Shuffle Up and Deal: A Simple Solution to Protect Online Poker from Malware

Aviel D. Rubin, Ph.D.

Abstract

As an avid poker player, I enjoyed playing low stakes cash games and low buy-in tournaments on Full Tilt Poker before Black Friday.[1] However, as a Computer Scientist specializing in network and software security, I would never play poker online for any significant stakes, due to security concerns around malware and malicious remote access tools. In this article, I describe a new solution that is easy to adopt, requires no new hardware or user training, and which I believe eliminates the primary threat of malware in online poker. Under my solution, implemented properly, I would be comfortable playing poker online for whatever stakes my bankroll would allow.

The risks of traditional online poker

The risks to online poker fall into several categories. Some have to do with the integrity of the game. Is the house cheating? Are the cards randomly shuffled? Are any employees at the poker game site trying to cheat? There are documented cases of serious problems with a corrupt house, the best known of which is the Absolute Poker scandal.[2] While these concerns are real, I believe that there is so much economic incentive for the large, legitimate corporations running poker sites to behave correctly, and very little for them to gain by cheating, that I think with proper audit and oversight, it is reasonable to trust the major industry players to run a poker site fairly.

Another real concern with online poker is that of collusion among poker players. In cash games, it is not too difficult for people to join the same poker table and to share information about their hole cards with each other over an out of band channel, such as over the phone. In online tournaments, it is more difficult for colluding players to sit at the same table, but when they do, they can cheat by dumping chips from one player to the other, potentially giving the receiving player a tremendous advantage in the tournament.

While collusion definitely happens, there are techniques, using statistical analysis, to detect and combat this type of cheating. Offending users can be banned from poker sites, and given that users are required to provide real-world identification and financial information to set up accounts, there is a limit to how many times such cheaters can join a site.

There are other security concerns in online poker including automated playing bots, denial of service attacks, and vulnerable user authentication. All of these have reasonable

mitigations, and I believe that an online poker site that is run by skilled administrators can handle these.

The biggest open problem with online poker is the prevalence of malware such as Remote Access Tools (RAT). There is no security solution that protects against an attacker running RAT tools on a victim's machine.

The problem of malware

Would you play online poker if your opponent were sitting directly behind you and could see your computer screen, including your hole cards? As a computer security expert who studies network security and malware, I contend that if you play high stakes online poker, your opponent may indeed be able to see your poker hands without being detected.

Remote Access Tools, which are very real, highly sophisticated, and widely available, allow an attacker to take complete control of a remote computer. Anyone who has ever seen a demonstration of this technology understands and appreciates the implications for online poker. Sadly, in this day and age, there is no way to guarantee that a standard Windows, Mac, or Linux computer is uninfected. The latest attacks can bypass even the most advanced host-based mechanisms such as anti-virus tools. What's even scarier is that poker-specific malware has been identified in the wild, and there are documented cases of attackers using RATs to cheat at poker by remotely observing players' hole cards in high-stakes games.[3] One of the best-known, poker-specific malware products is a Russian-based Trojan called i2Ninja, which collects information from a player's machine and sends it to the attacker.[4]

When the stakes are high, even low-tech threats abound. Case in point: an online poker pro named Douglas Polk lost $35,000 when an attacker manually inserted malware on his computer that allowed for remote viewing of his hole cards.[5] The attacker gained physical access to the computer when he stayed at Mr. Polk's house.

Avoiding malware

Nobody has solved the problem of malware on users' computers, and I am not offering a solution to that problem here. Instead, I am proposing a new solution for playing online poker in a way that is secure, *even if the user's computer is completely infected with malware*.

The idea is to *avoid* the malware.

Here's the key. A player's secret hole cards are sensitive information. Everything else on a poker table should be publicly known. So my proposal is simple: Do not display the player's hole cards on the online poker table on the computer. In fact, do not even communicate the information about which cards the player is dealt to the user's computer. If the computer does not know the hole cards, then that information is safe from any attacker, even one running RAT tools on the machine.

Instead, communicate the user's hole cards to another device held by the user, such as his smartphone or tablet. That is the central idea. While it is common for computers to be infected with malware, and while it is increasingly the case that smartphones are vulnerable as well, it is significantly more difficult for an attacker to compromise both a user's computer and the same user's smartphone *simultaneously* in such a way that allows cheating at poker.

The user in this solution plays poker with the same online poker application and the same interface to which he is accustomed. The only difference is that instead of displaying the hole cards on the screen, the cards are not shown at all, and the user learns which cards were dealt to him by looking at a companion app that is running on a smartphone. Here is an illustration. Below is a poker table from PokerStars, and the user's hole cards are hidden. The user's smartphone displays the hand # and the user's hole cards.

The players can perform all of the betting and other actions using their computer, as they've always done in the past. But they look at their smartphone to see what hand they are holding.

This solution can be added to existing online poker sites incrementally. Poker players can configure their account to use a smartphone for their hole cards, or to play the old fashioned way, and a poker table can consist of some players who are using smartphones for their hole cards and others who are just using their computers. Thus, this new solution gives poker players a way to trade off security and convenience, under their control.

I have worked out the technical design details that are required to implement this solution on a real poker site, and the specifics are beyond the scope of this article. The point here is to introduce the concept and to begin to educate the poker community about this simple and elegant way to avoid the influence of malware in online poker.

Multi-tabling

The smartphone app described above supports multi-tabling, where a user plays on multiple poker tables at once. One way to do this is to have the poker client on the computer inform the smartphone about which table has the current *focus*. For example, say that a user has 8 simultaneous poker tables running, and that the displays for those tables are stacked. So, the smartphone app has 8 hands to display, and those hands are linked to the corresponding tables on the user's computer. When it is a user's turn to act at one of the tables, that table's image pops up to the front of the screen on top of all the other tables. At the same time, the computer can communicate, either through the game server, or even over a direct WiFi or Bluetooth connection, a table or hand identifier to the smartphone, which can then automatically display the corresponding hole cards. The user can also scroll manually through the active hands by swiping on the smartphone screen and rotating through the active hands.

One way to help the user link the hands on the smartphone to the tables on the computer is to use visual cues, such as matching screen skins. For example, each table can have a corresponding background color and outline design that matches an outline color and design on the corresponding hand on the smartphone.

Another way to display the hole cards on the smartphone is to show small images of all of the hole cards for all the active hands. Depending on the screen size and resolution and the number of active tables, this option may be viable. It works even better if the player uses a tablet instead of a smartphone.

Other applications

The main idea described in this paper is to protect a user's online activities from malware on his or her computer by splitting an application into two components. One of the components runs on a user's computer, and the other runs on a smartphone, over an independent network channel. This can be applied to online banking and many other online applications that involve sensitive information that could be compromised by malware on the user's machine.

I have designed an online bill payment application where a customer logs into a bank from a computer and selects a payee. The user then logs into a bank app on a smartphone, indicates the amount of the bill, and completes the transaction. An attacker would have to

compromise the computer and the smartphone at the same time to make a rogue payment. The idea can be applied to online stock purchases, online access to health records, and many other types of applications.

Conclusions

I have described a simple solution to protect online poker hands, whereby a smartphone with an independent communication channel to the poker server is used to display the secret hole cards. This avoids the problem of malware on computers compromising the secrecy of user's cards and significantly raises the bar for an attacker. The solution is easy to implement and can be added incrementally to existing online poker servers. The technique can also be applied to online banking and other security-sensitive applications.

About the author

Dr. Aviel D. Rubin is Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. A former Fulbright Scholar, Rubin also directs the Health and Medical Security Lab at Johns Hopkins. Dr. Rubin has testified before the U.S. House and Senate on multiple occasions about information security, and he is author of several books on computer security. In January 2004, Baltimore Magazine named Rubin a Baltimorean of the Year for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award.

---

[1] Friday, April 15, 2011, is commonly referred to as Black Friday in the poker community. On that date, the US Department of Justice issued indictments against the largest online poker operators, effectively shutting them down in the United States.

[2] See http://freakonomics.com/2007/10/17/the-absolute-poker-cheating-scandal-blown-wide-open/

[3] See http://arstechnica.com/security/2013/12/card-sharks-infect-professional-poker-players-laptop-with-a-dirty-rat/ for an eye-opening account.

[4] See http://pokerfuse.com/news/media-and-software/new-financial-malware-targets-poker-players-with-pokergrabber-module-02-12/ and http://blog.trendmicro.com/online-poker-community-targeted-i2ninja-malware-module/.

[5] http://www.onlinepokerreport.com/8040/wcgrider-refunded-for-hacking-implicates-suspect/