# SICHERER SOFTWARE-SCHUTZ MIT EINEM ÖFFENTLICHEN VERFAHREN – WIE KANN DAS FUNKTIONIEREN?

## BlurryBox®: Innovativer Softwareschutz nach Kerckhoffs‘ Prinzip

**BlurryBox® ist ein innovatives Verfahren für Software-Schutz mit beweisbaren Sicherheitseigenschaften. Es wurde in einer Kooperation des FZI, KIT und der WIBU-SYSTEMS AG entwickelt und 2014 mit dem ersten Platz des deutschen IT-Sicherheitspreises prämiert. Der Demonstrator veranschaulicht die Prinzipien und die Funktionsweise des Verfahrens auf spielerische Weise. Die Anwendungsmöglichkeiten von BlurryBox® reichen vom Schutz traditioneller Software bis hin zur Sicherung von Industrieanlagen.**

*„Die Sicherheit eines kryptographischen Verfahrens darf nur von der Geheimhaltung des Schlüssels abhängig sein, nicht jedoch von der Geheimhaltung des Verfahrens.“*

Nach diesem Grundsatz, der „Kerckhoffs’sches Prinzip“ genannt wird, werden alle modernen Verschlüsselungsverfahren entworfen. Befolgt man diesen Grundsatz, kann man verhindern, dass allein durch das Bekanntwerden des Verfahrens alle damit geschützten Anwendungen gefährdet sind. Im Bereich des Software-Schutzes hat sich dieses Prinzip bisher jedoch noch nicht etabliert: die Effektivität aller gängigen Verfahren beruht auf deren Geheimhaltung. BlurryBox® ist das erste Software-Schutzverfahren, dessen Sicherheit auf der Geheimhaltung eines Schlüssels beruht. Dazu macht sich BlurryBox® die inhärente Komplexität der zu schützenden Software zu Nutze: je komplexer eine Software ist, desto effektiver ist der Schutz. BlurryBox® zerlegt die zu schützende Software in viele kleine Teile, die jeweils verschlüsselt und nur bei Bedarf wieder entschlüsselt werden. Die Entschlüsselung kann nur durch eine sichere Hardwarekomponente erfolgen, aus der der Schlüssel nicht auslesbar ist. Einem Angreifer, der ein geschütztes Programm kopieren möchte, bleibt keine andere Wahl, als alle verschiedenen Teile eines Programms zu benutzen, um sicher zu stellen, dass auch alle Teile des Programms entschlüsselt werden. Ist das geschützte Programm komplex genug, ist dies praktisch nicht möglich. Der auf der CeBIT gezeigte Demonstrator des FZI erlaubt es den Besuchern, die Funktionsweise des BlurryBox®-Verfahrens spielerisch nachzuvollziehen. Dazu dient ein einfaches, mittels BlurryBox® geschütztes Spiel, mit dem der Besucher interagieren kann. Parallel dazu kann er die Ausführung des Spiels beobachten und verschiedene Angriffe auf den Kopierschutz durchführen.

Die Anwendungsmöglichkeiten von BlurryBox® sind nahezu unbeschränkt: vom Kopierschutz von Office-Software über den Schutz von Motorsteuerungen bis hin zum Schutz von integrierten Systemen in Industrieanlagen. BlurryBox® ist auf nahezu alle Systeme mit komplexer Software anwendbar und liefert formal beweisbaren Software-Schutz nach Kerckhoffs‘ Prinzip.

ANSPRECH-PARTNER

Matthias Huber | mhuber@fzi.de | Tel. +49 721 9654-666

ÜBER DAS FZI

Das FZI Forschungszentrum Informatik am Karlsruher Institut für Technologie ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Es bringt die neuesten wissenschaftlichen Erkenntnisse der Informationstechnologie in Unternehmen und öffentliche Einrichtungen. Mehr Informationen unter: www.fzi.de