Perfect Key

Studiengang: BSc in Informatik | Vertiefung: Distributed Systems and IoT
Betreuer: Prof. Dr. Reto Koenig
Experte: Prof. Dr. Andreas Spichiger

Ist man mit dem Basiswissen der Kryptografie vertraut, kennt man das Problem des zu schützenden Private Keys. Es kommt einem Super-GAU nahe, sollte der private Schlüssel in nicht beabsichtigte Hände fallen. Dies ermöglicht Identitätsbetrug, mitlesen von verschlüsseltem Datenverkehr oder, ganz aktuell, den Diebstahl digitaler Währungen. Diese Bachelor Thesis beschäftigte sich mit der Umsetzung eines Proof of Concepts für ein System mit nicht-klonbaren Schlüsseln.

Ziel

Diese Bachelor-Thesis hat zum Ziel einen Prototypen zu konstruieren, um physische Schlüssel zu erfassen und auszuwerten. Jedoch anders als in der gegenwärtigen Kryptografie wird auf das Prinzip der Physical Unclonable Functions, oder kurz PUF, gesetzt.

Eines der Kriterien war, dass so ein PUF-analysierendes System prinzipiell von jeder Person nachgebaut werden kann. Folglich besteht der Prototyp aus handelsüblichen Materialien, die in jedem Baumarkt beschafft werden können.

Was sind Physical Unclonable Function

Im Themenfeld PUF versucht man die Einzigartigkeit, die an ein physisches Objekt (Perfect Key) gebunden ist, zu erfassen. Zum Beispiel die Partikel in einem Gegenstand.

Das Forschungsgebiet der PUF existiert bereits seit den Achtzigerjahren. Die praktische Anwendung fand bisher jedoch ihren Platz vor allem in der Elektronik. Optische PUF, so wie sie diese Bachelor-Arbeit nutzt, sind eher selten.

Perfect Key Box

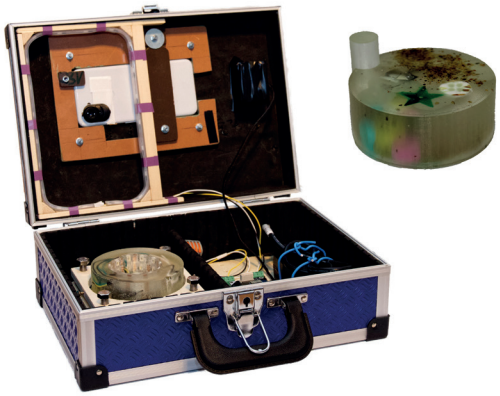
Der Prototyp ermöglicht diese Einzigartigkeit optisch zu erfassen. Um dies zu erreichen, ist es entscheidend, dass die Extraktion der Informationen aus dem Schlüssel immer unter denselben Bedingungen stattfindet. Dazu wurde die Perfect Key Box entwickelt. Sie garantiert, dass der Analyseprozess immer dieselben Resultate liefert. Die eingelegten Schlüssel durchlaufen bestimmte Sequenzen, wobei bei jeder ein Bild aufgenommen wird. Die Aufnahme wird dann mit den vorab registrierten Schlüsseln verglichen und bewertet. Die Unklonbarkeit wird weiter verbessert, indem jede Sequenz den Key anders beleuchtet (RGB + UV). Die «Response», das Bild, das daraus entsteht, kann so über mehrere Dimensionen erfolgen. Siehe Bild unten rechts, welches denselben Key unterschiedlich ausgeleuchtet zeigt.

Fazit

Der Proof of Concept hat gezeigt, dass es möglich ist mit sehr simplen Mitteln und Methoden ein System zur Auswertung von PUF zu bauen. Die gebaute Perfect Key Box analysiert die Aufnahme erfolgreich auf Basis von Feature-Points. Es können beliebige weitere messbare Grössen als zusätzliche Sequenzen eingebaut werden. Beispielsweise das Key-spezifische Magnetfeld.

Alain Keusen

Michel Kocher



Perfect Key System mit Box und Key

Vergleich Aufnahme mit unterschiedlicher Ausleuchtung