Summary

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.

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.

Review 3

Review: Novel idea and discussion of the SSO-privacy dilemma; Rigorous method and proof; Effective, efficient solutions to practical problems.

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 functions with elliptic curve cryptography. The details can be found in Section 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.

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.

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.

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.

Reference

[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.

Original Reviews

Review #360A

==========

* Updated: 14 Oct 2020 7:39:47pm CEST

Overall Recommendation

---

3. Major revision

Writing Quality

---

4. Well-written

Reviewer Confidence

---

2. Passable confidence

Paper Summary

The paper presents UPPRESSO, privacy-preserving single sign-on framework that can provide privacy in the face of a curious identity provider and offer security against collusive relying parties. UPPRESSO uses three transformations to hide users' and servers' ID. They incorporate discrete logarithm problem as the fundamental security block to design the transformations functions. Consequently, identity provider does not learn about the services and services cannot derive the real users' identity even if they collude.

Strengths

- Secure technique and neat presentation
- Proper comparison with related work

Weaknesses

- Technical work as presented in the paper is limited

Detailed Comments for Authors

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

- The paper discusses issues with the current systems multiple times. At some points, I found it tedious to read through Section IX as I found it quite repetitive. I understand the authors try to

emphasize the problems with the current systems and showcase strong points of the proposed system. However, it reads as if there is not sufficient technical contribution. The three transformations as presented in the introduction are reiterated throughout the paper with some added meat in each section.

- The uniqueness of IDs could cause an issue depending on the number of users registered with the ID provider. The discussion briefly mentions this issue. This discussion could be expanded as informal security analysis. How many registration efforts are needed by an attacker to impersonate a user and how long it takes the ID provider to notice such malicious activities?

* *

Review #360B

==========

Overall Recommendation

---

2. Leaning towards reject

Writing Quality

---

4. Well-written

Reviewer Confidence

---

1. Low confidence

Paper Summary

In this paper, the authors propose UPPRESSO, a protocol based on existing SSO protocols, in order to enhance the privacy of users, preventing IdPs (identity providers) and RPs (relying parties) from intruding users' privacy. Previous work could only either stop IdP-based login tracing or prevent RP-based identity linkage, but UPPRESSO could stop them both, without significantly changing the infrastructure of existing SSO protocols. The authors first formalize the mechanism of SSO and then propose the procedure of UPPRESSO. They then prove the security of UPPRESSO and evaluate its performance by experiments.

Strengths

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

Weaknesses

The threat tackled by the paper does not appear significant.

Detailed Comments for Authors

First of all, I appreciate the writing style of this paper. The flow and stakeholders are made clear in the paper, and the authors have explained their ideas well. Also, the idea of UPPRESSO is simple but reasonable, I do believe it could fulfill its mission.

However, I also have some concerns which make me doubt if this paper should make it into NDSS. The first concern is that I wonder if the tackled privacy issue is a real threat in existing SSO protocol? In most cases, the users use SSO for convenience, so that they do not need to input the same information again on RP's side. In other words, they are expecting IdP to provide their true ID_U (and maybe other information like email, nickname, etc.) to the RP. This information, of course, can be considered as privacy. But I think it is the privacy that the users are willing to give to both RP and IdP. Another thought is that IdPs (like Google) tend to control which RPs they would like to cooperate with. They want to know RPs not just to profile the users, but they also want to select which RPs they can provide users information to. This actually make me wonder and doubt if users and IdPs would like to use UPPRESSO.

The second concern is about the novelty of this paper. Although I appreciate the core idea, it sounds somehow similar to existing work, except that none of them proposed to stop RP-based issues and IdP-based issues at the same time. For example, PPID has proposed F(ID_U, ID_RP) but not F(ID_RP, T) and F(PID_U, T).

Beside these two major concerns, I am also worried about the implementation of UPPRESSO. For example, can a malicious RP trick users by letting them download a script that generates specific N_U? Also, the overhead does not look very good: UPPRESSO triples the processing time of MITREid.

Minor issues:
1. In Section V-A, before equation (1), I believe "N_RP" should be "N_U".
2. The reference of Dolev-Yao is not the Dolev-Yao's paper but SPRESSO.

* *

Review #360C

==========
* Updated: 12 Oct 2020 7:11:43pm CEST

Overall Recommendation
---
2. Leaning towards reject

Writing Quality
---
3. Adequate

Reviewer Confidence
---
3. Sufficient confidence

Paper Summary

The paper discusses privacy aspects in SSO systems. The goal is to design a scheme where users canot be linked by relying parties (RPs) and identity providers (IdP) cannot trace logins to different RPs. The authors discuss a scheme, argue security via formal analysis, and give implementations.

Strengths

Touches upon an important problem. In principle does everything correctly: design a scheme, show security, discuss efficiency.

Weaknesses

The paper displays clearly that the authors are not cryptographers. And since this affects also the design of the solution I don't think that one can fix this with major revisions.

Detailed Comments for Authors

I really like the topic and the ideas in your work, but there's a fundamental flaw in the reasoning, and this becomes apparent in the crypto part:

-First, I'm very surprised that you use residue classes over the integers for the discrete log problem, instead of elliptic curves (which are common today). I don't see a reason why you do so.

-Second, the discrete log assumption does not say that computing any information x from g^x is hard; it only says that computing x entirely is infeasible.

-In your analysis, you assume that the modpow function for different exponents and different bases is equivalent (definition 1). While this is true under the DDH assumption the situation here may be different, because the values may be under adversarial control.

-And here's the attack which is not covered by your analysis: RP and RP* pick their ID_RP/RP* in a correlated way, say ID_RP=(ID_RP*)^2. Then they can check that the account numbers at their side as A* = A^2?

In general I found it hard to understand what security guarantees your formal analysis gies. Theorem 1 just says it's secure. The following definitions and the appendix try to given more details, but I couldn't understand exactly what this means cryptographically. The descriptions in Section IV.A, Threat Model, are just too informal.

--- Post rebuttal

I don't think I follow your argument about DL. If you have a generator g of a cyclic group of order q, and pick a random x from ZZ_q, then g^x is just a random element in the group generated by g. This is nothing to do with DL or one-wayness; it's just information-theoretically true.

But my attack still stands: If two RPs know their correlation of ID_RP, then they may be able to correlate logins of the same users. You may want to argue that the ID_RP values are chosen trustworthily by IdP (which IMO is a strong assumption), but then you need to argue along the DDH problem.

You more or less run a DH key exchange protocol with your solution. It would be very surpising if you don't require the according assumption.

* *

Review #360D

==========

* Updated: 14 Oct 2020 2:43:02am CEST

Overall Recommendation

---

3. Major revision

Writing Quality

---

4. Well-written

Reviewer Confidence
---
2. Passable confidence

Paper Summary

This paper discusses the privacy dilemma in SSO and proposes a sound solution. The paper puts forward a fact that a curious IdP and a collusive RP will damage the privacy of users, and it is nontrivial to solve the impact of both on user privacy at the same time. The UPPRESSO proposed in the paper is the first model and system to solve this problem, and its modification of the existing SSO protocol is moderate. The overall impact on efficiency is within an acceptable range.

Strengths

+ Novel idea and discussion of the SSO-privacy dilemma
+ Rigorous method and proof
+ Effective, efficient solutions to practical problems

Weaknesses

Nothing significant:
- Lack of performance comparison from a server perspective
- Compared with the existing SSO, the delay of UPPRESSO proposed in the paper has increased significantly

Detailed Comments for Authors

I think this is an excellent work, and I enjoyed reading it. Overall, this paper proposes a new SSO system that solves a difficult problem in SSO login, and proves the safety and efficiency of the method through mathematical proofs and experiments. It seems to me UPPRESSO significantly improves the privacy properties of SSO protocols.

That said, I have a few questions for the authors to clarify.

- How practical a threat is RP-based identity linkage? If this is not a practical threat, prior works may not have been motivated to solve it. In that case, the motivation for the dilemma focused on in this paper is weakened.

- The paper mainly conducts experiments from the user's point of view, but I want to know whether the load of the SSO server is significantly affected for operating such UPPRESSO?

* *

Review #360E

==========

Overall Recommendation

---

2. Leaning towards reject

Writing Quality

---

2. Needs improvement

Reviewer Confidence

---

2. Passable confidence

Paper Summary

The paper introduces UPPRESSO a SSO system which protects user privacy on multiple fronts. In particular, we want to ensure that the Identity Provider (e.g., Google,Facebook) cannot discover the Relying Parties (websites) associated with a target user. Similarly, even if several Relying Parties collude they should not be able link the user's login requests.

Strengths

The problem of designing a SSO system that protects privacy against both the Identity Provider and colluding Relying Parties is natural and well motivated.

Weaknesses

Proofs are all pushed to the appendix. I had a look at a few of the proofs and they all felt too informal/handwavy to really build confidence that the proofs are correct and the protocol is secure.

No discussion of online attacks e.g., password spraying etc... and how defenses might be integrated with UPPRESSO

Detailed Comments for Authors

The security definitions are quite difficult to parse. For example, Theorem 1 says that UWS is secure, but I was not sure how to even interpret this statement. Is ``secure" formally defined somewhere?

Some of the Lemmas (e.g., Lemma 2) come out of the blue e.g., from the description of the protocol in Figure 3 and Section V it was not clear when the user password is used or how it is handled by the protocol. Then suddenly Lemma 2

Why the specific focus on subgroups of $$Z_p^*$$ of prime order q? Have you considered using elliptic curve groups?

Discrete Log Assumption: It seems likely to me that you would require a stronger assumption than DLOG. Definition 1 (indistinguishability of $$g_1^{n_1}$$ and $$g_2^{n_2}$$) would not necessarily hold in every group where the DLOG problem is hard. Would the Computational Diffie-Hellman or Decisional Diffie Hellman Assumption or some other standard cryptographic assumption suffice? At minimum it seems like the assumption can be justified in Shoup's generic group model.

Given that users often select low-entropy passwords it is crucial to protect them against offline attacks e.g., by locking an account after a few incorrect guesses or requiring the user/attacker to solve a CAPTCHA challenge. I was wondering if privacy/unlinkability makes it harder (impossible?) to achieve rate limit an online attacker. Would traditional defenses (e.g., 3-strikes lockout) integrate with UPPRESSO?

Nits:

Pg 6: the user selects a random number $$N_{RP}$$ (vs $$N_U$$)