Sicherer Formularservice

Fachgebiet: IT-Security
Betreuer: Prof. Gerhard Hassenstein, Prof. Dr. Annett Laube-Rosenpflanzer
Experte: Dr. Igor Metz (Glue Software Engineering AG)

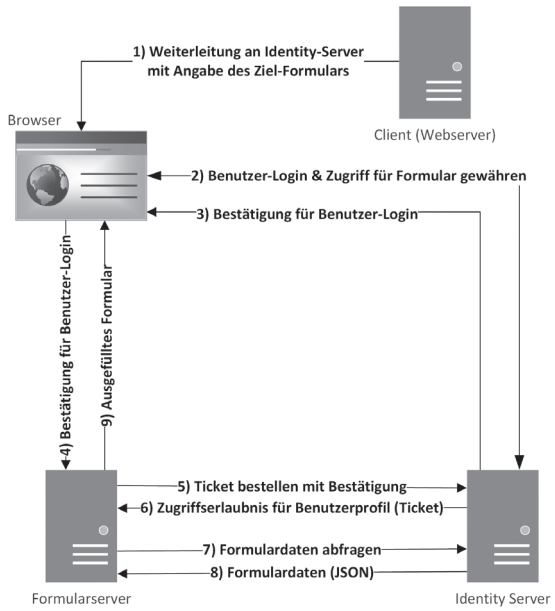
Automatisierte Formulare boomen – auch bei Gemeinden. Die Datenfelder werden nach erfolgter Anmeldung mit bereits bekannten Daten ausgefüllt. Der Benutzer muss nur noch deren Richtigkeit bestätigen und das Formular abschicken. Die Formulare werden meistens von Drittfirmen als Dienstleistung angeboten. Da teilweise grosse Sicherheitsmängel vorhanden sind, zeigt diese Arbeit anhand eines Konzepts und eines Prototyps wie ein sicherer Formularservice aussehen könnte.

Ausgangslage

Viele produktiv eingesetzte Formularservices beinhalten Sicherheitsmängel im Umgang mit den Benutzerdaten. Sei es, dass Formulare ohne Zustimmung des Benutzers mit dessen Daten ausgefüllt werden könnten oder aber schützenswerten Daten unverschlüsselt übertragen werden.

Ziele

Das Ziel dieser Arbeit war das Erarbeiten einer technologischen Architektur für einen – im Gesamtsystem betrachtet – sicheren Formularservice, eine Umsetzung dieser Architektur in einem Prototyp mit OAuth 2.0 und OpenID Connect, damit auch mobile Anwendungen umgesetzt werden können und die Erarbeitung einer Sicherheitsanalyse der umgesetzten Lösung. Von grosser Wichtigkeit war ausserdem, dass der Webauftritt einer Gemeinde, bzw. Firma nur geringfügig angepasst werden muss.



Vereinfachte Konzeptlösung für einen sicheren Formularservice

Konzeptarchitektur

Der Benutzer muss sich einmal bei einem Identity-Server registrieren. Die im Benutzerprofil gespeicherten Daten, kann der Benutzer jederzeit anpassen und auch wieder löschen.

Bei einem Klick auf einen Formularlink auf einer Webseite ruft der Webserver nicht direkt den Formularserver auf, sondern schickt den Browser erst zum Identity-Server. Dieser prüft, ob der Webserver das gewünschte Formular aufrufen darf und zeigt danach einen Login-Dialog an. Bei erfolgreichem Login muss der Benutzer nun über den Browser den Zugriff auf sein Profil für das Formular genehmigen. Nachdem der Identity-Server die Genehmigung bekommt hat, schickt er eine Bestätigung an den Browser, der diese umgehend an den Formularserver weiterleitet. Mit dieser Genehmigung ist der Formularserver einmalig berechtigt, sich ein «Ticket» ausstellen zu lassen. Dabei werden weitere Parameter übermittelt, die der Browser nicht kennt. Das «Ticket» ermächtigt den Formularserver schliesslich zum Zugriff auf die Profildaten beim Identity-Server, die er nutzt um das Formular automatisch auszufüllen. Alle Nachrichten werden über eine verschlüsselte Verbindung übertragen.

Über zwei Parameter im Formularlink werden die benötigten Zugriffsrechte und die Auswahl der kundenspezifischen Formularvorlage gesteuert.

Fazit

Die Lösungsarchitektur und der Prototyp zeigen, dass mit OAuth 2.0 und OpenID Connect sichere Formularservices implementiert werden können. Allerdings zeigte sich bei der Umsetzung auch, dass die erhältlichen Open-Source-Implementierungen von Identity-Servern derzeit noch diverse Mängel in der Umsetzung und Implementierung des OpenID-Connect-Standards haben und somit ein produktiver Einsatz leider noch nicht möglich ist.

Christian Brodbeck
christian.brodbeck@gmx.ch

Florian Buschor
info@florianbuschor.ch