TechInf
Institut für Technische Informatik

RI CODE Research Institute Cyber Defence
Universität der Bundeswehr München

Lehrstuhl für Kommunikationssysteme und Netzsicherheit

Konzeption eines verteilten Identitätsmanagements

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

Zusammenfassung:

Damit ein Nutzer einen Dienst einer anderen Organisation nutzen kann, werden über föderiertes Identitätsmanagement Benutzerinformationen von der Heimatorganisation des Nutzers zum Dienstbetreiber übertragen. Die Heimatorganisation des Nutzers wird auch Identity Provider (IDP) genannt, während der Dienstbetreiber Service Provider (SP) heißt. Der Informationsaustausch ist über ein vorher festgelegtes Protokoll geregelt, welches entweder SAML oder OAuth (OpenID Connect) ist. Die Provider können jeweils über sogenannte EntityIDs eindeutig identifiziert werden.

Im Hochschulumfeld wird überwiegend SAML eingesetzt. Auch wenn SAML keine festen, nationalen Föderationen vorschreibt, die vorab die Metadaten der teilnehmenden Organisationen aggregieren und austauschen, ist dies Realität. Über sogenannte Lokalisierungsdienste wird auf Grund der aggregierten Metadaten und der Nutzerauswahl der zugehörige IDP des Nutzers herausgefunden. Sind IDP und SP nicht Teil einer Föderation, kann der Nutzer nicht ohne Probleme den Dienst in Anspruch nehmen.
Im Gegensatz dazu sind Peer-to-Peer-Netzwerke oder Blockchains dezentral ausgerichtet, wodurch Metadaten direkt zwischen IDP und SP ausgetauscht werden können.

Aufgaben für die Themenbearbeitung:

In der Arbeit soll Identitätsmanagement auf Basis eines verteilten Protokolls, wie Peer-to-Peer-Nachrichten-Protokolls (z.B. Bitmessage), konzipiert werden. Dazu ist im ersten Schritt eine Analyse und Vergleich existierender Ansätze notwendig.
Im zweiten Schritt soll ein verteiltes Identitätsmanagement am Beispiel eines geeigneten Protokolls konzipiert werden. Dabei soll darauf geachtet werden, den für Benutzer bekannten Authorisierungsablauf nicht weiter zu verkomplizieren. Dazu wird im Fall von P2P mindestens eine geeignete Methode zum Abbilden der P2P-spezifischen Adressen zu EntityIDs benötigt. Ferner sollen mögliche Latenzen betrachtet werden.
Schlussendlich soll eine prototypische Implementierung als Proof-of-Concept den Metadaten- und Nachrichtenaustausch zeigen. Dazu können zum Beispiel PySAML2 und Bitmessage verwendet werden.

Voraussetzungen für die Bearbeitung:

Hilfreich für einen schnellen Einstieg in die Thematik, aber nicht zwingend erforderlich sind Vorkenntnisse in diesen Bereichen: Rechnernetze, 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