Thema D

Manipulationstests optischer Fingerabdruckscanner

In dieser Seminareinheit wurden die Herstellung eines Fakefingers sowie Tests mit Fingerabdruckscannern vorgestellt, ebenso wurde eine Einschätzung der verschiedenen Methoden und der Sicherheitsaspekte thematisiert.

Für die durchgeführten Manipulationstests wurde ein Fingerabdruckscanner in Verbindung mit dem Programm Fprint verwendet.

Als Vorlage für den Fake Finger diente der Fingerabdruck von Wolfgang Schäuble, welcher vom Chaos Computer Club Berlin im Internet zur Verfügung gestellt wird. Dieser Fingerabdruck wurde mit einem Laserprinter auf Folie gedruckt und mit Holzleim entsprechend bearbeitet, um den nachgemachten Fingerabdruck zu erhalten. Die Herstellung verläuft in drei Phasen: Realer Finger → Schablone → Fake Finger. Für die Herstellung ist eine detaillierte Schablone essentiell. Die Schablonen entstehen, indem die Negative auf Folie gedruckt werden. Die Wölbungen, die durch die Farbe entstehen, reichen für die Bearbeitung mit Holzleim aus. In der Praxis ist die Nachbearbeitung eines fotografierten Abdrucks am zeitaufwändigsten und mühseligsten.
Als Sensoren standen Nitgen FIM5360-LV und U.are.U4000 des Herstellers digitalPersona zur Verfügung. Da für den Arduino Scanner kein Kabel erhältlich war, konnte aber nur mit dem U.are.U4000-Scanner gearbeitet werden. Insgesamt ergaben sich bei den Tests viele Fehler und Nichterkennungen. Als problematisch stellte sich ebenfalls heraus, dass die Bilder zwar verschlüsselt gespeichert, aber über USB unverschlüsselt übertragen werden.
Als Testszenarien wurden echte Fingerabdrucke, Fake Finger aus Leim und Fake Finger aus Geliermittel verwendet. Das genutzte Programm Fprint vergleicht dabei nicht den gesamten Scan, sondern lediglich einzelne Punkte. Das Matching der beiden Fake Finger untereinander wurde insgesamt als gut bewertet, eine Täuschung des Scanners war aber nur in Einzelfällen möglich. Der gefälschte Fingerabdruck, der mittels der Vorlage, erstellt wurde, hat allerdings gut funktioniert.
Der verwendete U.are.U4000-Scanner wurde in Bezug auf den Sicherheitsaspekt letzten Endes als eindeutig nicht geeignet befunden. Der unverschlüsselte USB-Datenverkehr begünstigt nämlich Replay-Attacken.