Single Sign-On Sicherheit: OAuth & OpenID Connect

IT-Sicherheit Schulung

Schulungsinhalte

(2 TAGE)

Single Sign-On (SSO) Verfahren gehören zu den wichtigsten Internet-Technologien und werden von vielen Applikationen eingesetzt. Sie ermöglichen es die Registrierung und das Login für Benutzer möglichst einfach zu gestalten und Applikationen an soziale Netzwerke anzubinden. SSO basierend auf OAuth und OpenID Connect hat sich heutzutage als Standard etabliert. In den letzten Jahren wurden allerdings aufgrund von Implementierungsfehlern und Fehlern in den zugrundeliegenden Standards schwerwiegende Angriffe entdeckt. Die Angriffe nutzen die Komplexität der eingesetzten Standards aus und ermöglichen es Angreifern sich als beliebiger Benutzer zu authentisieren oder auf vertrauliche Daten der Benutzer zuzugreifen. Hierbei können die Daten ausgelesen, manipuliert oder gelöscht werden.

Durch die kritische Funktion, die SSO Verfahren bei dem Betrieb einer Applikation übernehmen, ist es wichtig, die Probleme dieser Technologien im Detail zu verstehen und zu adressieren. In der Schulung werden unter anderem die nachfolgenden Fragen beantwortet:

- Wann sollte OAuth verwenden werden, wann OpenID Connect?
- Worin unterscheiden sich die verschiedenen OpenID Connect Flows?
- Welche Angriffe auf SSO Flows gibt es; wie kann man sie verhindern?

Auf Wunsch ist es möglich diese Schulung durch weitere Details oder die Berücksichtigung von SAML auf 3 Tage zu erweitern.

Voraussetzungen

Diese Schulung richtet sich an zwei Gruppen: Einerseits an Entwickler, die Single Sign-On Verfahren basierend auf OAuth und OpenID Connect praktisch einsetzen; andererseits an Penetrationstester und Sicherheitsforscher, die sich mit den Standards OAuth und OpenID Connect vertraut machen und Applikationen, die entsprechende Single Sign-On Verfahren einsetzen, evaluieren möchten.

TAG 1

- Einführung in Single Sign-On
- OAuth und OpenID Connect Flows
  - Code Flow
  - Implicit Flow
  - Hybrid Flow
- Generische Angriffe auf SSO Verfahren
  - XSS, Clickjacking, CSRF, Open/Covert Redirects
- Erste OAuth und OpenID Connect spezifische Angriffe

TAG 2

- ID Token
  - Details & Angriffe
- Single-Phase Angriffe
  - ID Spoofing Angriffe
  - Signature Bypasses
- Cross-Phase Angriffe
  - Issuer Confusion
  - Malicious Endpoint Angriffe
  - IdP Confusion
- Weitere Technologien
  - Device Flow, Native Apps & PKCE
- Secure Token Bindings
  - Mutual TLS
  - Holder-of-Key

Dozent

Dr. Christian Mainka

Christian Mainka hat 2017 über die Themen Webservices und Single Sign-On promoviert. Er ist Mitgründer von Hackmanit und beschäftigt sich seit 2009 mit Sicherheitsaspekten die durch den Einsatz von Datenbeschreibungssprachen wie XML entstehen. Er hat das erste Webservice-spezifische Penetrationstest Tool „WS-Attacker“ entwickelt. Seitdem verbessert und erweitert er das Programm stetig, so dass es mittlerweile ein breites Spektrum der bekannten Angriffe auf Webservices vollautomatisch abdecken kann. In seiner Dissertation „On Message-Level Security“ analysiert er zudem die Sicherheit moderner Single Sign-On Verfahren wie SAML, OAuth und OpenID Connect und deckte zahlreiche Sicherheitslücken auf.

Kontakt

christian.mainka@hackmanit.de
www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum