Designing a User-centric Verifiable Lottery Interface: A Case Study on Course Selection

Li-Fei Kung[*], Hsun Lee, Ching-Shiuan Chen[*], Wen-Ning Chen[*] and Wei Jeng[*,+]
[*]*National Taiwan University, Taiwan*
[+]*National Institute of Cyber Security, Taiwan*

Abstract

Lotteries ensure fair distribution of supplies, but concerns arise over the transparency and verifiability of some systems. HeadStart, a cryptographic randomness generation protocol, was proposed to address these issues. Although this protocol ad-dresses transparency issues, its principal benefits must be conveyed to users through a comprehensible client interface, the creation of which is the focus of this study. This study explores the design of a user-friendly interface for HeadStart and perceptions towards a verifiable lottery system. Six participants were interviewed to understand their motivations to verify the lottery process and their perception of the current lottery client.

1. Introduction

The lottery is widely recognized as an effective method for upholding fairness in the allocation of supply. By mitigating biases, it ensures equitable opportunities for all participants. However, verifying the true randomness of the source used in the lottery remains challenging. Previous incidents [1, 2] have shown that third-party generated randomness may be compromised or contain errors. To address this, several research has proposed cryptographic randomness generation protocols [3]–[5] to provide verifiability.

The HeadStart cryptographic randomness generation protocol, proposed by Lee et al. [5] in 2022, is particularly commendable for its real-world practicality. It accommodates many individuals and enables direct participation and verification through personal personal device. By verifying the protocol, individuals can determine the security and fairness of the lottery result, including unpredictability and un-manipulability. However, the verifiability facet of HeadStart is still a startup concept. Non-technical users may lack a relevant mental model to interact with it, leading to a potential mismatch between developers' and users' understandings of the technology. Such a disparity could inadvertently create a vulnerable attack surface for malicious actors [6]. Therefore, it is crucial to explore users' perception of the verification process and ensure that the user interface accurately conveys technical concepts to non-technical users.

Despite the increasing prevalence of participatory randomness generators, there remains a scarcity of research exploring user perception of these systems. Several user studies on verifiable voting—sharing the origin to the participatory randomness generator – have illuminated valuable insights, laying a foundation for our exploratory research methodology. A study [7] explore voters' mental models of verifiability through interview towards Selene voting protocol [8],which preserves privacy by verifying plaintext votes. Another study [9] revealed that German users had diverse attitudes towards verifiable remote voting systems, ranging from negative views due to complexity to positive views due to its high security. Given these varying attitudes and perceptions towards verifiable voting systems, it becomes crucial to further understand user perceptions and motivations on verification, especially in varying contexts of public participation.

In this study, we designed an interface based on Lee et al.'s principles [5] and explored non-technical user perceptions of verifiable lottery mechanisms. We developed the HeadStart randomness generator and tested it in a lottery-based enrollment system. Afterward, we conducted six interviews to understand users' perception of the outcome and their motivation to verify it. Our goal is to evaluate if the current interface effectively communicates the technology's benefits and identify potential security issues arising from users' misunderstanding of technological concepts. The study centers on the following research questions:

RQ1: How does the interface design of client-based randomness generator influence the motivation of users to use the verification function in a lottery-based enrollment system?

RQ2: What are user's perceptions of a verifiable lottery system in the above context?

2. Case Study: Course Selection Lottery

In September 2022, this study implemented a lottery system for course selection at a research university in Taiwan for a highly sought-after course. After the initial course selection process, the instructor used HeadStart to conduct a lottery for additional spots. Hundreds of students attended the lottery to register their intent to attend the class and provide personal information and a self-set verification code. The students' verification codes were used as a random seed in HeadStart's cryptographic algorithms, thereby randomizing the students' order in the lottery pool. The lottery results were based on the number of extra spots available for each class. For example, if a class has three additional spots, the top three students in

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023. August 6 -- 8, 2023, Anaheim, CA, USA.

the randomized order will win the lottery. After the lottery, students could independently verify their result by clicking the verification button on the result page (Appendix A). Students could enter their self-set verification code and the system initiated a two-phase verification process.

3. Preliminary Result

The study's participants were recruited through the registration form used for the course selection lottery. Details on their characteristics are found in Appendix B. During a 30-minute in-person interview, participants shared their thoughts and feelings about the verification process and the HeadStart lottery system. All interviews were recorded with consent.

3.1 The interface design of verification process

The interface is guided by two principal design objectives: representing the system's verification status and revealing the impartiality of the lottery process by two phases. The initial phase ensures unpredictability by verifying that students' lots exist in the lottery pool and using cryptographic algorithms to prevent predictability. The second phase verifies un-manipulability by checking for tampering or interference. The interface includes three design highlights to enhance users' sense of protection (Appendix C for more details). One notable feature is a message that describes the utility of algorithms, such as "make sure your verification code is in the pool". The second highlight is a blue question mark icon, which provides explanatory annotations for technical jargon. Finally, the interface has a progress bar that strengthens users' sense of protection and encourages trust in the system's verification of the lottery.

3.2 Motivations to use the verification system

Out of six participants, four participants chose to verify their lottery results with Head-Start. Two motivations were behind the verification process: curiosity about the floating verification button (P01, P02) and misunderstanding that the verification process was necessary to access the final result (P03, P05). On the other hand, two participants did not verify their lottery results. One participant (P06) already knew they had won the prize, while the other (P04) was not very interested in the class. This result shows that the price of the lottery and users' desire for a prize may affect their willingness to verify the impartiality of the lottery process.

3.3 User’s Perception toward Verifiable Lottery System

User perception of verifiable lottery systems is based on three aspects: verification code, overall experience and affection for the lottery system, and user interface design of the system.

The concept of a verification code in a lottery system was relatively novel, and some users were unfamiliar with it. This resulted in several misunderstandings about its purpose. For example, one participant considered it as a form of identification, like a password for the system to confirm authority (P01), and used her daily password as a verification code during the lottery. Other misunderstandings, such as those related to the "lots" in the lottery (P04, P05) or their impact on the odds of winning (P03, P04), will not endanger users' security. However, the actual purpose of the verification code in HeadStart is to affect the generation of randomness by disordering all lots.

Overall, our participants found the lottery experience to be unique and engaging (P01, P05). They also thought that HeadStart is a fast, convenient, and professional lottery tool (P03). Participants shared their perceptions of the verification user interface, evaluating it based on two elements: content description and visual components. Some participants reported being confused by certain jargon, such as "unpredictable," "random seed," and "delay() function" (P01, P02, P05, P06), terms specific to the HeadStart algorithms. Although the blue question mark icon was designed to explain the jargon, its effectiveness was limited. Diverse perceptions of the progress bar were expressed by participants. Several participants considered the progress bar to be present fluently, which made them doubt whether the system was really conducting the verification process (P01, P04). However, the representation of the progress bar made several participants believe that the system was verifying the result and made them trust the system (P02, P05).

4. Next Steps

This study design a verifiable lottery client in the context of course selection, and evaluate it with six interviews. Our preliminary findings suggests that the current HeadStart client could enhance its communication regarding the functioning of HeadStart and its verification codes through its interface. Several improvements could more accurately align users' mental models with reality. First, we discovered that users treat verification codes as passwords, which is insecure since the verification codes are open to every participant. One possible solution is to use micro-animation to deliver the function of the verification code. This would involve showing all the verification codes to users while they are registering for the lottery and informing them that the verification code is public. Second, further exploration is needed to address the trust issues surrounding the progress bar's representation. Our interviews revealed that the speed of the progress bar can affect users' trust in the honesty of the lottery verification protocol. One possible solution is to display the actual action of the system on the progress bar, providing users with more information and increasing their trust in the system.

Promoting the importance of verifying the lottery process to government, society, and commercial industries—including the gaming industry that incorporates lotteries in their games— necessitates the creation of a transparent and comprehensible lottery system client. With a transparent and understandable lottery system, public trust and confidence would build, facilitating public scrutiny and oversight of the lottery's operations.

5. Reference

[1] "US Apologizes for Visa Lottery Error," *VOANEWS*, May 12, 2011. "Hot lotto fraud scandal," https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-iowa-lottery-fraud-mystery.html, accessed on 2020-12-01.

[2] Kali White Vanbaale, "The Hot Lotto Scandal: Computer Codes, Cons and Bigfoot," *A&E*, Aug. 16, 2022. https://www.aetv.com/real-crime/hot-lotto-scandal, accessed Aug. 26, 2022.

[3] P. Schindler, A. Judmayer, N. Stifter, and E. Weippl, "HydRand: Efficient Continuous Distributed Randomness," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 73–89. doi: 10.1109/SP40000.2020.00003.

[4] P. Schindler, A. Judmayer, M. Hittmeir, N. Stifter, and E. R. Weippl, "RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 942, 2020.

[5] H. Lee *et al.*, "HeadStart: Efficiently Verifiable and Low-Latency Participatory Randomness Generation at Scale," in *Proceedings 2022 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, 2022. doi: 10.14722/ndss.2022.24234.

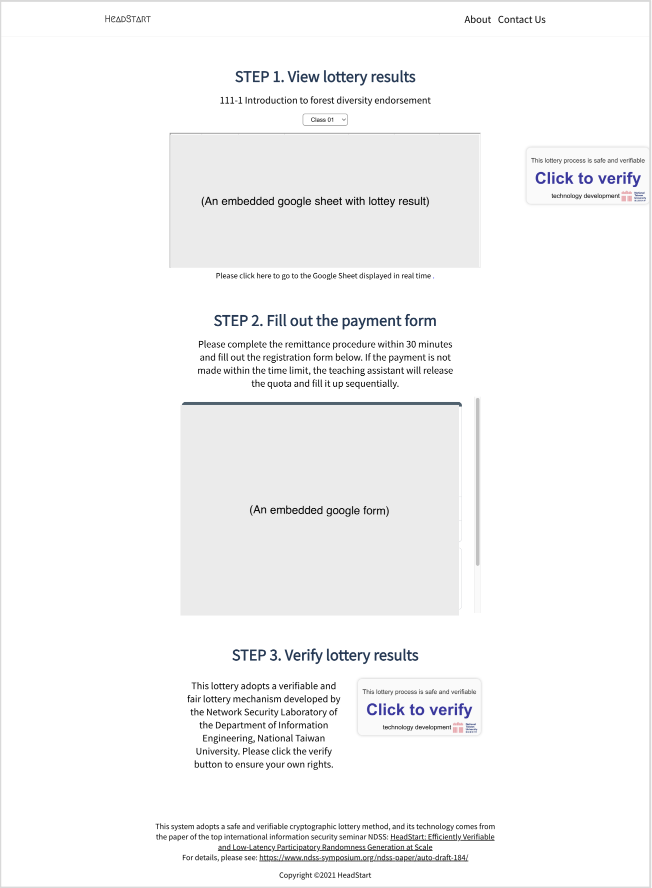
[6] K. Baig, E. Kazan, K. Hundlani, S. Maqsood, and S. Chiasson, "Replication: Effects of Media on the Mental Models of Technical Users," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, USENIX Association, Aug. 2021, pp. 119–138. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/baig

[7] E. and R. P. Y. A. and M. K. Zollinger Marie-Laure and Estaji, "``Just for the Sake of Transparency'': Exploring Voter Mental Models of Verifiability," in *Electronic Voting*, M. and D.-C. D. and K. O. and R. P. and S. M. and G. M. Krimmer Robert and Volkamer, Ed., Cham: Springer International Publishing, 2021, pp. 155–170.

[8] P. B. and I. V. Ryan Peter Y. A. and Rønne, "Selene: Voting with Transparent Verifiability and Coercion-Mitigation," in *Financial Cryptography and Data Security*, S. and R. P. Y. A. and W. D. and B. M. and R. K. Clark Jeremy and Meiklejohn, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 176–192.

[9] O. Kulyk, M. Volkamer, N. Fuhrberg, B. Berens, and R. Krimmer, "German voters' attitudes towards voting online with a verifiable system," in *Workshop on Advances in Secure Electronic Voting (VOTING), Grenada, February 18, 2022*, 2022.

Appendix A: The lottery result interface



STEP 1. View lottery results

111-1 Introduction to forest diversity endorsement

(An embedded google sheet with lottery result)

Please click here to go to the Google Sheet displayed in real time .

STEP 2. Fill out the payment form

Please complete the remittance procedure within 30 minutes and fill out the registration form below. If the payment is not made within the time limit, the teaching assistant will release the quota and fill it up sequentially.

(An embedded google form)

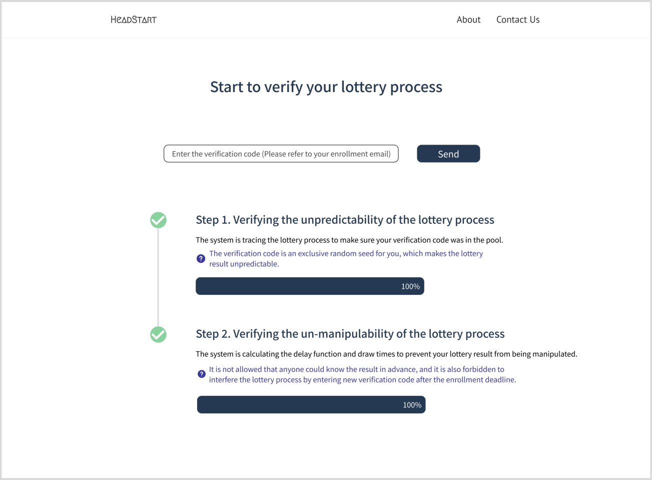
STEP 3. Verify lottery results

This lottery adopts a verifiable and fair lottery mechanism developed by the Network Security Laboratory of the Department of Information Engineering, National Taiwan University. Please click the verify button to ensure your own rights.

This system adopts a safe and verifiable cryptographic lottery method, and its technology comes from the paper of the top international information security seminar NDSS: HeadStart: Efficiently Verifiable and Low-Latency Participatory Randomness Generation at Scale
For details, please see: https://www.ndss-symposium.org/ndss-paper/auto-draft-184/

Copyright ©2021 HeadStart

Appendix C: The verification interface



Start to verify your lottery process

Enter the verification code (Please refer to your enrollment email)

Step 1. Verifying the unpredictability of the lottery process

The system is tracing the lottery process to make sure your verification code was in the pool.

The verification code is an exclusive random seed for you, which makes the lottery result unpredictable.

Step 2. Verifying the un-manipulability of the lottery process

The system is calculating the delay function and draw times to prevent your lottery result from being manipulated.

It is not allowed that anyone could know the result in advance, and it is also forbidden to interfere the lottery process by entering new verification code after the enrollment deadline.

Appendix B: Participants Demographics

Participant	**College/School**	**Grade**	**Winning the price**	**Verify the lottery**
P01	Art and Humanities	Senior	No	Yes
P02	Business	Senior	Yes	Yes
P03	Social Science	Senior	No	Yes
P04	Journalism	Master degree	No	No
P05	Nursing	Post-graduate	Yes	Yes
P06	Social Science	Senior	Yes	No