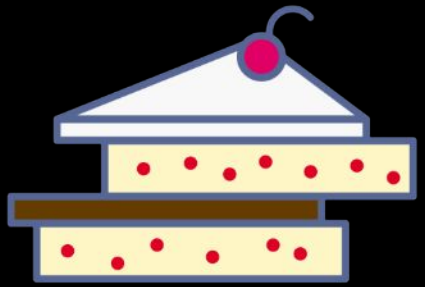
Shufflecake

l'evoluzione di TrueCrypt per la negabilità plausibile su disco



Tommaso Gagliardoni, Kudelski Security

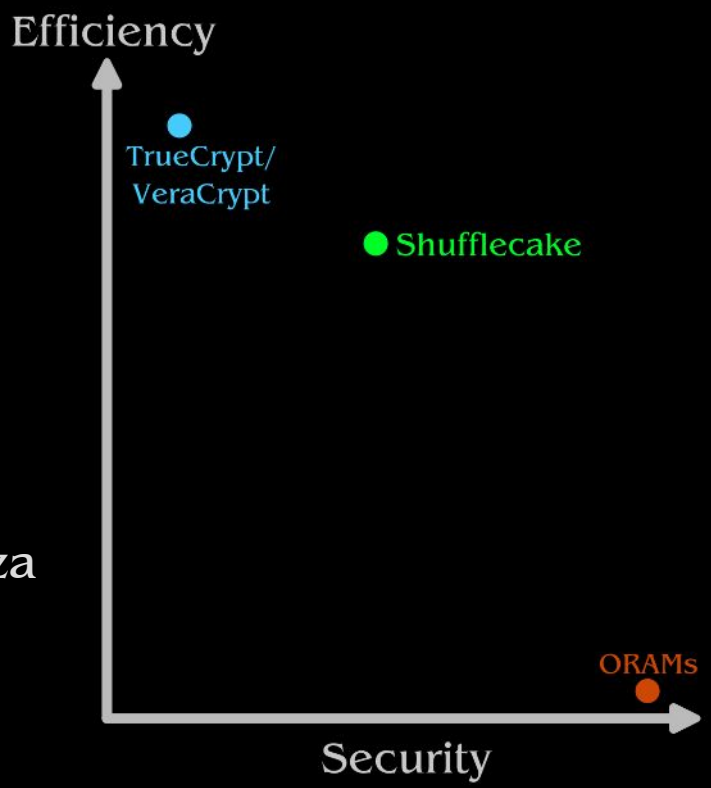
Da una collaborazione con Elia Anzuoni

E-Privacy XXXIV (2024)

2024-05-16, Firenze, Italy

Shufflecake: TL;DR

- Nasconde l'esistenza di partizioni su disco
- Negabilità plausibile – non steganografia
- Evoluzione rispetto a TrueCrypt/VeraCrypt
- Dimostrazione formale di sicurezza crittografica
- Più performante di soluzioni ORAM
- FLOSS ("free" as in "freedom")
- Possibilità di migliorare ulteriormente la sicurezza



Shufflecake: TL;DR

Shufflecake

AKA TrueCrypt on Steroids for Linux

DEF CON 31 Demo Labs

2023-08-11, Las Vegas (NV), USA

Introducing Shufflecake: Plausible Deniability For Multiple Hidden Filesystems on Linux (kudelskisecurity.com) 90

Posted by EditorDavid on Saturday November 12, 2022 @02:34PM from the magic-mounting dept.

Thursday the Kudelski Group's cybersecurity division released "a tool for Linux that allows creation of 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."

"Each volume is encrypted with a different secret key, scrambled across the empty space of an underlying existing storage medium, and indistinguishable from random noise when not decrypted."

> Even if the presence of the Shufflecake software itself cannot be hidden — and hence the

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 making the presence of such data not even identifiable, thus allow-

30th Anniversary 2023 acm SIGSAC

ACM CCS 2023

26-30 NOV., 2023

Radici nel passato di E-Privacy

Negabilità plausibile su disco: luci e ombre di Truecrypt

Tommaso Gagliardoni

tommaso[AT)gagliardoni(DOT]net

E-privacy 2011

Firenze, 3 Giugno 2011

Radici nel passato di E-Privacy

Negabilità plausibile su disco: luci e ombre di Truecrypt

Tommaso Gagliardoni

tommaso[AT)gagliardoni(DOT]net

E-privacy 2011

Firenze, 3 Giugno 2011

Mi presento

Tommaso “tomgag” Gagliardoni

- Attivo nel Progetto Winson Smith circa 2007-2012
- Laurea in matematica all’Università degli Studi di Perugia
- Dottorato di ricerca in crittografia alla TU Darmstadt, Germania
- Post-doc a IBM Research a Zurigo, gruppo Security & Privacy
- Dal 2019: ricercatore crittografo a Kudelski Security, Svizzera

Mi presento

Tommaso “tomgag” Gagliardoni

- Attivo nel Progetto Winson Smith circa 2007-2012
- Laurea in matematica all’Università degli Studi di Perugia
- Dottorato di ricerca in crittografia alla TU Darmstadt, Germania
- Post-doc a IBM Research a Zurigo, gruppo Security & Privacy
- Dal 2019: ricercatore crittografo a Kudelski Security, Svizzera

More business ⟷ Less business

Sommario

- TL;DR
- Bio
- Introduzione
- TrueCrypt (e VeraCrypt)
- ORAMs e wo-ORAMs
- Shufflecake
- Implementazione e benchmarks
- Direzioni future
- Come contribuire

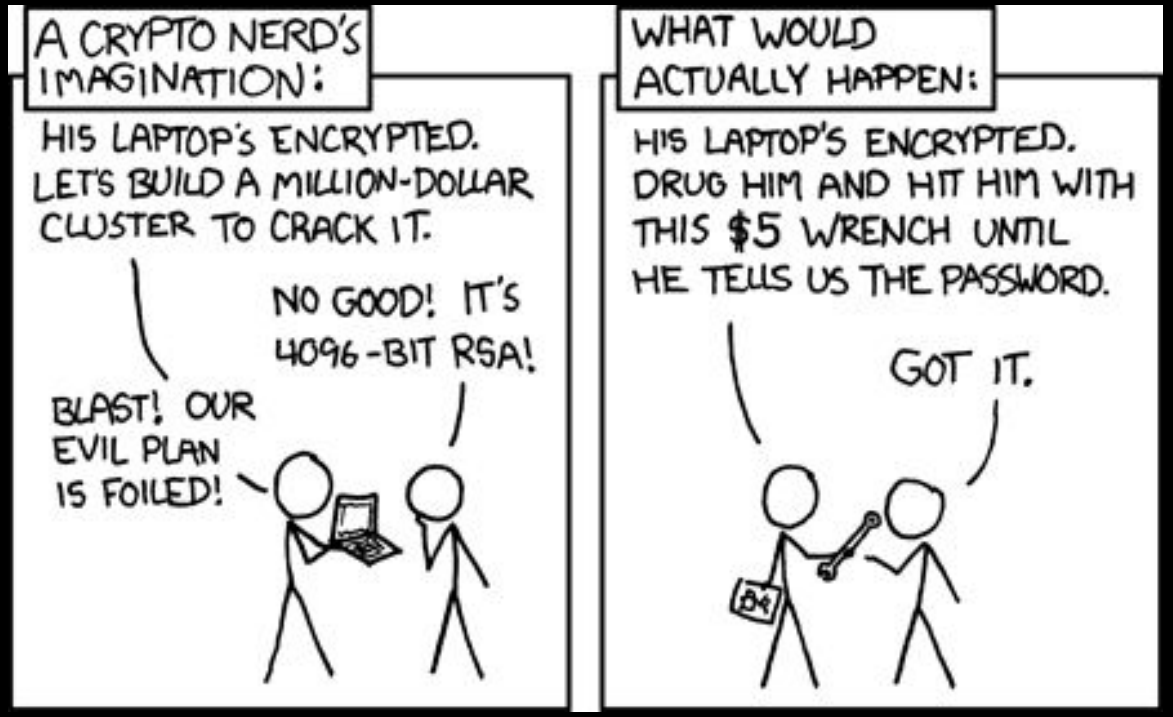
Introduzione

Introduzione

- BitLocker (Windows)
- FileVault 2 (MacOS)
- LUKS (Linux)
- ...

Introduzione

- BitLocker (Windows)
- FileVault 2 (MacOS)
- LUKS (Linux)
- ...



How bad is it?

How bad is it?

Legislation by nation
- Antigua and Barbuda
- Australia
- Belgium
- Cambodia
- Canada
- Czech Republic
- Finland
- France
- Germany
- Iceland
- India
- Ireland
- New Zealand
- Poland
- South Africa
- Spain
- Sweden
- Switzerla

Key disclosure law

Article Talk

From Wikipedia, the free encyclop

Key disclosure laws, also known a

law enforcement. The purpose is t

Man jailed over computer password refusal

5 October 2010

Campaigners hit by decryption law

By Mark Ward

Technology correspondent, BBC News website

Animal rights activists are thought to be the first Britons to

FRONTIER FOUNDATION

US v. Fricosu

EFF urged a federal district court in Colorado to block the government's attempt to force a woman to enter a password into an encrypted laptop, arguing that it would violate her Fifth Amendment

How a Syrian refugee risked his life to bear witness to atrocities

A few hours before leaving his home in Syria to begin a new life in Canada, Mostafa picked up a kitchen knife and began cutting into his left arm

Why Cage director was guilty of withholding password

25 September 2017

TrueCrypt (e VeraCrypt)

TrueCrypt: una delle prime soluzioni efficienti di disk encryption (2004)

TrueCrypt (e VeraCrypt)

TrueCrypt: una delle prime soluzioni efficienti di disk encryption (2004)

Storia travagliata, sviluppo interrotto nel 2014, rimpiazzato da VeraCrypt

Don't mess up with this guy lol

TrueCrypt (e VeraCrypt)

TrueCrypt: una delle prime soluzioni efficienti di disk encryption (2004)

Storia travagliata, sviluppo interrotto nel 2014, rimpiazzato da VeraCrypt

User data (FAT16 filesystem)

Empty Space (FAT16 Filesystem: Contiguous)

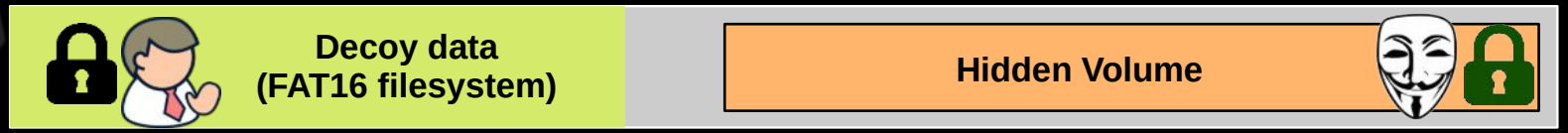
Normal (Disk Encryption) Mode

TrueCrypt (e VeraCrypt)

TrueCrypt: una delle prime soluzioni efficienti di disk encryption (2004)

Storia travagliata, sviluppo interrotto nel 2014, rimpiazzato da VeraCrypt

Normal (Disk Encryption) Mode



Plausible Deniability Mode

TrueCrypt (e VeraCrypt)

TrueCrypt: una delle prime soluzioni efficienti di disk encryption (2004)

Storia travagliata, sviluppo interrotto nel 2014, rimpiazzato da VeraCrypt

Normal (Disk Encryption) Mode

Plausible Deniability Mode

A chi serve?

- Minoranze represse in paesi a bassa democrazia
- Giornalisti investigativi
- Whistleblowers
- Attivisti dei diritti umani in regimi oppressivi

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

- TrueCrypt è morto, si usa VeraCrypt ora

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

- TrueCrypt è morto, si usa VeraCrypt ora Stesso.

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

- TrueCrypt è morto, si usa VeraCrypt ora Stesso.
- Ma io uso ancora FAT sul mio laptop

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

- TrueCrypt è morto, si usa VeraCrypt ora Stesso.
- Ma io uso ancora FAT sul mio laptop
- Uso VeraCrypt ma senza partizioni nascoste, giuro!

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

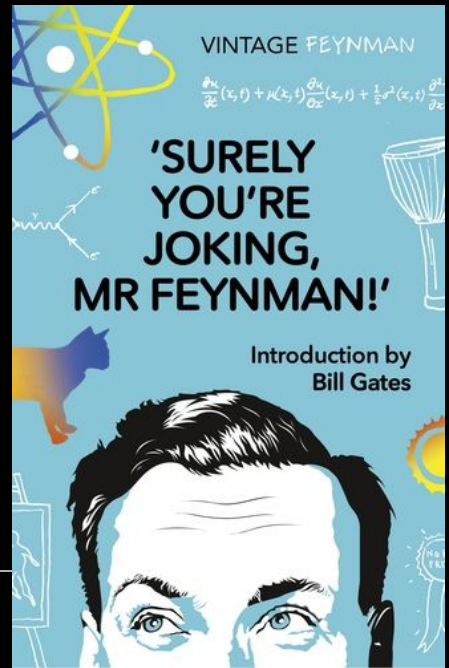
- TrueCrypt è morto, si usa VeraCrypt ora Stesso.
- Ma io uso ancora FAT sul mio laptop
- Uso VeraCrypt ma senza partizioni nascoste, giuro!
- Anche LUKS offre negabilità plausibile, tutto quel che bisogna fare è sovrascrivere il disco con dati random, creare una chiavetta USB bootabile con dentro il tuo bootloader, crearci dentro un file che contiene un header LUKS separato, e poi creare un filesystem cifrato sul disco usando quel file separato come header. Sarebbe meglio fare anche un backup di quel file header, e magari nasconderlo nella chiavetta usando un altro sistema di cifratura senza headers. Il tutto funziona bene, fintanto che sia la chiavetta USB che il disco restano all'interno del pentacolo che hai disegnato sul pavimento con sangue di gallo nero...

Problemi di TrueCrypt

- Sicurezza solo single-snapshot
- Il filesystem del volume container può solo essere FAT
- Solo 2 livelli di sicurezza

Obiezioni

- TrueCrypt è morto, si usa VeraCrypt ora Stesso.
- Ma io uso ancora FAT sul mio laptop
- Uso VeraCrypt ma senza partizioni nascoste, giuro!
- Anche LUKS offre negabilità plausibile, tutto quel che bisogna fare è sovrascrivere il disco con dati random, creare una chiavetta USB bootabile con dentro il tuo bootloader, crearci dentro un file che contiene un header LUKS separato, e poi creare un filesystem cifrato sul disco usando quel file separato come header. Sarebbe meglio fare anche un backup di quel file header, e magari nasconderlo nella chiavetta usando un altro sistema di cifratura senza headers. Il tutto funziona bene, fintanto che sia la chiavetta USB che il disco restano all'interno del pentacolo che hai disegnato sul pavimento con sangue di gallo nero...

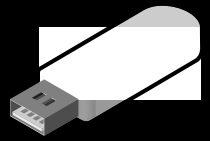


Parliamo di... multi-snapshot!

Physical volume (hard disk/partition)

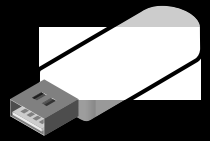
Decoy data (FAT16 filesystem)	Empty space (?)

Parliamo di… multi-snapshot!



"modern" solid-state drives: caching / layering / TRIM

Parliamo di… multi-snapshot!



"modern" solid-state drives: caching / layering / TRIM

Sicurezza multi-snapshot

- Gli attacchi multi-snapshot sono estremamente difficili da eludere
- Ma sono davvero possibili in pratica? Difficile a dirsi
- Soluzioni single-snapshot hanno già avuto successo in passato

Sicurezza multi-snapshot

- Gli attacchi multi-snapshot sono estremamente difficili da eludere
- Ma sono davvero possibili in pratica? Difficile a dirsi
- Soluzioni single-snapshot hanno già avuto successo in passato

- Esiste un modo: ORAMs (Oblivious Random Access Machines)
- Sicurissimo, ma ridicolmente lento (non pratico per i nostri scopi)

Sicurezza multi-snapshot

- Gli attacchi multi-snapshot sono estremamente difficili da eludere
- Ma sono davvero possibili in pratica? Difficile a dirsi
- Soluzioni single-snapshot hanno già avuto successo in passato

- Esiste un modo: ORAMs (Oblivious Random Access Machines)
- Sicurissimo, ma ridicolmente lento (non pratico per i nostri scopi)

- Recentemente: write-only ORAMs (wo-ORAMs)
- Ricerca attiva, potenzialmente più efficienti di ORAM pure

Sicurezza multi-snapshot

- Gli attacchi multi-snapshot sono estremamente difficili da eludere
- Ma sono davvero possibili in pratica? Difficile a dirsi
- Soluzioni single-snapshot hanno già avuto successo in passato

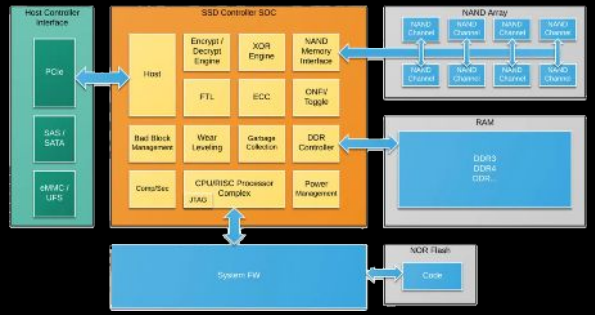
- Esiste un modo: ORAMs (Oblivious Random Access Machines)
- Sicurissimo, ma ridicolmente lento (non pratico per i nostri scopi)

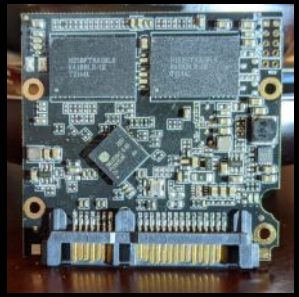
- Recentemente: write-only ORAMs (wo-ORAMs)
- Ricerca attiva, potenzialmente più efficienti di ORAM pure
- Ma comunque orribilmente inefficienti (~200x slowdown in I/O, spreco del 75% di spazio su disco, etc)
- L'uso di wo-ORAMs per la NP su disco si basa sull'osservazione che le operazioni di *read* non cambiano lo stato del disco

Possiamo fare di meglio?

Possiamo fare di meglio?

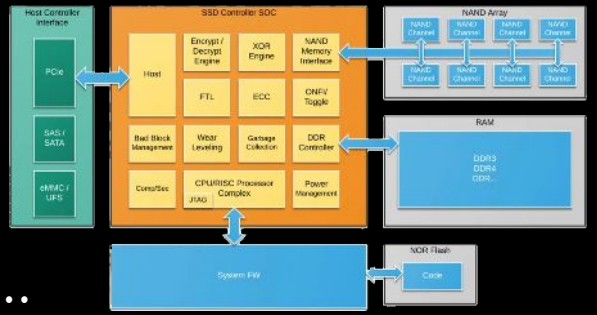
- Wo-ORAM: davvero sicure?

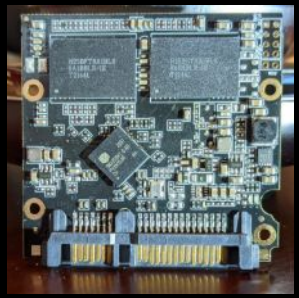




Possiamo fare di meglio?

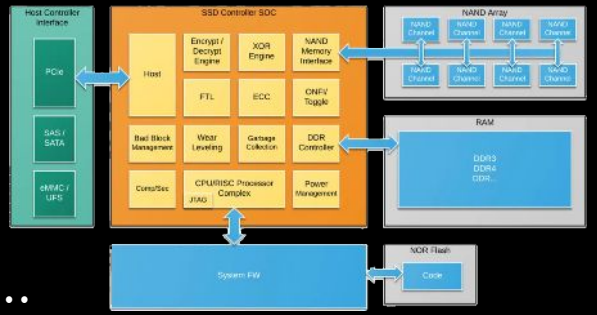
- Wo-ORAM: davvero sicure?
- Sicurezza 100% = ORAM
- Ma le ORAMs sono troppo lente...

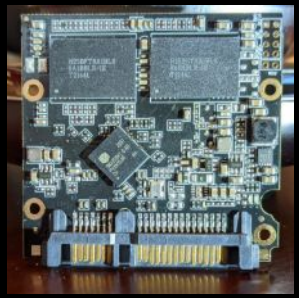




Possiamo fare di meglio?

- Wo-ORAM: davvero sicure?
- Sicurezza 100% = ORAM
- Ma le ORAMs sono troppo lente…

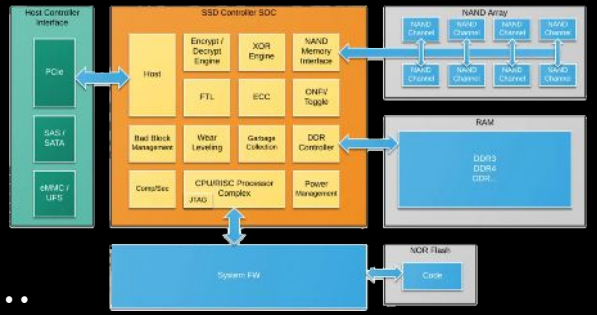


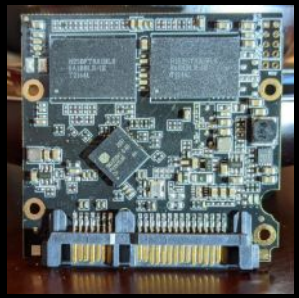


- E a riguardo di sicurezza pratica / legale ?
- Sicuri con "probabilità sufficientemente alta"?
- Colpevolezza *"con 2/3 di probabilità"*?

Possiamo fare di meglio?

- Wo-ORAM: davvero sicure?
- Sicurezza 100% = ORAM
- Ma le ORAMs sono troppo lente…



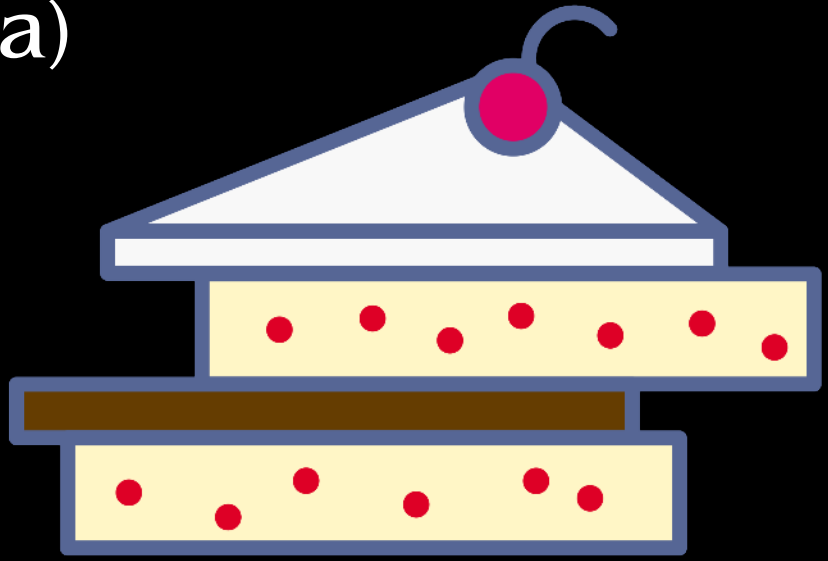


- E a riguardo di sicurezza pratica / legale ?
- Sicuri con "probabilità sufficientemente alta"?
- Colpevolezza *"con 2/3 di probabilità"*?

- E per quanto riguarda la sicurezza operativa ?
- E le limitazioni su, es., tipo di filesystem, o numero di livelli di sicurezza?

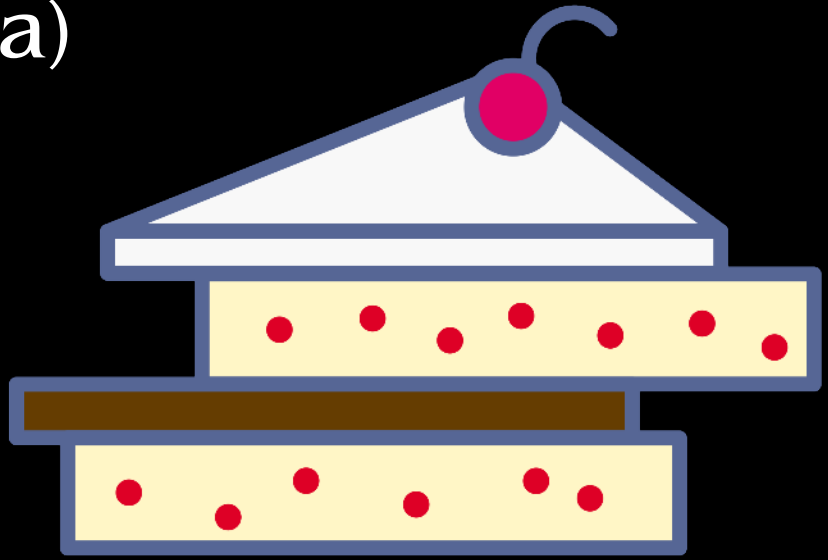
Shufflecake

- Nativo per Linux (per ora)
- Filesystem-agnostico
- Livelli nidificati multipli
- 1-password to open
- Block re-randomization
- GPLv2



Shufflecake

- Nativo per Linux (per ora)
- Filesystem-agnostico
- Livelli nidificati multipli
- 1-password to open
- Block re-randomization
- GPLv2 "o superiore"



Shufflecake

Principi operativi

- 1 dispositivo = volumi multipli
- 1 volume = 1 password
- Volumi numerati (dal meno al più sicuro)
- Sblocco del volume N sblocca anche il volume N-1

Shufflecake

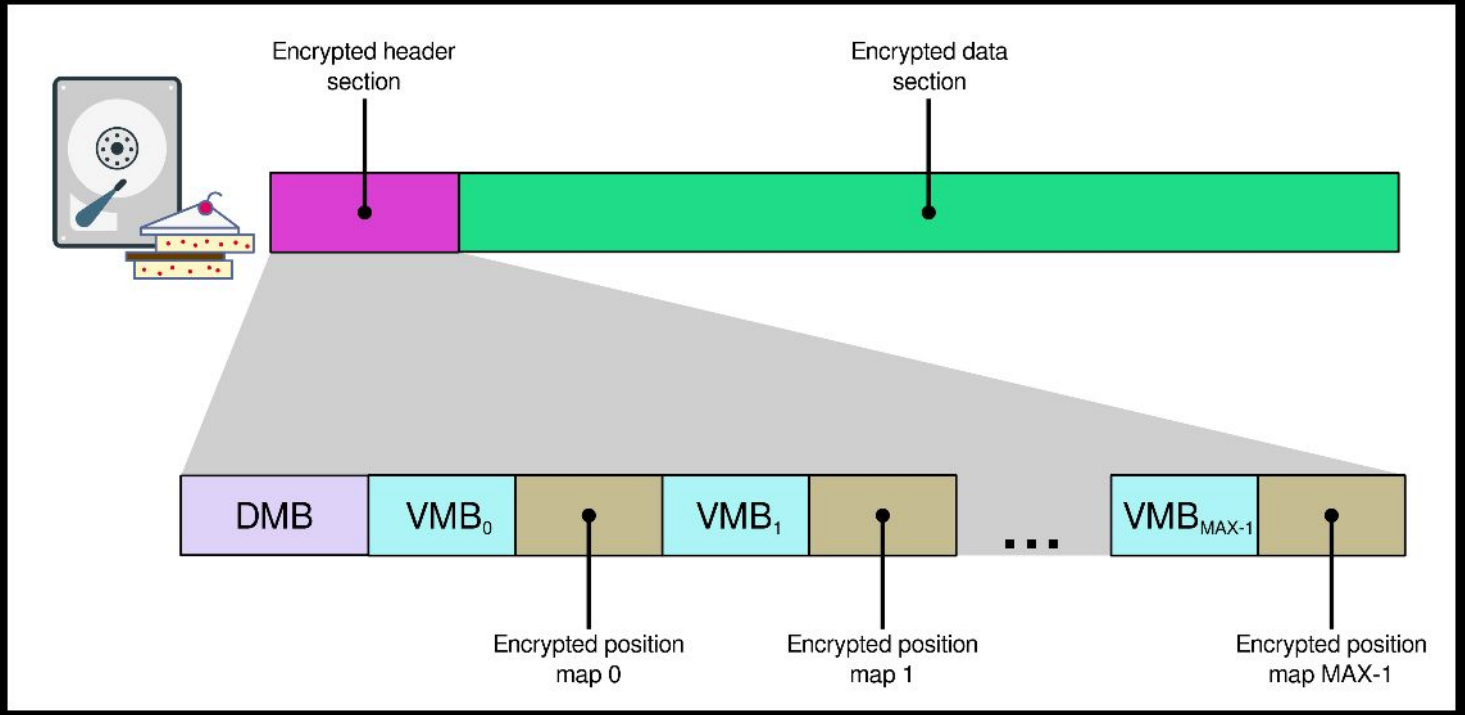
Principi operativi

- 1 dispositivo = volumi multipli
- 1 volume = 1 password
- Volumi numerati (dal meno al più sicuro)
- Sblocco del volume N sblocca anche il volume N-1

Crittografia

- Cifrari standard e ben testati (Argon2id, AES)
- Dimostrazione matematica di sicurezza (per il caso single-snapshot)

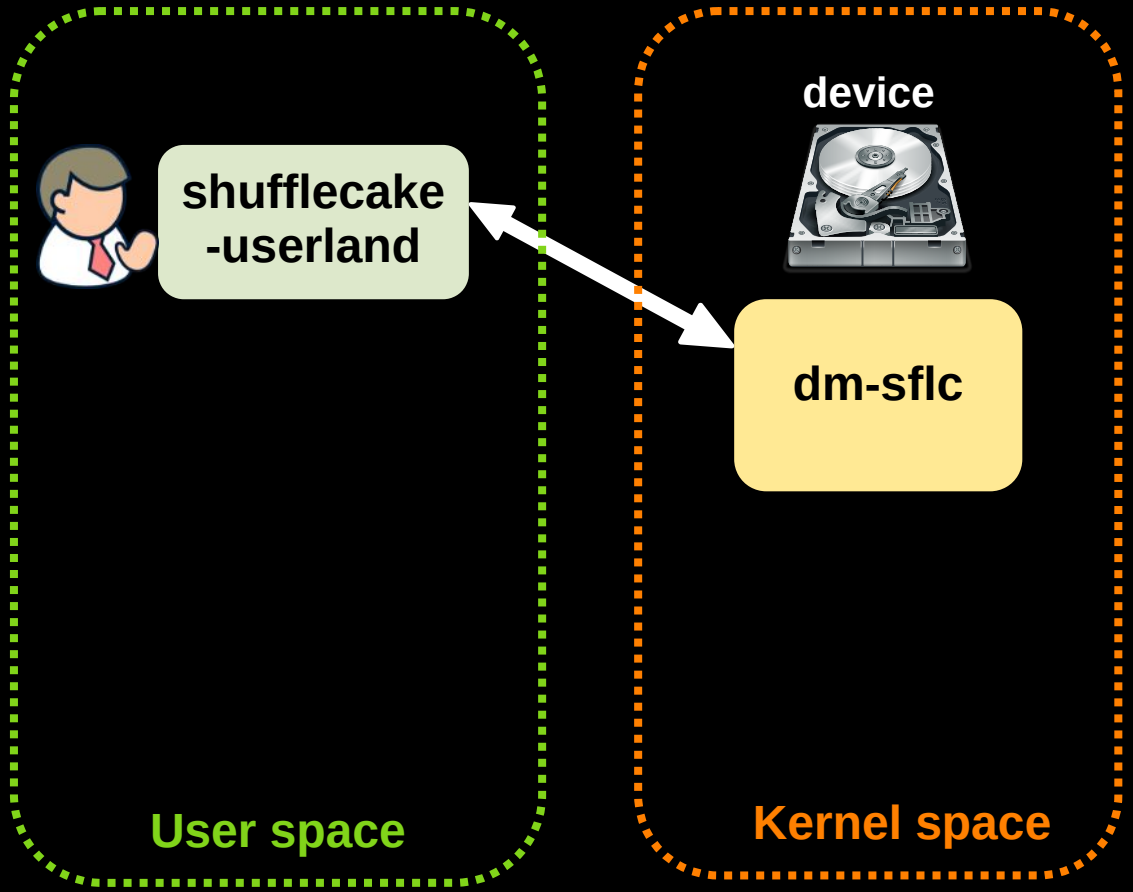
Shufflecake: disk layout



DMB = Device Master Block VMB = Volume Master Block

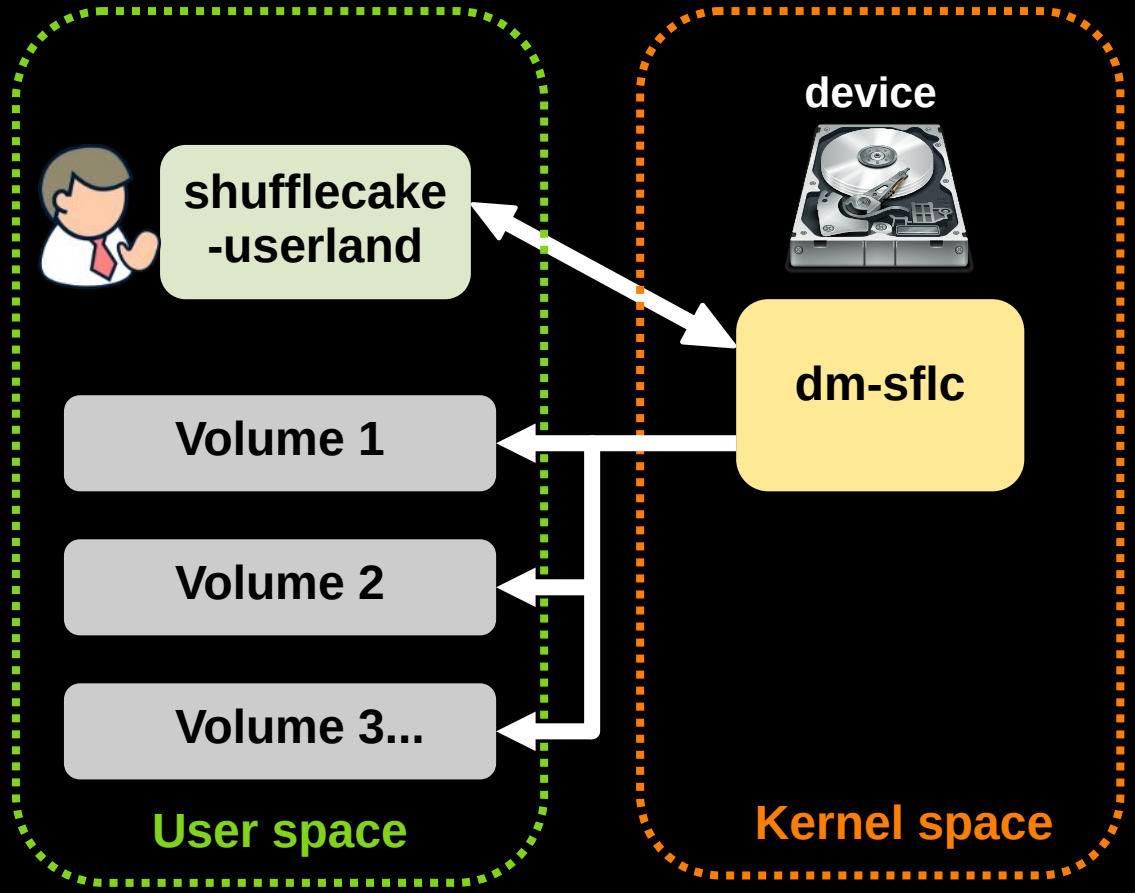
Header size: 60 MiB per disco da 1 TB (caso peggiore)

Shufflecake: implementazione



- Crittografia più avanzata in userspace
- Migliore integrazione, gestione errori, etc
- Uso di `/sys` per comunicazione e stats

Shufflecake: implementazione



- Crittografia più avanzata in userspace
- Migliore integrazione, gestione errori, etc
- Uso di `/sys` per comunicazione e stats
- Volumi nascosti appaiono come `/dev/mapper/sflc_X_Y`
- Possono essere usati come qualsiasi block device (formattati a piacere, montati, etc)

Shufflecake: implementazione

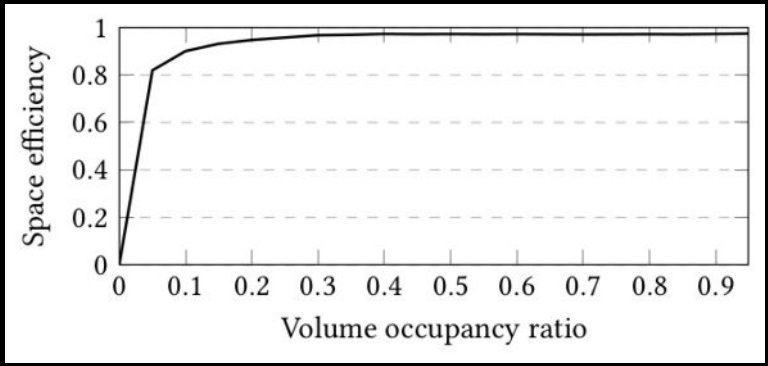
- `shufflecake init <block_device>`
- `shufflecake open <block_device>`
- `shufflecake close <block_device>`

Shufflecake: implementazione

- `shufflecake init <block_device>`
- `shufflecake open <block_device>`
- `shufflecake close <block_device>`

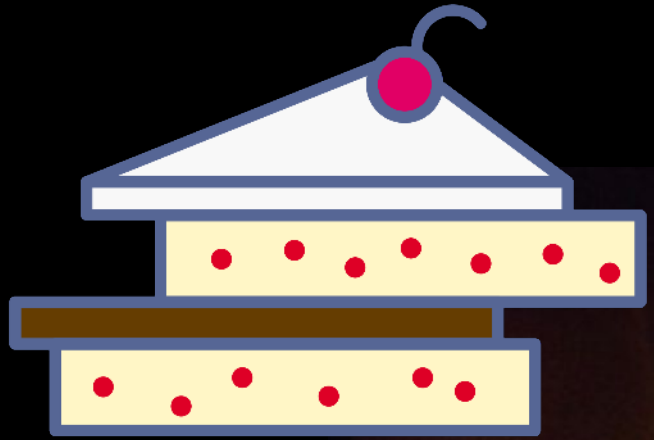
	Shufflecake	dm-crypt/LUKS	VeraCrypt
random write	26.77	38.43	39.07
random read	26.78	38.44	39.09
sequential write	176.87	247.14	247.75
sequential read	177.10	247.43	248.04

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



- ~30% più lento di LUKS/VeraCrypt
- Spreco di spazio trascurabile

Direzioni future



Minuzie e collaborazioni esterne

Shufflecake è ancora un tool sperimentale molto a basso livello

- Espandere ad altre distro Linux (per ora: Debian, Ubuntu)
- **`make install`**
- Distribuire il modulo kernel con DKMS
- Pacchettizzazione (.deb, .rpm etc)
- Documentazione developer

Minuzie e collaborazioni esterne

Shufflecake è ancora un tool sperimentale molto a basso livello

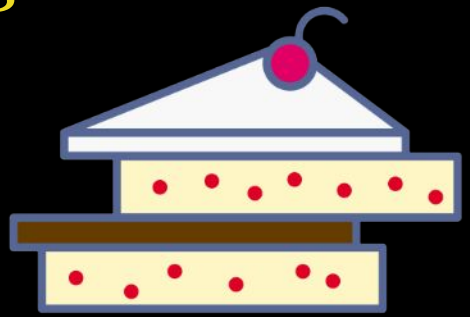
- Espandere ad altre distro Linux (per ora: Debian, Ubuntu)
- **`make install`**
- Distribuire il modulo kernel con DKMS
- Pacchettizzazione (.deb, .rpm etc)
- Documentazione developer
- Porting in Rust?
- GUI?
- Versione Windows/iOS?

Work in progress e piani futuri

- Crash consistency
- (Partial) multi-snapshot security
- Shufflecake “Lite”
- Corruption resistance
- Use of volume metadata
- Reclaiming unused slices
- Anti-safeword: unbounded number of volumes
- Hidden Shufflecake OS
- Shufflecake mobile

Come contribuire

- Code https://codeberg.org/shufflecake
- Jabber xmpp:shufflecake@conference.draugr.de
- Mastodon @shufflecake@fosstodon.org
- Website https://shufflecake.net
- E-mail website@shufflecake.net



Grazie per l'attenzione!