Chapter 6

On Cryptographically Strong Bindings of SAML Assertions to Transport Layer Security

Florian Kohlar
Ruhr University Bochum, Germany

Jörg Schwenk
Ruhr University Bochum, Germany

Meiko Jensen
Ruhr University Bochum, Germany

Sebastian Gajek
Tel Aviv University, Israel

ABSTRACT

In recent research, two approaches to protect SAML based Federated Identity Management (FIM) against man-in-the-middle attacks have been proposed. One approach is to bind the SAML assertion and the SAML artifact to the public key contained in a TLS client certificate. Another approach is to strengthen the Same Origin Policy of the browser by taking into account the security guarantees TLS gives. This work presents a third approach which is of further interest beyond IDM protocols, especially for mobile devices relying heavily on the security offered by web technologies. By binding the SAML assertion to cryptographically derived values of the TLS session that has been agreed upon between client and the service provider, this approach provides anonymity of the (mobile) browser while allowing Relying Party and Identity Provider to detect the presence of a man-in-the-middle attack.

DOI: 10.4018/978-1-4666-2163-3.ch006
INTRODUCTION

In browser-based Federated Identity Management (FIM) protocols, data has to be transported from a trusted third party to the service provider with an intermediate step at the browser. The trusted third party—called Identity Provider (IP)—is asked to issue a security token that is valid for a fixed time period and permits access to some service (hosted by a service provider, in this context called Relying Party (RP)). This token is first transmitted to the browser and in a following step transferred to the RP. Data stored in the browser is susceptible to attacks on the Same Origin Policy (SOP) of the browser, like Cross Site Scripting (XSS) or dynamic pharming. Mobile devices are especially vulnerable, since all data sent or received by the device is transmitted “over the Air” and can therefore be easily sniffed. Since the SOP relies on the Domain Name System (DNS), the data can also be accessed by a variety of spoofing attacks, from ARP and IP spoofing to DNS spoofing (Pharming). This even applies if sophisticated security measures are in place (e.g., see the latest attack on Microsoft’s, Cardspace, Gajek, Schwenk, & Chen, 2008). Mobile Browsers (Figure 1) in general often lack the latest patches/updates and still contain known and easily exploitable security holes. To protect these devices special security measurements are needed.

Two approaches have been proposed for SAML based Federated Identity Management to counter these attack threats. The first approach is to bind the SAML assertion and the SAML artifact to the TLS client’s certificate public key. It was proposed in Gajek (2008) and Gajek, Jager, Manulis, and Schwenk (2008) and has already been adapted for standardization (Klingenstein, 2009). The other approach is to combine the security of TLS with the browser’s Same Origin Policy (Gajek, Liao, & Schwenk, 2008). In this paper, we present a third approach which further enhances IDM protocols: We bind the SAML assertion to the TLS session that has been agreed upon between client and Relying Party (RP) and as a result rely on the user authentication. Furthermore do we achieve security even in the case, when an adversary is able to impersonate the RP by presenting a valid (e.g., self signed), but different, certificate for the requested RP to the browser. We do so by including the public key as part of the SAML assertion.

(MOBILE) BROWSER-BASED FEDERATED IDENTITY MANAGEMENT PROTOCOLS

The (mobile) browser plays an important role in Federated Identity Management (FIM) standards/frameworks like Liberty Alliance (Pfitzmann & Waidner, 2003), SAML (OASIS Security Services (SAML) TC) or Microsoft Cardspace (Gajek, Schwenk, & Chen, 2008). This is due to the fact that he can be used as a platform-independent client application with a (commonly) rich set of features, and a provably secure cryptographic functionality: SSL/TLS (Dierks & Allen, 1999, Dierks & Rescorla, 2006). Protocols realizable within the constraints of standard web browsers