Truecrypt

Alfredo De Santis

Dipartimento di Informatica

Università di Salerno

ads@dia.unisa.it

http://www.dia.unisa.it/professori/ads

Aprile 2014

TrueCrypt

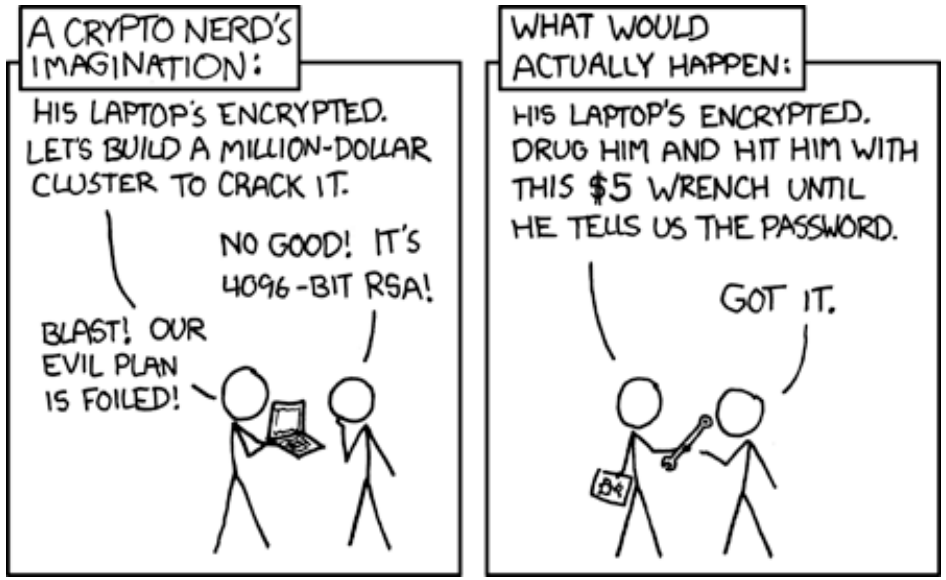
- Cifratura di partizioni o intera storage device (come hard-disk/USB flash drive)
- Crea disco virtuale cifrato in un file e lo monta come un disco reale
- Windows 7/Vista/XP, Mac OS X, Linux
- Versioni:
  - Version 1.0, feb 2004
  - …
  - Version 7.1, sett 2011
  - Version 7.1a, feb 2012
- Scritto in C, C++, assembly
- Freeware

TrueCrypt

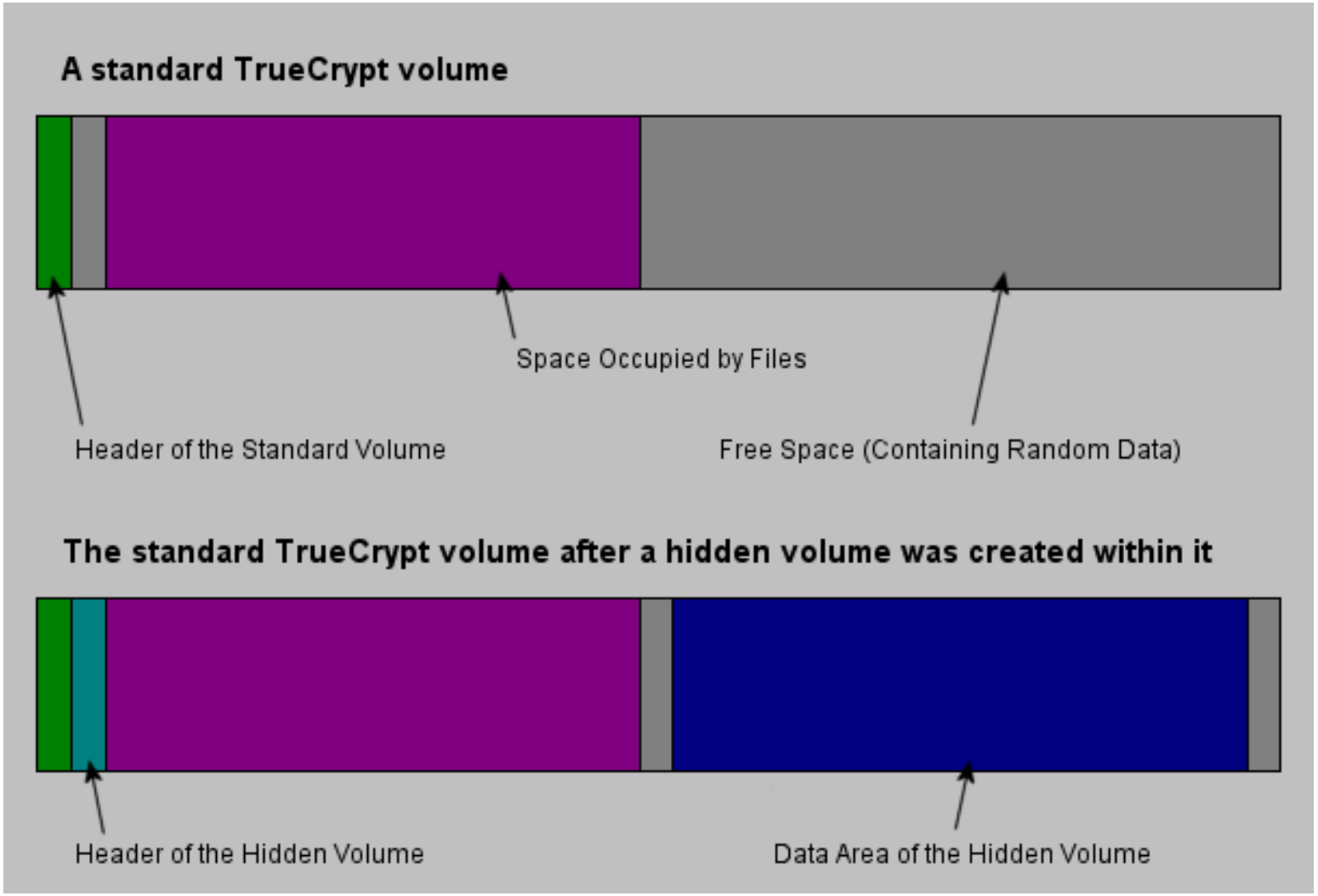
- Cifrari:
  - AES (256-bit key)
  - Serpent (256-bit key)
  - Twofish (256-bit key)
- Modi di cifratura: XTS mode
- Supporta 5 combinazioni di cascading algorithms
  - Prima una cifratura in XTS mode e poi la seguente in XTS mode
  - AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent
- Funzioni hash
  - RIPEMD-160
  - SHA-512
  - Whirlpool (output 512 bit)

TrueCrypt

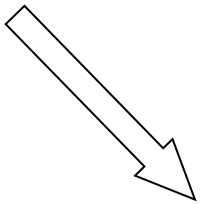
- Plausible deniability (negabilità plausibile)
  - Se si è forzati a rivelare la chiave, il contenuto non viene rivelato
  - Idea: cifrato con una seconda chiave, in zona nascosta del file



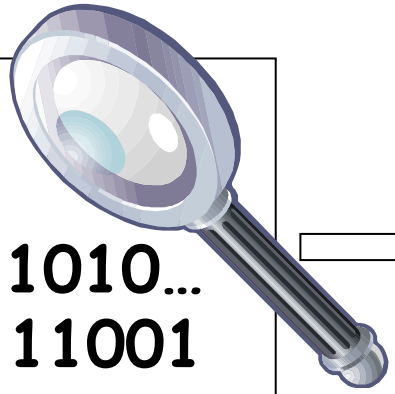
TrueCrypt


A standard TrueCrypt volume
Space Occupied by Files
Header of the Standard Volume
Free Space (Containing Random Data)
The standard TrueCrypt volume after a hidden volume was created within it
Header of the Hidden Volume
Data Area of the Hidden Volume

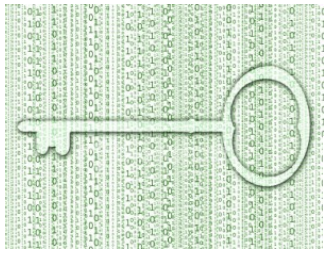
Indistinguibilità



Casuale o cifrato?



011010…
110111001



TrueCrypt

- Header hidden volume non è in chiaro
- E' costituito da:
  - Valori casuali (se non ci sono dati nascosti), oppure
  - Cifratura di info
- Come faccio a distinguere?

TrueCrypt

- Header hidden volume non è in chiaro
- E' costituito da:
  - Valori casuali (se non ci sono dati nascosti), oppure
  - Cifratura di info
- Come faccio a distinguere?
- Se decifro con la chiave giusta, trovo una caratteristica stabilita
- Altrimenti significa che
  - La chiave non è corretta, oppure
  - Non ci sono info nascoste

TrueCrypt

- Header hidden volume non è in chiaro
- E' costituito da:
  - Valori casuali (se no
  - Cifratura di info
- Come faccio a distinguere?
- Se decifro con la chiave giusta, trovo una caratteristica sta
- Altrimenti signifi
  - La chiave non è co
  - Non ci sono info nascoste

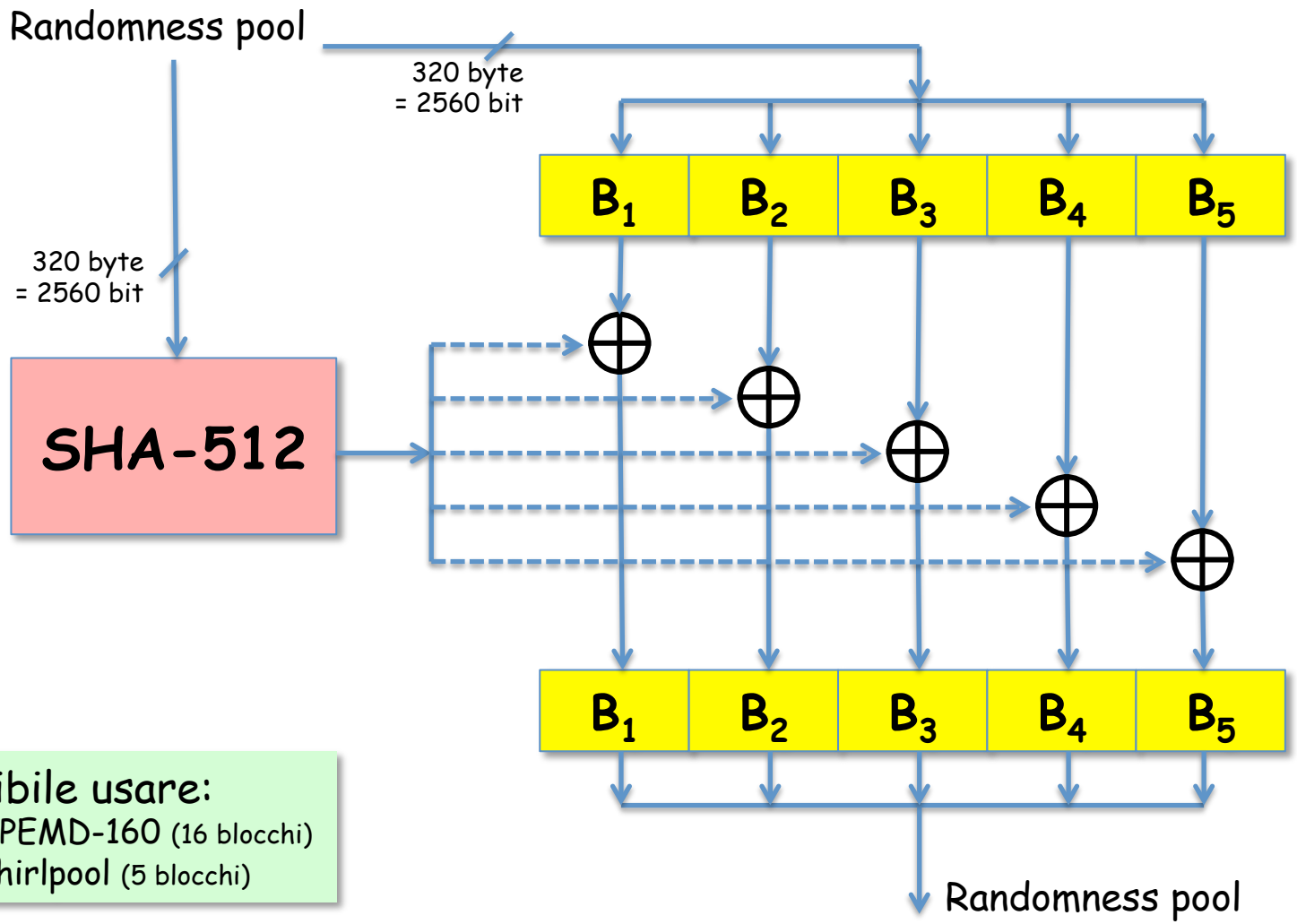
L'area del volume dove può essere l'hidden volume header è tra i bytes 65536-131071

- I primi 4 byte dei dati decifrati sono la stringa ASCII "TRUE"
- CRC-32 degli ultimi 256 byte dei dati decifrati = byte #8 dati decifrati

Random Number Generator

- Random Number Generator (RNG) usato per:
  - master encryption key
  - secondary key (XTS mode)
  - salt
  - keyfiles
- Crea una randomness pool di 320 byte in memoria RAM.
- Sorgenti usate per la randomness pool:
  - Mouse movements
  - Keystrokes
  - Mac OS X and Linux: Values generated by the built-in RNG (both /dev/random and /dev/urandom)
  - MS Windows: Windows CryptoAPI (collected regularly at 500-ms interval)
  - MS Windows: Network interface statistics (NETAPI32)
  - MS Windows: Various Win32 handles, time variables, and counters (collected regularly at 500-ms interval)
- Byte ottenuti dalle sorgenti vengono sommati mod 2^8 ai precedenti
  - Ordine aggiornamento da sx a dx e poi circolarmente
- Dopo ogni 16 byte ottenuti si applica una Pool Mixing Function
  - Principio della diffusione (per evitare dipendenze statistiche)

Pool Mixing Function



Possibile usare:

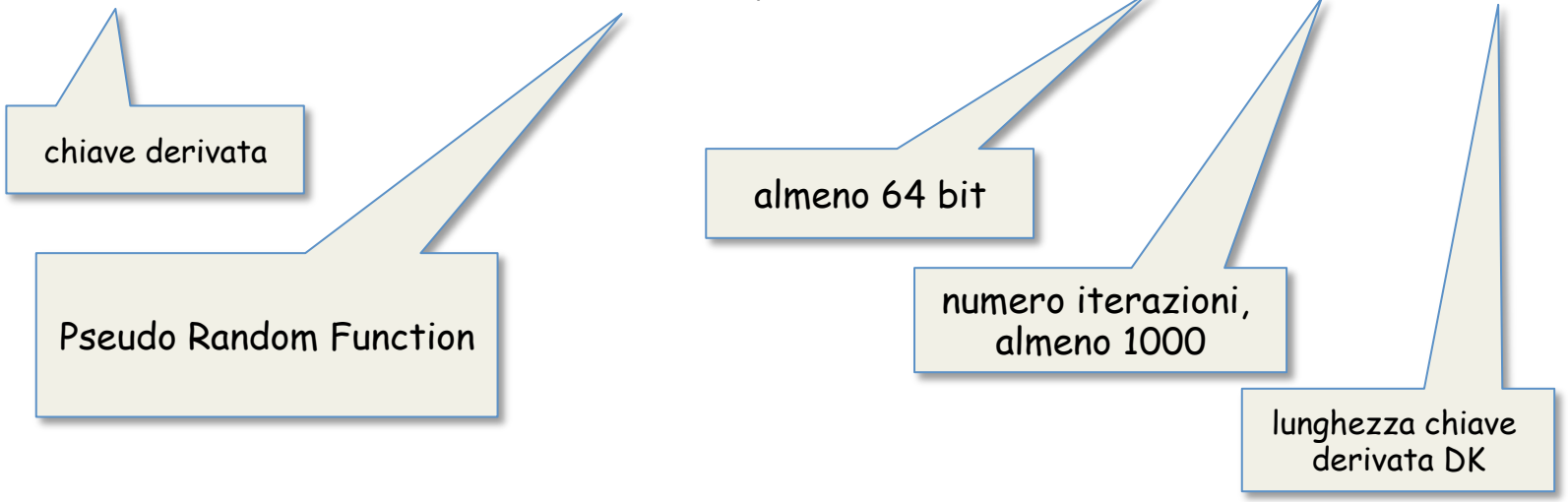
- RIPEMD-160 (16 blocchi)
- Whirlpool (5 blocchi)

Generazione chiavi

- PKCS #5 v2.0, Password-Based Cryptography Standard, RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), March 25, 1999
- PBKDF2 (Password-Based Key Derivation Function)
- Precedente: PBKDF1, per chiavi ≤160 bit
- Per rendere più difficile password cracking:
  - Usa "salt" e un fissato numero di iterazioni
  - Tecniche di questo tipo sono chiamate Key stretching

PBKDF2

DK = PBKDF2(PRF, password, salt, c, dkLen)



PBKDF2

DK = PBKDF2(PRF, password, salt, c, dkLen)

chiave derivata

Pseudo Random Function
TrueCrypt:
- HMAC-SHA-512
- HMAC-RIPEMD-160
- HMAC-Whirlpool

almeno 64 bit
TrueCrypt: 512 bit

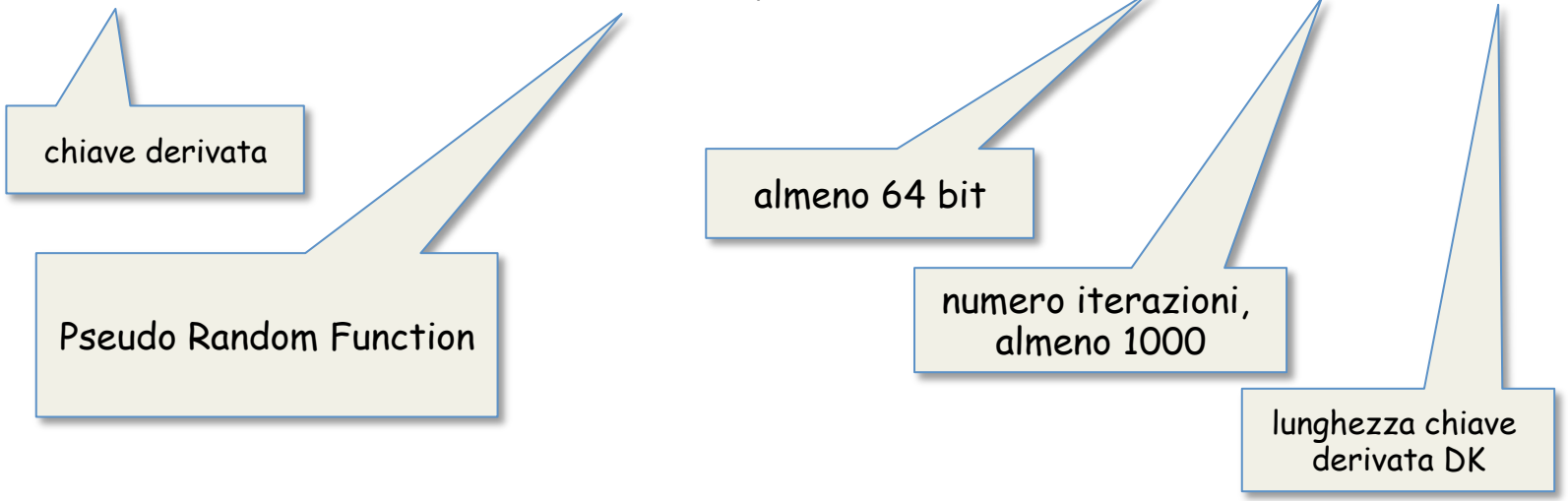
numero iterazioni,
TrueCrypt:
- HMAC-SHA-512 1000
- HMAC-RIPEMD-160 2000
- HMAC-Whirlpool 1000

lunghezza chiave derivata DK

Esempio:
AES-Twofish-Serpent cascade in XTS-mode
Occorre chiave formata da 3+3 chiavi di 256 bit
dklen = 1536 bit

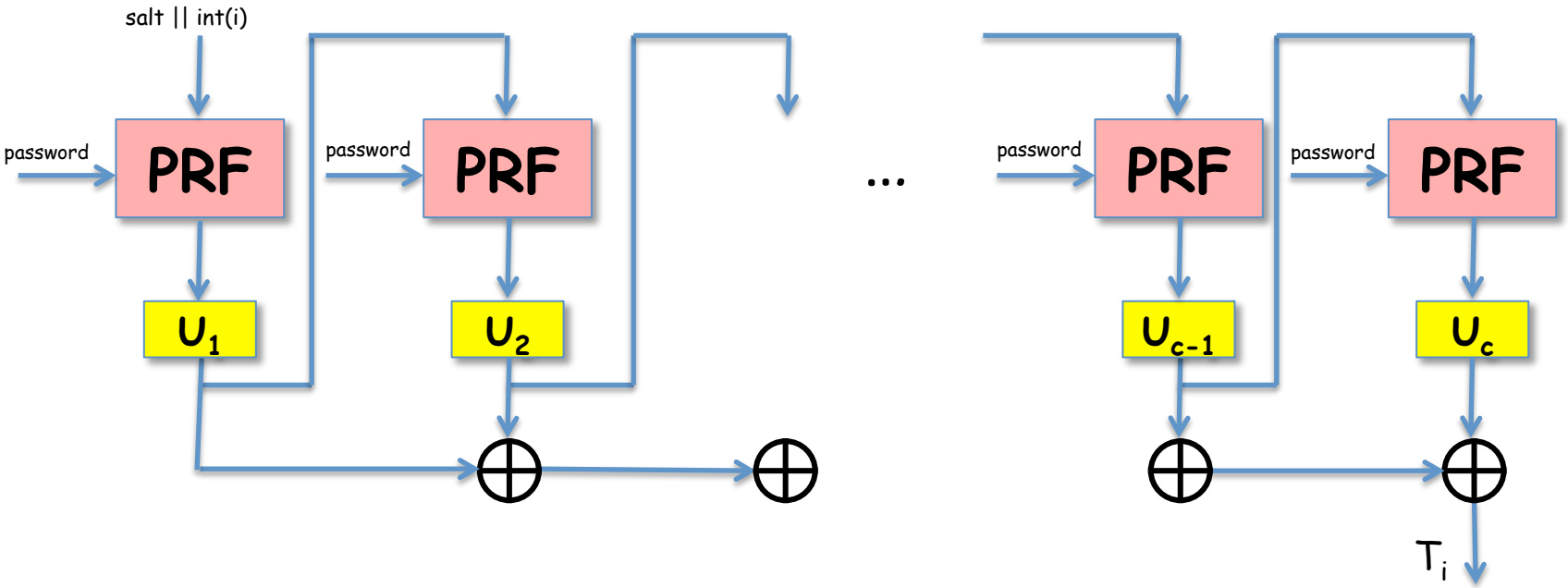
PBKDF2

DK = PBKDF2(PRF, password, salt, c, dkLen)



Per esempio, WPA2 usa:
DK = PBKDF2(HMAC-SHA1, passphrase, ssid, 4096, 256)

PBKDF2



$$DK = T_1 \,||\, T_1 \,||\, \ldots \,||\, T_{dklen/|output\ PRF|}$$

globo.com | notícias | esportes | entretenimento | vídeos

G1 English

English | Español | G1.com.br | globoesporte.com

25/06/2010 10h35 - Atualizado em 25/06/2010 15h15

Not even FBI was able to decrypt files of Daniel Dantas

Hard drives were seized by the feds during Operation Satyagraha, in 2008. Information is protected by sophisticated encryption system.

G1 imprimi

The FBI failed to break the encryption code of hard drives seized by federal police at the apartment of banker Daniel Dantas, in Rio de Janeiro, during Operation Satyagraha. The operation began in July 2008. According to a report published on Friday (25) by the newspaper Folha de S. Paulo, after a year of unsuccessful attempts, the U.S. federal police returned the equipment to Brazil in April.

According to the report, the fed only requested help from USA in early 2009, after experts from the National Institute of Criminology (INC) failed to decode the passwords on the hard drives. The government has no legal instrument to compel the manufacturer of the American encryption system or Dantas to give the access codes.

The equipment will remain under the protection of the feds. INC expect that new research data or technology could help them break the security codes. Opportunity Group reported that the two programs used in the equipment are available online. One is called Truecrypt and is free. The programs were used due to suspected espionage.

According to the report, the FBI and the INC used the same technology to try to break the password. It is a mechanism called a "dictionary" - a computer system that tests password combinations from known data and police information. Experts from the INC used this technique for five months, until December 2008, when the discs were sent to the United States.

http://g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html

The Register®

Hardware Software Music & Media Networks Security Cloud Public Sector Business Jobs

Crime Malware Enterprise Security Spam ID

Print Tweet Mi piace 1 Alert

Brazilian banker's crypto baffles FBI

18 months of failure

By John Leyden • Get more from this author

Posted in Enterprise Security, 28th June 2010 11:49 GMT

WIN - A free one year, 25 user licence of Microsoft Office 365!

Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.

Brazilian police seized five hard drives when they raided the Rio apartment of banker Daniel Dantas as part of Operation Satyagraha in July 2008. But subsequent efforts to decrypt files held on the hardware using a variety of dictionary-based attacks failed even after the South Americans called in the assistance of the FBI.

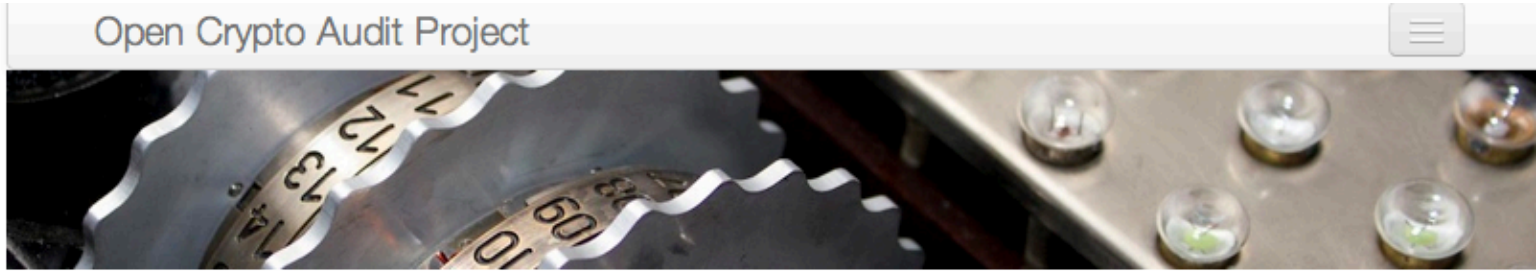
The files were encrypted using Truecrypt and an unnamed algorithm, reportedly based on the 256-bit AES standard. In the UK, Dantas would be compelled to reveal his passphrase under threat of imprisonment, but no such law exists in Brazil.

The Brazilian National Institute of Criminology (INC) tried for five months to obtain access to the encrypted data without success before turning over the job to code-breakers at the FBI in early 2009. US computer specialists also drew a blank even after 12 months of efforts to crack the code, Brazil's *Globo* newspaper reports.

The case is an illustration of how care in choosing secure (hard-to-guess) passwords and applying encryption techniques to avoid leaving file fragments that could aid code breakers are more important in maintaining security than the algorithm a code maker chooses. In other cases, law enforcement officials have defeated suspects' use of encryption because of weak cryptographic trade craft or poor passwords, rather than inherent flaws in encryption packages. ®

http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/

Open Crypto Audit Project



Welcome to the Open Crypto Audit Project

The Open Crypto Audit Project (OCAP) is a community-driven global initiative which grew out of the first comprehensive public audit and cryptanalysis of the widely used encryption software TrueCrypt®. Our charter is to:

- provide technical assistance to free open source software ("FOSS") projects in the public interest
- to coordinate volunteer technical experts in security, software engineering, and cryptography
- to conduct analysis and research on FOSS and other widely software in the public interest
- contract with professional security researchers and information security firms to provide highly specialized technical assistance, analysis and research on FOSS and other widely used software in the public interest

We operate as a U.S. non-profit organization, incorporated in the state of North Carolina, and are currently seeking federal 501c(3) tax-exempt designation.

https://opencryptoaudit.org

Open Crypto Audit Project

- Analisi versione 7.1a, feb 2012 (versione corrente)
- Security Assessment
  - Report 14 aprile 2014

- Crittoanalisi (in corso)

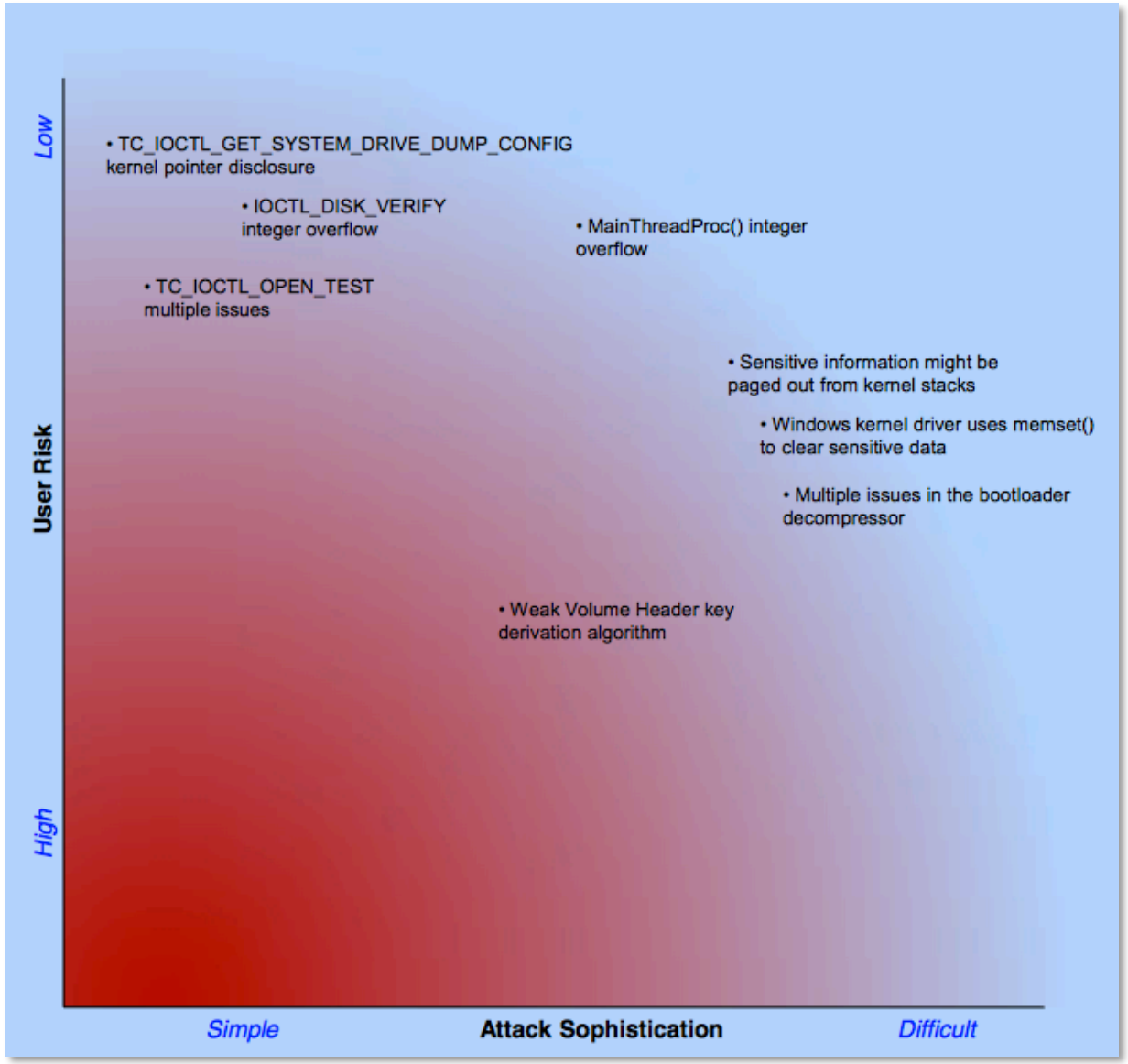
Security Assessment

iSECpartners
part of nccgroup

"iSEC found no evidence of backdoors or otherwise intentionally malicious code in the assessed areas. The vulnerabilities described later in this document all appear to be unintentional, introduced as the result of bugs rather than malice."

Security Assessment

iSECpartners
part of nccgroup

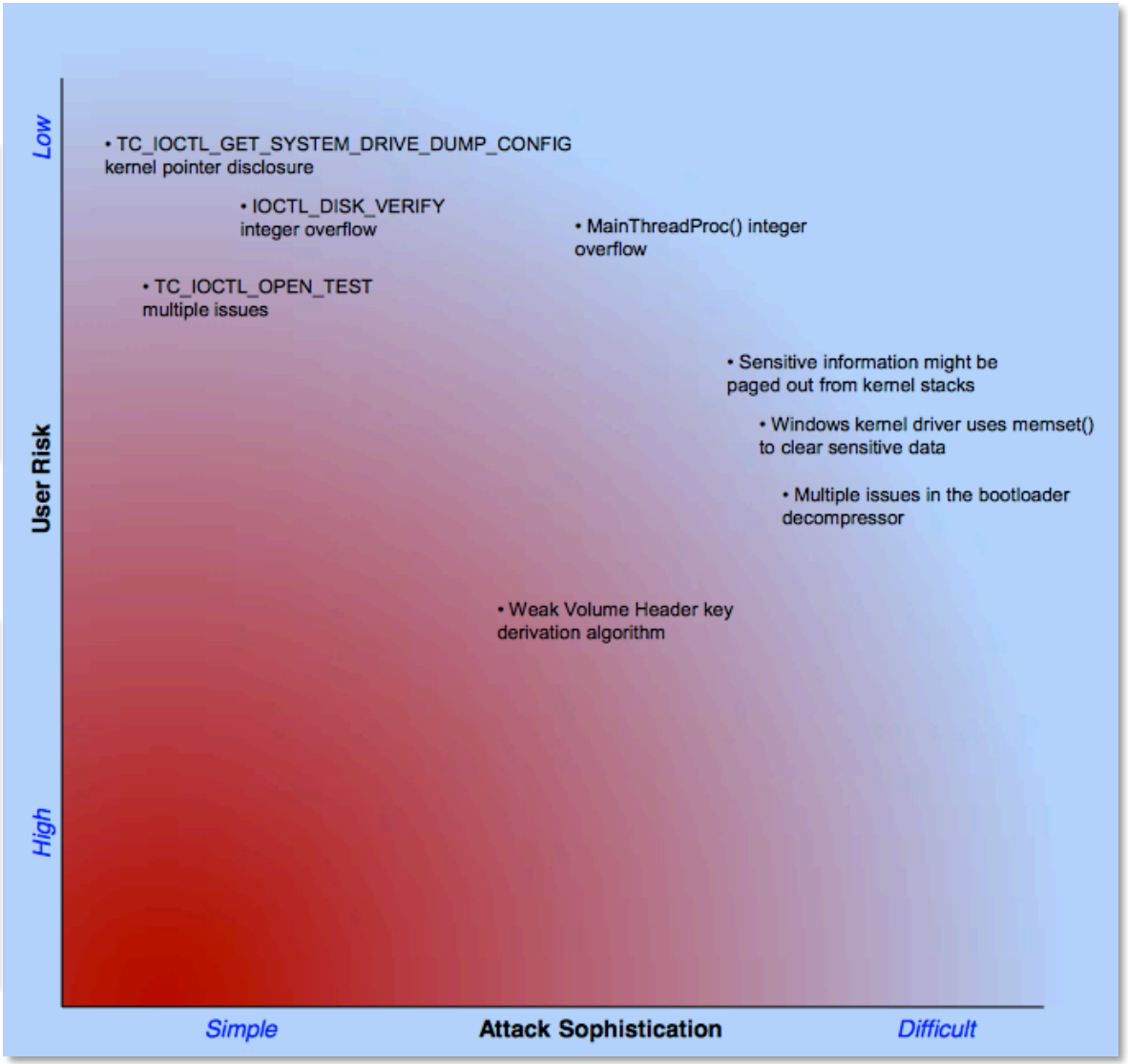


Security Assessment

iSECpartners part of nccgroup

Difficulty Levels	
Difficulty	**Description**
Undetermined	The difficulty of exploit was not determined during this engagement
Low	Commonly exploited, public tools exist or can be scripted that exploit this flaw
Medium	Attackers must write an exploit, or need an in-depth knowledge of a complex system
High	The attacker must have privileged insider access to the system, may need to know extremely complex technical details or must discover other weaknesses in order to exploit this issue

Severity Categories	
Severity	**Description**
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or Defense in Depth
Undetermined	The extent of the risk was not determined during this engagement
Low	The risk is relatively small or is not a risk the customer has indicated is important
Medium	Individual user's information is at risk, exploitation would be bad for client's reputation, moderate financial impact, possible legal implications for client
High	Large numbers of users, very bad for client's reputation, or serious legal or financial implications



1. Weak Volume Header key derivation algorithm

Class: Cryptography	**Severity:** Medium	**Difficulty:** Medium

FINDING ID: iSEC-OCAP-11

TARGETS: Encrypted Volume Header

DESCRIPTION: The key used to encrypt the TrueCrypt Volume Header is derived using PBKDF2, a standard key derivation algorithm[5]. Developers are responsible for specifying an iteration count that influences the computational cost of deriving a key from a password. The iteration count used by TrueCrypt is either 1000 or 2000, depending on the hash function and use case.

In both cases, this iteration count is too small to prevent password guessing attacks for even moderately complex passwords. The paper that introduces scrypt[6], an alternate key derivation function, demonstrates the challenge of using PBKDF2 even with a very high iteration count – brute-forcing key derivation is easily parallelized and becomes more efficient each year with advances in CPU performance. The use of a small iteration count in TrueCrypt permits efficient brute-force attacks against its header key.

EXPLOIT SCENARIO: An attacker captures an encrypted TrueCrypt volume and performs an offline brute-force and / or dictionary attack to identify the key used to encrypt the Volume Header. They use the recovered key to decrypt the volume.

SHORT TERM SOLUTION: Support the use of configurable iteration counts for PBKDF2 to keep pace with advances in CPU and GPU speed. If the current volume format does not include reserved space to store such a value, and if changes to the Volume Header cannot be made, this value might be derived from a portion of the salt, so long as it is guaranteed to exceed a certain minimum value.

LONG TERM SOLUTION: Consider supporting the use of additional key derivation functions. Scrypt, in particular, requires the use of large amounts of memory and requires more expensive hardware to brute-force.

Downloads

19 aprile 2014

Category	Count
Total Number of Downloads	30,501,697
Number of Downloads Yesterday	10,673

Latest Stable Version • **Most-Downloaded Past Versions**

Package	Number of Downloads
TrueCrypt 7.1a (Windows)	6,525,983
TrueCrypt 7.1 (Windows)	1,460,087
TrueCrypt 7.0a (Windows)	3,368,672
TrueCrypt 6.3a (Windows)	2,142,598
TrueCrypt 6.2a (Windows)	1,101,840
TrueCrypt 6.1a (Windows)	1,428,729
TrueCrypt 6.0a (Windows)	1,005,665
TrueCrypt 4.3a (Windows)	1,218,079

Domande?