README.md

RIOT OS Kryptotutorials

In diesen Tutorials wird erklärt wie man verschiedene Kryptoalgorithmen im ioT-Betriebssystem RIOT verwenden kann. Diese Tutorials sind eine Projektabgabe für das Fach "IT-Sicherheit 2" an der Hochschule für Technik Stuttgart.

Die Tutorials sind in 3 Kapitel gegliedert:

Kapitel 1: Grundlagen

Kapitel 1 vermittelt Grundwissen zu RIOT und wie man mit RIOT lauffähige Programme schreiben und ausführen kann.

Teil 1: Installation

Teil 1 beschreibt den RIOT Installationsprozess sowie welche Vorraussetzungen benötigt werden. Es wird sich auf die verwendung von RIOT unter Linux fokusiert.

Teil 2: Programmaufbau

Teil 2 beschreibt den Aufbau des minimalen RIOT Programmes, u.a. wie die Makefile eines RIOT-Programmes auszusehen hat und wie man dieses dann unter Linux laufen lassen kann.

Teil 3: Shell und Commands

Teil 3 liefert erste Einblicke, wie man unter Verwendung der Shell Interaktive Programme mit RIOT schreiben kann. Es wird ein einfacher Command Handler geschrieben und die Shell gestartet.

Kapitel 2: Crypto

Kapitel 2 vermittelt das notwendige Wissen um in RIOT Programme zu schreiben, die Kryptographische Algorithmen nutzen. Es werden die Algorithmen AES-ECB, AES-CBC sowie RSA behandelt.

Teil 4: AES im Electronic Codebook (ECB) Modus

In diesem Teil werden die Basics der Verwendung von AES im ECB-Modus unter RIOT präsentiert.

Teil 5: AES im Cipher Block Chaining (CBC) Modus

In diesem Teil wird das Programm erweitert, sodass Daten im Cipher Block Chaining Modus verschlüsselt werden können.

Exkurs: Übertragen von AES-CBC verschlüsselten Daten über das Netzwerk

In diesem Teil wird kein neuer Crypto-Algorithmus angesprochen, es wird der nun bekannte AES-CBC Algorithmus angewendet um mithilfe eines Client und Servers geheime Nachrichten auszutauschen.

Teil 6: RSA Verschlüsselung mithilfe des RELIC-Tookits

In diesem Teil wird gezeigt, wie man mithilfe des RELIC-Toolkit's Daten mithilfe von RSA verschlüsseln kann.

Kapitel 3: Benchmarking und Ergebnisse

In diesem kurzen Kapitel werden Ergebnisse von simplen Benchmark Algorithmen präsentiert