Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	Conducting Expert Studies to Measure API Design Influence on Secure Password Storage
Tag der Einreichung:	14.12.2016
Hochschule:	Rheinische Friedrich-Wilhelms-Universität Bonn
Name des Verfassers:	Alena Naiakshina
Betreuender Professor:	Prof. Dr. Matthew Smith

*Kurze Beschreibung (1 Seite !) der **Kernthesen**.*

Was ist die Quintessenz der Arbeit?

Die meisten Unternehmen speichern Benutzeranmeldeinformationen, z.B. um Online-Banking zu ermöglichen, Benutzer an sich zu binden oder gar Nutzerdaten an Marktunternehmen zu verkaufen. Nutzern wird dabei oft die Bürde auferlegt komplizierte Passwörter unterschiedlichster Länge mit diversen Sonderzeichen anzulegen. Eine Reihe von Datenlecks haben jedoch gezeigt, dass es meist keine Rolle spielt, wie komplex die von den Nutzern erstellten Passwörter sind (z.B. 2012: LinkedIn, 2013: Adobe, Yahoo, 2014: eBay, Yahoo, 2015: Ashley Madison, 2016: Yahoo). Vielmehr ist es entscheidend, welche Techniken Softwareentwickler zur sicheren Passwortspeicherung verwenden. So waren die Nutzerdaten aus dem Yahoo Hackerangriff von 2013 lediglich mit MD5 gesichert, einem veralteten und schon längst als unsicher eingestuften Hash Algorithmus. Umso gravierender ist die Tatsache, dass Nutzer dazu neigen ihre Passwörter auf diversen Webseiten wiederzuverwenden und diese auch nur in den seltensten Fällen, wenn überhaupt, ändern.

Sichere Datenspeicherung ist dementsprechend nicht von den von Nutzern gewählten Passwörtern, sondern viel mehr von Softwareentwicklern und ihren Implementierungsentscheidungen abhängig. Um Benutzeranmeldeinformationen zu speichern machen Entwickler gerne Gebrauch von Anwendungsprogrammierschnittstellen (engl. APIs: application programming interfaces). Dabei nimmt das Design einer API eine ausschlaggebende Funktion bei sicherheitsrelevanten Implementierungsentscheidungen ein. In der zugrunde liegenden Arbeit werden daher folgende Forschungsfragen erörtert:

1. Wie werden Entwickler darauf aufmerksam, dass Benutzeranmeldeinformationen sicher gespeichert werden müssen?

2. Welche Informationsquellen nutzen Entwickler um sicherheitsrelevante Probleme bezüglich der sicheren Passwortspeicherung zu lösen?

3. Besteht ein Zusammenhang zwischen den genutzten Informationsquellen und der Sicherheit und Funktionalität der implementierten Lösungen?

4. Beeinflusst das Design einer API die Wahrscheinlichkeit, dass ein Nutzer-Passwort sicher gespeichert wird?

5. Vergleicht man die Implementierungsentscheidungen für sichere Passwortspeicherung verschiedener APIs, welche schneiden besser ab, im Sinne von „Benutzerfreundlichkeit“?

6. Gibt es einen Effekt, wenn einer Studien-Gruppe von Entwicklern explizit gesagt wird sie soll auf Sicherheit achten und einer anderen nicht?

Um die oben aufgeführten Fragen beantworten zu können, müssen Studien mit Softwareentwicklern durchgeführt werden. Während Studien mit End-Nutzern in der Wissenschaft weit verbreitet sind, gibt es praktisch keine Forschung darüber, wie Studien mit Entwicklern und Administratoren durchgeführt werden sollen. Wir haben uns der Herausforderung gestellt und eine Studie zur sicheren Passwortspeicherung für Entwickler entworfen. In einem Experiment müssen Entwickler ein Programmiergerüst mit einem vorausgewählten Java Webframework, Spring oder Java Server Faces (JSF), vervollständigen. Als Anwendungsfall wurde eine soziale Plattform der Universität Bonn gewählt. Dadurch werden die Entwickler nicht ausdrücklich mit Sicherheit konfrontiert, wie das bei einem Anwendungsfall mit finanziellem Kontext wäre, z.B. das Speichern von Benutzeranmeldeinformationen für ein Bankkonto. Dies erlaubt uns das

Studieren der 6. Forschungsfrage. Das Experiment wird kontrolliert durchgeführt. Die Teilnehmer werden vor Ort eingeladen und müssen Benutzeranmeldeinformationen von Studenten und Universitätsmitarbeitern der Universität Bonn in eine Datenbank speichern sowie ein Login mit den zugehörigen Zugangsdaten ermöglichen. Dies ermöglicht uns die gesamte Arbeit der Teilnehmer einzusehen, diese auf Sicherheit und Funktionalität zu untersuchen sowie anschließend ein ausführliches Interview mit ihnen durchzuführen.

Um unseren Entwurf zu testen, haben wir eine Vorstudie mit zwei Masterstudierenden und zwei Mitarbeitern der Universität Bonn, Fachbereich Informatik, getestet. Die Ergebnisse der Studie verdeutlichen die Komplexität und Vielschichtigkeit eines Studiendesigns mit Entwicklern und Administratoren und zeigen neue Herausforderungen auf, denen in weiterführender Arbeit begegnet werden muss.