Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	How to Conduct Expert Studies to Measure API Design Influence on Secure Crypto Library Usage
Tag der Einreichung:	14.12.2016
Hochschule:	Universität Bonn
Name des Verfassers:	Anastasia Danilova
Betreuender Professor:	Prof. Dr. Matthew Smith

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

Was ist die Quintessenz der Arbeit?

Die Arbeit behandelt zwei wichtige Aspekte: die Methodik zur Durchführung von Studien mit Softwareentwicklern und die Benutzbarkeit der Java Standard Bibliothek für sichere Server-Client Kommunikation. Wie in vorausgehender Literatur festgestellt, weisen viele mobile Applikationen TLS-Fehler auf. Vor allem in der Testphase, wo zahlreiche Entwickler mit selbst-signierten Zertifikaten arbeiten, schalten die Entwickler oftmals die Zertifikatsvalidierung in der Client-Software komplett aus. Anschließend wird nach der Testphase die Validierung nicht mehr geändert und bietet somit die Möglichkeit für Man-In-The-Middle Attacken.

In der eigens entwickelten Studie erhielten die Teilnehmer die Aufgabe eine REST Client- Anwendung zu vervollständigen. Dabei soll der Client sensible Login Daten an den Server senden und einige Informationen abfragen. Im Idealfall würde eine TLS/SSL Verbindung hergestellt und das selbst-signierte Zertifikat des Servers gespeichert werden. Es gab jedoch auch die Möglichkeit die Aufgabe mit HTTP zu lösen, da beide Ports für HTTP und HTTPS geöffnet waren.

Der Effekt des „Priming“, die Beeinflussung von Studienteilnehmer durch bestimmte Reize, in unserem Fall das Hinweisen auf Sicherheit in der Aufgabenstellung, ist die fundamentale Variable in dieser Arbeit.

In End-User Studien wurde dieser Effekt bereits untersucht, während er in Expertenstudien noch nicht betrachtet wurde.

In dieser Arbeit wurde daher mit zwei Bedingungen getestet, ob es einen Effekt gibt, wenn Teilnehmer auf Sicherheit aufmerksam gemacht werden. Es gab also zwei Gruppen: P: Primed + JSSE und NP: Non-Primed + Bibliothek Ihrer Wahl. Es geht darum zu bestimmen, ob die sicherheitsrelevante Aufgabe je nach Studiendesign anders gelöst wird. Des Weiteren war es von Interesse welche Bibliothek die Teilnehmer der Gruppe NP wählen.

Das Experiment bestand aus einer Implementierungsphase und einem Interview. Vor der Implementierungsphase wurde, nach kurzem Studieren der Aufgabe, die Erwartung bezüglich der Komplexität der Aufgabe abgefragt und nach der Implementierung mit der wahrgenommenen Komplexität verglichen.

Die während der Implementierungsphase entstandenen Metriken wie Zeit, Browser Chronik und Think-Aloud sowie Desktop Aufnahmen wurden protokolliert.

Es wurden 3 Pilotstudien durchgeführt, vollständig transkribiert und die gesammelten Daten ausgewertet.

Keinem der Teilnehmer gelang es eine vollständig sichere Lösung abzugeben. Die Teilnehmer hatten Schwierigkeit mit dem Akzeptieren des selbst-signierten Zertifikats. Insgesamt wurde deutlich, dass die Zertifikatsvalidierung den Entwicklern erhebliche Schwierigkeiten bereitet.

Es wurde eine Verbesserung der Dokumentation sowie eine Erweiterung der Java Standard Bibliothek für TLS vorgeschlagen.