How Does Match-Fixing Inform Computer Game Security?

Jeff Yan(✉)

Linköping University, Linköping, Sweden
jeff.yan@liu.se

Abstract. Match fixing is an increasingly popular phenomenon in eSports, namely competitive computer gaming between professional players. We first revisit the notion of security for computer games in the context of match fixing, which was never considered before. Then we offer a security economics analysis, and discuss potential countermeasures for addressing this threat. We propose a novel crowd-sourcing method for match-fixing detection. Our approach is incentive-compatible and it works for both traditional sports and eSports. We expect to raise awareness of these new issues and encourage further academic research.

Keywords: Security economics · Incentives
Crowd-sourcing for fraud detection · Security notions
Online game security

1 Introduction

As an interesting recent development, competitive computer-gaming, or eSports, has become a new spectator sport. It attracts a global audience of about 400 million a year. Popular eSports competitions between professional game players are physically viewed in big stadiums, televised by major TV channels, or streamed online over the Internet[1].

In sport, if a match is played to a completely or partially pre-determined result, it is match fixing. This is a dishonest practice of determining the outcome of a match before it is played. According to a recent article in The Economist [1], matching fixing is a big growing problem in sports, and it mostly remains undiscovered. Criminal groups launder a huge sum by match-fixing and illegal betting each year. Match-fixing can bend legitimate sport betting and rip off a large number of gamblers, too.

As eSports become popular, match-fixing goes digital, too. The first confirmed matching-fixing scandal in eSports occurred in 2010. One of the biggest

[1] I spent several months visiting Microsoft Research (Beijing) in 2004. During the visit, a project which we conceived and investigated in the Systems Group was to support online game spectating via a peer-to-peer infrastructure. This vision has become reality for years.

V. Matyáš et al. (Eds.): Security Protocols 2018, LNCS 11286, pp. 166–170, 2018.
https://doi.org/10.1007/978-3-030-03251-7_19

names in eSports was banned for life in 2016 in South Korea because of his role in a series of fixes in StarCraft II. According to The Economist [2], the eSports industry is estimated to be worth $700 m annually and expected to rise to $1.5 bn by 2020. Betting on eSports has an annual turnover of about $40 bn, and this figure is expected to exceed $150 bn a year by 2020. Many more match-fixings in eSports are to come, discovered or not.

Security can mean different things in different contexts. A context change warrants a revisit of established security notions for the new context. For example, the Needham-Schroeder public-key protocol was secure in the original setting which the protocol was proposed for, but when insider threats were considered, the protocol could be broken by a sophisticated attack. The emerging phenomenon of match-fixing in eSports raises an opportunity to revisit the notion of security for computer games, and to discuss how this new phenomenon informs computer game security.

2 Computer Game Security: A Revisit

Security for computer games has been an evolving concept. It was largely concerned with copy protection in the early days of single-player games.

With the emergence of networked or online computer games, security became an inherent design issue for games, just like graphics and artificial intelligence. What security meant the most for these games was fairness enforcement, i.e. making the play fair for each user (player) so that one does not have any unfair advantage over opponents [4,5].

The social norms and structures for either preventing or discouraging cheating in the non-electronic world were no longer in place for networked games. It was security that became an alternative but necessary mechanism for fairness enforcement [4,5]. Some years later, Bruce Schneier in 2012 echoed this view and generalised it to formulate a thought-provoking perspective on how trust is enabled in socio-technical systems via moral, reputational, institutional and security mechanisms [3].

We say that the focus of games security, previously, was on dealing with players cheating to beat their opponents unfairly. Now with match-fixing emerging in the scene, we should *also* explicitly address the issue of players cheating or underperforming to lose the games for illicit gains outside of the virtual worlds, such as manipulating gambling results in the real world.

Another interesting change in the context is the following. In the past, we considered security as concerning only game players, developers and operators. That is, security was a matter merely between gamers, and between gamers and developers/operators. Now, a lot more stakeholders get involved; newcomers include gambling sites, as well as a large number of people who bet on eSport results. A lot more stakeholders than before desire the fairness of game play enforced, rather than games rigged in one way or another.

Therefore, security for online games is still about fairness enforcement. This overall observation formulated more than fifteen years ago remains valid.

3 The Road Ahead

Match-fixing goes digital; countermeasures should go digital, too. Otherwise, scalability will become a serious issue that impedes effective countermeasures, given the stunning number of eSport games played every day. Let alone the lack of resources (including human power), which is already a serious problem for match-fixing detection and investigation in traditional sports.

A possible technical solution for match-fixing detection is to track, profile, analyse the performance of each player (or team) per play meticulously. Brief and coarse versions of these are available in some computer games but ineffective in dealing with match-fixing. Technically, game developers are best positioned to develop new tools and algorithms, since they have access to the games' data structure and access to players' in-game behaviour data and can interpret them expertly.

These new tools arguably should become a part of standard security toolboxes for eSport games, at least in theory. But we argue that game developers might not have sufficient incentives to do it, since they would be better off by investing in other elements of a game, e.g.

- Game play, special effects and AI and so on that help to attract a big player base which the developers can cash in. The experience of the player in a game, i.e. in-game experience, used to be the only priority for developers.
- Dedicated eSports features that support high level competition. Many successful eSports games such as StarCraft II, League of Legends and DOTA have all been designed for professional competition play.
- Enhanced spectator support that offers dedicated and convenient observing features for the benefit of spectators. These features attract spectators and increase eSports' stickiness.

On the other hand, if the game developers beef up a match-fixing detection system, the stakeholder that benefit the most would be gambling sites. Little gain for the game developers themselves by offering a sophisticated technology. A misaligned incentive, isn't it?

Instead, both gambling sites and sport gamblers have a stronger incentive to mitigate match-fixing than game developers do.

Thus, a third-party solution look like the best for match-fixing detection, since this way it is easier to make it incentive-compatible.

For example, an independent service that analyses betting patterns and the fluctuations of game odds is a useful approach for match-fixing detection. However, it has its limitations. For example, it faces issues like false positives and false negatives, the same as any other anomaly detection systems. And bad guys can evolve to stay just below the detection threshold.

Here we propose a new solution that is incentive-compatible and thus looks promising. It is a crowdsourcing platform which supports a range of functions for match-fixing detection. They include archiving key match data (such as gameplay videos, bet patterns and fluctuations of game odds), supporting game replay and review, recording whistle-blowing and suspicion reporting, correlating suspicions in gameplay and anomalies in betting patterns and game odds, summarizing confirmed evidence, and etc. A large number of gamblers have a stake in it and therefore they will be willing to contribute to the crowdsourcing efforts. The more such eyeballs, the better the crowdsourcing platform performs.

Also, a key point here is that this crowdsourcing service, together with dedicated gamblers, will spot suspicious behaviours that suggest match fixing, and will establish incriminating patterns based on these behaviours. On the contrary, occasional spectators cannot achieve this by viewing a game or two in the field; otherwise it cannot explain why a majority of match-fixing in sport remains undiscovered. On the other hand, a one-off fix of a single game might be virtually impossible to spot, and the evidence collected from the single game will be circumstantial at most.

Another key point here is that things that are not computationally tractable can be handled by human brains. For example, some tale-telling behaviour patterns can be entirely unknown at the beginning, and thus they cannot be described and programmed into code at all. However, human brains can abstract these behaviour patterns into useful heuristics that can be applied and shared. This is another power of crowd sourcing.

We note that our proposal appears to work for both traditional sports and eSports. In traditional sports such as football, match-fixing can be implemented via corrupting referees or tampering with the appointment of referees[2]. However, this does not invalidate our proposal.

We also note that our solution should take care to cope with and mitigate malicious users in the crowd whose interest is to mislead or wreck our system.

As a startup idea, a good crowd-sourcing platform for match-fixing detection will likely be financially supported by gambling sites; eventually it will likely be acquired by them, too.

4 Concluding Remarks

Fairness enforcement appears to remain as the main security issue for online computer games, even if the new threat of match-fixing is taken into consideration. When we first conceived this security notion for computer games many

[2] In 2012, several high-profile referees were convicted for fixing football matches in China [6]. At least the following contributed to their arrests and convictions. First, the referees' judgement calls and decisions had repeatedly triggered controversy and anger. The referees were either addicted to the easy money from match fixing, or blackmailed by the fixes they did before; they cheated again and again but did not stop after a single fix. Their behaviours exhibited somehow systematic suspicious patterns that smelled fishy even to outsiders and spectators. Second, whistleblowers and suspect-turned-prosecution-witnesses offered substantial incriminating evidences. These Chinese cases appear to suggest that it is likely to catch the fixers without correlating suspicious behaviours (of players, referees or both) to betting patterns and game odds in some circumstances.

years ago, the recent emerging match-fixing phenomenon in eSports did not exist. However, our revisit suggests that it is unnecessary to revise the security notion to address match-fixing.

Match-fixing is a big and realistic problem for regulators and the society at large. It is also an interesting research problem calling computer scientists for novel research. Our security economics analysis suggests that a crowd-sourcing approach appears to be promising for detecting match-fixing both in traditional sports and in eSports, since it is incentive compatible, and since it can make good use of the power and flexibility of human brains to tackle pattern recognition problems that are computationally hard or intractable.

Acknowledgements. I thank Ross Anderson, John Chuang, Dah Ming Chiu and the workshop attendees for their input and stimulating discussions. This work was supported by the Knut and Alice Wallenberg Foundation.

References

1. The Economist, Match-fixing is more common than ever - regulators need to up their game, 23 September 2017. https://www.economist.com/news/international/21729427-regulators-need-up-their-game-match-fixing-more-common-ever
2. The Economist, Match-fixing goes digital, 21 September 2017. https://www.economist.com/news/international/21729428-esports-are-likely-see-much-more-corruption-coming-years-match-fixing-goes
3. Schneier, B.: Liars and Outliers: Enabling the Trust that Society Needs to Thrive. O'Reilly, Sebastopol (2012)
4. Yan, J.: Security design in online games. In: Proceedings of 19th Annual Computer Security Applications Conference, ACSAC 2003, pp. 286–295 (2003)
5. Yan, J., Randell, B.: A systematic classification of cheating in online games. In: Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support for Games (NetGames 2005), pp. 1–9 (2005)
6. Four crooked referees (in Chinese). https://baike.baidu.com/item/%E5%9B%9B%E5%A4%A7%E9%BB%91%E5%93%A8