Negabilità plausibile su disco: luci e ombre di Truecrypt

Tommaso Gagliardoni

tommaso[AT)gagliardoni(DOT]net

E-privacy 2011

Firenze, 3 Giugno 2011

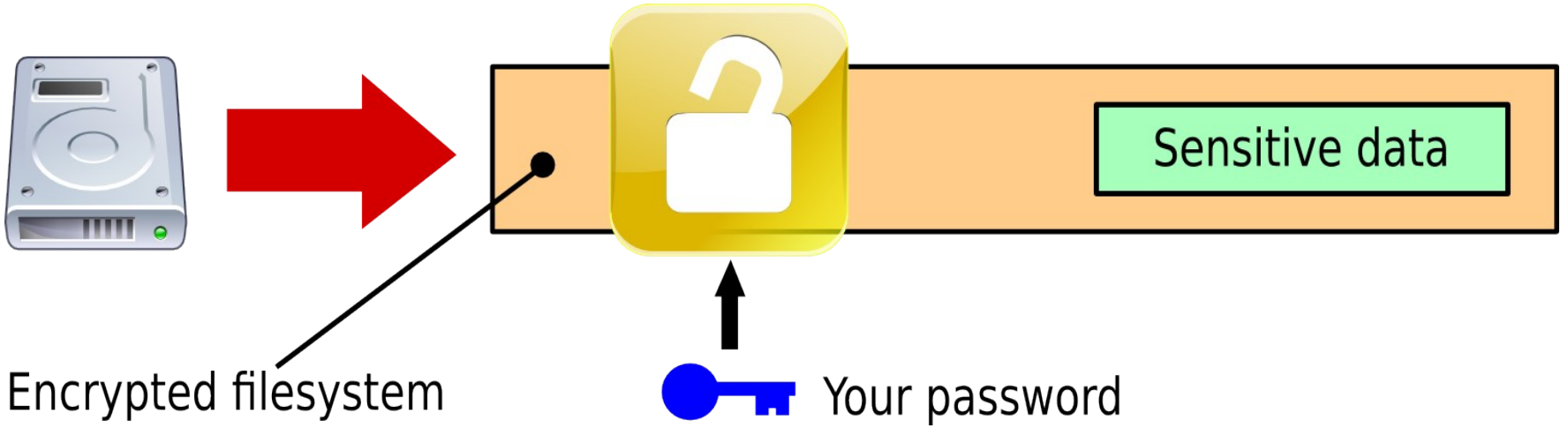
Sommario

- Introduzione
- Truecrypt
- Problemi di Truecrypt
- Conclusioni

Scenario: sei in possesso di informazioni preziose che qualcuno può essere molto motivato ad ottenere (ad esempio, sei un giornalista in contatto con un gruppo dissidente in un paese a bassa democrazia, e possiedi numeri di telefono/email/indirizzi di alcuni membri).

Vuoi tenere queste informazioni nel tuo computer per l'uso quotidiano.

Proteggi queste informazioni usando schemi di cifratura forte (ad esempio, sono salvate in un filesystem cifrato).



Problema: sei, per l'appunto, in un paese a bassa democrazia.

picture taken from xkcd.com

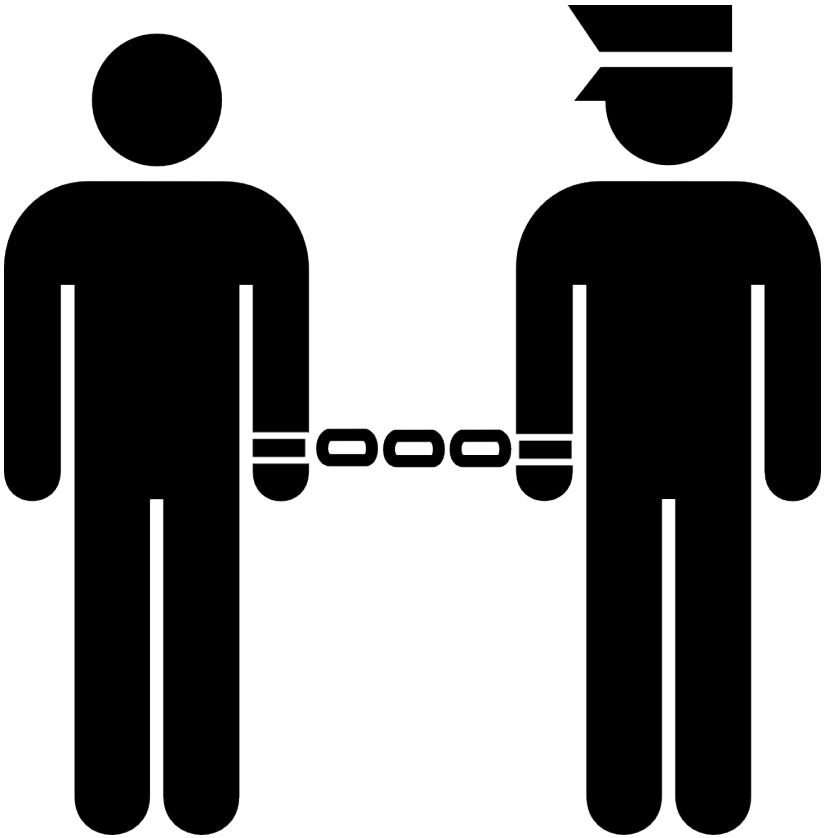
Non solo bassa democrazia:

Anche governi occidentali: Key Disclosure Laws. Alcuni esempi:

Belgio: un giudice può richiedere collaborazione **coatta e segreta**, pena fino a **1 anno di detenzione** e 100,000 EUR

UK: legge RIPA, ogni cittadino ha l'obbligo di fornire alle autorità informazioni di decrittazione su richiesta, pena fino a **2 anni di detenzione**.

France: come sopra, ma il rifiuto alla collaborazione comporta fino a **5 anni di detenzione** e 75,000 EUR.



Si tratta di leggi severe, ma che indubbiamente andranno usate solo nei casi più estremi. Speriamo non vengano mai usate.

Oh aspetta... È già successo!

UK, 2009: un **uomo schizofrenico** si rifiuta di consegnare una password durante una perquisizione, appellandosi al **diritto al silenzio**. Incarcerato per **9 mesi** e poi ricoverato in un **ospedale psichiatrico**. **Non vi era sospetto** che i dati cifrati in questione potessero contenere materiale illegale e l'uomo è stato in seguito giudicato **non rappresentare un pericolo** per la sicurezza nazionale.

UK, 2010: Oliver Drage, un ragazzo di **19 anni**, investigato per possesso di **materiale pedopornografico**. Al rifiuto di fornire la sua password di **50 caratteri** si è visto condannato a **4 mesi di reclusione**.

Negabilità Plausibile

L'idea è di proteggere le tue informazioni in modo da poter, qualora ce ne fosse il bisogno, mentire in maniera credibile sull'esistenza di quelle informazioni, la tua consapevolezza di esse o la tua capacità di accedervi.

Alcuni esempi:

Metodo 1: **“Ho dimenticato la password”** (difficilmente credibile, in molti casi un'analisi forense può provare il contrario)

Metodo 2: **dati cifrati** che, senza la corretta password, appaiono **tecnicamente indistinguibili da dati random** (ma chi è che tiene gigabytes di dati random nel proprio computer?)

Metodo 3: **dati nascosti**, cioè: “Ho un dato segreto cifrato nel computer, ma non puoi nemmeno dimostrare che esiste senza la giusta password”

Sommario

- Introduzione
- Truecrypt
- Problemi di Truecrypt
- Conclusioni

Truecrypt

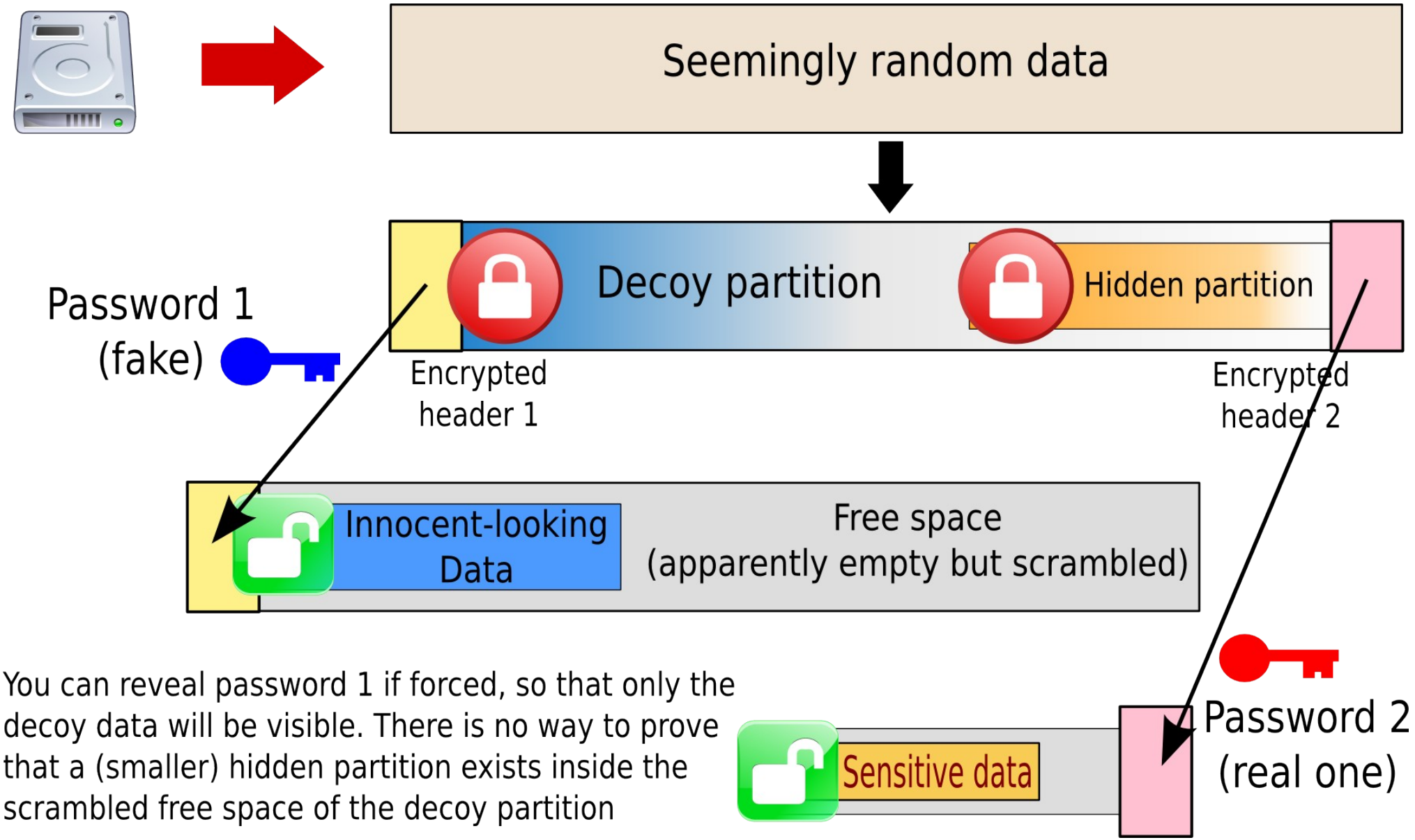
Truecrypt è un'utility per fare On-The-Fly-Encryption su disco

http:// www.truecrypt.org

- Multipiattaforma: supporta Linux, Mac OS X e diverse versioni di Windows
- Open source
- Può creare dischi virtuali cifrati multipli e indipendenti
- Può bootare un intero OS cifrato
- Usa algoritmi di cifratura military-grade (AES, Serpent, Blowfish, ...)
- Sviluppato dalla Truecrypt Foundation
- Negabilità Plausibile attraverso l'uso di **partizioni nascoste**

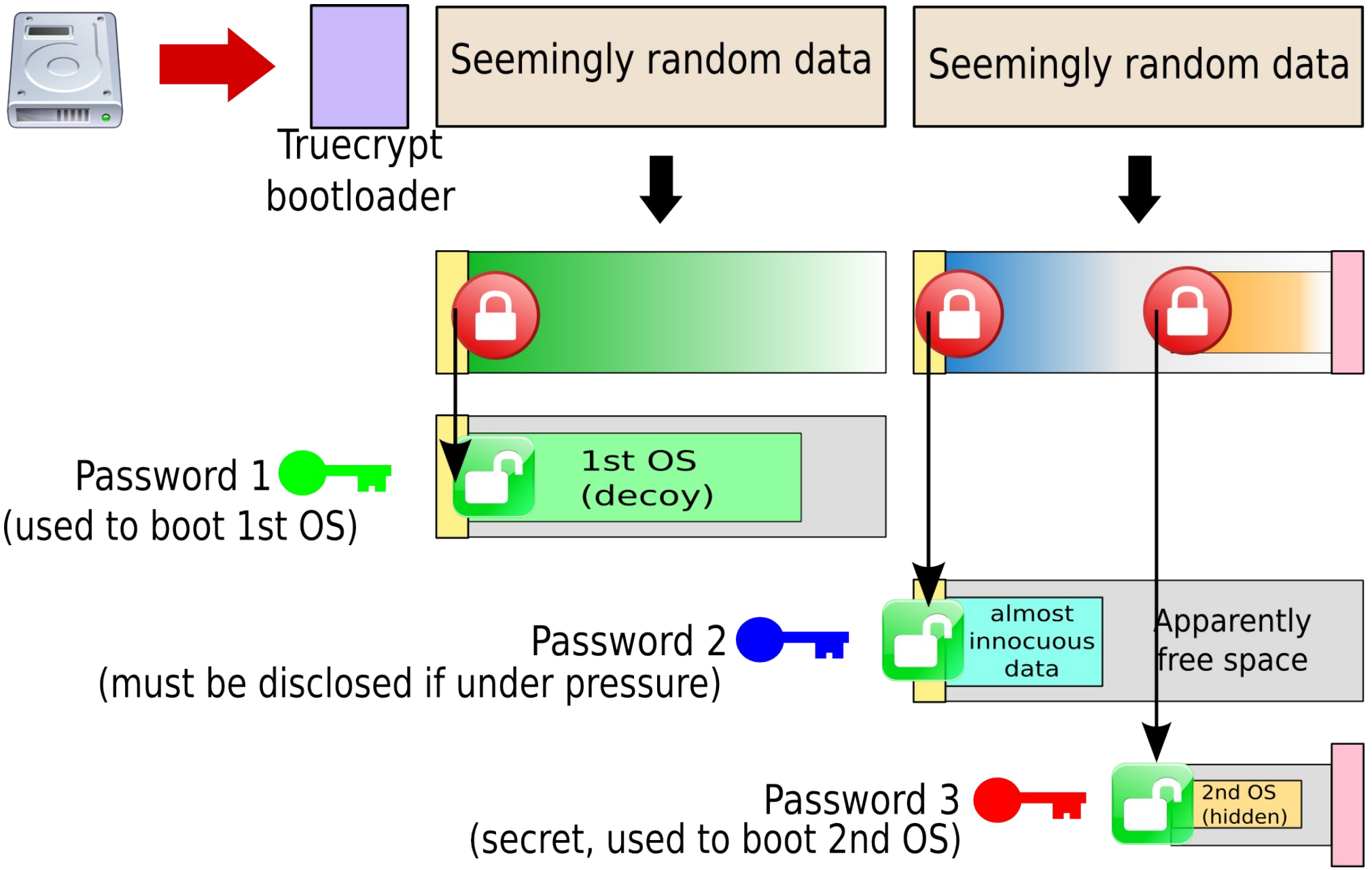
Operation Satyagraha (2008): l'FBI non è riuscita a recuperare dati protetti con Truecrypt nel pc di un agente bancario brasiliano.

Partizioni nascoste



You can reveal password 1 if forced, so that only the decoy data will be visible. There is no way to prove that a (smaller) hidden partition exists inside the scrambled free space of the decoy partition

Hidden OS


Seemingly random data
Seemingly random data
Truecrypt
bootloader
1st OS
(decoy)
Password 1
(used to boot 1st OS)
almost
innocuous
data
Apparently
free space
Password 2
(must be disclosed if under pressure)
2nd OS
(hidden)
Password 3
(secret, used to boot 2nd OS)

Altre features

- **Portabilità: Truecrypt può essere eseguito da una chiavetta USB**
- **Molti algoritmi crittografici supportati, possono anche essere nidificati per ulteriore protezione**
- **Veloce, supporta anche diversi hardware di accelerazione crittografica**
- **I volumi Truecrypt possono essere contenuti sia dentro altri files-contenitore che direttamente dentro partizioni del disco rigido.**
- **Un volume Truecrypt è tecnicamente indistinguibile da dati random senza la giusta password**
- **Molto facile da installare ed usare. Provare per credere!**

Sommario

- Introduzione
- Truecrypt
- Problemi di Truecrypt
- Conclusioni

Precauzioni

- **Un malintenzionato può sempre compromettere un computer (ad esempio installando un malware) anche se il disco è cifrato**
- **A causa del comportamento di alcuni software, dati cifrati possono essere accidentalmente trasferiti da partizioni nascoste a partizioni non nascoste. Hidden OS necessario per stare sicuri**
- **Per la stessa ragione è generalmente da evitare l'uso di Truecrypt in ambienti multiutente**
- **L'uso di Truecrypt con moderni SSD drive o chiavette USB può rivelare la presenza di partizioni nascoste**
- **Bisogna effettuare il backup usando accorgimenti particolari, per evitare di svelare la presenza di partizioni nascoste.**

Supporto Linux limitato

- **Il tipo di filesystem di una partizione-esca può solo essere FAT (quindi non si può montare una home di linux on-the-fly al login, a causa del mancato supporto dei permessi utente)**

- **Truecrypt non boota Linux (niente Linux come hidden OS)**

- **Nessuna di queste feature è prevista per il futuro.**

Mancanza di trasparenza

- **Nonostante sia “open source” e freeware, Truecrypt non è considerato “free software” da praticamente TUTTE le principali distribuzioni Linux, a causa di una licenza molto oppressiva (screenshots in queste slides?)**

- **Gli sviluppatori di Truecrypt sono anonimi: nessuno sa chi si cela dietro la Truecrypt Foundation**

- **Il forum di Truecrypt è pesantemente censurato su discussioni che riguardino, tra le altre cose, software simili o mod di Truecrypt; inoltre è possibile postare solo se si è iscritti con un'email del proprio provider**

- **Il codice di Truecrypt è sempre più difficile da compilare e da analizzare**

Sommario

- Introduzione
- Truecrypt
- Problemi di Truecrypt
- Conclusioni

Conclusioni

- **A volte cifrare i dati non è abbastanza: in alcune circostanze potresti essere costretto a rivelare la password**
- **Con la negabilità Plausibile puoi mentire sulla tua capacità di accedere a dati protetti (o perfino sulla loro esistenza)**
- **Usando una partizione nascosta hai DUE diversi "contenitori" per nascondere i dati: uno è una "partizione-esca" che conterrà solo dati di scarsa rilevanza (così che se ne possa rivelare la password se costretti), l'altra è una "partizione segreta" che contiene le cose davvero importanti (e non c'è modo di provare la sua esistenza senza la giusta password)**
- **Truecrypt è un software robusto ed open-source per ottenere negabilità plausibile mediante l'uso di partizioni nascoste o addirittura OS nascosti**
- **Truecrypt ha qualche limitazione che bisogna tenere a mente per un uso responsabile**

Fine

Grazie a tutti per l'attenzione.