HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Studierenden	**Bruno Krieg** **Daniel Wydler**
Studienjahr	**SS 07**
Titel der Studienarbeit	**FIPS-140-2 Zertifizierung für strongSwan**
Examinatorin / Examinator	**Prof. Dr. Andreas Steffen**

Kurzfassung der Studienarbeit

Im Projekt "FIPS-140-2 Zertifizierung für strongSwan" ging es darum das Library-Modul auf eine mögliche FIPS-Zertifizierung vorzubereiten. Dabei wurde der Schwerpunkt auf die beiden Teilbereiche "Sicherstellung der Integrität der strongSwan-Library" und "Überprüfung der kryptographischen Funktionen mit Self-Tests auf Korrektheit" gelegt. Die realisierten Integritäts- und Self-Tests bieten den Anwendern von strongSwan die Möglichkeit, ihre strongSwan- Implementation zu überprüfen.

Der Integritätstest ermöglicht das Überprüfen der strongSwan-Library zur Programmausführung. Dazu wird eine Integritätsprüfung des Memory-Inhalts durchgeführt. Der gehashte Referenzwert dazu wird beim Erstellen der Applikation in strongSwan eingearbeitet, damit dieser nachträglich nicht verändert werden kann. Die Integritätstests sind standardmässig nicht Bestandteil der strongSwan Applikation, können jedoch bei Bedarf mit einer configure-Option aktiviert werden.

Es wurden Self-Tests für alle Cryptofunktionen realisiert, die von FIPS verlangt werden. Zu diesen Cryptofunktionen gehören Hashers, HMAC, Signers, PRF's, Crypters und RSA. Mit den realisierten Self-Tests werden die Crypto-Funktionen auf ihre Korrektheit überprüft. Manipulationen können somit festgestellt werden. Die Crypto-Funktionen können kritisch oder unkritisch eingestuft werden. Dies erlaubt dem Anwender verschiedene Szenarien auszuarbeiten, wie sich das Programm im Fehlerfall verhalten soll.
Die Selftests werden standardmässig mitcompiliert, können jedoch durch eine configure-Option deaktiviert werden.