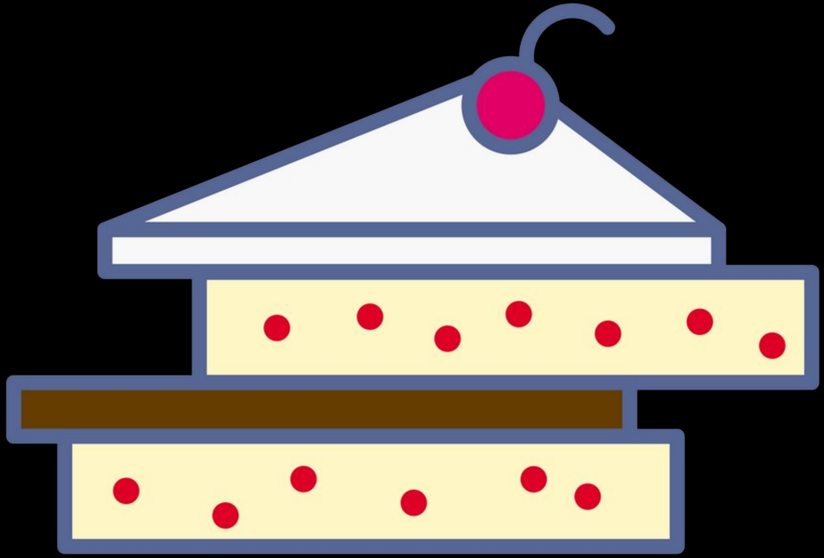
Shufflecake

AKA TrueCrypt on Steroids for Linux



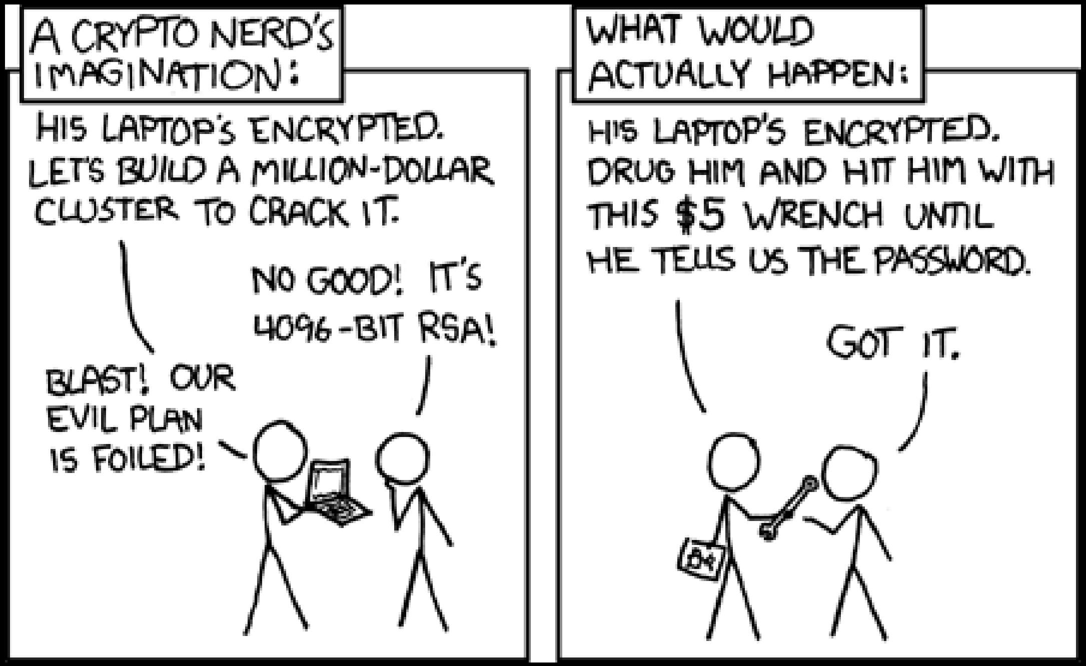
Elia Anzuoni and Tommaso “tomgag” Gagliardoni
Kudelski Security, Switzerland

DEF CON 31 Demo Labs
2023-08-11, Las Vegas (NV), USA

Overview

- Plausible Deniability
- TrueCrypt (and VeraCrypt)
- Shufflecake
- Future directions

Plausible Deniability

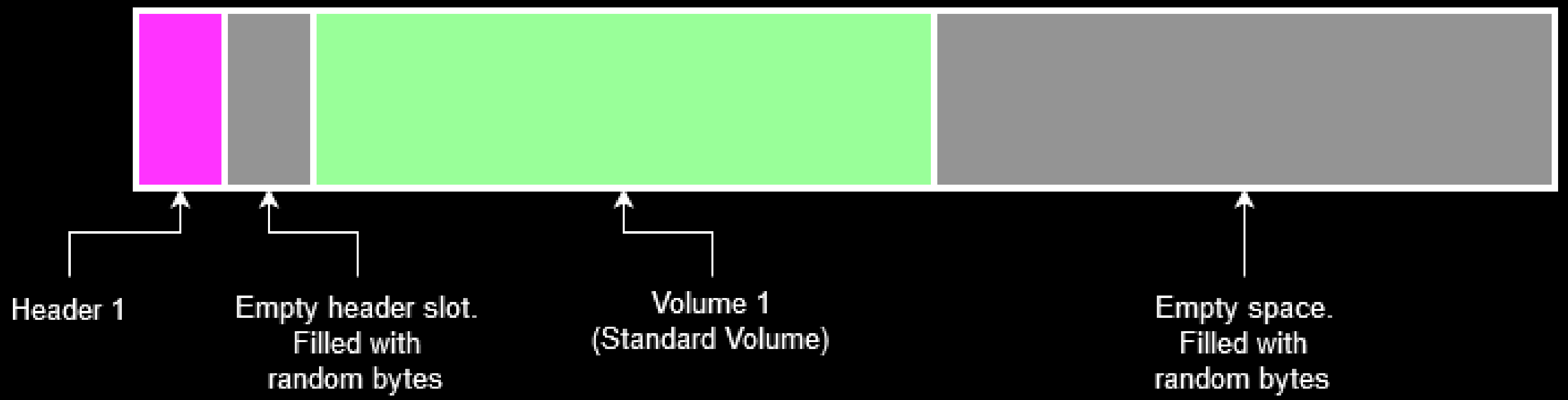


TrueCrypt (and VeraCrypt)

TrueCrypt: one of the earliest, efficient full-disk encryption software (released 2004)

Troubled history, discontinued in 2014, replaced by VeraCrypt

A TrueCrypt disk with just the Standard Volume



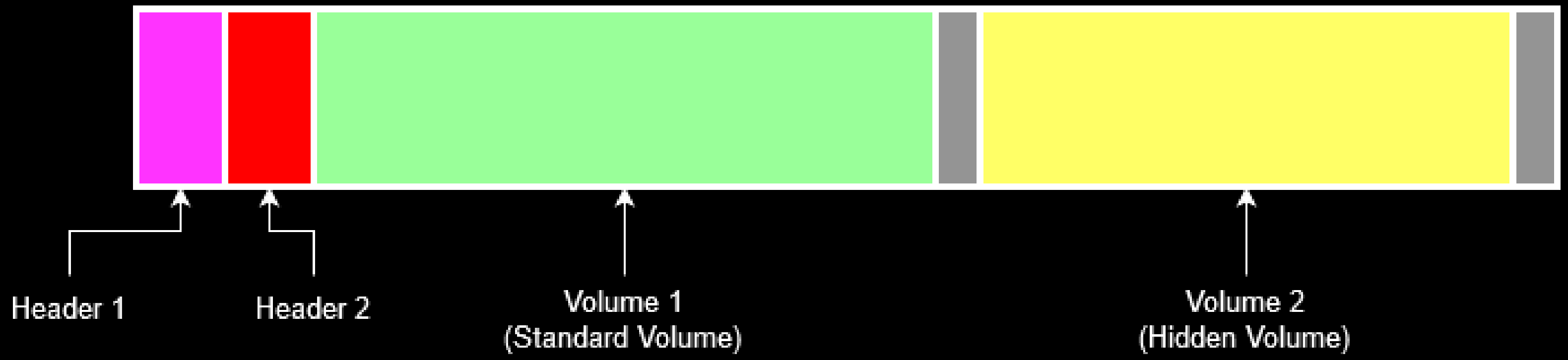
TrueCrypt (and VeraCrypt)

TrueCrypt: one of the earliest, efficient full-disk encryption software (released 2004)

Troubled history, discontinued in 2014, replaced by VeraCrypt

VeraCrypt

A TrueCrypt disk with the Standard Volume and the Hidden Volume



Who is this for?

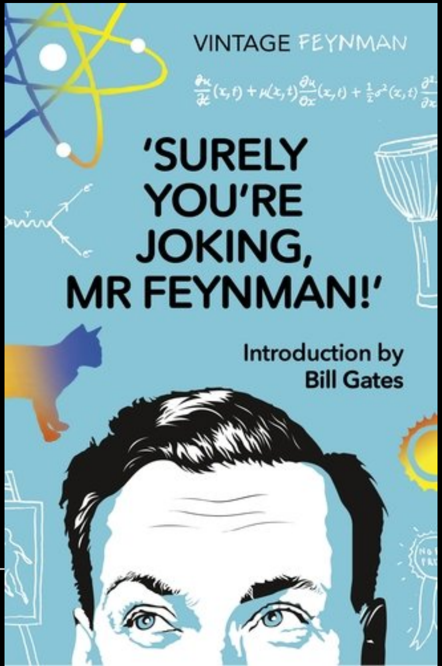
- Repressed minorities in low-democracy countries
- Investigative journalists
- Whistleblowers
- Human right activists in repressive regimes

Problems with TrueCrypt

- Single-snapshot secure
- Container must be FAT
- Only 2 layers of secrecy

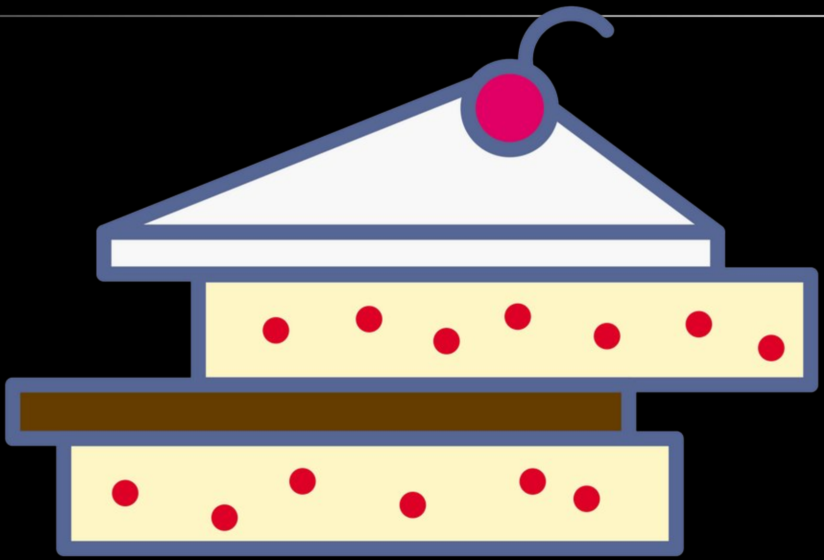
Objections

- TrueCrypt is dead, we use VeraCrypt now Same.
- I still use FAT on my laptop
- I only use the FDE feature of VeraCrypt
- LUKS can do plausible deniability too, you just need to fill the disc with random data, make a bootable USB drive with your bootloader on it, make a LUKS header only file on that USB drive, and then create an encrypted filesystem on the disc using that detached header file. You'll want to backup that header file, and possibly hide it with another encrypted volume using a headerless encryption on the USB drive. It's OK as long as both the USB drive and the disc stay inside the pentacle you just painted on the floor with black chicken blood.



Shufflecake

- Native for Linux
- File-System agnostic
- Nested volumes
- One password to open
- Block re-randomization
- GPLv2 "or superior"
- Low-level tool



Shufflecake

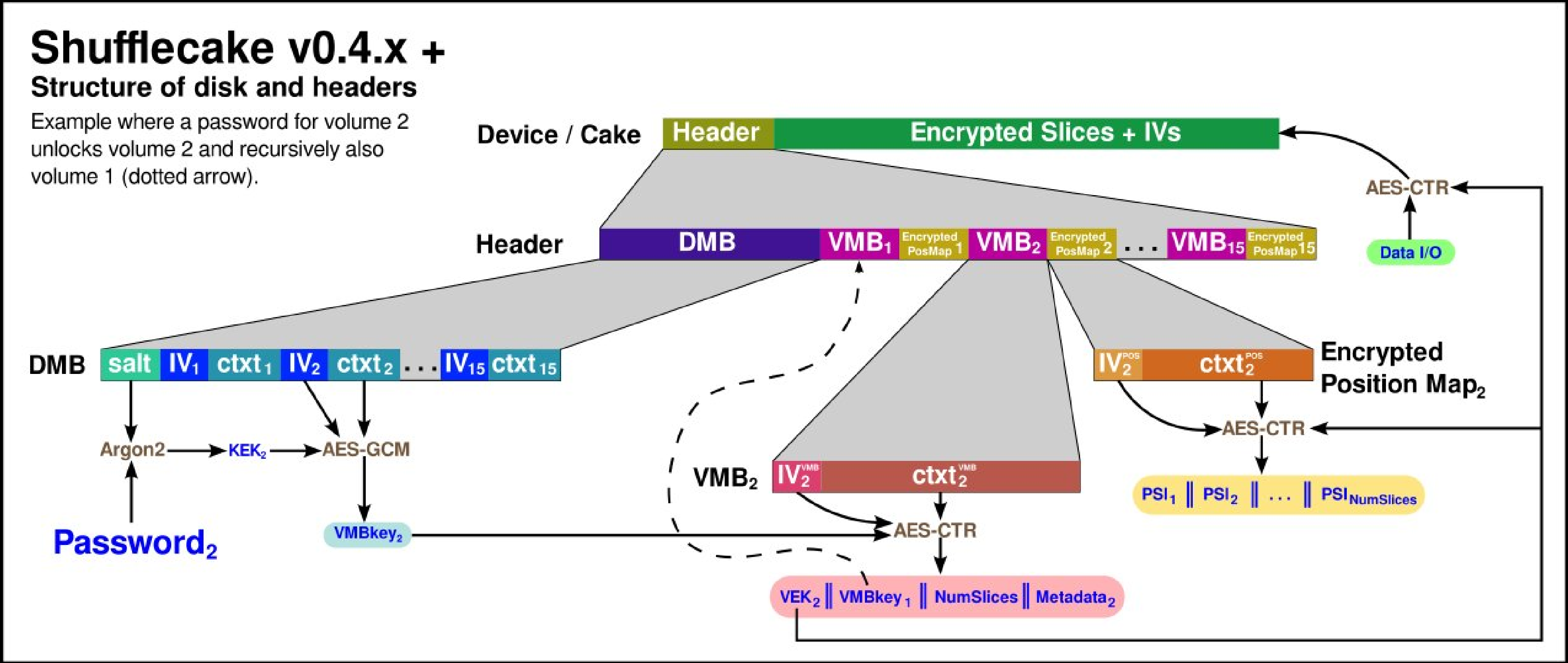
Operating Principles

- One device = multiple volumes
- 1 volume = 1 password
- Volumes are numbered (from less to most secret)
- Unlocking volume N also unlocks volume N-1

Cryptography

- Argon2id for KDF
- AES-GCM for authentication
- AES-CTR for bulk encryption (not XTS, why?)

Shufflecake



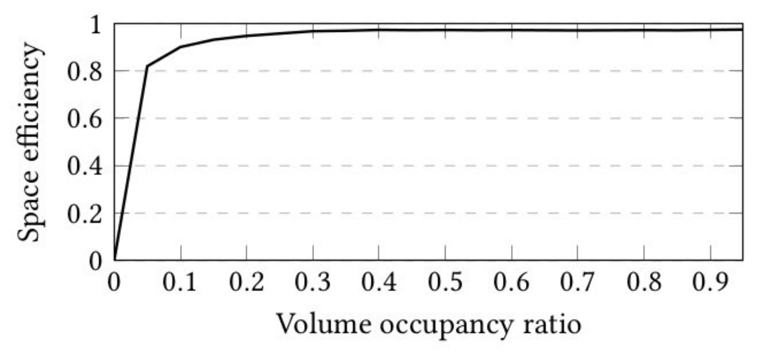
Shufflecake

- init <block_device>
- open <block_device>
- close <block_device>

DEMO

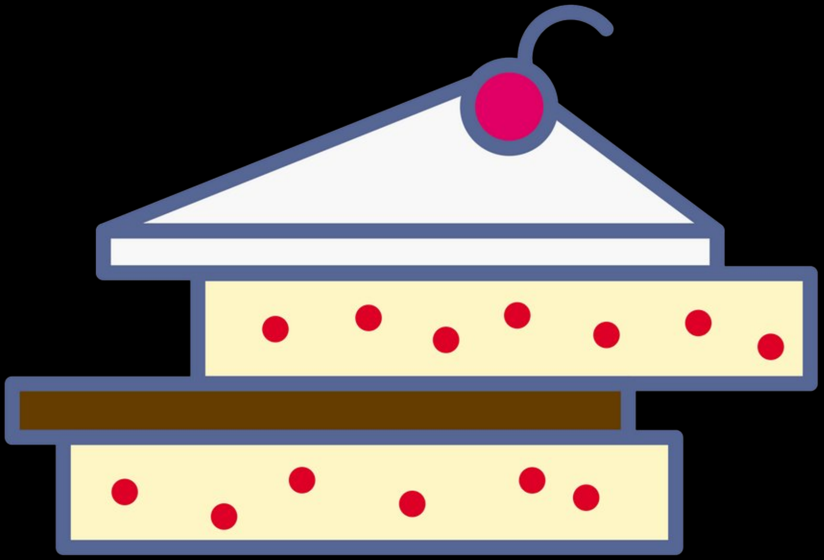
	Shufflecake	dm-crypt/LUKS	VeraCrypt
random write	26.77	38.43	39.07
random read	26.78	38.44	39.09
sequential write	176.87	247.14	247.75
sequential read	177.10	247.43	248.04

Table 1: I/O performance (in MB/s) of Shufflecake, dm-crypt/LUKS, and VeraCrypt.



Future Directions

- Multi-snapshot security
- Start from bootloader (FDE)
- Shufflecake OS
- Crash consistency
- Corruption resistance
- “Lite” version
- Unbounded volumes
- Distribute through DKMS
- Packetization



Future Directions

Coming soon…

Shufflecake: Plausible Deniability For Multiple Hidden Filesystems On Linux

Elia Anzuoni
ETHZ and EPFL and Kudelski Security
Switzerland

Tommaso Gagliardoni
Kudelski Security
Switzerland

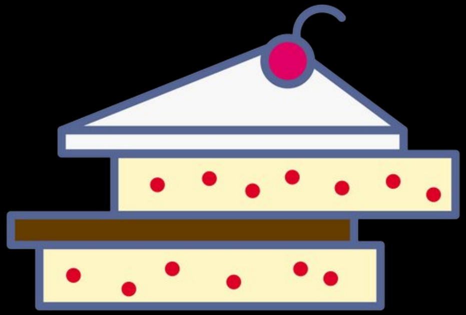
ABSTRACT

We present Shufflecake, a new plausible deniability design to hide the existence of encrypted data on a storage medium making it very difficult for an adversary to prove the existence of such data.

by means of (physical, legal, psychological) coercion, they can obtain the encryption keys to any encrypted content identifiable on the user's device. The security goal in this scenario, then, becomes to still retain secrecy of some selected, "crucial" data on the disk, by

How to contribute

- Code https://codeberg.org/shufflecake
- Jabber xmpp:shufflecakeATconference.draugr.de
- Mastodon @shufflecake@fosstodon.org
- Website https://shufflecake.net
- Email websiteATshufflecakeDOTnet



Thank you for your attention!