Universität Konstanz

Computer and Information Science

Fachbereichs-kolloqium

Summer semester 2024

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)

Universität Konstanz

Abstract

Shufflecake (ACM CCS 2023, DEF CON Demo Labs 2023) is a tool for Linux that allows tocreate multiple hidden volumes on a storage device in such a way that it is very difficult, evenunder forensic inspection, to prove the existence of such volumes. This is useful for peoplewhose freedom of expression is threatened through coercion by repressive authorities ordangerous criminal organizations, in particular: whistleblowers, investigative journalists, andactivists for human rights in oppressive regimes. You can consider Shufflecake a "spiritualsuccessor" of tools such as TrueCrypt and VeraCrypt, but vastly improved: it works nativelyon Linux, it supports any filesystem of choice, and can manage multiple nested volumes perdevice, so to make deniability of the existence of these partitions really plausible.Shufflecake is FLOSS (Free/Libre, Open Source Software) released under the GNU GeneralPublic License v2.0 or superior.

Speaker's Bio

Tommaso Gagliardoni is a cryptographer, privacy hacktivist, and quantum security expert. He works as a researcher and innovation leader at Kudelski Security, a Swiss-American security company providing tailored solutions to enterprises and public-sector clients.

Tommaso published influential peer-reviewed papers in the areas of cryptography, quantum computing, security, and privacy, and spoke at many international conferences in these fields. He is known, among other achievements, for his collaborations in solving the longstanding problem of adaptive quantum authentication (EUROCRYPT 2018, TQC 2019) and breaking the security of ISO-standard smart card protocol PLAID (Real World Crypto 2015, SSR 2015). He serves as a Program Committee member at international academic conferences focused on cryptography and quantum computing, such as PQCRYPTO. He also has a background in privacy hacktivism and ethical hacking, speaking at venues such as the International Journalism Festival and the E-Privacy Meeting, and being a strong advocate of the FOSS philosophy and digital freedoms.

Tommaso obtained an M.Sc. in Mathematics at the University of Perugia, Italy, and a PhD at the Technical University of Darmstadt, Germany, with a dissertation on the quantum security of cryptographic primitives. Before joining Kudelski Security, he worked in the Security and Privacy group at IBM Research Zurich.