FAPPAT - frappant gut!

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Reto Koenig
Experte: Prof. Dr.Andreas Spichiger

Die beiden Singles Erika und Philippe suchen ihre Liebe fürs Leben und nehmen daher an einem Speed-Dating Abend teil. Bevor die Singles aufeinandertreffen, müssen sie 5 Eigenschaften auswählen, welche sie selbst vertreten und sich vom Gegenüber wünschen. Diese, inklusive ihrem Namen, legen sie jeweils im FAPPAT-Tresor ab. Mit 3 übereinstimmenden Eigenschaften öffnet sich ein fremder Tresor und der Name wird bekannt. Welche drei es waren, wurde dabei nicht offengelegt.

Einleitung

Das einleitende Beispiel stellt eine Möglichkeit eines „Privacy-Protected Matching“ dar. Alle Eigenschaften wurden in einem Tresor (Vault) abgespeichert. Die Geschichte soll aufzeigen, dass ohne Bekanntgabe der Eigenschaften ein Matching entstehen kann.
Um den Tresor öffnen zu können, müssen nicht alle Eigenschaften übereinstimmen. Dies führt zu einer gewünschten Unschärfe (Fuzziness).

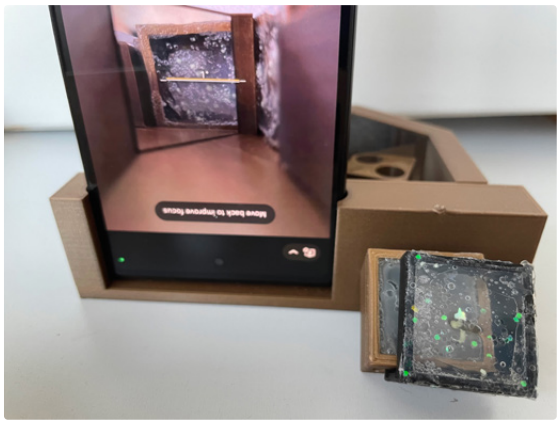
Welche Rolle spielen „Physical Unclonable Functions (PUF)“ und was gibt es dabei zu beachten?
Die Antwort ist in der Bachelor-Thesis namens „Practical Management of Asymmetric Optical Physical Unclonable Functions“ zu finden.

Ziel

Ziel der Thesis ist die einfache Herstellung von PUFs, sowie die Verwaltung von PUF-Responses in einem Fuzzy Vault. Um Informationen aus der PUF auszulesen, soll eine Schablone eingesetzt werden, welche als Halterung der einzelnen Komponenten dient.

Idee

Der Fokus liegt in der Übertragung der Eigenschaften eines physischen Objekts in die digitale Welt. Ein Computer ist deterministisch und kennt keinen Zufall.



Asymmetrische PUFs und Schablone

Daher ist es optimal, wenn eine PUF als Zufallseingabe in der digitalen Welt dient. Wenn der Benutzende zudem die Eingabe, die PUF als manifestierte Entropie, selbst herstellen kann, wird die Skepsis gegenüber heutigen Zufallsgeneratoren abnehmen.

Umsetzung

Die Demo-Lösung namens FAPPAT verlangt als Input ein Abbild (Foto) der asymmetrischen PUFs und erzeugt daraus Punkte auf einem Polynom, die in einem Vault abgespeichert werden. Dank des asymmetrischen PUF-Ansatzes des Challenge-Response-Protokolls dürfen alle benötigten Komponenten öffentlich sein.

Fazit

Während der gesamten Projektabwicklung wurden verschiedene Experimente mit FAPPAT durchgeführt. Dadurch konnten wertvolle Erkenntnisse vom Foto bis zum Vault gewonnen werden. Schwierigkeiten liegen im Gewinnen robuster Werte aus einem durch Umwelt beeinflussten rauschenden Foto.
Im Grundsatz funktioniert die Verwaltung von PUF-Responses im FAPPAT. Die erreichten Ergebnisse beweisen die Machbarkeit. Die Verarbeitung der Eingabe sollte in einer weiteren Thesis vertieft werden.

Schlusswort

Unser FAPPAT: Heute frappant benannt, morgen weltweit bekannt!

Patrick Robin Friedli

Michelle Wiedmer