Thema Bachelor / Master / Projektarbeit
Two Factor Authentication (2FA)

Das Problem

Aufgrund vieler Sicherheitseinbrüche in Websites einerseits und der zunehmenden Bedeutung einzelner Websites andererseits (Bsp: Facebook, Google, Banking uvm.) werden zunehmend Two Factor Authentication (2FA) Technologien in Webdiensten eingesetzt. In praktischen Anwendungen entstehen dabei aber zusätzliche Probleme.

Bequemlichkeit des Anwenders: Siehe etwa https://en.wikipedia.org/wiki/Multi-factor_authentication über die Probleme des Mobiltelefons als 2FA.

Recovery: Während bei Passwörtern das Recovery des authentisierenden Faktors meist relativ einfach ist (etwa: Zusenden eines Reset-Links an eine Email Adresse), ist das Recovery weiterer Faktoren eher umständlich, da es grundsätzlich unmöglich ist (etwa: nach Diebstahl eines biometrischen Signals), Kosten erzeugt (etwa: Verlust eines Photo-Tan Geräts) oder einen separaten, sicher authentisierbaren Kanal benötigt, der ja gerade durch den Verlust eines Faktors abhanden gekommen ist (etwa: nach Neuinstallation eines Mobiltelefons ist die Konfiguration der 2FA App verloren gegangen).

Initiales Deployment: Wie setzt man eine sichere, auf mindestens zwei Faktoren beruhende Authentisierung über das Netz auf, wenn man vom Benutzer noch überhaupt keine Daten hat. (Lösung etwa: Post Ident, ist aber nur 1FA).

Pseudonyme 2FA: Wie etabliert man eine die Privatheit erhaltende 2FA, etwa für ein Pseudonym, das nicht mit einer realen Identität gekoppelt sein soll?

Context-Bindung: Die Illustration dieses Problems soll anhand eines Beispiels erfolgen. Eine Telebanking Anwendung nutzt 2FA in der folgenden Weise: Nachdem der Nutzer auf der Webseite seine UserId und sein Passwort eingegeben hat, erhält er für die Bestätigung jeder Transaktion auf das Handy eine weitere PIN per SMS, die er einzugeben hat. Ein möglicher Angriff ist nun dieser: Eine böswillige Software-Komponente auf dem Browser sendet modifizierte Transaktionsdaten (etwa veränderte Überweisungsbeträge) an den Server. Dieser Angriff kann beispielsweise unterbunden werden, wenn die SMS auch die Context-Daten enthält (also im Beispiel den Überweisungsbetrag, den der Benutzer dann überprüft).

Mögliche Aufgabenstellungen

Je nach Art der Arbeit (Bachelor, Master, Projekt), nach Interesse und Vorbildung des Bearbeiters sollen im Rahmen dieser Arbeit einige der folgenden Fragen beantwortet werden. Eine Bearbeitung von verbundenen Themen durch ein Team ist ebenso denkbar. Die genaue Fragestellung definieren wir in der Vorbesprechung.

In dieser Arbeit soll ein Katalog an **(1) Sicherheits- und (2) Bequemlichkeitskriterien** für 2FA aufgestellt werden und **(3) mit typischen Web Use Cases** verknüpft werden (Telebanking, social networking und Egovernment Anwendungen haben völlig verschiedene Anforderungen an Identität). Anschließend sollen bestehende 2FA Techniken von Identitätsprovidern und von großen Websites, welche 2FA oder Identitätsprovider nutzen in diesem Katalog **(4) klassifiziert** werden. Schließlich soll **(5) eine Übersicht** über standardisierte und offene Protokolle und Frameworks gegeben werden (wie etwa OAuth oder Passport).

Ansprechpartner: Prof. Clemens Cap