Informatik Forum Stuttgart

bwcon

infos-Kolloquium in Kooperation mit bwcon

Formale Sicherheitsanalyse und Angriffe auf die OpenID Financial-grade API

Mittwoch, 14. November 2018, 17:30 Uhr
Informatikgebäude, Hörsaal 38.02

Universitätsstraße 38
70569 Stuttgart

Durch die Payment Service Directive 2 wurde auf europäischer Ebene festgelegt, dass es ab September 2019 Drittanbietern ermöglicht werden soll, Dienstleistungen von Kreditinstituten zu nutzen. Dadurch können FinTech Unternehmen mithilfe von APIs auf Daten eines Bankkunden zugreifen und diesem etwa per App komfortable neue Dienste anbieten. Die OpenID Financial-grade API (FAPI) bietet ein Verfahren für den Zugriff auf Daten und Ressourcen für u.a. derartige Finanzanwendungen. Basierend auf dem OAuth 2.0 Authorization Framework zielt die FAPI darauf ab, Sicherheit trotz bestimmter erfolgreicher Angriffe auf die Infrastruktur, von denen in solch einem Kontext auszugehen ist, zu gewährleisten.

Als Teil unserer Forschungsarbeit im Bereich der Websicherheit haben wir die FAPI auf Basis eines am Institut für Informationssicherheit entwickelten Modells der Webinfrastruktur analysiert.

Durch unsere formale Analyse haben wir mehrere Angriffe entdeckt, die trotz der komplexen Sicherheitsmaßnahmen einem Angreifer Zugriff auf Ressourcen eines Bankkunden geben können, etwa um unerlaubt Überweisungen im Namen des Bankkunden zu tätigen. Zur Verhinderung dieser Angriffe haben wir Gegenmaßnahmen vorgeschlagen und gezeigt, dass die modifizierten Verfahren sicher im Sinne unserer Sicherheitsdefinitionen sind. Wir stehen im engen Kontakt mit der OpenID Foundation, die für die Standardisierung der FAPI zuständig ist.

Im Rahmen des Vortrags werden die Grundlagen der Financial-grade API zusammen mit ausgewählten Aspekten der formalen Analyse vorgestellt. Des Weiteren werden die gefundenen Angriffsszenarien sowie die entwickelten Gegenmaßnahmen erläutert.

Prof. Dr. **Ralf Küsters** ist Leiter des Instituts für Informationssicherheit der Universität Stuttgart.
Vor seiner Zeit in Stuttgart hat er vor allem an der Uni Kiel, der Stanford University, der ETH Zürich sowie der Uni Trier gelehrt und geforscht.

Um Anmeldung bis spätestens 12.11.2018 wird gebeten:
https://infosev.informatik.uni-stuttgart.de/reg/register.php