KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Subversion-Resilient Protocols in HSMs with Public Verifiability

Master's Thesis

Since the Snowden revelations in 2013, the feasibility of state-level mass surveillance has become evident. **Algorithm Substitution Attacks (ASAs)** represent a general class of attacks in which an adversary substitutes a cryptographic implementation, such as an encryption or signing scheme. A concrete form of ASAs are **subversion attacks**, where the modified algorithm remains indistinguishable from the legitimate one while preserving its apparent correctness, yet embeds a covert channel that leaks secret information—typically private-key material—to an eavesdropper.

The primary object of interest in this work is the **Hardware Security Module (HSM)**. An HSM is a specialized device designed to execute cryptographic operations within a physically and logically isolated environment, ensuring that cryptographic keys are generated, stored, and used exclusively inside its protected boundary. A leakage of an HSM's signing key would be particularly severe, as it would immediately undermine any associated encryption, authentication, or certificate infrastructure and render these mechanisms effectively obsolete. Biasing the device's internal randomness is a typical vector for enabling such subversion.

A common mitigation technique is the use of **Reverse Firewalls**, which aim to counteract implementation-level manipulation. In addition, **public verifiability (PVC)** provides a practical and lightweight mechanism to detect dishonest behavior. By allowing the public to verify that cheating has been detected, hardware manufacturers are discouraged from implementing malicious cryptographic primitives due to the potential reputational damage if such subversion were exposed.

Keywords

Algorithm Substitution Attacks, Reverse Firewalls, Covert Channels, Public Verifiability, Hardware Security Modules.

Objective

A potential thesis aims to design, analyze, and evaluate a **subversion-resilient protocol** that operates with an untrusted or partially compromised HSM and provides **public verifiability** of its outputs. The protocol should rely on existing HSM architectures without requiring internal modifications.

Scope of the work

- **Protocol design** providing subversion resilience and public verifiability.
- **Prototype implementation** in Python, C, or C++, including a measurement environment for empirical evaluation.
- **Formal security analysis**, ideally within the Universal Composability (UC) framework.
- **Benchmarking and comparison** with existing open-source solutions

Requirements

- Master student in Computer Science, Mathematics, Electrical Engineering, or related fields.
- Programming experience in **Python**, **C**, or **C++**.
- High motivation for cryptographic research.
- Basic knowledge of the **Universal Composability** framework is beneficial.

What We Offer

- The opportunity to contribute to a scientific publication.
- Close supervision and guidance.
- Work on a timely and practically relevant research topic.

Contact

In case of interest or for further information, please contact Modjtaba Gharibyar, `Modjtaba.Gharibyar@kit.edu`.