Poster: Challenges in Stopping Ticket Scalping Bots

Hao-Cheng Yang
b06902097@csie.ntu.edu.tw
National Taiwan University

Hsun Lee
leexun@csie.ntu.edu.tw
National Taiwan University

Hsu-Chun Hsiao
hchsiao@csie.ntu.edu.tw
National Taiwan University

ABSTRACT

The existence of ticket scalpers is a negative impact to all performers, audience, and primary ticket sellers. Automated ticket scalping bots, especially, generate serious damages to the online ticketing systems, and cause an extremely unfair competition between malicious ticket scalpers and normal users. However, little work had been done to address this security issue and propose solutions. In this paper, we will formulate this problem, propose an evaluation framework to systematize some known defenses, and provide several directions that can be further researched to mitigate automated ticket scalping bots.

ACM Reference Format:
Hao-Cheng Yang, Hsun Lee, and Hsu-Chun Hsiao. 2020. Poster: Challenges in Stopping Ticket Scalping Bots. In *15th ACM Asia Conference on Computer and Communications Security (ASIA CCS'20), October 5–9, 2020, Taipei, Taiwan.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3320269.3405448

1 INTRODUCTION

The advent of online ticketing systems created enormous commercial value by making people more convenient to acquire tickets to various events, like concerts, art performances, or sport competitions. Since popular performers have large fan bases, and the number of available tickets is limited, users of online ticketing systems have to compete for tickets by completing the purchasing procedures faster as soon as the ticket grabbing event starts. However, malicious parties will try to profit from these events by snapping up a large number of tickets and reselling them; we call them ticket scalpers.

Ticket scalpers are people who buy a lot of tickets, using illegal or unintended actions, and sell them to others with much higher price to profit. Before online ticketing systems appeared, ticket scalpers had been scalping tickets by phone. After the advent of online ticketing systems, ticket scalpers gained even more power by using automated ticket scalping bots, which are low-cost, fast, and can be simultaneously launched. In the OWASP Automated Threat Handbook, the identity code OAT-005 defines scalping as "obtaining limited-availability and/or preferred goods/services by unfair methods" [7]. Automated ticket scalping bots contribute significantly to the extremely unfair competition between ticket scalpers and normal users. In fact, Ticketmaster once claimed that Prestige Entertainment used automated scalping bots to lock up 40 percent of available tickets for the musical *Hamilton* [4].

To fight against ticket scalpers, major online ticketing systems employ various kinds of defenses to stop ticket scalpers, such as CAPTCHA, prior detection of suspicious accounts, throttling, Proof of Work, and paperless tickets. However, most of the known defenses are not ideal, for they have disadvantages in performance, security, usability, and/or deployability aspects. Also, ticket scalpers will constantly invent new techniques to bypass known defenses. The race between ticket scalpers and sellers is never ending.

The goal of our paper is to formulate this problem, propose an evaluation framework to systematize known defenses, and provide several directions that can be further researched to mitigate automated ticket scalping machines.

2 PROBLEM DEFINITION

2.1 Online Ticketing System

The process of purchasing a ticket varies in different online ticketing systems, but most of them share common important procedures: authentication, quantity and seat selection, payment, and optional bot detection tests. First, the users have to enter their identity information manually, or login their account first. Then, they have to fill in or select the number and kind of tickets they want to buy. Usually the maximum number of tickets a user can buy is limited. During the process, there might be bot detection mechanisms deployed at either frontend or backend of the website that the users have to pass. After completing these procedures, if the requested number of tickets are available, they will be reserved for the users and they can take their time filling in the mailing and billing information.

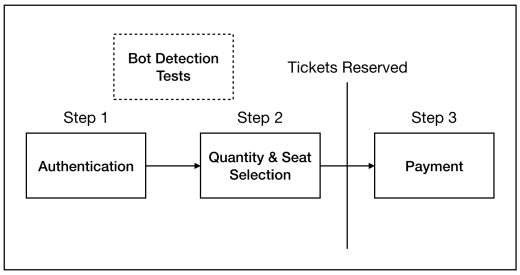

Figure 1: Sample ticket purchasing procedures

2.2 Attacker Model

We consider attackers that attempt to buy a large number of tickets from primary ticket sellers through online ticketing system by launching automated scalping bots. The bots are capable of completing the ticket purchasing process much faster than manual users, by auto filling and selecting on the browser, or sending POST requests directly to the server with user data. More advanced bots are even able to break or bypass defenses, such as CAPTCHAs.

ASIA CCS '20, October 5–9, 2020, Taipei, Taiwan

ACM ISBN 978-1-4503-6750-9/20/10.
https://doi.org/10.1145/3320269.3405448

Note that there are many kinds of ticket scalpers, some may collect their tickets by hiring a large number of labors with low cost to snap up the tickets. However, scalpers not using automated scalping bots are not included in our attacker model, since those are more unrelated to the information security field, and pose less threat to the online ticket selling service itself.

3 EVALUATION FRAMEWORK

Although there are many existing defenses in ticketing systems, they do not seem to be effective. First of all, many existing defenses are vulnerable to targeted attacks. That is, the attacker is often able to bypass the defenses if he know what defenses are deployed. On the other hand, although there are some secure construction of CAPTCHA (complicated video-based or game-based CAPTCHA, Google's reCAPTCHA v3), they are not chosen for deployment because of performance or usability issue. When improving a existing defense or developing a new one, it is important to strike a balance between different aspects. Therefore, in this section we are going to propose an evaluation framework.

The evaluation framework consists of three different aspects to evaluate defense measures toward automated ticket scalping bots: security, usability and deployability. A good defense measure should be secure against attackers, effect user experience as minimum as possible, and can be deployed on online ticketing systems with reasonable cost and performance.

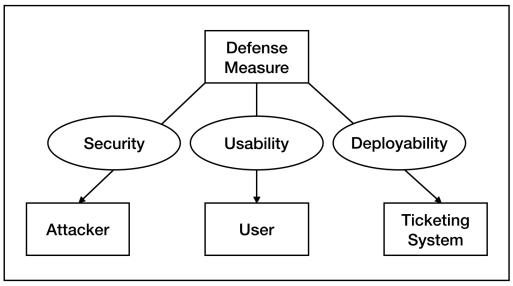

Figure 2: The evaluation framework

3.1 Security

A good defense measure has to be secure against attackers. The security of a defense measure is evaluated by whether it effectively stops attackers in our attacker model. That is, a defense is secure if it can prevent all attackers from launching successful attacks.

3.2 Usability

A good defense measure should also have high usability, meaning that it effects user experience as minimum as possible. We classify usability into learnability, extra operation time, and false rejects. Learnability evaluates whether users can understand the new ticket purchasing procedure after the defense is applied without detailed explanation. Extra operation time evaluates how much extra time average users have to spend to complete the new procedure. And at last, the number of false rejects produced by the defense measure is also essential to user experience and fairness. The usability aspect is included in our evaluation framework to require that defense measures strike a balance between stopping ticket scalping bots and preserving user experience.

3.3 Deployability

Deployability contains factors that ticketing system developers may concern, such as performance, measured by queries per second, and deployment cost. A major difficulty of ticketing systems is to maintain the stability of the system when the user requests burst in during ticket grabbing events. Defenses with high performance can prevent scalping bots from damaging the system while providing a reliable platform for genuine users. Deployment cost is also important to developers, depending on extra labor, server, development cost, and also whether there are existing services to use.

In the following section, we will evaluate some known defenses by the evaluation framework we proposed.

4 KNOWN DEFENSES AND EVALUATION

4.1 CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) provides a high level of security if well-implemented. One of the common practices of preventing form submissions by scripting is to put a CAPTCHA challenge to check whether or not the user is a human.

However, from the perspective of users, some kinds of CAPTCHA does not provide good usability, because they interrupt and slow down the purchasing process. Some CAPTCHAs are even too complicated that genuine users may fail in passing them, causing them unable to reserve their tickets in time. This is why Google's reCAPTCHA service continues to decrease the effort required for normal users to complete in newer versions.

Google's reCAPTCHA service is the most mature CAPTCHA system. However, there is a quota limit even in its enterprise version. This is why most online ticketing systems create their own customized CAPTCHA systems. Nevertheless, self-designed CAPTCHA systems are often more vulnerable, and fell short in the security aspect. Due to design flaws, some CAPTCHA systems using graphic codes are not complicated enough, which can be responded by deep learning algorithms, or even naive pattern recognition algorithms easily[8]. Developing an efficient and secure CAPTCHA system can be a good direction to mitigate automated ticket scalping bots. Some recent researches utilize adversarial perturbation, a feature in machine learning that is imperceptible by human but results in great misclassification error for machine learning models, to create "adversarial CAPTCHAs" that fool automatic CAPTCHA solvers [3] [5]. This might be a method to increase text and image-based CAPTCHAs' security without sacrificing usability.

4.2 Prior Detection of Suspicious Accounts

Ticketing systems could collect user actions and profiles such as active client IPs, contact addresses, and verification of email and mobile phone. Based on these information, it is possible to achieve prior detection of suspicious accounts. For example, an account is suspicious if its contact address is not in the same country as its mobile phone or IP address. Although there are online platforms which provide programmable SMS and email verification, this kind of account-based detection still forces attackers to put more effort generating reasonable profiles for the bot accounts. Nevertheless, this measure fells short in security and usability aspects due to the

aspect		reCAPTCHA	self-designed CAPTCHA	prior detection	throttling	PoW	paperless ticket
security		O	△	X	X	O	O
usability	learnability	△	△	O	O	O	△
	extra time	△	X	O	O	X	△
	false reject	△	△	△	O	X	O
deployability	performance	X	△	O	O	O	O
	deployment cost	O	X	△	O	O	X

Table 1: Evaluation of known defenses (O: satisfactory, X: unsatisfactory, △: normal or hard to judge). Note that "O" for "extra time" should be interpreted as satisfactory extra time, or low extra time.

potential risk of not detecting carefully designed bots and blocking some genuine users. However, this measure has an advantage in that it doesn't modify the ticket purchasing procedures, which preserves user experience for most users.

There are some other proposed bot detection methods, like the web honeypot technique [2] or using website fingerprinting [6]. However, currently they are still vulnerable to targeted attacks and hence won't increase much security.

4.3 Throttling

To mitigate unnecessary waste of resources, ticketing systems usually adopt a throttling controller, which is responsible for regulating the rate of resource requests from clients. It is often based on the client IP forwarded by the CDN provider, or based on the account ID. Throttling is good at preventing waste of resources, but there is usually an upper limit of maximum tickets that can be bought per account, so resubmitting the form continuously will not increase the chance of getting more tickets. That is why most of the scalping bots don't repeatedly replay requests. Instead, scalpers launch several bots to perform single form requests.

This method provides little security, but it possesses high usability and deployability, because it enhances server performance by filtering requests, and there are various mature throttling frameworks nowadays that can be deployed directly.

4.4 Proof of Work

Proof of work (PoW) provides high security against attackers that aim to launch a large number of attacks. PoW is a challenge that requires the requester prove it spent enough computational power. PoW is a good method of defending automated scalping bots, since it takes high computational cost to launch lots of bots that all solve PoW challenges efficient enough. However, users with inefficient hardware will not be able to pass PoW challenges fast enough to reserve their tickets. Different magnitude of computational power in personal computers, mobile devices, and ticket vending machines should also be taken into consider. Whether the usage of PoW is fair in the ticket purchasing process is worth exploring.

A previous work [1] proposed a geographic PoW, which increases its difficulty with the distance between the physical location of the requester's IP address to the location of the concert. The author claimed that a concert tends to attract normal users living near the concert. Also, ticket scalpers have to either accept large computational cost, or gather fake IPs or recruit workers near the location of every different concert, both resulting in extra cost. Although there are several problems in this scheme, continue researching for schemes that discourage ticket scalpers while influencing normal users as little as possible may be a promising future direction.

4.5 Paperless Ticket

Paperless ticket is a new form of ticket, where users bring their identity and credit cards used to purchase their tickets to the concert, and swipe for entry. Since paperless tickets cannot be resold, it is a method that ultimately stops ticket scalpers. Although paperless ticket is very secure, it has low usability and deployability. For example, users cannot enter the concert if they accidentally filled in incorrect information. Also, the time and labor cost needed to allow all audience to enter increases significantly.

5 CONCLUSION AND FUTURE WORK

In this paper, we formulated the problems of automated ticket scalping bots, propose an evaluation framework to systematize known defenses, and provide several directions that can be further researched to mitigate automated ticket scalping bots. In the future, we will research on new defense measures that perform better in the evaluation framework we proposed. Our ultimate goal is to find an ideal method to stop automated ticket scalping bots and bring a fair competition back to online ticketing systems.

Acknowledgements. This research was supported by the Ministry of Science and Technology of Taiwan under grant MOST 109-2636-E-002-021.

REFERENCES

[1] Edward Kaiser and Wu-chang Feng. 2010. Helping TicketMaster: Changing the Economics of Ticket Robots with Geographic Proof-of-Work. 1 – 6. https://doi.org/10.1109/INFCOMW.2010.5466663

[2] N. Nassar and G. Miller. 2012. Method for a two dimensional honeypot to deter web bots in commerce systems. In *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*. 250–256.

[3] M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman, and D. Pérez-Cabo. 2017. No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation. *IEEE Transactions on Information Forensics and Security* 12, 11 (2017), 2640–2653.

[4] Edvard Pettersson. 2017. *Ticketmaster Sues Broker Over Use of 'Bots' to Buy Up Tickets.* https://www.bloomberg.com/news/articles/2017-10-02/ticketmaster-sues-broker-over-use-of-bots-to-buy-up-tickets

[5] Chenghui Shi, Xiaogang Xu, Shouling Ji, Kai Bu, Jianhai Chen, Raheem A. Beyah, and Ting Wang. 2019. Adversarial CAPTCHAs. *CoRR* abs/1901.01107 (2019). arXiv:1901.01107 http://arxiv.org/abs/1901.01107

[6] Antoine Vastel, Walter Rudametkin, Romain Rouvoy, and Xavier Blanc. 2020. FP-Crawlers: Studying the Resilience of Browser Fingerprinting to Block Crawlers. In *MADWeb'20 - NDSS Workshop on Measurements, Attacks, and Defenses for the Web*, Oleksii Starov, Alexandros Kapravelos, and Nick Nikiforakis (Eds.). San Diego, United States. https://doi.org/10.14722/ndss.2020.23xxx

[7] Colin Watson and Tin Zaw. 2018. *OWASPAutomated Threat Handbook Web Applications, Version 1.2.*

[8] Jeff Yan and Ahmad Ahmad. 2008. Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms. 279–291. https://doi.org/10.1109/ACSAC.2007.47