Der Weg zur sicheren und nutzbaren Nutzerauthentifizierung auf mobilen Geräten

Autor: Sebastian Uellenbeck

Heutzutage sind mobile Geräte wie Smartphones und Tablets allgegenwärtig. Auf ihnen werden viele private Informationen, wie Kontakte, Fotos oder E-Mails gespeichert, deren Wert ihren Besitzern oft nicht bewusst ist. Nicht nur Geheimdienste oder große Unternehmen sind daran interessiert an diese Informationen zu gelangen, um beispielsweise Nutzerprofile zu erstellen. Ist ein Gerät entsperrt, so kann es auch von einem Dieb genutzt werden, um einen Identitätsdiebstahl zu begehen oder zumindest um einen finanziellen Schaden durch Mehrwertdienste anzurichten. Die Authentifizierung des Nutzers ist daher eine geeignete Gegenmaßnahme, um diese Angriffsmöglichkeit zu unterbinden. Unglücklicherweise sind die bisher vorhandenen Mechanismen jedoch entweder unsicher, schwer nutzbar oder deren Sicherheit ist unbekannt.

Die vorliegende Dissertation beschäftigt sich daher mit zwei Themenfeldern im Bereich der Nutzerauthentifizierung: Zum einen werden existierende Methoden bezüglich ihrer praktischen Sicherheit untersucht, zum anderen werden neue Methoden vorgestellt, die einzelne Aspekte in Bezug auf ihre Sicherheit und Nutzbarkeit verbessern. Dazu werden die folgenden Schwerpunkte behandelt.

Zuerst wird das graphische Authentifizierungssystem *Android Unlock Patterns* untersucht. Mit Hilfe mehrerer Nutzerstudien wird die Sicherheit des Systems evaluiert, Schwachstellen werden aufgedeckt und vier neue Punktanordnungen vorgeschlagen, die das System verbessern. Jeder einzelne Ansatz zielt darauf ab einen Teilaspekt der identifizierten Schwachstellen zu beheben. Für das Schema *Circle* kann dabei empirisch nachgewiesen werden, dass es das ursprüngliche System in Bezug auf seine Sicherheit verbessert.

Ausgehend von graphischen Authentifizierungssystemen wird ein alternatives System vorgeschlagen, das geometrische Objekte, Farben und Positionen als Geheimnis verwendet. Es wird gezeigt, dass dieses System nicht nur theoretisch sicherer ist als etablierte Systeme sondern auch praktisch nutzbar ist.

Danach wird der Fokus auf die Erweiterung der Authentifizierung mit Hilfe von PINs gelegt. Da PINs nicht sicher gegen Shoulder-Surfing-Angriffe sind, wird der Vibrationsmotor eines Smartphones verwendet, um einen sicheren Kanal zwischen dem Nutzer und dem Gerät aufzubauen. Es wird gezeigt, dass das vorgestellte Verfahren sowohl nutzbar als auch sicher gegen komplexe Shoulder-Surfing-Angriffe ist.

Anschließend wird ein biometrisches Authentifizierungssystem vorgestellt. Ein Software-Keyboard verarbeitet hierbei Bewegungsinformationen während der Nutzer Texte schreibt, um daraus einen *verhaltensbasierten Fingerabdruck* zu generieren. Dieser wird später zur durchgängigen und transparenten Authentifizierung verwendet.

Schlussendlich wird untersucht, ob Nutzer das komplexe Berechtigungssystem des Betriebssystems Android verstehen. Die Ergebnisse einer Nutzerstudie zeigen, dass Angriffsvektoren durch kombinierte Berechtigungen nicht erkannt werden. In diesem Zusammenhang wird ein Prototyp vorgestellt und durch diesen untersucht, ob verständliche Hilfestellungen die Auswahl von Applikationen beeinflussen und den Nutzer diesbezüglich sensibilisieren. Die Resultate einer weiteren Nutzerstudie belegen, dass Nutzer dazu bereit sind Applikationen mit offensichtlich gefährlichen Kombinationen von Berechtigungen zu entfernen, sofern sie verständlich über die Gefahren informiert werden.

Die innerhalb dieser Arbeit vorgestellten Systeme zeigen neue Ansätze oder untersuchen und verbessern etablierte Authentifizierungsmethoden. Die durchgeführten Studien belegen, dass diese Methoden trotz Verbesserung der Sicherheitsaspekte weiterhin nutzbar und einsetzbar sind. Der entstandene Mehraufwand ist entweder zu vernachlässigen oder angemessen in Hinblick auf das Angreifermodell.