Karlsruher Institut für Technologie

**Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL)**

**Institut für Theoretische Informatik**

# Softwareschutz nach Kerckhoffs' Prinzip

**Software hat einen immer größeren Anteil an der Wertschöpfung. Der Schutz von Software wird daher ein immer wichtigeres Teilgebiet der IT-Sicherheit. Softwareschutz verhindert das Kopieren und das Reverse-Engineering von Softwareprodukten und schützt so vor Industriespionage. Softwareschutz ist auch eine Grundlage für manipulationssichere Software und sichert so die Industrie der Zukunft vor Cyber-Sabotage.**

Der bisher in der Praxis verwendete Softwareschutz funktioniert nur dann gut, wenn die verwendeten Methoden geheim gehalten werden. Ein Angreifer, der diese Methoden genau kennt, hat es deutlich einfacher den Softwareschutz zu brechen. Dieses Vorgehen widerspricht Kerckhoffs' Prinzip, dass die Sicherheit auf der Geheimhaltung eines (kurzen) Schlüssels beruhen soll und NICHT auf der Geheimhaltung der Methode. Man kennt Methoden die einen wirksamen Softwareschutz nach Kerckhoffs' Prinzip garantieren, diese sind für die Praxis aber wertlos, da sie viel zu aufwendig sind. Es wäre dann sogar noch günstiger für jedes Programm einen „eigenen Rechner" mitzuliefern, auf dem nur diese Software läuft und die diesen Rechner nie verlässt. Stattdessen verwendet Blurry Box® nur eine kleine externe Hardware – das sogenannte Dongle (siehe Abbildung).

Das Blurry-Box®-Verfahren respektiert Kerckhoffs' Prinzip und beweist sogar die Sicherheit des Softwareschutzes.


Security Token der Firma Wibu-Systems

Dieser Beweis baut auf der einfachen Voraussetzungen auf: Der Angreifer (Hacker) kennt die Funktionsweise des geschützten Programmes nicht (vollständig), ansonsten könnte es das Programm ja selber schreiben und müsste nicht den Kopierschutz brechen. Mit dieser Voraussetzung lässt sich beweisen, dass der Hacker nur offensichtliches über das Programm lernt: Er kann Daten eingeben und erhält die entsprechenden Ausgaben. Auch die genaue Kenntnis des Kopierschutzes hilft ihm dabei nicht weiter.

Um dieses Ziel zu erreichen wird die Komplexität des Programmflusses ausgenutzt. Die einzelnen Abschnitte der Ausführungspfade werden in separaten Paketen verschlüsselt. Der PC fragt beim Dongle den Schlüssel für das benötigte Paket an und kann es damit entschlüsseln. Der Zusammenhang zwischen den Abschnitten wird im geschützten Speicher des Dongles berechnet. Dadurch kann eine Kontrolle der Ausführungsreihenfolge durch das Dongle stattfinden.

Diese Wahrung des Kerckhoffs'schen Prinzips erlaubt die unabhängige Untersuchung und Beurteilung der Sicherheit des Kopierschutzes – dies ist ein großer Vorteil gegenüber allen bisher üblichen Verfahren, bei denen die eingesetzten Methoden geheim gehaltenen werden. Blurry-Box® bietet Vorteile beim Schutz gegen Industriespionage und -sabotage und führt dadurch zu ausgezeichneten Marktchancen für Softwareprodukte, die damit geschützte sind.


**Den 1. Platz des IT-Sicherheitspreises belegte die Anwendung des Kerckhoffs'schen Prinzips für den Softwareschutz. (©RUB, Foto: Sadrowski)**

Karlsruher Institut für Technologie
Am Fasanengarten 5
76131 Karlsruhe

Prof. Dr. Jörn Müller-Quade
Institut für Theoretische Informatik
Telefon: +49 721 608-44205
E-Mail: crypto-info@iti.kit.edu

KASTEL

Zertifikat seit 2010
audit familiengerechte hochschule