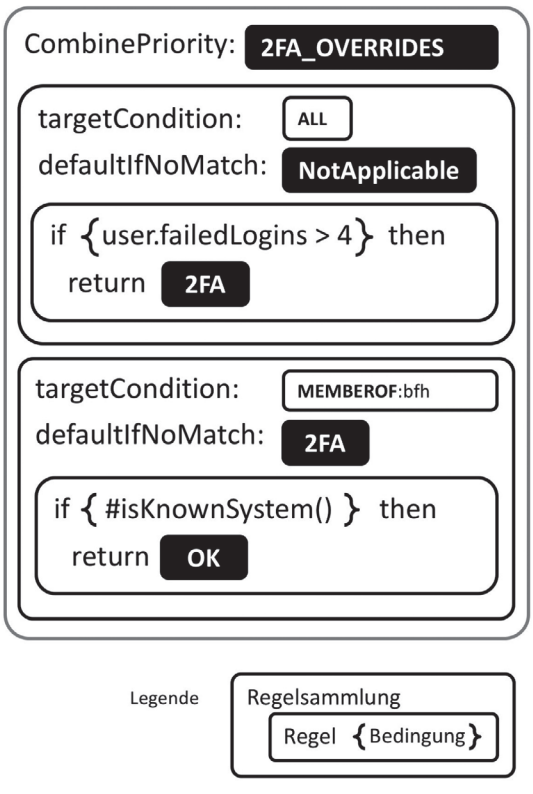
CASA / Context-Aware Strong Authentication

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Dr. Kai Brünnler
Experte: Jean-Marie Leclerc (Sword Group)
Industriepartner: Swisscom AG

Zwei-Faktor-Authentifizierung (2FA) hat in den letzten Jahren an Bedeutung zugenommen. Ein zweiter Faktor erhöht die Sicherheit aber auch den Aufwand für den Benutzer. Mit CASA wird während dem Login evaluiert, ob sich der Benutzer mit einem zweiten Faktor authentisieren muss oder ob die definierte Policy dies nicht erfordert.

Zweit-Faktor erforderlich?

Internetdienste, die beim Login zweit Faktor unterstützen, bieten oft nur die Möglichkeit den zusätzlichen Faktor immer oder nie zu verwenden. CASA prüft die Benutzer- und Metadaten gemäss definierter Policy und ist somit eine Erweiterung für bestehende Authentisierung-Systeme. Der Rückgabewert ist eine Empfehlung, ob ein Zweit-Faktor angefordert werden soll oder dies nicht erforderlich ist. Die Entscheidung eine 2FA zu verlangen bleibt beim Authentisierung-System.
Die vier Rückgabewerte:
- Indeterminate – Fehler bei der Auswertung
- 2FA – 2FA erforderlich
- OK – Kein 2FA notwendig
- NotApplicable – Trifft nicht zu



Beispiel CASA Policy

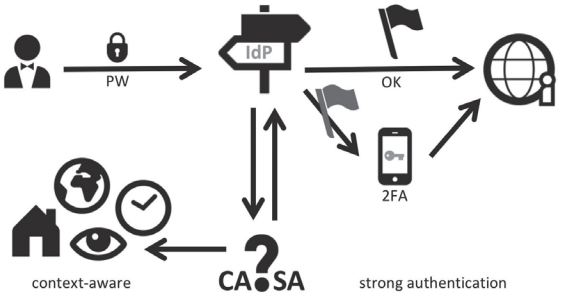
Policy

Die Policy bestimmt wann ein Benutzer eine 2FA benötigt. Sie wird mit folgender Sprache definiert: Eine CASA Policy besteht aus mehreren Regelsammlungen und einer Strategie (CombinePriority), die definiert ob der Rückgabewert OK oder 2FA dominiert. Eine Regelsammlung besteht aus der Zielgruppe (TargetCondition), einem Rückgabewert falls keine Regel zutrifft (DefaultIfNoMatch) und Regeln. Jede Regel hat eine Bedingung und einen Rückgabewert falls die Bedingung stimmt.

Eine Regel trifft entweder zu oder nicht (true/false). Die Bedingung wird mit Spring Expression Language ausgewertet, dies erlaubt die Verwendung von Operatoren und CASA Funktionen.
Beispiele für Regel Bedingungen:
- context.app == 'is-academia'
- user.failedLogins > 3
- #isKnownSystem()
- #isIPinRange('195.186.19.0/28','2001:0db8::/32')

Architektur

CASA ist in Java programmiert und modular aufgebaut. Das API Modul ist die Schnittstelle zwischen dem Authentisierung-Systeme und CASA. Das Service Modul lädt die Policy und verarbeitet die Anfragen. Das Core Modul enthält die Logik zur Prüfung der Policy und kann auch als eigenständige Bibliothek verwendet werden.



Andreas Stoller
stola3@mailbox.org