TechInf
Institut für Technische Informatik

RI CODE Research Institute Cyber Defence
Universität der Bundeswehr München

Lehrstuhl für Kommunikationssysteme und Netzsicherheit

Zentrales Level of Assurance Management in Föderationen

Form der Arbeit: MA
Sprache: Deutsch/Englisch
Themenschwerpunkt: Identitätsmanagement

Zusammenfassung:

Im Rahmen des föderierten Identitätsmanagement ist es Nutzern möglich Dienste von anderen Organisationen zu nutzen. Die Benutzerinformationen liegen bei der Heimatorganisation, auch Identity Provider (IDP) genannt. Die Organisation, die den Dienst bereitstellt, wird als Service Provider (SP) bezeichnet. SPs benötigen, neben einer erfolgreichen Authentifizierung, bestimmte Benutzerinformationen, damit ihr Dienst funktioniert. Diese Informationen werden über ein vorher festgelegtes Protokoll ausgetauscht. Zusätzlich können weitere Benutzerinformationen über eine unabhängige Organisation, Attribute Authority genannt, abgefragt werden.

Eine mögliche zusätzliche Information ist die Verlässlichkeit von IDPs. Aktuelle Föderationen haben ihre eigenen Verlässlichkeitsklassen, auch Level of Assurance (LoA) genannt. Zudem existieren verschiedene Normen zu LoA, beispielsweise von NIST. Die meisten Föderationen und IDPs erreichen einen niedrigen Level, was für einen Großteil der Dienste, wie foodle, ausreicht. Gleichzeitig gibt es wenige Dienste, die höhere Ansprüche haben. Beispielsweise muss für diese Dienste die Authentifizierung des Nutzers sicherer sein als für einfache Webdienste. Eine weitere mögliche Anforderung ist die Dokumentation und eine erfolgreiche Auditierung.

Damit nicht eine gesamte Föderation mit ihren IDPs einen höheren Level erreichen muss für wenige Nutzer, ist es effizienter, dies auf diejenigen IDPs oder gar Nutzer beschränkt ist, die unbedingt diese Ansprüche erfüllen müssen.

Aufgaben für die Themenbearbeitung:

In der Arbeit soll die Möglichkeit eines zentralen LoA-Managements für Föderationen untersucht werden. In einem ersten Schritt sollen dazu unterschiedlichen bereits existierenden LoA analysiert werden. Dadurch soll die Differenz zwischen den unterschiedlichen Levels ersichtlich sein. Zudem lässt sich dadurch analysieren, wie viele SPs ein höheres Level benötigen.

Im zweiten Schritt soll ein zentrales, allgemein gültiges Management-Tool konzipiert werden. Hierbei sind nötige Rollen, Workflows und die technische Einbindung (z.B. als Attribute Authority) in den üblichen SAML-Workflow zu beachten. Ferner gilt es die Unterschiede in den verschiedenen LoA zu bedenken. Schlussendlich soll eine prototypische Implementierung die Machbarkeit eines zentralen LoA-Management-Tools zeigen.

Voraussetzungen für die Bearbeitung:

Hilfreich für einen schnellen Einstieg in die Thematik, aber nicht zwingend erforderlich sind Vorkenntnisse in diesen Bereichen: IT-Sicherheit, Identitätsmanagement, Programmieren

Betreuende Person:

Bei Interesse am ausgeschriebenen Thema, nehmen Sie bitte Kontakt auf mit:

Dr. Daniela Pöhn (UniBw-M), E-Mail: daniela.poehn@unibw.de, Tel 089-6004-7313