Chapter 5

User-Centric Identity Management Architecture Using Credential-Holding Identity Agents

Daisuke Mashima  
Georgia Institute of Technology, USA

David Bauer  
Georgia Institute of Technology, USA

Mustaque Ahamad  
Georgia Institute of Technology, USA

Douglas M. Blough  
Georgia Institute of Technology, USA

ABSTRACT

The pervasive use of digital identities in today’s cyberspace has led to an increasing interest in the area of identity management. Recently proposed user-centric identity management systems have accomplished higher-level of user control over online identity credentials. However, while the lack of a central authority that governs the entire system requires users to be responsible for their own digital identity credentials, the existing user-centric identity management systems still have problems in terms of security, privacy, and system availability. In this chapter, we present an identity management architecture that addresses these problems. Our scheme relies on user-controlled identity agents. Identity agents realize fine-grained control over online identity disclosure by using a minimal-disclosure identity credential scheme and also improve users’ awareness over their credential usage via an identity-usage monitoring system that includes a real-time risk scoring mechanism. A proof-of-concept implementation is shown and evaluated in terms of security, user-centricity, and performance.

DOI: 10.4018/978-1-61350-498-7.ch005
INTRODUCTION

Digital identity credentials such as passwords, tokens and keys are used to ensure that only authorized users are able to access online services. Because of sensitive and valuable information managed by such services, they have become attractive targets of a variety of online attacks. For example, online financial services must use stronger credentials for authentication to avoid fraud. Because of serious threats and widespread theft and misuse of identity credentials, there is considerable interest in the area of identity management, which addresses secure use of identity credentials.

User-centric identity management, which allows users to flexibly choose what identity information is released to other entities in each transaction, offers better control over the use of identity credentials. For instance, users can choose an identity provider that they believe is the most appropriate for each transaction and control identity information to be disclosed to service providers. However, such user-centricity requires that disclosure of identity information be under user control and also expects users to assume more responsibility over their identity usage owing to the absence of a centralized authority (Hansen, 2004). Unfortunately, existing identity management schemes, such as OpenID and Windows CardSpace, have weaknesses against identity theft and misuse. For example, OpenID is susceptible to phishing attacks, and it does not offer effective protection after credentials are compromised. Moreover, at the high level, OpenID and Windows CardSpace heavily rely on online identity providers that issue context-scoped short-term identity credentials and thereby empower users to exercise flexible control over identity information. This fact implies that both schemes suffer from privacy issues because identity providers can potentially infer user’s behavior. Additionally, unavailability of such online identity providers impacts the completion of transactions.

In this context, we propose a new identity management system architecture based on the concept of an identity agent that deals with identity credentials under user control. Identity agents are designed to offload many identity-related tasks from users. Through such identity agents and a minimal-disclosure identity credential scheme (Bauer, 2008), our system allows users to exercise flexible control over identity credential usage without relying on online identity providers. Furthermore, since disclosure of identity credentials is mediated by identity agents, it is possible to implement a user-centric identity usage monitoring mechanism (Mashima, 2008) to improve users’ awareness of the use of their identity credentials, which reduces the risk and damage of online identity theft and misuse. We incorporate such a monitoring system with a real-time risk scoring mechanism into our architecture. In addition, we show how our architecture satisfies properties proposed in The Laws of Identity (Cameron, 2005) and how it addresses general drawbacks of two types of existing identity management schemes, which are credential-focused systems and relationship-focused systems (Bhargav-Spantzel, 2007). Our contribution also includes the implementation of a proof of concept prototype and its evaluation.

This chapter starts with enumerating requirements that our user-centric identity management system should meet and discusses our approach. Then, we discuss our architecture and its key components that address these requirements. After that, we present the prototype implementation of our identity management scheme, followed by its evaluation in terms of security, user-centricity, and performance. Finally, we conclude the chapter with a discussion of future work.

RELATED WORK AND DESIGN GOALS

In this section, we start by reviewing issues and threats against existing user-centric identity