1 Reviews and Replies

1.1 Review 1

Review. The problem is tackled nicely, the motivation is clear and the proposed technique provides the desired security. I enjoyed reading this well-written paper.

1.2 Review 2

Review. The method appears solid. There is a well-defined advantage over previous work: achieving both a stop of IdP-based login tracing and prevention of RP-based identity linkage

1.3 Review 3

Review. Novel idea and discussion of the SSO-privacy dilemma.

1.4 Review 4

Review. Why does UPPRESSO adopt residue classes over the integers for the discrete log problem, instead of elliptic curves.
Reply. Now we have redesigned the protocol and implemented the three identifier transformation function with elliptic curve cryptography. The details can be found in Section 5.

1.5 Review 5

Review. The analysis of UPPRESSO is not appropriate, such that there may be vulnerabilities that breaks the privacy properties of UPPRESSO.
Reply. We offer the provable security analysis of privacy in Section 6, which proves that the attacks breaking the privacy properties are computationally infeasible.

1.6 Review 6

Review. This work may be lack of novelty.
Reply. Existing solutions only prevent either RP-based or IdP-based threats. More importantly, they are mutually exclusive and cannot be simply combined. This work has identified the key challenge towards a comprehensive privacy solution, formalized it as an id-transformation problem, and proposed the trapdoor-based transformation solution. Therefore, we consider this work novel. The details are provided in Section 3.

1.7 Review 7

Review. The motivation of this work may be not strong enough. The privacy scheme breaks the agreements between RP and IdP on sharing information. It should be considered whether tackled privacy issue is a real threat or not.
Reply. We agree that IdPs may want to know the RPs and they even have this knowledge by default in some SSO systems, which raised privacy concerns about IdP-based tracking and caught attention from both academia (SPRESSO [1]) and industry (Mozilla's BrowserID [2]). Moreover, some users may willingly share personal information with RPs, but identifiable information such as email is commonly considered as privacy, especially by privacy-savvy users. Therefore, a solution against RP-based linkage is expected. In fact, the RP-based linkage threat is widely recognized in the literature on federated identity management and SSO, and PPID is well-accepted to prevent this threat. The details have been well discussed in Paragraph 3-5, Section 1.

1.8 Review 8

Review. Compared with the existing SSO, the delay of UPPRESSO proposed in the paper has increased significantly.
Reply. We have improved the implementation of UPPRESSO, by using efficient elliptic curve cryptography instead of modular exponentiation. Now UPPRESSO takes almost the same time as SPRESSO [1] but offering comprehensive privacy protection. The details of implementation and evaluation are provided in Section 8.

References

[1] Fett et. al. *"SPRESSO: A secure, privacy-respecting single sign-on system for the web," in ACM CCS, 2015.*

[2] *https://github.com/mozilla/id-specs/blob/prod/browserid/index.md.*