COMPUTERS & SECURITY ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements

Giada Sciarretta [a,b,*], *Roberto Carbone* [a], *Silvio Ranise* [a], *Alessandro Armando* [a,c]

[a] *Security & Trust, FBK-ICT, Trento, Italy*
[b] *University of Trento, Italy*
[c] *DIBRIS, University of Genova, Italy*

ARTICLE INFO

Article history:
Available online

Keywords:
Single sign-on
Digital identity
Authentication
Mobile devices
OAuth 2.0

ABSTRACT

While there exist many secure authentication and authorization solutions for web applications, their adaptation in the mobile context is a new and open challenge. In this paper, we argue that the lack of a proper reference model for Single Sign-On (SSO) for mobile native applications drives many social network vendors (acting as Identity Providers) to develop their own mobile solution. However, as the implementation details are not well documented, it is difficult to establish the proper security level of these solutions. We thus provide a rational reconstruction of the Facebook SSO flow, including a comparison with the OAuth 2.0 standard and a security analysis obtained testing the Facebook SSO reconstruction against a set of identified SSO attacks. Based on this analysis, we have modified and generalized the Facebook solution proposing a native SSO abstract model and a related implementation capable of solving the identified vulnerabilities and accommodating any Identity Provider. Finally, we have analyzed the new native SSO solution proposed by the OAuth Working Group, extracted the related abstract model and made a comparison with our proposal.

1. Introduction

Single Sign-On (SSO) protocols are arguably one of the most successful solutions available today. They allow users to access multiple services through a single authentication act carried out with an authentication server acting as an Identity Provider (IdP). By reducing the number of digital identities (and credentials) a user has to deal with, SSO protocols improve at the same time user's experience (usability) and security (e.g., stronger password selection).

While for web applications there exist many secure authentication and authorization solutions to protect the user's digital identities and online resources, this is not the case for mobile applications. Existing protocols, such as OAuth 2.0 (IETF, 2012a) and OpenID Connect (OIDF, 2014a), provide only a partial support for mobile native applications, leaving many implementation details to developers. Leveraging these protocols, many social networks have already deployed their own authentication and authorization solutions, which have been tremendously successful: most Facebook and Google users routinely and transparently use them on their smartphones and

* *Corresponding author.*
E-mail addresses: giada.sciarretta@fbk.eu (G. Sciarretta), carbone@fbk.eu (R. Carbone), ranise@fbk.eu (S. Ranise), armando@fbk.eu (A. Armando).

http://dx.doi.org/10.1016/j.cose.2017.04.011
0167-4048/

tablets. However, the adaptation of protocols originally designed to work in a traditional web scenario, together with the lack of a complete SSO standard for mobile native applications (hereafter native SSO) – the only available solutions we are aware of are draft versions released by the working group NAPPS (OIDF, 2014b) of the OpenID Foundation and the OAuth Working Group (WG) (OAuth Working Group, 2016) – have caused the spread of a number of serious vulnerabilities and attacks. There are many studies in the literature, such as Chen et al. (2014), Shehab and Mohsen (2014) and Wang et al. (2013), which focus on the analysis and description of common vulnerabilities and attacks caused by incorrect implementation assumptions; however – to the best of our knowledge – it remains unclear how to implement native SSO solutions in a secure way.

This paper provides an abstract model which can be used to support the native SSO development. More specifically, we make the following contributions. First, we provide a rational reconstruction of the Facebook native SSO. Second, we give detailed security considerations for the Facebook solution. Third, we propose an abstract model for native SSO solutions inspired by the Facebook native SSO but capable of solving the identified vulnerabilities. The described flow is presented independently from a specific OS and implementation technique. In order to perform a security analysis of our model, we have also identified the security assumptions and the security goals of a native SSO solution, and proved that the specified assumptions are necessary to prevent a violation of the security goals. Finally, by extracting the related abstract model, we present the new native SSO solution proposed by the OAuth WG and make a comparison with our proposal.

An implementation of the proposed model is currently tested by the users of TreC. TreC (acronym for Cartella Clinica del Cittadino, i.e. Citizens' Clinical Record) is a platform[1] developed in the Trentino region (Italy) for managing personal health records. Besides the web platform, which is routinely used by around 63,000 users, TreC is currently designing and implementing a number of native Android applications to support self-management and remote monitoring of chronic conditions. These applications are used in a "living lab" by voluntary chronic patients according to their hospital physicians. An example is the "TreC-Lab: Diario Diabete" app, which is a mobile diary that allows patients to record health data, such as the blood glucose level and physical activity. While in the traditional web scenario, patients access services using their local health care system credentials (leveraging a SAML-based SSO (OASIS, 2005) solution), a solution for native SSO is currently missing. The solution we propose will allow patients to access different TreC e-health mobile applications (and possibly other third-party e-health applications) through a single authentication act.

This paper revises and considerably extends our previous work (Sciarretta et al., 2016) with new material, as detailed below:

- We describe an abstract model for SSO for native applications that is independent from a specific operating system and implementation technique. For the described model, we identify the security assumptions and prove that they are necessary to prevent a violation of the identified security goals.
- We present the latest mechanism released by the different operating systems to support native SSO, the consequent new native SSO solution proposed by the OAuth WG, and a comparison with our solution.

Structure of the paper. In Section 2, we describe the basic notions of a SSO scenario and we give a short overview of the OAuth 2.0 protocol. In Section 3, we detail our rational reconstruction and security analysis of Facebook solution. Together with the description of the flow, we make a comparison with OAuth flows and explain Facebook native SSO security issues. In Section 4, we describe an abstract model for native SSO solution and identify the corresponding security assumptions and security goals. In order to perform a security analysis of our model, we prove that the specified assumptions are necessary to prevent a violation of the identified security goals. We show how the vulnerabilities discovered in Facebook are strictly related to the non-fulfillment of some of the required assumptions (Section 4.2). In Section 5, we describe an implementation of our abstract model with the related security assessment. An alternative native SSO solution proposed by the OAuth WG is analyzed in Section 6. In Section 7, we evaluate the improvements of our solution making a comparison with the analyzed native SSO solutions in terms of the security assumptions presented in Sections 4 and 6. Finally, we describe the related work in Section 8, and we draw our conclusions and discuss future work in Section 9. In addition, the Appendix contains a detailed description of the flow of our native SSO solution.

2. Background

The goal of this section is to provide the basic notions required to clearly understand the rational reconstruction performed on the Facebook native SSO solution. Section 2.1 describes the entities involved and the functional requirements of a SSO process. In Section 2.2, we give an overview of the OAuth 2.0 protocol, used by Facebook to perform the login process.

2.1. *SSO: entities and requirements*

SSO protocols allow users to access multiple services through a single authentication act. The *User* participates in the protocol through a *User Agent* (UA) and authenticates with an *Identity Provider* (IdP) with the purpose of proving her identity to a *Client* entity (C). We assume a SSO solution meets the following two requirements:

(R1) The IdP user credentials can be used to gain access to several Cs. This implies that users do not need to have credentials with a C to access it.

[1] The development of the platform is supported by a joint project between Fondazione Bruno Kessler and Municipality of Trento (Italy). More information is available at https://trec.trentinosalute.net/.

Please cite this article in press as: Giada Sciarretta, Roberto Carbone, Silvio Ranise, Alessandro Armando, Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements, computers & security (2017), doi: 10.1016/j.cose.2017.04.011