Authentic Storage

Advisor(s): Thomas Unterluggauer

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

The encryption and authentication of both random access memory (RAM) and long-term storage is becoming increasingly important to protect data against people with unallowed physical access. While disk encryption is therefore widely implemented nowadays, authentication of stored data is hardly found.
In this project, the aim is to equip an existing file system with authenticity features. In particular, the goal is to extend the file-level disk encryption within the ext4 file system with an authenticity mechanism. This will finally allow to maintain both confidentiality and authenticity of stored data for selected parts of the file system.

Goals and Tasks

- Understand the file system encryption in ext4.
- Understand authenticity mechanisms with random access.
- Research previous approaches to incorporate authenticity into the file system.
- Design the required changes to the file system implementation.
- Implement the authenticity mechanism.

Literature

- M. Halcrow et al.
  Ext4 Encryption Design Document
- Linux Kernel Organization Inc.
  Linux Kernel Source Tree
  https://www.kernel.org
- R. Elbaz et al.
  TEC-Tree: A Low-Cost, Parallelizable Tree for Efficient Defense Against Memory Replay Attacks
  Cryptographic Hardware and Embedded Systems - CHES 2007

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- C/C++ programming
- Linux kernel or ext4 knowledge beneficial

Advisor / Contact

thomas.unterluggauer@iaik.tugraz.at