OAuth 2.0 Mix-Up Mitigation: Status and Next Steps

Michael B. Jones

Identity Standards Architect, Microsoft

May 21, 2016

Submission to July 2016 OAuth Security Workshop at University of Trier

1 Introduction

At the OAuth security workshop in Darmstadt, Germany the week of December 14, 2015, several classes of attacks against OAuth 2.0 deployments were described and discussed and mitigations designed. The IdP Mix-Up and Malicious Endpoint Attacks described in “A Comprehensive Formal Security Analysis of OAuth 2.0” [arXiv.1601.01229v2] and “On the security of modern Single Sign-On Protocols: Second-Order Vulnerabilities in OpenID Connect” [arXiv.1508.04324v2] were discussed. Likewise, cut-and-paste attacks, in which some values from a legitimate message are extracted “cut” and then replaced “pasted” into a message constructed by the attacker.

In response to the discussions at the December 2015 workshop and subsequent discussions by the IETF OAuth working group, the “OAuth 2.0 Mix-Up Mitigation” [I-D.ietf-oauth-mix-up-mitigation] specification was developed and adopted by the working group to mitigate these threats.

2 Proposal for July 2016 Workshop Discussions

Should this proposal be accepted, during the workshop I plan to lead a highly interactive discussion among the participants on the status of the mitigations described in the working group specification and the possible next steps for the specification. Topics to be discussed will include:

- Threats mitigated
- Conditions under which these mitigations are and are not needed
- Gathering data on existing implementations and deployments of these mitigations
- Whether there are other threats we also need to mitigate, and if so, how to do so
- Possible next steps for the “OAuth 2.0 Mix-Up Mitigation” specification

3 Capturing the Results of the Workshop Discussions

I plan to capture the important points raised during the discussion among the participants in notes. Those notes and conclusions from the discussions will then be written up in a revised version of this submission, to be published in the workshop proceedings.

4 References

[arXiv.1508.04324v2] Mladenov, V., Mainka, C., and J. Schwenk, "On the security of modern Single Sign-On Protocols: Second-Order Vulnerabilities in OpenID Connect," arXiv 1508.04324v2, January 2016.

[arXiv.1601.01229v2] Fett, D., Küsters, R., and G. Schmitz, "A Comprehensive Formal Security Analysis of OAuth 2.0," arXiv 1601.01229v2, January 2016.

[I-D.ietf-oauth-mix-up-mitigation] Jones, M., Bradley, J., and N. Sakimura, "OAuth 2.0 Mix-Up Mitigation," draft-ietf-oauth-mix-up-mitigation-00 (work in progress), March 2016 (TXT).