How to Own Website Accounts Using Weibo Single Sign-On Vulnerabilities

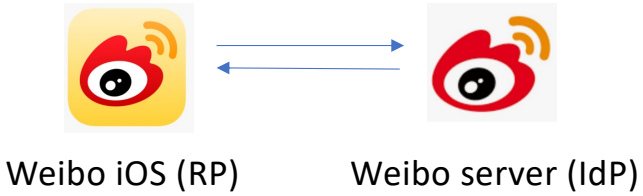
Xin'an Zhou, UC Riverside
Yuhong Nan, Sun Yat-sen University
Zhemin Yang, Fudan University
Min Yang, Fudan University

In-person Short Talk
43rd IEEE Symposium on Security and Privacy

Introduction

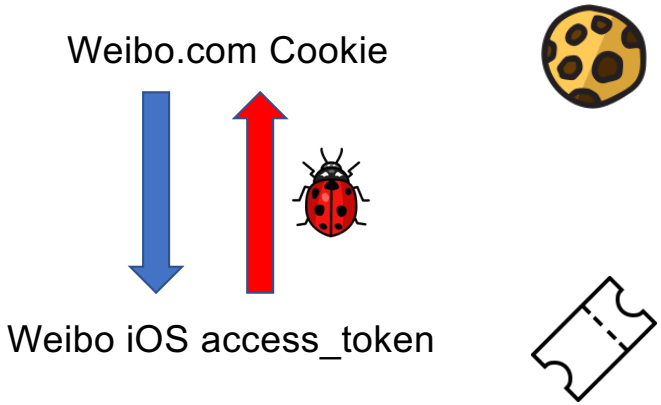
1. Websites are increasingly interconnected with each other.
   - For example, “log into Reddit using your Google account”.
2. Relying on identity providers (IdP) can be both beneficial and risky for a relying party (RP).
3. The security of IdPs' SSO implementations has not been fully studied. We decided to study Weibo, the largest microblogging website in China.

Weibo OAuth 2.0



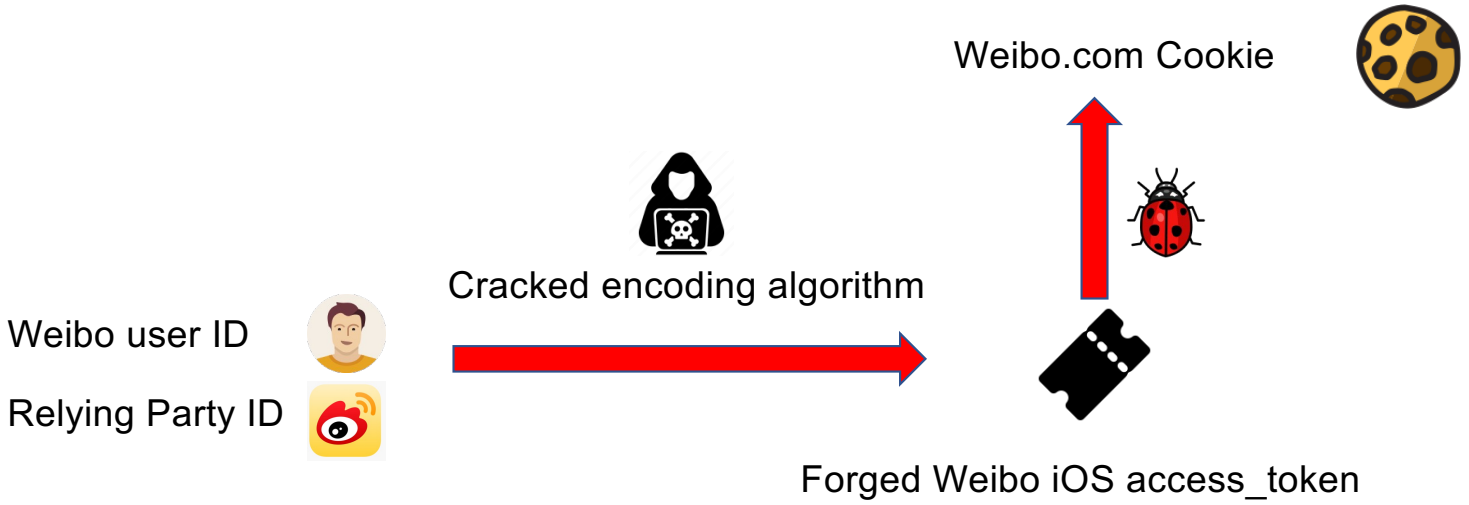
1. Using Weibo OAuth 2.0, a Weibo user can authenticate to other relying parties (RP).
2. Weibo did some ad-hoc modifications to its OAuth 2.0 system.
   - E.g. Weibo iOS client is itself a relying party (RP) with special privileges.
   - E.g. There was an API to exchange Weibo iOS client's access_token for cookies of multiple domains including weibo.com

Weibo OAuth 2.0



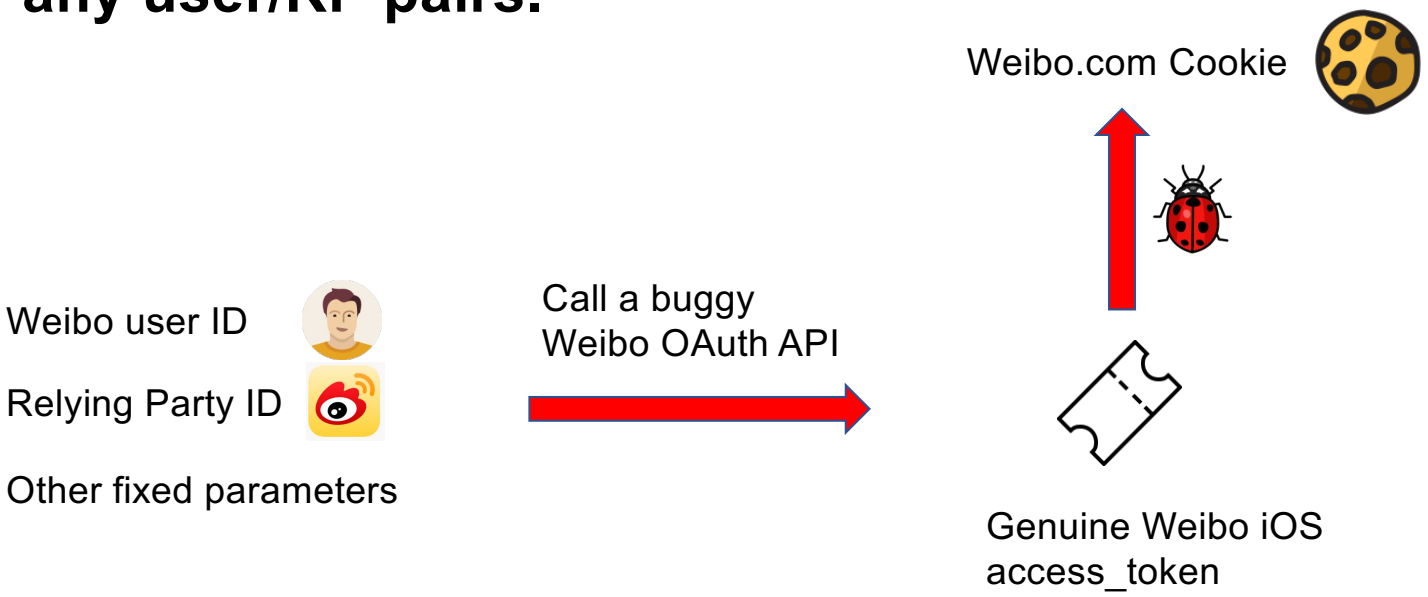
Our findings

1. **A remote attacker could forge Weibo's OAuth 2.0 access token for any user/RP pairs.**



Our findings

2. **A remote attacker could leverage a special combination of HTTP parameters to obtain genuine OAuth 2.0 access tokens for any user/RP pairs.**



Our findings

3. As a result, an attacker could get cookies of weibo.com and spoof any Weibo users.
4. Finally, the attacker could log into any relying parties such as Taobao and Zhihu. Zhihu is the “Chinese equivalent of Quora”, and Taobao is a famous Chinese shopping site. They are with Alexa rankings around 10.

Root Cause of the Vulnerabilities

1. Maintaining access_token states can be costly for large-scale SSO systems, so they might encode user/RP information directly in the access_token to save efforts, using encoding algorithms vulnerable to cryptanalysis.
2. OAuth APIs might be full of logic bugs in the real world because of huge software complexity.
3. Sina Weibo did not design or implement its credential management system in a secure manner.

Conclusions

1. Large-scale SSO systems are hard to design correctly, costly to maintain, may be overwhelmed with logic bugs, and must be handled with extra carefulness.
2. All the bugs have been fixed by Weibo.

Any Questions?
Thank you!