h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

ATHENE
National Research Center
for Applied Cybersecurity

Masterarbeit / F&E Studie: Testing Framework für PQC

Motivation

Angesichts der zunehmenden Bedeutung von Quantencomputern und ihrer Fähigkeit, Kryptosysteme zu gefährden, die in verschiedenen IT-Anwendungen eingesetzt werden, werden bereits quantenresistente kryptografische Algorithmen, sogenannte Post-Quantum-Algorithmen, entwickelt. Diese Algorithmen befinden sich noch im Standardisierungsprozess und sind noch nicht weit verbreitet. Ihre Implementierung und Integration in Anwendungen hat gerade erst begonnen. Die Entwickler der Algorithmen und Anwendungen verfügen derzeit nicht über ausreichende Werkzeuge, um ihre Implementierung auf Korrektheit und Interoperabilität zu prüfen.

Ziel

- Ziel dieser Arbeit ist es, ein Test-Framework zu entwerfen und zu implementieren. Dieses Framework kann von Designern und Entwicklern von post-quantum kryptographischen Bibliotheken und/oder Anwendungen verwendet werden, um die Interoperabilität und Korrektheit zu überprüfen.

Aufgaben

- Entwurf der Software.
- Implementierung der entworfenen Software in Java.
- Entwurf eines benutzbaren grafischen User Interfaces.
- Erstellung von Testvektoren zu Interoperabilitätszwecken.

Voraussetzungen

- Gutes Wissen über Software Design.
- Sehr gutes Wissen über Java.
- Interesse und grundlegendes Wissen über IT-Sicherheit und Kryptographie.
- Thesissprache kann sowohl Englisch als auch Deutsch sein.

Referenzen

- NIST PQC Standardization Process
- NCCoE Crypto-Agility

Start:

- Sofort oder nach Absprache

Die **User-Centered Security** (UCS) Forschungsgruppe untersucht das Design, die Entwicklung und evaluiert benutzbare, vertrauenswürdige, sichere, interaktive und kollaborative Software und IT-Systeme, basierend auf etablierte oder moderne IT-Sicherheit und HCI Prinzipien und Mechanismen.

Die **Applied Cyber Security Darmstadt** (ACSD) Forschungsgruppe ist auf den Schutz von IT-Systemen und Anwendungen spezialisiert. Unsere Lösungen beinhalten Aspekte, je nach Anwendungsfall, wie Haltbarkeit, Belegbarkeit, oder Methoden der offensiven Sicherheit (White Hacking).

Contact
Nicolai Schmitt, M. Sc.
nicolai.schmitt@h-da.de

Prof. Dr. Andreas Heinemann
andreas.heinemann@h-da.de

Prof. Dr. Alexander Wiesmaier
alexander.wiesmaier@h-da.de

Websites
https://ucs.fbi.h-da.de
https://acsd.h-da.de

Office
Schöfferstr. 10
64287 Darmstadt

UCS
USER-CENTERED SECURITY
DARMSTADT ∞ BERLIN

acsd applied cyber security darmstadt