Abstract

Single Sign-On (SSO) is a simplified approach which relieves users from the burden of dealing with multiple credentials but at the same time presents new security challenges. With three different parties participating in the authentication process, SSO solutions involve different layers of communication and exchange of credentials that are enabled by using HTTP redirection and JavaScript, which creates several vulnerabilities for attackers to exploit and makes SSO a launch pad for typical attacks. A formal method is needed to evaluate the flaws in the SSO protocol implementation. The security service Availability is important to ensure that the information concerned is readily accessible to the authorized persons; here the problem of Violation of Availability in SSO is addressed. This work WSASRESSO provides a framework which evaluates SAML based SSO protocols using Burp suite extension with a combination of EsPReSSO algorithm for identification of the SSO protocols along with SAML Raider for fetching the protocol infrastructure details and integration of WS-Attacker to perform black box penetration testing. Since new types of SSO attacks are evolving over time, the proposed
security framework can be used to find the strength of the SSO protocols. Here, signature
based attacks like XML Signature Wrapping and XML Signature Faking attacks have been
simulated and tested which can be categorized under Phishing attacks.

References

Recognition, Processing and Attacking of Single Sign-On Protocols with Burp Suite,” Open
Identity Summit, 2015.
2. Yuchen Zhou, David Evans, “SSOScan: Automated Testing of Web Applications for
3. R. Wang, S. Chen and X. Wang, “Signing Me onto Your Accounts through Facebook and
Penetration Testing on Web Services," IEEE 20th International Conference on Web Services
(ICWS), 2013, pp.491,498.
7. E. A. N. Sakimura, J. Bradley (2014), OpenID Connect Core 1.0 incorporating errata set
1, OpenID Foundation OpenID Connect 1.0. Available:
http://openid.net/specs/openid-connect-core-1_0.html.s
and Schwenk, Jörg, "Your Software at my Service: Security Analysis of SaaS Single Sign-On
9. S. Gajek, M. Jensen, L. Liao, and J. Schwenk, "Analysis of signature wrapping attacks
Connect,”.
Assertion Markup Language (SAML) V2.0," Mar. Available:
http://docs.oasis-open.org/security/saml/v2.0/.
Infrastructure: Definition and Application to the BrowserID SSO System," IEEE Computer
18. OpenID - A Descriptive Document, Available:
http://openid.net/get-an-openid/what-is-openid.

Index Terms

Computer Science  Software Engineering

Keywords