



Computer and
Information Science

Fachbereichs-
kolloqium

Summer semester 2024

Title

Shufflecake: plausible deniability for multiple hidden filesystems on Linux

Speaker and Title

Tommaso Gagliardoni (Kudelski Security)

Time and Room

April 10th (Wednesday)
1:30pm - 3:00pm
ZT 1204 (Data Theatre)

Abstract

Shufflecake (ACM CCS 2023, DEF CON Demo Labs 2023) is a tool for Linux that allows to create multiple hidden volumes on a storage device in such a way that it is very difficult, even under forensic inspection, to prove the existence of such volumes. This is useful for people whose freedom of expression is threatened through coercion by repressive authorities or dangerous criminal organizations, in particular: whistleblowers, investigative journalists, and activists for human rights in oppressive regimes. You can consider Shufflecake a "spiritual successor" of tools such as TrueCrypt and VeraCrypt, but vastly improved: it works natively on Linux, it supports any filesystem of choice, and can manage multiple nested volumes per device, so to make deniability of the existence of these partitions really plausible.

Shufflecake is FLOSS (Free/Libre, Open Source Software) released under the GNU General Public License v2.0 or superior.

Speaker's Bio