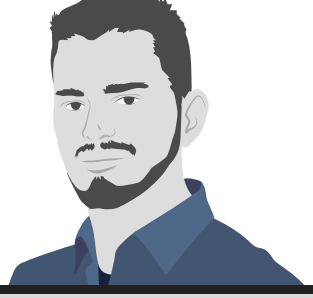
Single Sign-On Security: SAML

IT-Security Training



Training Contents

(2 DAYS)

Single Sign-On (SSO) procedures are one of the most important Internet technologies and are used by many applications. They allow to design the registration and login process as easy as possible for users and enable applications to be connected to social networks. The use of SAML-based SSO procedures is widespread. However, SSO procedures have become the target of serious attacks due to implementation flaws and flaws in the underlying standards in recent years. These attacks exploit the complexity of the underlying standards and enable attackers to authenticate themselves as arbitrary users or to access confidential user data. In this way, the data can be read, manipulated or deleted.

Due to the crucial role that single sign-on procedures fulfill in an application, it is essential to understand and address the problems of these technologies in detail. The training will address the following questions, among others:

- How do I use an XML parser correctly?
- Which types of XML signatures are available for different use cases?
- How do I validate a SAML message securely?
- How can I protect my service or identity provider from well-known attacks?

Requirements

This training is designed for two groups: For developers who practically use XML and SAML-based Single Sign-On procedures. Further on, penetration testers and security researchers who want to learn how to evaluate the security of SAML-based Single Sign-On procedures are addressed.

DAY 1

- Introduction
  - XML and SOAP-based Web Services
  - XML Parsing (DOM vs. SAX)
  - XML Schema
- Document Type Definition
  - XML (External) Entity Attacks
- XML-specific Denial-of-Service Attacks
- XSLT
- XML Signature
  - ID- and XPath-based XML Signatures

DAY 2

- SAML-based Single Sign-On
- Attacks on SAML Service Provider
  - Replay Attacks
  - Signature Exclusion
  - XML Signature Wrapping (XSW)
  - Certificate Faking and Injection Attacks
  - Covert Redirect Attacks
- Attacks on SAML Identity Provider
- SAML Secure Bindings
- Apply the knowledge you have acquired to your own applications

Lecturer

Dr. Christian Mainka

Christian Mainka received his doctorate in 2017 with a thesis on web services and single sign-on. He is the co-founder of Hackmanit and since 2009 he has been dealing with security aspects in the context of data description languages, such as XML. He developed the first web service-specific penetration testing tool "WS-Attacker". Since then he has continuously improved and expanded the tool, such that it can be used to automatically survey a broad spectrum of known attacks on web services. In his dissertation, "On Message-Level Security" he analyzes the security of modern single sign-on systems such as SAML, OAuth and OpenID Connect and discovered numerous security vulnerabilities.

Contact

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

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum
Germany