PrOfESSOS: Automated OpenID Connect Security Assessment

Christian Mainka, Vladislav Mladenov, Tobias Wich

Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

Abstract

OAuth is the new de facto standard for delegating authorization in the web. An important limitation of OAuth is the fact that it was designed for authorization and not for authentication. The usage of OAuth for authentication thus leads to serious vulnerabilities as shown by Zhou et. al. in [1] and Chen et. al. in [2].

OpenID Connect was created on top of OAuth to fill this gap by providing federated identity management and user authentication. OpenID Connect was standardized in February 2014, but leading companies like Google, Microsoft, AOL and PayPal are already using it in their web applications.

As part of our current research we provided the first in-depth analysis of OpenID Connect [3] where we categorized all attacks in five different classes: Malicious Endpoint Attacks, ID Spoofing, Signature Bypass, Session Overwriting, Trivial Attacks.

For the assessment of OpenID Connect service providers (SP), a fully-automated penetration testing tool, PrOfESSOS, has been developed. The Java based tool is controlled via a webinterface and is capable of performing tests on multiple SPs in parallel, so that it can be offered as a service. The availability of a test service greatly reduces the efforts needed to set up a working test environment to a level where performing a test run can be done in a very short time and does not require the tester to be a security expert. All tests have a specification which both documents and parameterizes the implementation it references.

In this presentation we will explain the architecture of PrOfESSOS, show how new tests are specified and implemented, and talk about the current status as well as our future plans. We will also discuss possibilities to integrate the tool into Continuous Integration Systems and the use in security centric certifications.

[1] D. E. Yuchen Zhou. Automated Testing of Web Applications for Single Sign-On Vulnerabilities. In *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA, Aug. 2014. USENIX Association. URL https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/zhou.

[2] E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystied for Mobile Application Developers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. ACM - Association for Computing Machinery, November 2014. URL http://research.microsoft.com/apps/pubs/default.aspx?id=231728.

[3] C. Mainka, V. Mladenov, and T. Wich. Systematically Breaking and Fixing OpenID Connect. In AppSec Europe 2016, Rome, Italy, Jul. 2016. OWASP Foundation.