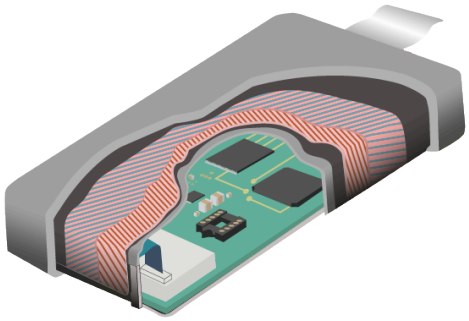
PUF-basierter Tamperschutz für Cyber Physical Systems

Vincent Immler[1], Johannes Obermaier[1], Martin König[2], Matthias Hiller[1], und Georg Sigl[1,3]
[1]Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC,
Parkring 4, 85748 Garching b. München
[2]Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT
Hansastraße 27d, 80686 München
[3]Lehrstuhl für Sicherheit in der Informationstechnik, Technische Universität München
Arcisstraße 21, 80333 München

{vorname.nachname}@{aisec,emft}.fraunhofer.de

Gehärtete Cyber Physical Systems sind eine Voraussetzung für vertrauenswürdige Kommunikation, abgesicherte kritische Infrastruktur oder sichere Fahrzeuge. Neben typischen Cyberangriffen sind diese Systeme zusätzlich physischen Angriffen z.B. durch Messsonden oder Bohrwerkzeuge ausgesetzt. Bisherige Lösungen verwenden Schutzumhüllungen, die kritische Teile des Systems umschließen und ununterbrochen durch eine batteriegepufferte Schaltung überwacht werden müssen. Im Falle eines Angriffes werden kritische Daten in flüchtigen Speichern gelöscht. Die Lösung kann jedoch wegen eingeschränkter Lagerdauer, Erschütterungsempfindlichkeit und engem zulässigen Temperaturbereich nur stationär und in kontrollierten Umgebungen eingesetzt werden.



Im Gegensatz dazu misst die von uns entwickelte batterielose Tamperschutzlösung die kapazitiven Eigenschaften der Schutzumhüllung als Physical Unclonable Function (PUF), um daraus einen individuellen Schlüssel für jedes Gerät abzuleiten, mit dem die Daten im System verschlüsselt werden. Im ausgeschalteten Zustand liegen alle Daten nur in verschlüsselter Form vor. Beim Start können die Daten nur bei einer völlig intakten Umhüllung wiederhergestellt werden. Eine Manipulation verändert die physikalischen Eigenschaften der Folie dauerhaft und zerstört somit den Schlüssel. Nach einem erfolgreichen Start wird das System kontinuierlich auf Kurzschlüsse, Unterbrechungen und Kapazitätsänderungen überprüft, um auch zur Laufzeit Angriffe zu detektieren und darauf reagieren zu können.

Praktische Tests auf Basis von über 150 Schutzfolien haben gezeigt, dass die vorgestellte Technologie einerseits genug Variation in jeder Folie enthält, um kryptografische Schlüssel abzuleiten, und andererseits in Temperaturbereichen von -20 °C bis +60 °C funktionsfähig ist. Exemplarische Angriffe mit einem Bohrdurchmesser von 0.3 mm wurden zuverlässig erkannt und führten zu einer Zerstörung des kryptografischen Schlüssels. Im nächsten Schritt werden nun Skalierungsfragen geklärt und weitere Verbesserungen an der Materialzusammensetzung vorgenommen. Mittelfristiges Ziel ist die Weiterentwicklung des Technologiedemonstrators zur Produktreife.