Physikalische

Fingerabdrücke gegen Produkt-Piraterie

Produkt-Piraterie stellt ein schwerwiegendes und bisher ungelöstes Problem der heutigen Zeit dar und verursacht wirtschaftliche Schäden in Milliardenhöhe. Existierende technische Lösungsansätze weisen unterschiedliche Schwächen auf, beispielsweise haben sie nur eine begrenzte Anwendbarkeit oder verfehlen die geforderten Sicherheitsziele.
Einen vollständig neuen Ansatz stellen Physikalisch unklonbare Funktionen – kurz PUFs – dar. Hierbei werden die bei Herstellungsprozessen unvermeidbaren physikalischen Variationen ausgenutzt, um unter anderem ein physikalisches Pendant zum biometrischen Fingerabdruck zu erzeugen.

Using physical fingerprints against product piracy

Today, product piracy represents a severe and so far unsolved problem, causing commercial damages going into the billions. Existing technical solutions have different drawbacks, e.g., being not universally applicable or missing the required security goals. A completely new approach is the use of Physically Unclonable Functions – short PUFs. Hereby unavoidable physical variations of manufacturing processes are exploited, e.g., for creating a physical variant of biometric fingerprints.

Frederik Armknecht, Ahmad-Reza Sadeghi •

„Besser gut kopiert als schlecht erfunden“ heißt eine bekannte Redewendung. Im Kontext von Produktpiraterie nimmt dies jedoch bedrohliche Ausmaße an. Unter Produktpiraterie versteht man das illegale Geschäft mit Imitaten. Diese werden mit dem Ziel hergestellt, einer Originalware zum Verwechseln ähnlich zu sein, können aber weit unter dem Originalpreis angeboten werden. Die Problematik betrifft nahezu jede Produktgruppe, beispielsweise Bekleidung, Fahr- und Flugzeugteile, Consumer Electronics, Steuergeräte in Anlagen sowie Medikamente und Software.
Dabei werden Markenrechte oder wettbewerbsrechtliche Vorschriften verletzt und immense wirtschaftliche Schäden verursacht. Schätzungen zufolge verursachen diese illegalen Geschäfte jährlich einen wirtschaftlichen Schaden von etwa 600–1200 Mrd. US-Dollar (ca. 10 % des Welthandels), davon allein 30 Mrd. Euro in Deutschland, und kosten jährlich weltweit 750.000 Arbeitsplätze (davon 70.000 in Deutschland). Selbst wenn es möglich wäre, Waren von minderer Qualität einfach zu erkennen und aus dem Handel zu

Ahmad-Reza Sadeghi

nehmen, wäre die Gefahr nicht gebannt. Ein verwandtes Problem, welches vor allem die Chip-Produktion betrifft, ist die unautorisierte Überproduktion von Waren und deren illegaler Verkauf. Hierbei wird an den Originalproduktionsstätten vom Hersteller, die zumeist in kosteneffektiven und lohnschwachen Ländern liegen, unbemerkt zusätzliche Ware produziert und diese ohne sein Wissen verkauft.

Produktpiraterie hat ernsthafte wirtschaftliche und politische Konsequenzen. Da sie durch gesetzliche Maßnahmen allein nicht zu verhindern ist, wird verstärkt nach effektiven und effizienten technischen Gegenmaßnahmen gesucht. Die existierenden Lösungen weisen jedoch unterschiedliche Schwächen auf: Sie sind entweder zu aufwändig und somit für viele kommerzielle Produkte nicht geeignet, erreichen nicht die angestrebten Sicherheitsziele oder sie sind stark produktabhängig und daher nicht allgemein einsetzbar. Insbesondere zeigt das Problem der Überproduktion deutlich, dass es nicht ausreicht, den Herstellungsort eines Produktes feststellen zu können. Idealerweise sollten die Produkte selbst eindeutig identifizierbar und wieder zu erkennen sein.

Physikalische Fingerabdrücke

Hier bietet die Biometrie Inspiration: Genau wie Menschen anhand ihres biologischen Fingerabdrucks identifiziert werden können, werden eine eindeutige Identifizierung der Ware mittels eines physikalischen Fingerabdruckes angestrebt. Basierend auf solchen physikalischen Fingerabdrücken sieht eine momentan industriell angewandte Lösung wie folgt aus: Sobald die Ware produziert wurde, aber noch bevor sie in den Handel gelangt, wird deren physikalischer Fingerabdruck beim Hersteller registriert. Wenn dann später eine beteiligte Instanz, z.B. ein Händler oder Zöllner, die Rechtmäßigkeit einer erhaltenen Ware überprüfen möchte, wird zunächst ihr physikalischer Fingerabdruck bestimmt und anschließend beim Hersteller erfragt. Sollte der Fingerabdruck nicht beim Hersteller registriert sein, dann bedeutet dies, dass die Ware entweder eine Fälschung ist oder im Rahmen einer Überproduktion erzeugt wurde (siehe Abbildung 1). Da bei der Überprüfung der Fingerabdrücke nur digitale Daten ausgetauscht werden müssen, kann man auf etablierte kryptographische Verfahren wie SSL zurückgreifen, um diese Kommunikation abzusichern.

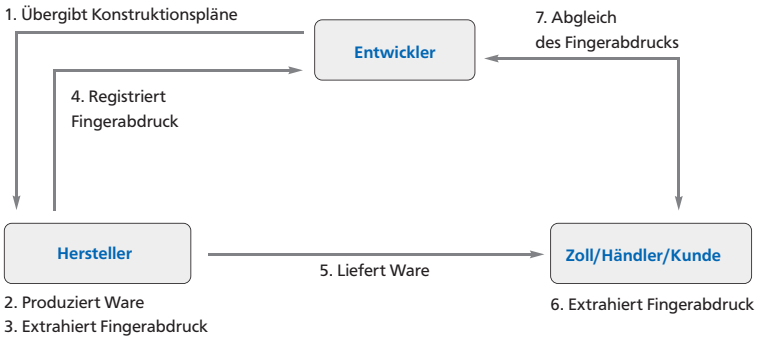

Abbildung 1
Technischer Ansatz zum Schutz vor Produktfälschungen und Überproduktion basierend auf PUFs

Physikalisch unklonbare Funktionen

Wie kann man nun geeignete physikalische Fingerabdrücke erhalten? Ähnlich zum menschlichen Fingerabdruck sollten physikalische Fingerabdrücke effizient verifizierbar, eindeutig und fälschungssicher sein. Weitere wichtige Eigenschaften sind, je nach Anwendung, geringe Größe und Herstellungskosten, effiziente Integration und damit weite Einsetzbarkeit der technischen Lösung. Eine Antwort auf die Frage bietet eine neuartige Technologie: Physikalisch unklonbare Funktionen (PUFs). Vereinfacht gesagt ist eine PUF ein physikalisches Gerät, bei dem es möglich ist, Eingaben zu stellen und Ausgaben zu erhalten. Der wesentliche Aspekt hierbei ist, dass das Eingabe-Ausgabe-Verhalten hochgradig von den physikalischen Eigenschaften des Gerätes abhängig ist. Diese wiederum sind weder planbar noch reproduzierbar.

Ein Beispiel sind die sogenannten optischen PUFs. Eine optische PUF besteht aus einem transparenten Material, das mit winzigen lichtstreuenden Partikeln durchsetzt ist, die während des Herstellungsprozesses beigemengt werden. Wenn ein Laserstrahl

Institut für Mathematik und Informatik an der Universität Mannheim
Prof. Dr. Frederik Armknecht
Tel. 0621/1812483
E-Mail: armknecht@informatik.uni-mannheim.de
http://th.informatik.uni-mannheim.de/

Fachgebiet Systemsicherheit der TU Darmstadt
Prof. Dr.-Ing. Ahmad-Reza Sadeghi
E-Mail: ahmad.sadeghi@cased.de
www.trust.rub.de/

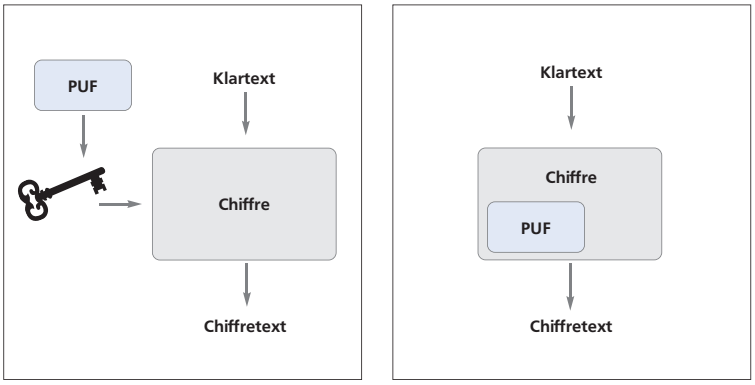

Abbildung 2
PUF als sicherer Schlüsselspeicher

Abbildung 3
Integration der PUF in die Chiffre

auf das Material trifft, wird dieser partiell gestreut, so dass der Strahl ein Fleckenmuster wirft. Da dieses Muster durch die Positionen der Partikel bestimmt wird und die Interaktion zwischen dem Laser und den Partikeln sehr komplex ist, ist das Muster zufällig und einzigartig. Insbesondere ist es praktisch unmöglich, eine optische PUF so zu duplizieren, dass das Duplikat das gleiche Fleckenmuster wie das Original erzeugt. Die PUF ist somit unklonbar.

Ein weiteres Beispiel ist die SRAM-PUF, die bereits industriell implementiert wird. SRAM steht für: Static Random Access Memory (Statisches RAM). Hierbei werden gewöhnliche SRAM-Bausteine verwendet, die jedoch direkt nach dem Einschalten ausgelesen werden, also noch bevor sie initialisiert wurden oder Werte gespeichert haben. Ausführliche Experimente haben gezeigt, dass diese Werte von SRAM-Baustein zu SRAM-Baustein variieren und bei der Produktion nicht beeinflusst werden können.

Inzwischen gibt es verschiedene Vorschläge für PUF-Konstruktionen. Allen gemeinsam ist, dass ihr Verhalten stark durch unvermeidbare natürliche physikalische Variationen des Herstellungsprozesses bestimmt wird. Ein wesentlicher Vorteil hierbei ist, dass die ausgenutzten physikalischen Phänomene nicht künstlich erzeugt oder bei der Herstellung speziell berücksichtigt werden müssen. Dies ermöglicht einerseits eine vergleichsweise effiziente und kostengünstige Herstellung und erlaubt andererseits eine Vielzahl von unterschiedlichen PUF-Typen.

Die Einsatzmöglichkeiten von PUFs gehen weit über die oben genannten Anwendungsfelder hinaus. Ein weiteres Anwendungsbeispiel ist der Schutz von Software. Hierbei wird der zu schützende Code mit einem durch die PUF generierten Schlüssel verschlüsselt. Dadurch kann dieser nur auf der vorgesehenen Anwenderplattform entschlüsselt werden, in welche die PUF eingebettet ist (siehe Abbildung 2). Ein weiteres Beispiel ist ein von uns entwickelter Verschlüsselungsalgorithmus, in dem PUFs nicht mehr nur als Schlüssellieferant verwendet werden, sondern direkt in den Ver- und Entschlüsselungsprozess integriert sind (siehe Abbildung 3). Für diese Konstruktion kann man die Sicherheit sowohl gegen gewisse algorithmische als auch physikalische Angriffe beweisen, falls die eingesetzten PUFs bestimmte Eigenschaften erfüllen. Im Rahmen des EU-Projektes UNIQUE erforschen und entwickeln wir mit Partnern aus der Industrie und dem akademischen Umfeld neue PUF-basierte Lösungen und Konzepte und streben deren prototypische Implementierung an.

PUFs sind sowohl von hoher wissenschaftlicher als auch industrieller Relevanz. Seit PUFs 2002 erstmals öffentlich in einer Doktorarbeit am Massachusetts Institute of Technology (MIT) diskutiert wurden, haben sie sich zu einem vielbeachteten Forschungsthema entwickelt. Das belegen eindrucksvoll weit über 70 Publikationen in teils sehr namhaften Journalen wie „Science“ und mehrere Workshops und Seminare zum Thema PUF. PUFs sind aber nicht nur aus akademischer Sicht interessant, sondern werden, wie bereits erwähnt, schon heute industriell eingesetzt. Als Beispiele seien hier die Firmen Intrinsic ID, eine Auskopplung von Philips, und Verayo, eine Ausgründung des MIT, genannt.

PUFs stellen somit ein hochaktuelles und wichtiges Forschungsgebiet dar und gehören zu den Schlüsseltechnologien der Zukunft, welche die Sicherheit in vielen Anwendungsbereichen verbessern können.

Frederik Armknecht ist Juniorprofessor für Kryptographie an der Universität Mannheim.

Ahmad-Reza Sadeghi ist seit Oktober 2010 Professor am Fachbereich Informatik der Technischen Universität Darmstadt und leitet das Fachgebiet Systemsicherheit. Zudem ist er Principal Investigator des LOEWE-Zentrums CASED.