# Cryptographic Discovery


Students

**Petra Heeb**

**Lara Gubler**

**Christopher Hilfing**

Advisor
**Prof. Dr. Nathalie Weiler**

Subject Area
**Security**

Project Partner
**IBM Research - Zürich, Rüschlikon**


Initial Situation: The imminent next generation of computers will rely on quantum computing. This poses a threat to many of the cryptographic algorithms in use today. Quantum computers will be able to break the mathematical primitives of many of the cryptographic algorithms in the not-so-distant future.
A transition from existing cryptographic algorithms to newer, quantum-safe algorithms such as CRYSTALS-Dilithium and CRYSTALS-Kyber is therefore of high importance for enterprises, to maintain a secure environment. But where are the new quantum-safe algorithms to be applied?

The goal of this student research work is to find a way to identify used cryptographic algorithms on a system so that the engineers can change insecure cryptographic algorithms to quantum-safe cryptography. In particular, we focus on the challenge to identify and model the cryptographic assets, which are in use within the network of an enterprise. This involves scanning and collecting data from a variety of sources, cataloging assets and building an understanding, of how the collected data artifacts are related to each other.

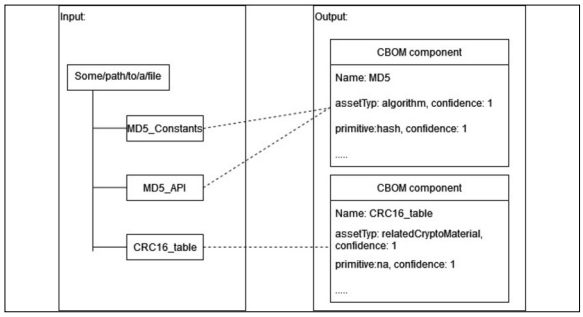
Approach / Technology: In this thesis, the newly written scanner, which crawls the system autonomously for information, will be used for the detection and cataloging of cryptographic assets.
An evaluation of various open-source scanners was conducted, regarding possible implementation in this project. Osquery and YARA were promising candidates, regarding how they could be used for the challenge at hand.

As a solution, the Python-based command line tool named Crypto-Scanner based on YARA rules was implemented during this thesis. The output of the scanner must be converted into a CBOM standard in CycloneDX format. Therefore, a Python-based command line tool called CBOM generator was developed using the CycloneDX python library.

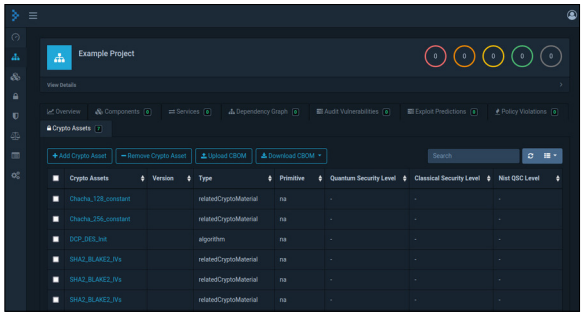
Furthermore, Dependency Track, an existing methodology for visualizing SBOM standards, was extended so that CBOM formats, which are extended SBOM formats, can be utilized for the visualization of the existing cryptographic inventory.
Dependency Track is an open-source tool that has been used in trials for similar challenges and has proven to be a great asset for the analysis of the SBOM and also the CBOM standard.

Result: The result of our student research work demonstrates the potential of static scanners in the area of cryptographic discovery. With this work, a basis for further research in this area has been created, which aids in the first step toward the transition to quantum-safe algorithms. This result demonstrates possible ways to identify implemented and used cryptographic algorithms and creates a standardized CBOM format from the identified cryptographic assets. This CBOM format can be uploaded in the extended Dependency Track to visualize the location of the algorithm implementation.

**Input and output matching CBOM-generator**
Own presentment




**Dependency Track**
Own presentment




**High-Level Cryptographic Discovery Overview**
Own presentment