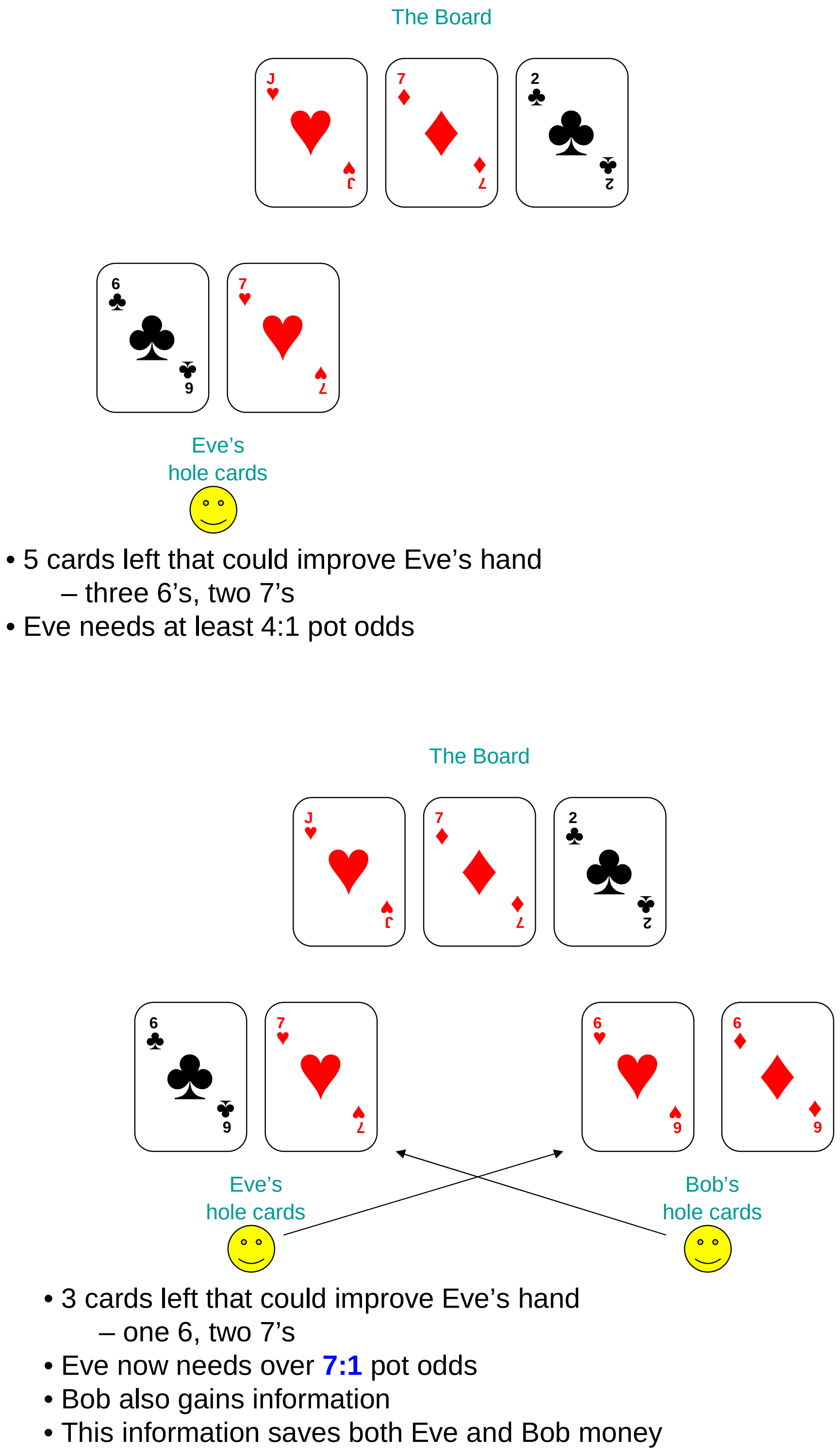
Figure 3 demonstrates this concept. Without knowing Bob's hold cards, there are 5 cards remaining in the deck that can improve Eve's hand. Thus with 2 more cards to be dealt, she has a 20% chance of obtaining what is very likely a winning hand. Calling a bet will only be profitable, long-term, if she is getting at least 4:1 pot odds. However, having Bob's hole card information allows Eve to improve the accuracy of the pot odds. Since Bob has 2 of the cards that would improve her hand, there are only 3 cards remaining in the deck that can improve Eve's hand giving her a 12.5% chance of winning. Now she needs at least 7:1 pot odds. If the pot is giving her 6:1 for example, that appears to be a very good bet until she sees Bob's hole cards. Now she is able to make a better decision and save money.

4.3 Whipsawing

Whipsawing refers to a scenario where two or more players with a small number of players in between them raise and re-raise one another in a coordinated effort to force the players in the middle to fold. This can be extremely frustrating for players who fall victim to this cheat. However, it is also fairly easy to spot when it occurs with any kind of repetition.

4.4 Countermeasures

Most sites have two common mechanisms for preventing collusion: IP checking and collusion-detection algorithms.



- 5 cards left that could improve Eve's hand
  - three 6's, two 7's
- Eve needs at least 4:1 pot odds

- 3 cards left that could improve Eve's hand
  - one 6, two 7's
- Eve now needs over **7:1** pot odds
- Bob also gains information
- This information saves both Eve and Bob money

Figure 3: Eve and Bob are sharing hole card information which gives them an advantage in calculating pot odds

4.4.1 IP Checking

A site can easily detect two players with similar IP addresses sitting at the same table together. Similar IP addresses usually implies a similar location. However, with the numerous means for connecting to the internet nowadays this may not be as effective as it once was. For example, one player could connect via wifi while another player in the same physical location could connect via another close-by wifi network or tethering with their cell phone. With the number of methods for connecting on-line increasing (for example, new vehicular networking technology is likely to be deployed during the year of this writing), IP checking will lose further effectiveness as time goes on. Even when this method is effective in keeping physical distance between players at a table, nothing can prevent the players from communicating via phone, instant message, walkie talkie, etc.

4.4.2 Collusion-Detection Algorithms

Most sites have algorithms for detecting collusion. For example, in the case of whipsawing one can determine algorithmically whether or not this form of cheating is present with a high degree of probability. If two players are regularly raising and re-raising, thereby causing players in the middle to fold then these two players are usually collaborating. However in the case of sharing hole card information, detecting players committing this form of cheating can be extremely difficult. Another example of cheating will later be presented regarding a case where a player had the ability to see the hole cards of all of his opponents yet the effect this had on his decision-making was never detected by the site. Therefore, this form of collusion where a player has information about only two additional cards is even far less likely to be detected even though it creates a significant advantage.

The most effective defense against collusion is for on-line gambling sites to track player statistics and conduct regular investigations of players whose statistics lie too far outside the standard deviation [9]. This can help to prevent huge advantages that a cheater might gain over an extended period of time.

5 Software Exploits

In any type of software, hacking can come in many forms and take place in various components of its overall functionality. On-line gaming is no different. The cheater can look for software exploits that can be performed on his or her own computer by investigating and/or modifying the client code of the game, the network packets being communicated back and forth, or the memory of the system. In order to reduce the opportunity for vulnerabilities, modern day game design dictates that the client should not perform any critical decisions nor calculations that will have an impact on the outcome of the game. Otherwise any of these client-side attacks can be used to artificially produce an outcome that favours the cheater. The problem with many on-line games is that there are CPU-intensive computations for which performance can be greatly improved when they are offloaded to the client. This is usually the case in a graphics-intensive or high-action environment with a large number of operations so it is not uncommon to find a vulnerability in a game's client.

However, running an on-line gambling game generally requires little processing power so these types of games are generally not victims of this tradeoff. As a result, it is not likely that the client will be designed in such a way that it will control any of the critical decisions. There are a number of what-if scenarios that could be dreamt up for hacking the client if it had control over some critical decision but that just is not likely to happen for on-line gambling with the absence of the security/performance trade-off. Therefore, this section will focus only on attacks that are actually likely to happen or have already happened.

5.1 Exploit Vulnerability

Many vulnerabilities exist with any software. One potential area of vulnerability that exists in all computers is the inability to generate truly random data. While there are many flavors of casino games, they all have one thing in common. At their foundation is randomness and players bet on this randomness. With casino games moving into a virtual environment, the random number generator provides a natural point of attack.

5.1.1 Computer Randomness - Shuffling

How computers generate random numbers is another method that hackers can utilize to exploit on-line poker. ASF Software started an on-line poker site and displayed their shuffling algorithm on-line to show how fair this algorithm was. This is following the design principle that security should not be through obscurity. However, Cigital Software (an on-line security company) was quickly able to break the shuffler in real time [8]. This allowed them to predict what cards players held in their hands and what cards would come down for the shared cards.

Basically they knew how the deck had been shuffled. A seed number is generally used to start a “random” sequence in a computer. If the seed and algorithm are known, then the next number in the “random” sequence can be predicted. ASF started with a 32 bit seed, which right away is not good. This is because a real deck has 52! possible ways to be shuffled. A 32 bit seed can only shuffle a deck in four billion different combinations. Though four billion is a large number, this is still significantly less than 52!. Next, once a day, AFS initialized the seed with the number of milliseconds since midnight. There are only 86 million milliseconds in one day, so this implies even fewer possible shuffles.

Cigital Software was able to estimate when the seed was generated and what the server clock was at that time. With this information Cigital Software reduced the number of possible shuffles to less than 200,000 (which a computer can quickly figure out). Once five cards were known by Cigital Software (hole cards and shared cards), they immediately knew what cards their opponents had and what cards would be dealt in the future. This is of course an overwhelming advantage in the game of poker. Figure 4 shows the Cigital GUI used in the shuffling attack.

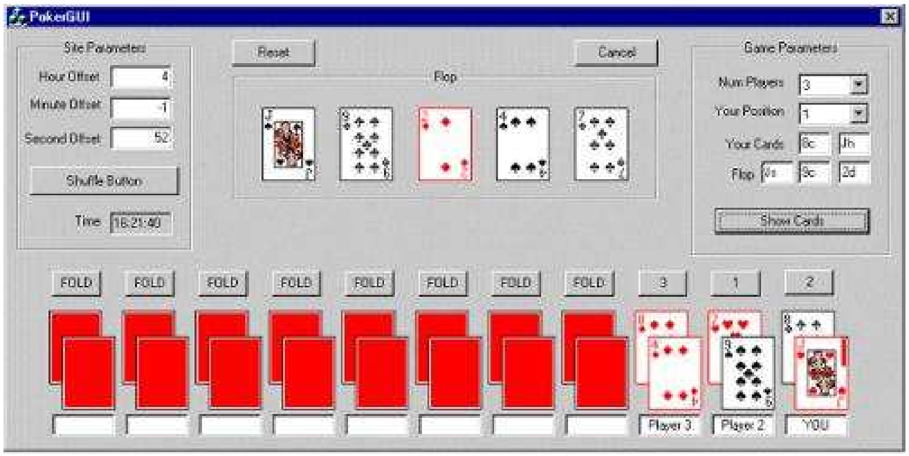
5.2 Insider Attack

Another major area of concern for many on-line gambling sites is insider attacks. With all of the protections and security measures available to companies trying to guard against attacks, external cheaters are limited in the frequency and impact of their attacks. A cheater on a company’s payroll, however, essentially has the keys to the city, particularly if they are an administrator or someone else in a role with increased privileges.

5.2.1 AbsolutePoker Attack

One well publicized case of an insider attack took place at AbsolutePoker [14]. A handful of accounts playing at their high stakes tables were winning at an alarming rate. Officials for the company claimed that they did not discover any cheating when the issue was raised by other players.

This prompted an investigation by a group of players who lost large amounts of money to the suspect accounts - one player estimated his losses at $400,000 to $700,000. The group was able to



Hour Offset 4
Minute Offset -1
Second Offset 52
Time 16:21:40

Num Players 3
Your Position 1
Your Cards 8c Jh
Flop Js 9c 2d

Figure 4: Cigital GUI

obtain the hand histories of their play from AbsolutePoker, including the hole cards of each player. Analysis of the play by these accounts showed that if their play was simply due to "luck" it would be statistically equivalent to winning the jackpot of a lottery with 1 in a million odds 6 times in a row.

The hand history data sent by AbsolutePoker also contained IP address information which they were able to use to discover that the cheating was taking place on a computer within AbsolutePoker's own network - a possible insider attack! AbsolutePoker was able to identify the employee but agreed to allow him to remain anonymous in exchange for details on how the attack was executed. He exploited a vulnerability in their system to gain the ability to see the hole cards of each of the other players at the table. AbsolutePoker never revealed what that vulnerability was, only that they have since patched it. The money was paid back with interest to the victims as AbsolutePoker officials indicated that it had never been withdrawn by the employee.

6 Conclusion

Computer security has been likened to other forms of security in that there is no silver bullet to completely securing a system. Effectively securing one's home or vehicle to prevent theft typically requires that multiple security measures be put in place, including placing locks on the windows and doors and perhaps even installing an alarm system. For houses, a surveillance system may also be appropriate in certain situations, while steering wheel and tire locks may be used for vehicles. As criminals thwart these different forms of security, new security devices are designed and employed to protect people's property. Likewise, securing software, online gambling software included, requires multiple security methods and continued effort to maintain security. Attackers will continue to discover new ways to cheat online games so security needs to be thought of as an ongoing battle to continue to make it more difficult for attackers to exploit a game [9].

Given that security turns into a game of cat-and-mouse, attackers will occasionally have success. Extremely important for gaming companies is to employ a good disaster recovery scheme. If an attack is successful, the environment may need to be reverted to a previous state or have certain attributes reverted. In addition, any attack that results in loss of availability can cost a company large amounts of money by the hour so it is important that they are able to quickly failover to a secondary site to maintain business continuity.

6.1 Gaming in General

This report has focused on exploiting on-line gambling games such as Texas Hold'em Poker, however the techniques described can be applied to any genre of game (and often with software in general). For example, in World of Warcraft bots are often used to farm resources. Farming is the process of performing a repetitive task automatically to accumulate game resources (for example World of Warcraft gold). Collusion is used to gain advantages in all types of games (Chess, FPS, MMPORGs, etc.). Denial of service attacks against opponents also have obvious advantages in almost any game. DLL Injections are used in all types of software to monitor and modify target processes memory and are important tools in creating sophisticated attacks like wall hacks (seeing through walls in a FPS) and aim bots (which can also be created with bots).

Something that became clear during the exploration of on-line cheating in gambling is that money certainly adds a motivating factor in the protection of any game regardless of whether the transfer of money is in-band as it is for on-line gambling or out-of-band as it is for many other MMOs (massively multi-player on-line games). Regardless of whether a game company itself supports the outside market for virtual items, it adds importance from the players' perspective. This adds pressure on game designers to protect the integrity of their product in order to keep customer satisfaction high. Another excellent point about added motivation to prevent cheating that the exchange of money can generate is found in Steven Davis' book [6]. In it he reminds the user "And, of course, there is one kind of help you usually don't want: the government. Game violence, addiction, privacy, obscenity, pedophiles, gambling, marketing, terrorists, hackers, criminals–all sorts of issues can get you on the government's radar.". Most companies would like to avoid this at all costs.

6.2 Final Thoughts

The study of exploiting on-line games is both technically interesting and of great importance. The importance lies in both the financial power of the video game market and the relation to computer security in general. Game exploiters will always exist and continue to innovate and find new ways to cheat their favorite games. Game companies have to decide how much effort they wish to put into anti-cheat capabilities.

7 Overview of References

Noa Bar-Yosef provides an overview of the various methods for cheating online gambling sites [3]. Greg Hoglund and Gary McGraw have a very popular book detailing various aspects of exploiting online games [8]. They also wrote a precursor to this book which is less exhuastive but gives a brief yet sufficient overview of online game cheats [10]. Stephen Davis provides another book which goes into depth on cheating online games and countermeasures [6]. Adam Lake's book provides information on general principles for protecting games [9]. CBS News provides their investigation of the most popular attack in online poker [14].

References

[1] Cheating in online games. Wikipedia, February 2012. `http://en.wikipedia.org/wiki/Cheating_in_online_games`.

[2] Online gambling - american gaming association, 2012. `http://www.americangaming.org/government-affairs/key-issues/online-gamb%ling`.

[3] Noa Bar-Yosef. Hacking the house: How cybercriminals attack online casinos. Security Week, August 2011. `http://www.securityweek.com/hacking-house-how-cybercriminals-attack-onl%ine-casinos`.

[4] Simon Carlass. *Gaming Hacks*. O'Reilly Media, Inc., 2004.

[5] Darawk. Dll injection. Blizz Hackers, March 2006. `http://www.blizzhackers.cc/viewtopic.php?p=2483118`.

[6] Stephen Davis. *Protecting Games: A Security Handbook for Game Developers and Publishers*. Course Technology PTR, 2009.

[7] Jack M. Germain. Global extortion: Online gambling and organized hacking. TechNewsWorld, March 2004. `http://www.technewsworld.com/story/33171.html`.

[8] Greg Hoglund and Gary McGraw. *Exploiting Online Games: Cheating Massively Distributed Systems*. Addison-Wesley Professional, 2007.

[9] Adam Lake. *Game Programming Gems 8*. Course Technology PTR, 2010.

[10] Gary McGraw and Greg Hoglund. *Cheating Online Games*. Addison-Wesley Professional, 2006.

[11] Matthew Pritchard. How to hurt the hackers: The scoop on internet cheating and how you can combat it. Gamasutra, July 2000. `http://www.gamasutra.com/view/feature/3149/how_to_hurt_the_hackers_the_%scoop_.php`.

[12] Shahen Ramezany. Hacking / exploiting / cheating in online games. Abysssec, March 2011. `http://www.abysssec.com/blog/wp-content/uploads/2011/03/Exploiting-Onli%ne-Games.pdf`.

[13] Andrew Rollins and Ernest Adams. *Andrew Rollings and Ernest Adams on Game Design*. New Riders, 2003.

[14] Ira Rosen. How online gamblers unmaksed cheaters. CBS News, June 2009. `http://www.cbsnews.com/2100-18560_162-4633254.html?tag=contentMain`.

[15] Nikola Strahija. Russian hackers raid largest online gaming operation and destroy data in blackma. Xatrix Security, February 2003. `http://www.xatrix.org/article/russian-hackers-raid-largest-online-gamin%g-operation-and-destroy-data-in-blackma/2726/`.

[16] Daniel Terdiman. Hacking online games a widespread problem. CNET, April 2009. `http://news.cnet.com/8301-10797_3-10226485-235.html`.