Hardware Reverse Engineering anhand eines FlickerTAN-Generators

Das Ziel unserer Gruppe bestand darin, die genaue Funktionsweise eines Flicker TAN-Generators nachzuvollziehen. Bei dieser Art TAN-Generator werden die Transaktionsdaten auf optischem Wege auf das Kleingerät übertragen. Mithilfe der eingeschobenen EC-Karte bestimmt dieses Gerät anschließend eine TAN mit der die gewünschte Transaktion authentifiziert wird.

An dieser Stelle begann unsere Arbeit, das sogenannte „Reverse Engineering“: Mithilfe einer besonderen Platine (Breakout-Board) untersuchten wir die Kommunikation zwischen TAN-Generator und EC-Karte ein. Ein Oszilloskop half uns dabei, die Bedeutung der einzelnen PINs der Karte zu bestimmen. Nachdem wir ermittelt hatten, wie die Signalübertragung funktioniert, haben wir mittels „Buspirate“ die übermittelten Daten mitgeschnitten, um sie danach auszuwerten.

Dabei sind uns bestimmte Regelmäßigkeiten aufgefallen, die es uns ermöglichten die Rohdaten in Frage (des TAN-Generators) und Antwort (der Karte) aufzuteilen. Weiterhin fanden sich in den Fragen als ASCII codierte Transaktionsdaten wieder und in den Antworten unterschiedliche Kartendaten. Indem wir selber den Prozess der TAN-Generierung nachahmten und dabei Fragen veränderten konnten wir mittels der nun anderen Antwort die Bedeutung einiger Fragen erschließen.

Der komplette Vorgang zur Generierung einer TAN ist unten zu sehen. Im Anschluss an das Nachvollziehen des Vorgangs wurde dieser in einem Python Script implementiert, sodass nun ohne TAN-Generator, nur mit dem Kartenleser des Laptops TANs generiert werden können. Im Test konnten wir eine selber ermittelte TAN dazu verwenden, eine Transaktion zu authentifizieren.