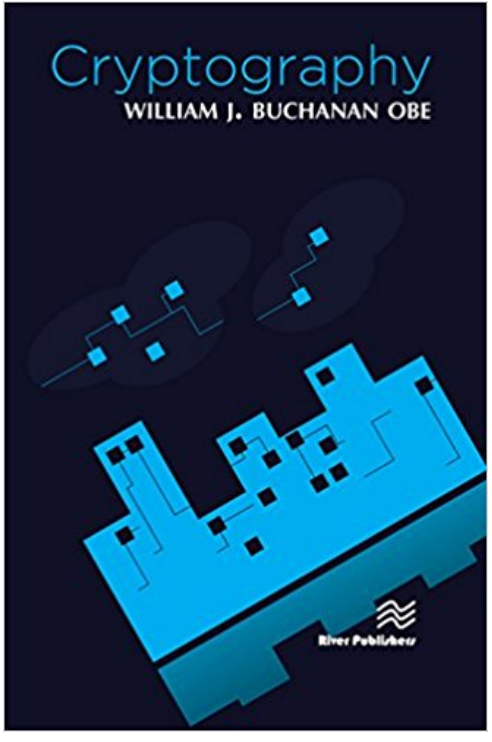
11. Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity



Host Security

Linux

Mac OSX

Windows

BIOS initialises hardware

↓

BIOS calls MBR (Master Boot Record)

↓

Load code from boot sector of active partition

↓

Bootloader runs code and starts up operating system

Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity

TPM 1.2 and 2.0

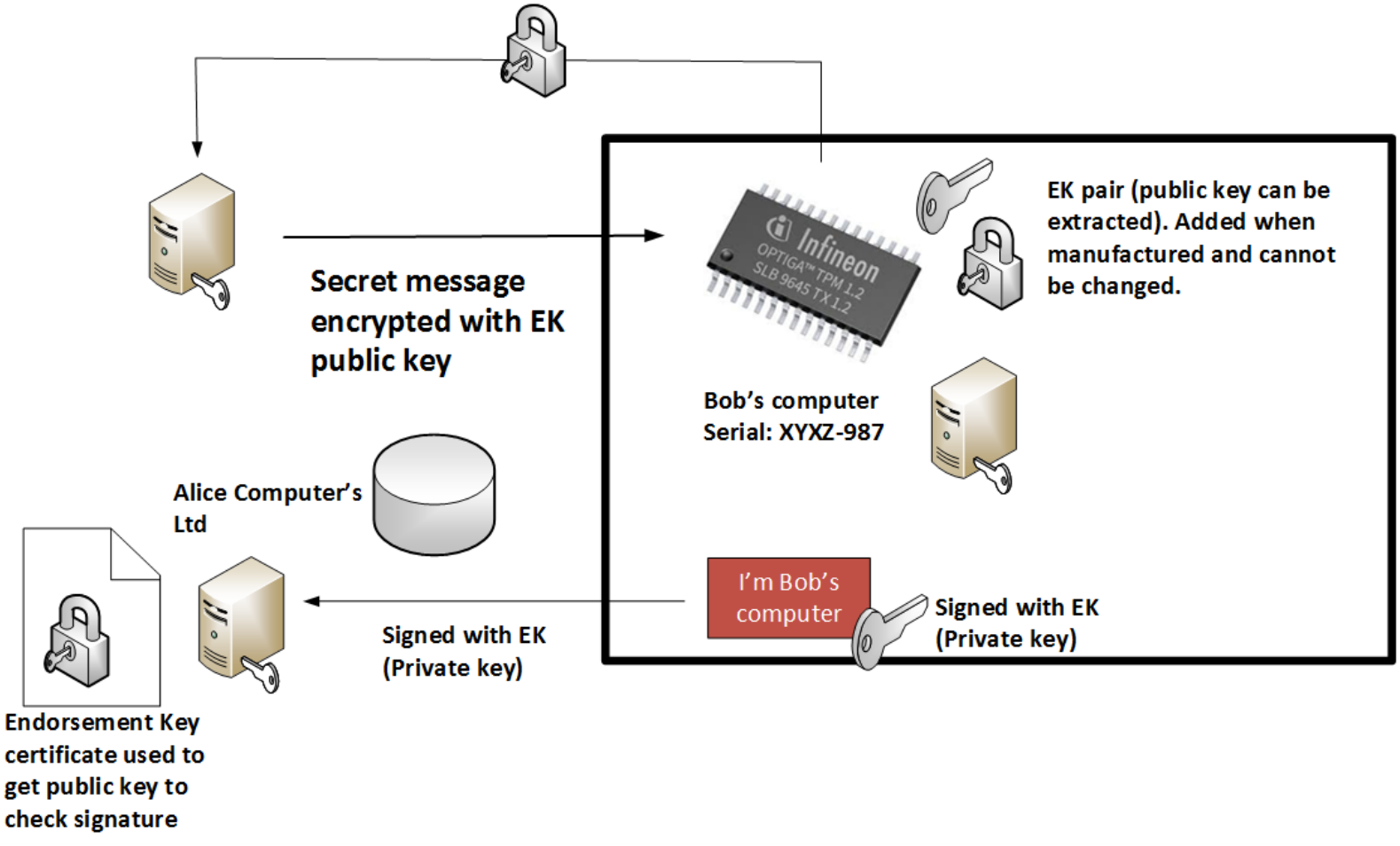
- **Platform integrity.** Makes sure the boot process is correct.
- **Disk encryption.** The encryption key used for dis encryption is fully or partially defined by the SRK.
- **Password protection.** The storage of the user's password in the chip.

Crypto-processor
- Random number generator.
- RSA/ECC key generator.
- HMAC generator.
- SHA-1/SHA-256 hash generator.
- Signature engine

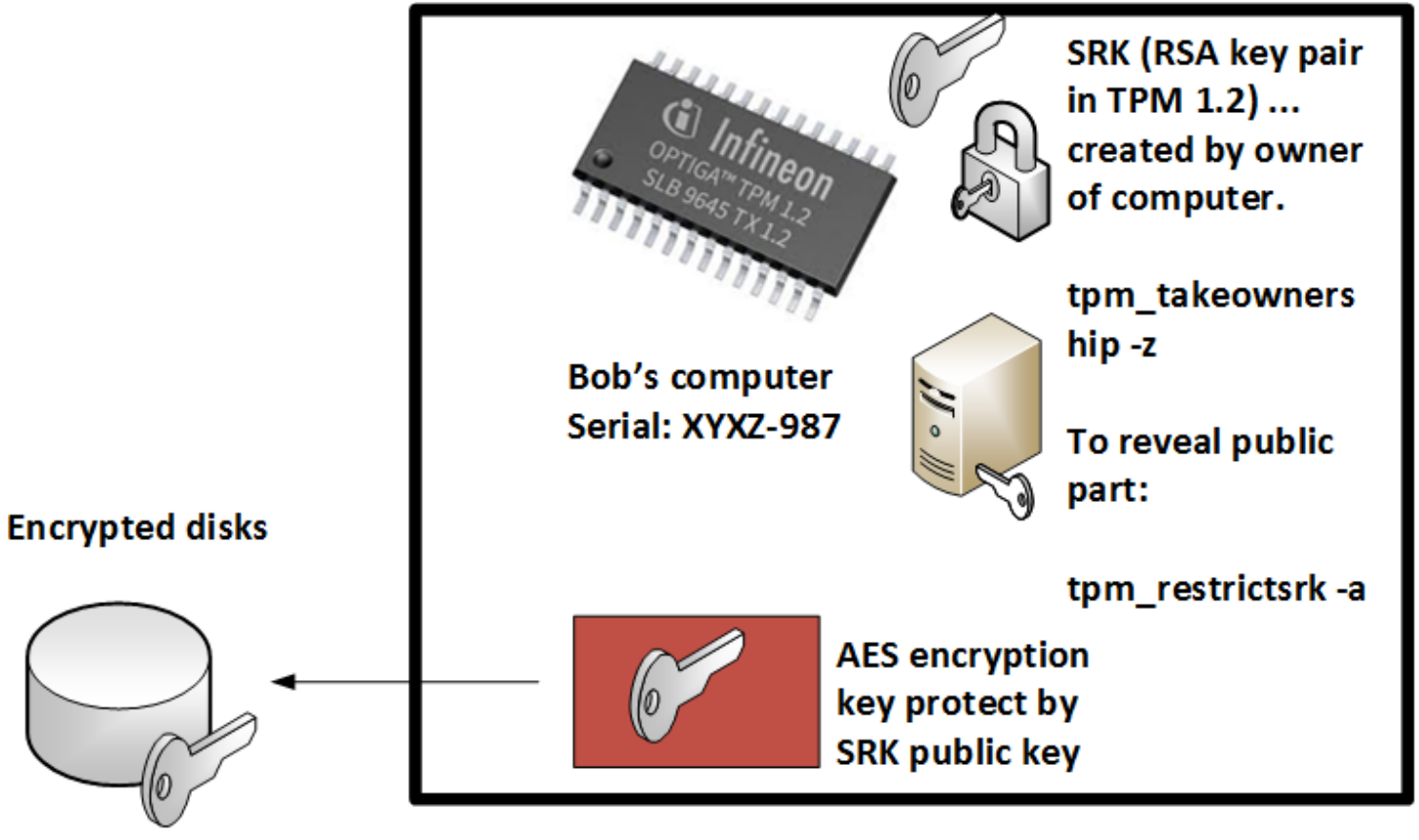
Versatile memory:
- Platform Configuration Registers (PCR).
- Attestation Identity Keys (AIK).
- Storage Keys.

Persistent memory:
- Endorsement Key (EK). A private key from a key pair. A user wishing to send a message to this TPM uses the public key to encrypt. Public key is also stored on TPM.
- Storage Root Key (SRK). Used to encrypt disk storage.

Endorsement Key (EK)



Storage Root Key (SRK)



ROCA

ROCA

Weak prime Number generator (RSALib)

[Back] With the ROCA (Return of the Coppersmith Attack) vulnerability an RSA private key can be recovered from the knowledge of the public key. It has the CVE identifier of CVE-2017-15361. The vulnerability related to the Infineon RSA library on the Infineon Trusted Platform Module (TPM) firmware. It affected BitLocker with TPM 1.2 and YubiKey 4. In this case we calculate the prime number with $Prime = k \times M + (65537^a \mod M)$:

Parameters

No of prime numbers to use: 39

k: 3

a: 12

Determine

For RSALib, with a key size between 512-bit to 960-bit, n = 39 (M = 2 * 3 * ... * 167) is used for prime number generation.

n = 71, 126, 225 for key sizes of intervals of: [992, 1952]; [1984, 3936]; and [3968, 4096], respectively.

```
k= 3
a= 12
Number of prime numbers used= 39
======
M= 962947420735983927056946215901134429196419130606213075415963491270

Prime= 28888422684862029846771832244101148077859019965161804576999836270 91
Value is prime
```

Key size	University cluster (Intel E5-2650 v3@3GHz Q2/2014)	Rented Amazon c4 instance (2x Intel E5-2666 v3@2.90GHz, estimated)	Energy-only price ($0.2/kWh) (Intel E5-2660 v3@2.60GHz, estimated)
512 b	1.93 CPU hours *(verified)*	0.63 hours, $0.063	$0.002
1024 b	97.1 CPU days *(verified)*	31.71 days, $76	$1.78
2048 b	140.8 CPU years	45.98 years, $40,305	$944
3072 b	$2.84 * 10^{25}$ years	$9.28 * 10^{24}$ years, $8.13 * 10^{27}$	$1.90 * 10^{26}$
4096 b	$1.28 * 10^{9}$ years	$4.18 * 10^{8}$ years, $3.66 * 10^{11}$	$8.58 * 10^{9}$

k: 3

a: 12

Determine

For RSALib, with a key size between 512-bit to 960-bit, n = 39 (M = 2 * 3 * ... * 167) is used for prime number generation.

n = 71, 126, 225 for key sizes of intervals of: [992, 1952]; [1984, 3936]; and [3968, 4096], respectively.

```
Prime= 28888422684862029846771832244101148077859019965161804576999836270 91
Value is prime
```

Key size	University cluster (Intel E5-2650 v3@3GHz Q2/2014)	Rented Amazon c4 instance (2x Intel E5-2666 v3@2.90GHz, estimated)	Energy-only price ($0.2/kWh) (Intel E5-2660 v3@2.60GHz, estimated)
512 b	1.93 CPU hours *(verified)*	0.63 hours, $0.063	$0.002
1024 b	97.1 CPU days *(verified)*	31.71 days, $76	$1.78
2048 b	140.8 CPU years	45.98 years, $40,305	$944
3072 b	$2.84 * 10^{25}$ years	$9.28 * 10^{24}$ years, $\$8.13 * 10^{27}$	$\$1.90 * 10^{26}$
4096 b	$1.28 * 10^{9}$ years	$4.18 * 10^{8}$ years, $\$3.66 * 10^{11}$	$\$8.58 * 10^{9}$

Domain name	Used length (bits)	Pub. key availability	Misuse
TLS/HTTPS	2048	easy	MitM/eavesdropping
Message security (PGP)	1024/2048	easy	message eavesdropping, forgery
Trusted boot (TPM)	2048	limited	unseal data, forged attestation
Electronic IDs (eID, ePassport)	2048	limited	clone passport, e-gov document forgery
Payment cards (EMV)*	768/960/1024/1182	limited	clone card, fraudulent transaction
Certification authorities (root, intermediate)*	2048 or higher	easy	forged certificates, MitM
Authentication tokens	2048 or higher	limited	unauthorized access or operation
Software signing	2048 or bigger	easy	malicious application update
Programmable smartcard (Java Card)	1024-4096	depends on use	depends on use

Key size	University cluster (Intel E5-2650 v3@3GHz Q2/2014)	Rented Amazon c4 instance (2x Intel E5-2666 v3@2.90GHz, estimated)	Energy-only price ($0.2/kWh) (Intel E5-2660 v3@2.60GHz, estimated)
512 b	1.93 CPU hours *(verified)*	0.63 hours, $0.063	$0.002
1024 b	97.1 CPU days *(verified)*	31.71 days, $76	$1.78

Domain name	Analyzed datasets	# Vuln. keys/devices	% Vulnerable
Complete/larger-scale datasets			
Certification authorities	all browser-trusted roots (173), level ⩽ 3 intermediates (1,869)	0 keys	0
ePass signing certificates	ICAO Document Signing Certificates, CSCA Master Lists	0 keys	0
Estonian eID	sample of 130,152 randomly selected citizens	71,417 keys	54.87
Estonian mobile eID	sample of 30,471 randomly selected citizens	0 keys	0
Estonian e-residents	sample of 4,414 e-residents	4,414 keys	100
Message security (PGP)	complete PGP key server dump (9 M)	2,892 keys	0.03
Software signing (GitHub)	SSH keys for GitHub developers (4.7 M)	447 keys	0.01
Software signing (Maven)	signing keys for all public Maven artifacts	5 keys	0.003
TLS/HTTPS	complete IPv4 scan, Certificate Transparency	15 keys	<0.001
Trusted boot (TPM)	41 laptops with different chips by 6 TPM manufacturers	10 devices	24.39
Limited, custom-collected datasets			
Payment cards (EMV)	13 cards from 4 EU countries, 6 with *Manufacturer* chip	0 keys	0
Programmable smartcard	25 cards from JCAlgTest.org database, 6 with *Manufacturer* chip	2 cards	8.67
Software signing (Android)	1,080 top ranking applications and games	0 keys	0

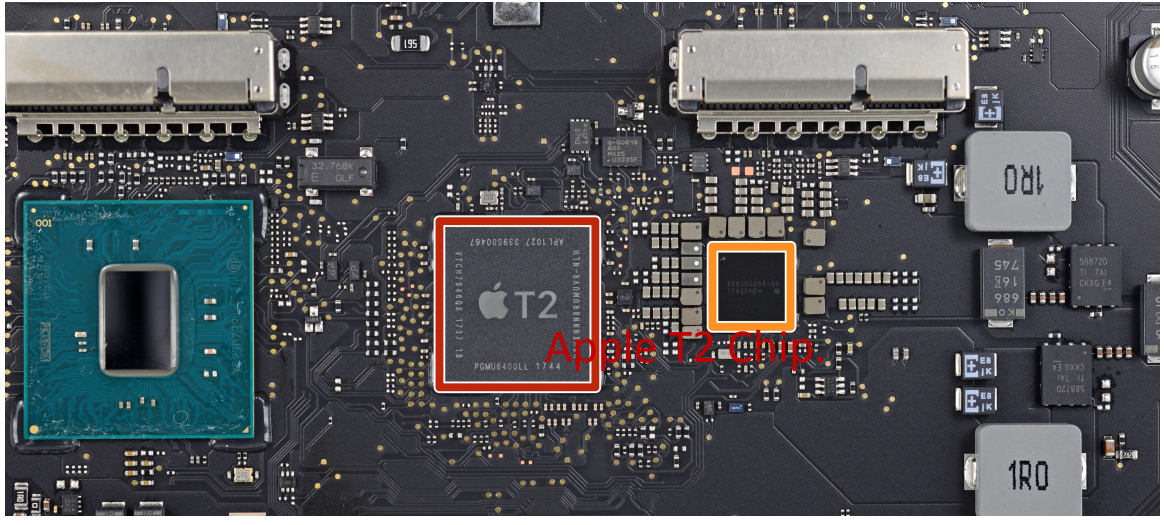
Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity

Apple T2 Chip



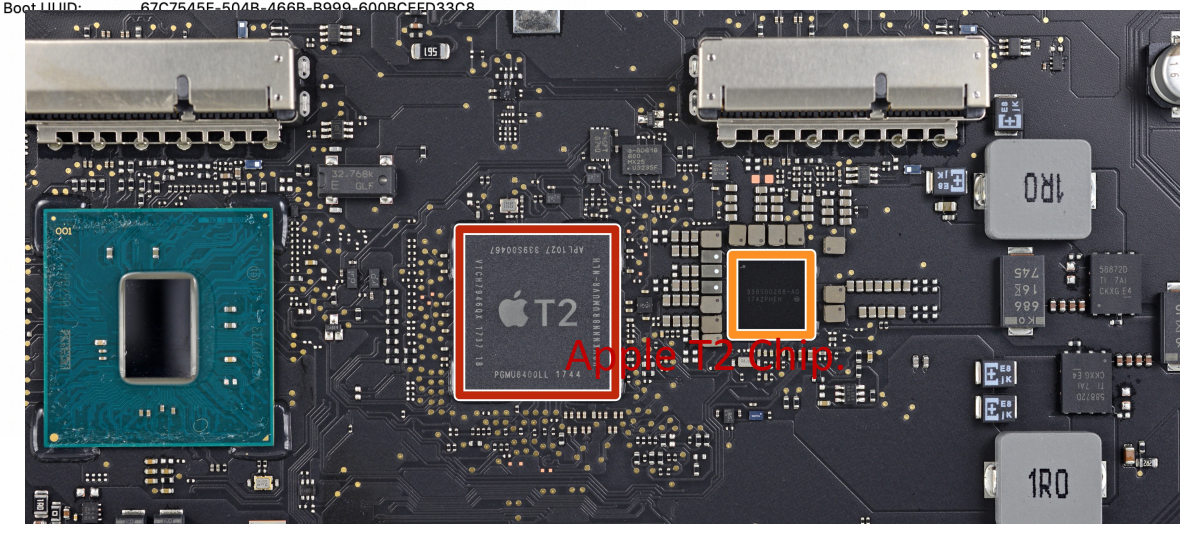
Apple T2 Chip

MacBook Pro

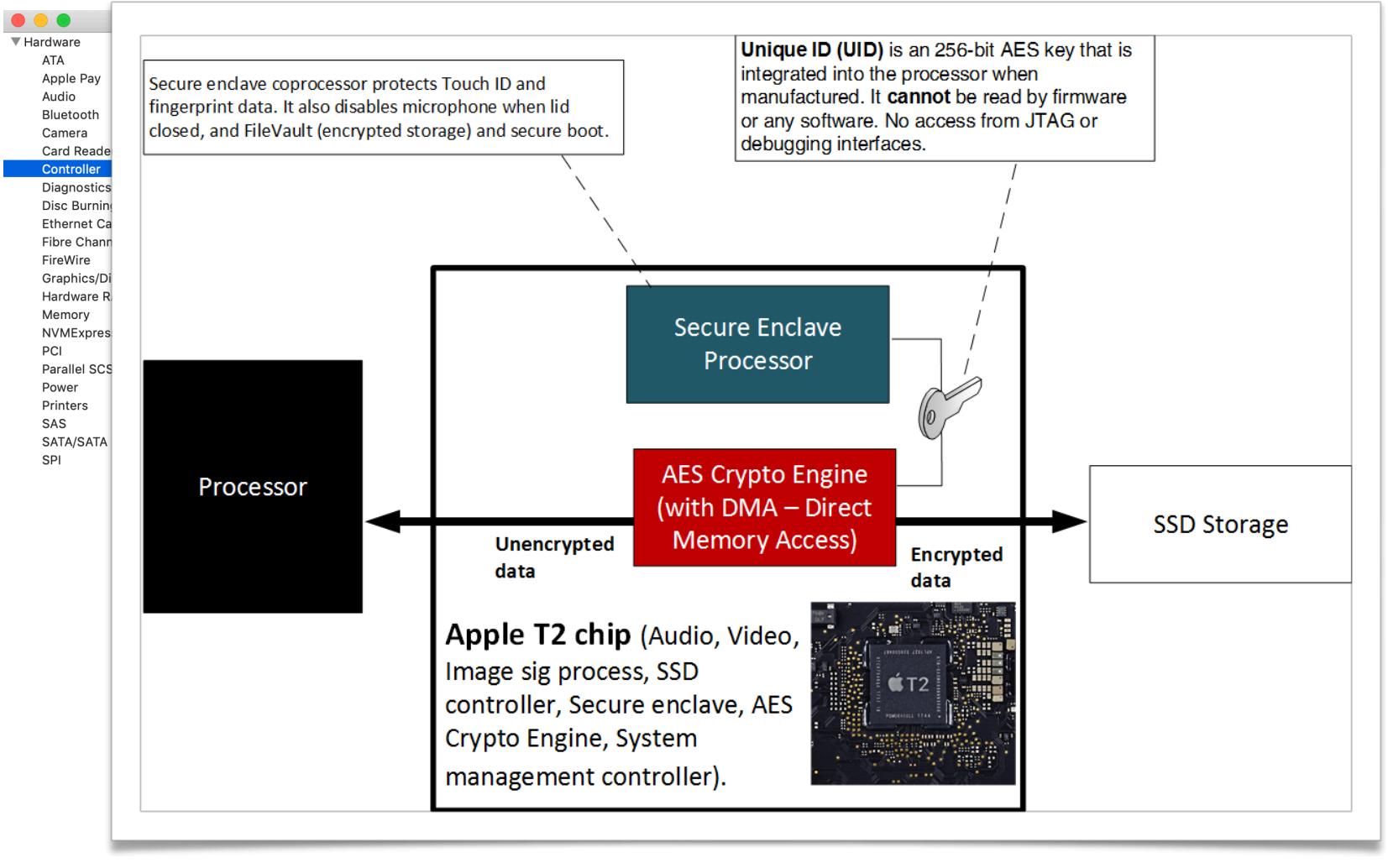
- Hardware
  - ATA
  - Apple Pay
  - Audio
  - Bluetooth
  - Camera
  - Card Reader
  - Controller
  - Diagnostics
  - Disc Burning
  - Ethernet Cards
  - Fibre Channel
  - FireWire
  - Graphics/Displays
  - Hardware RAID
  - Memory
  - NVMExpress
  - PCI
  - Parallel SCSI
  - Power
  - Printers
  - SAS
  - SATA/SATA Express
  - SPI

Controller Information:

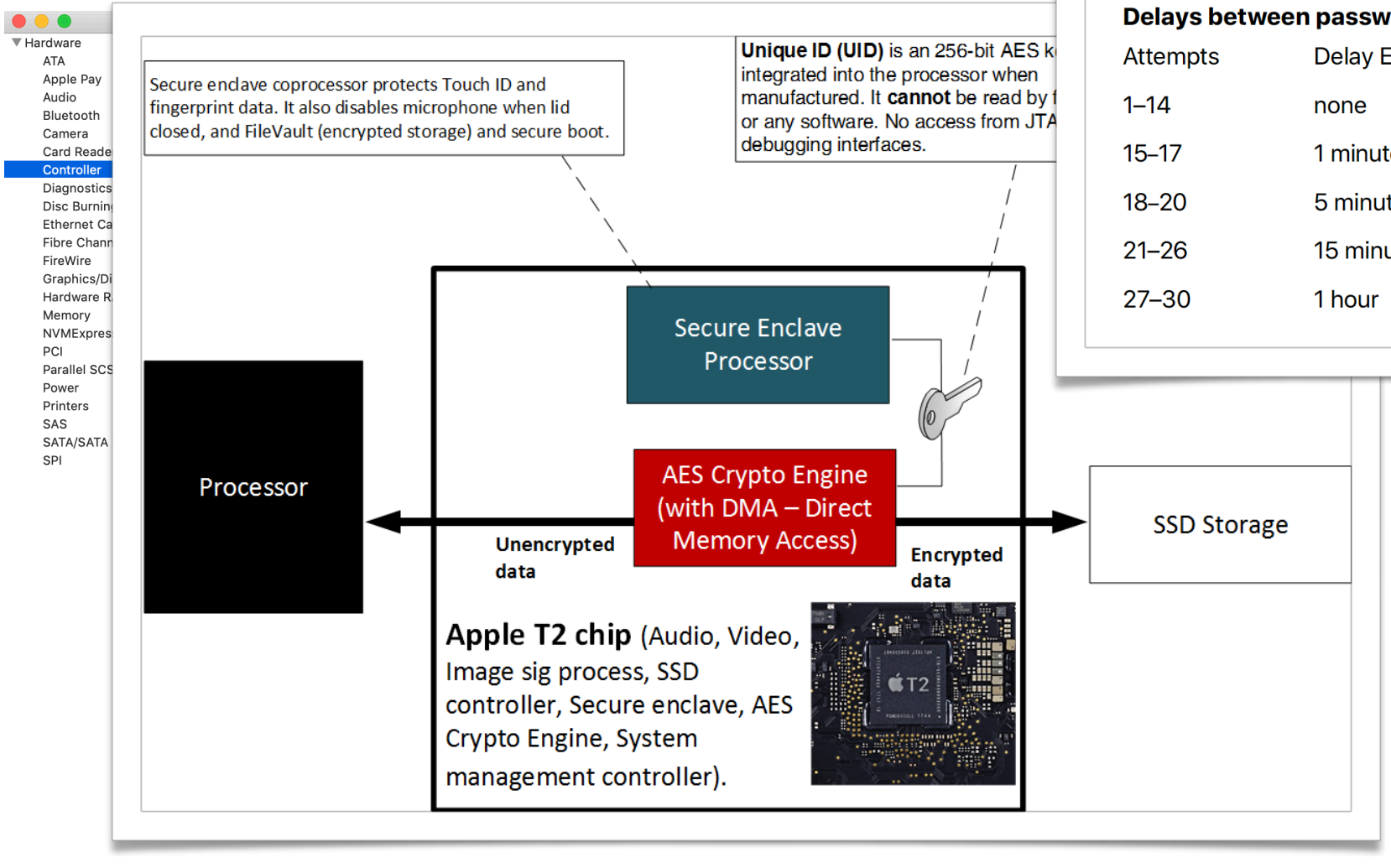
Model Name: Apple T2 Security Chip
Firmware Version: 16P4507
Boot UUID: 67C7545E-504B-466B-B999-600BCFED33C8



Apple T2 Chip



Apple T2 Chip



Delays between password attempts

Attempts	Delay Enforced
1–14	none
15–17	1 minute
18–20	5 minutes
21–26	15 minutes
27–30	1 hour

Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

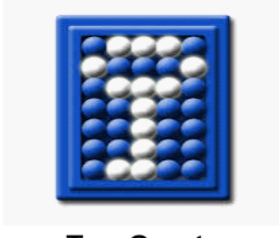
http://asecuritysite.com/esecurity

File/Folder Encryption

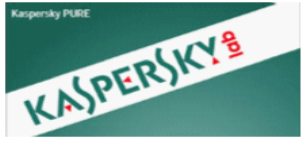
Disk Encryption

Microsoft Bitlocker

Check Point Full Disk Encryption Software



TrueCrypt



McAfee Endpoint Encryption Encryption Software

Axanum (.AXX)

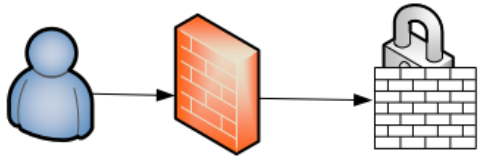
Sophos SafeGuard Disk Encryption

Author: Prof Bill Buchanan

FIPS

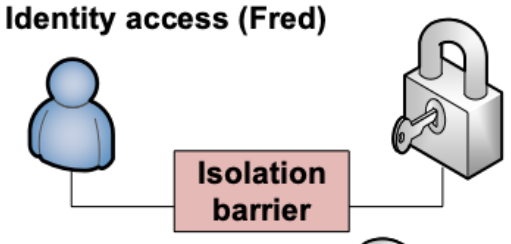
FIPS 140-2 Level 4

- **Physical security requirements more stringent.**
- **Robustness against environment attacks**



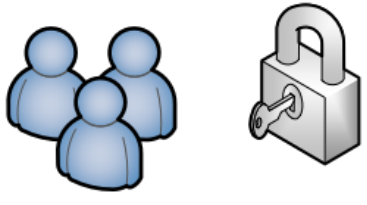
FIPS 140-2 Level 3

- **Physical tamper-resistance.**
- **Identity-based authentication.**
- **Physical or logical separation between the interface by which the key security parameters are entered or passed.**



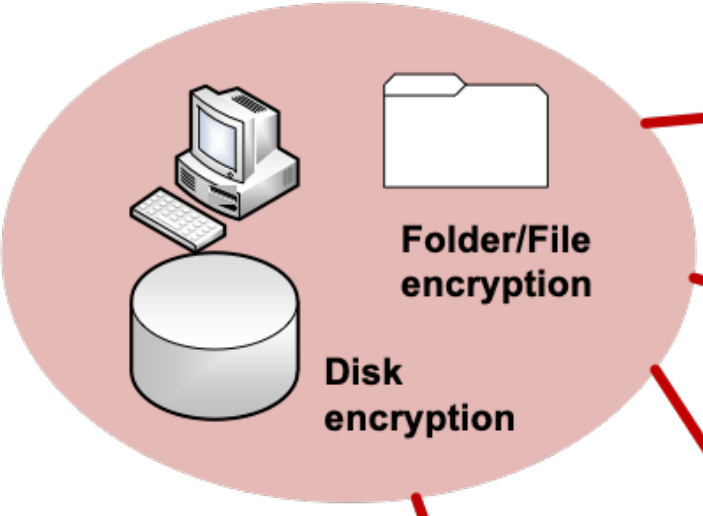
FIPS 140-2 Level 2

- **Physical tamper-evidence.**
- **Role-based authentication.**



FIPS (Federal Information Processing Standards) 140-2 Level 1

- **Lowest level limited requirements**



Folder/File encryption

Disk encryption

Napl5r123$

Password or passphase

USB drive with encryption key

OTP device such as an RSA token

Biometric device
(eg fingerprint reader_ with Trusted Platform Module (TPM) which holds the actual encryption key)

Multi-factor authentication uses two or more of these

EFS – Drive or Folder encryption

Transparent operation mode Uses TPM

- Trusted Platform Module (TPM) 1.2 hardware where user powers up and logs into Windows as normal.
- Encryption key is sealed (encrypted) in the TPM chip and released to the OS loader code if the early boot files appear to be unmodified.
- Pre-OS components of BitLocker use Static Root of Trust Measurement defined by the Trusted Computing Group (TCG). Mode is vulnerable with cold boot attack, where the intruder can boot the powered-down machine.

BitLocker Logical volume encryption

- NTFS Drive 1: Boot drive (unencrypted)
- NTFS Drive 2: Operating system – eg c: drive (encrypted)

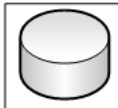
User authentication mode

Pre-boot PIN required

USB Key Mode

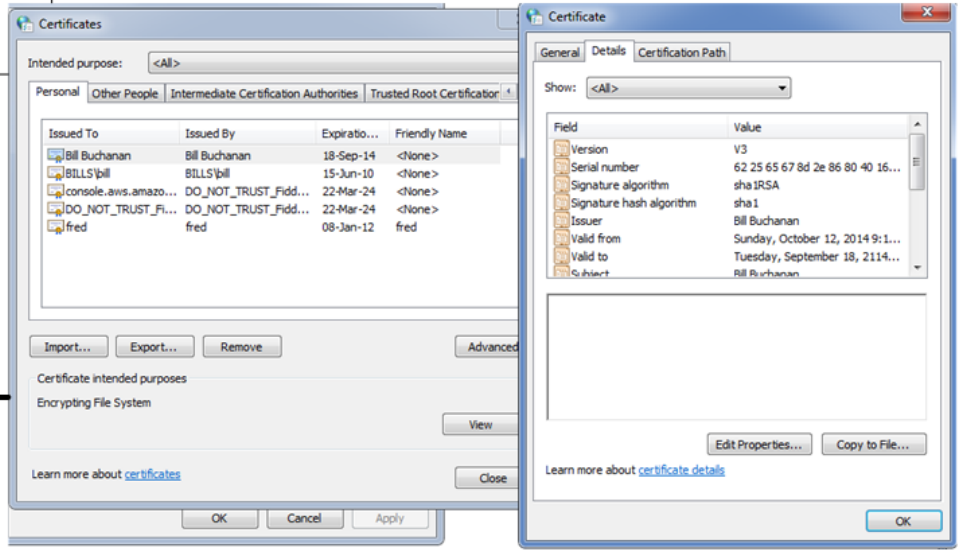
- Users inserts a USB device with a startup key into the computer for the boot to protected OS.
- BIOS must support the reading of USB devices in the pre-OS environment.

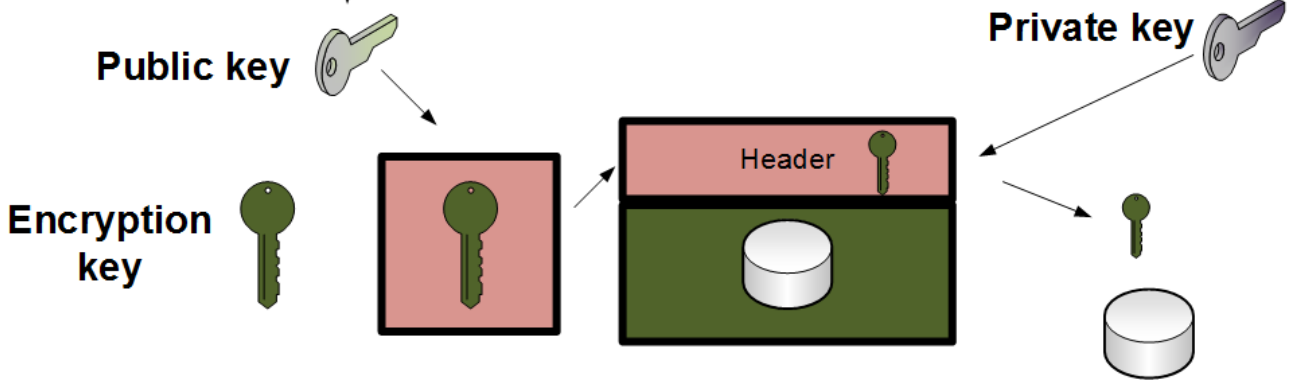
Microsoft EFS



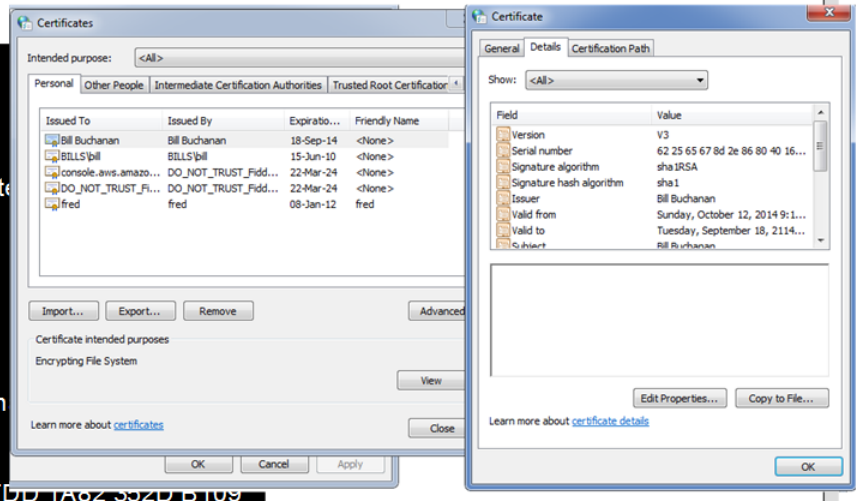
EFS – Drive or Folder encryption

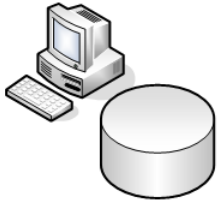
- CER file – Contains certificate.
- PFX – Contains certificate and private key.





```
C:\enc\test>cipher /c test.docx

 Listing C:\enc\test\
 New files added to this directory will be encrypte

E test.docx
  Compatibility Level:
    Windows XP/Server 2003

  Users who can decrypt:
    WIN-98UTFANB55G\Bill Buchanan [Bill Buch
Buchanan@WIN-98UTFANB55G

    Certificate thumbprint: 1E77 C3D6 BCCB DFDD 1A82 352D B109
3136 A830 76E0

  No recovery certificate found.

  Key Information:
    Algorithm: AES
    Key Length: 256
    Key Entropy: 256
```





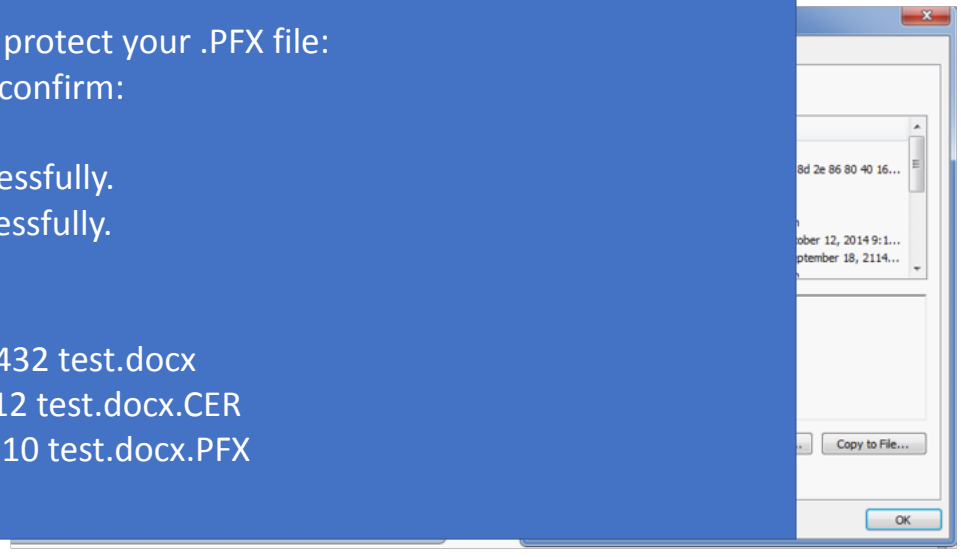
```
C:\enc\test>cipher /r:test.docx
Please type in the password to protect your .PFX file:
Please retype the password to confirm:

Your .CER file was created successfully.
Your .PFX file was created successfully.

C:\enc\test>dir
12-Oct-14  08:39 PM            11,432 test.docx
12-Oct-14  08:43 PM               912 test.docx.CER
12-Oct-14  08:43 PM             2,710 test.docx.PFX
```

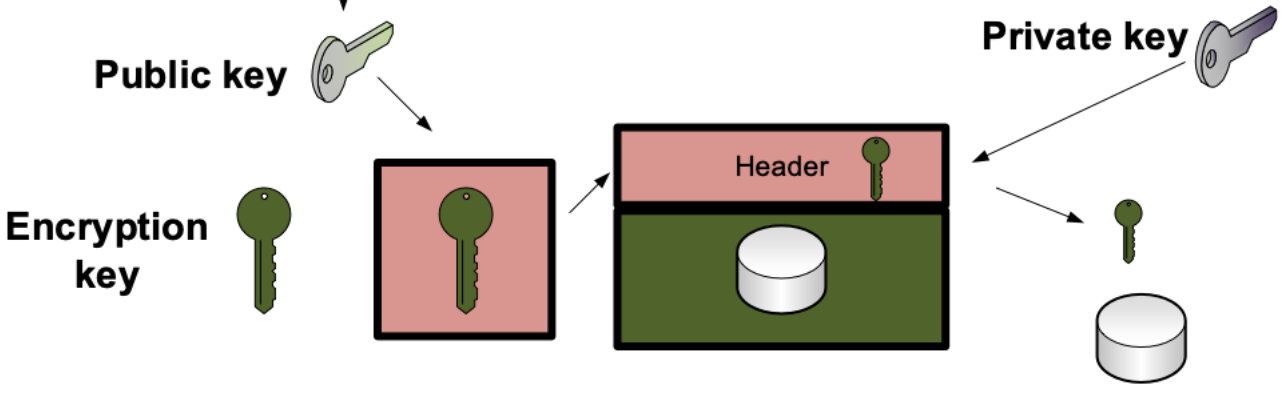
```
C:\enc\test>cipher /c test.docx
 Listing C:\enc\test\
 New files added to this directory will be encrypted.

E test.docx
  Compatibility Level:
    Windows XP/Server 2003

  Users who can decrypt:
    WIN-98UTFANB55G\Bill Buchanan [Bill Buchanan(Bill
Buchanan@WIN-98UTFANB55G

    Certificate thumbprint: 1E77 C3D6 BCCB DFDD 1A82 352D B109 3136 A830 76E0

  No recovery certificate found.

  Key Information:
    Algorithm: AES
    Key Length: 256
    Key Entropy: 256
```

EFS – Drive or

```
C:\enc\test>cipher /r:test.docx
Please type in the password to protect your .PFX file:
Please retype the password to confirm:

Your .CER file was created successfully.
Your .PFX file was created successfully.

C:\enc\test>dir
12-Oct-14  08:39 PM          11,432 test.docx
12-Oct-14  08:43 PM             912 test.docx.CER
12-Oct-14  08:43 PM           2,710 test.docx.PFX
```

- CER
  certi
- PFX
  certi
  key.





Host Security

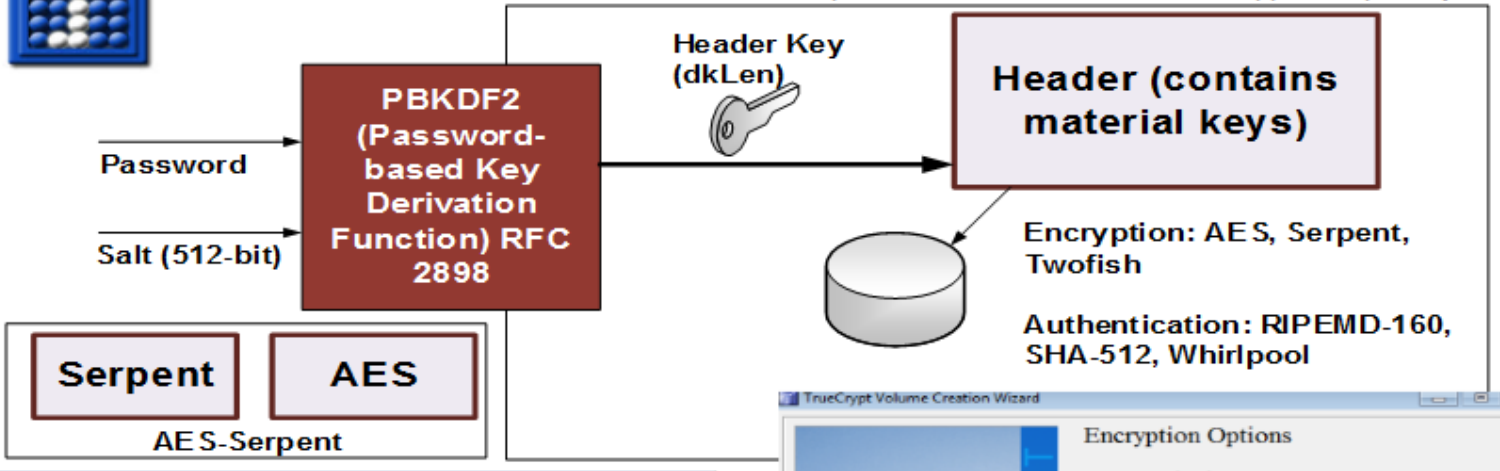
TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

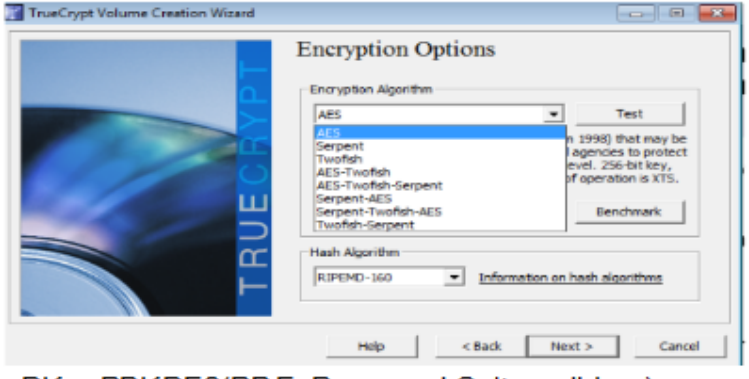
Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity

TrueCrypt

Advantages: Open-source. Windows/Linux/OS X. Free
Disadvantages: If you lose the pass phrase – almost impossible to recover. Current support is patchy.

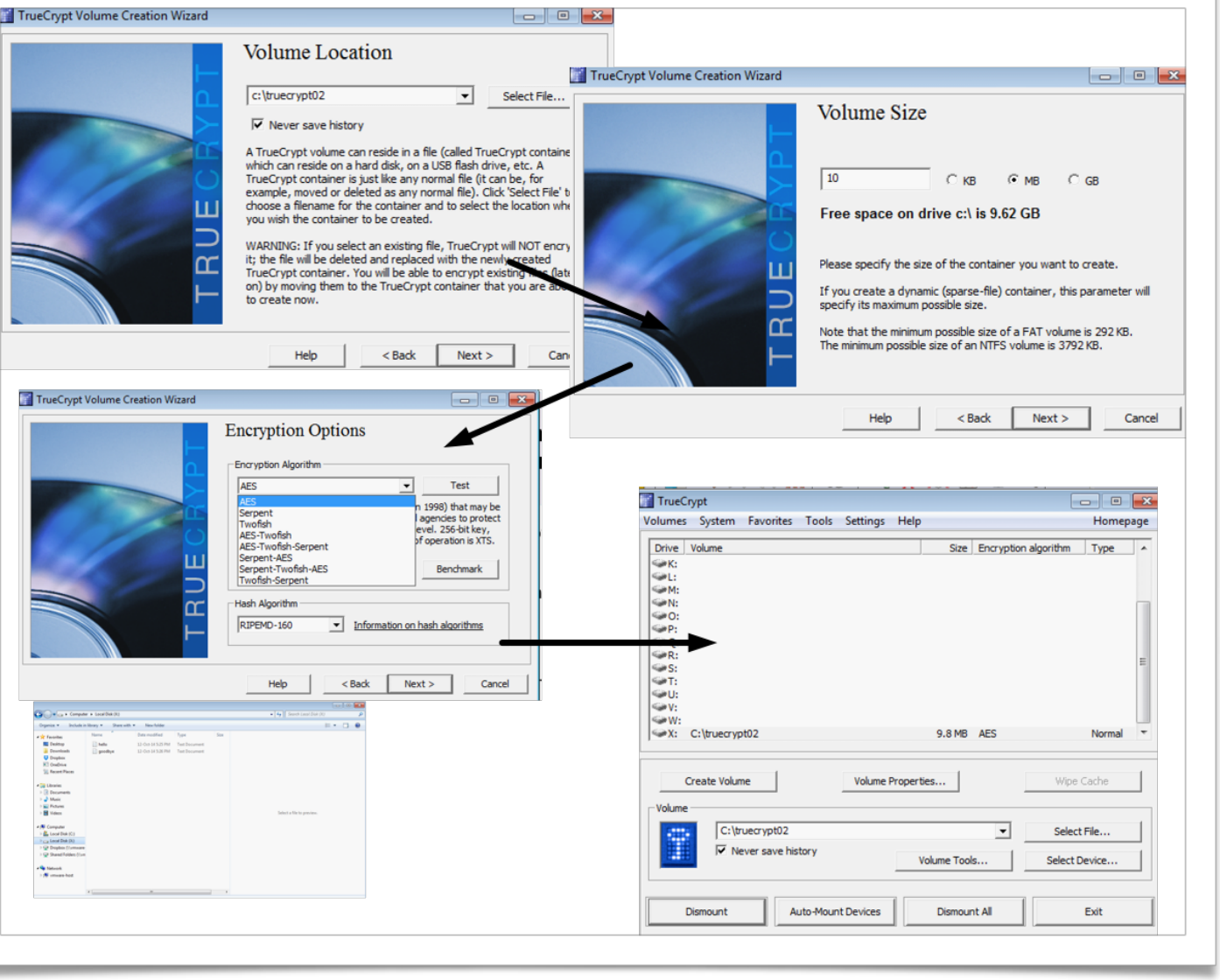


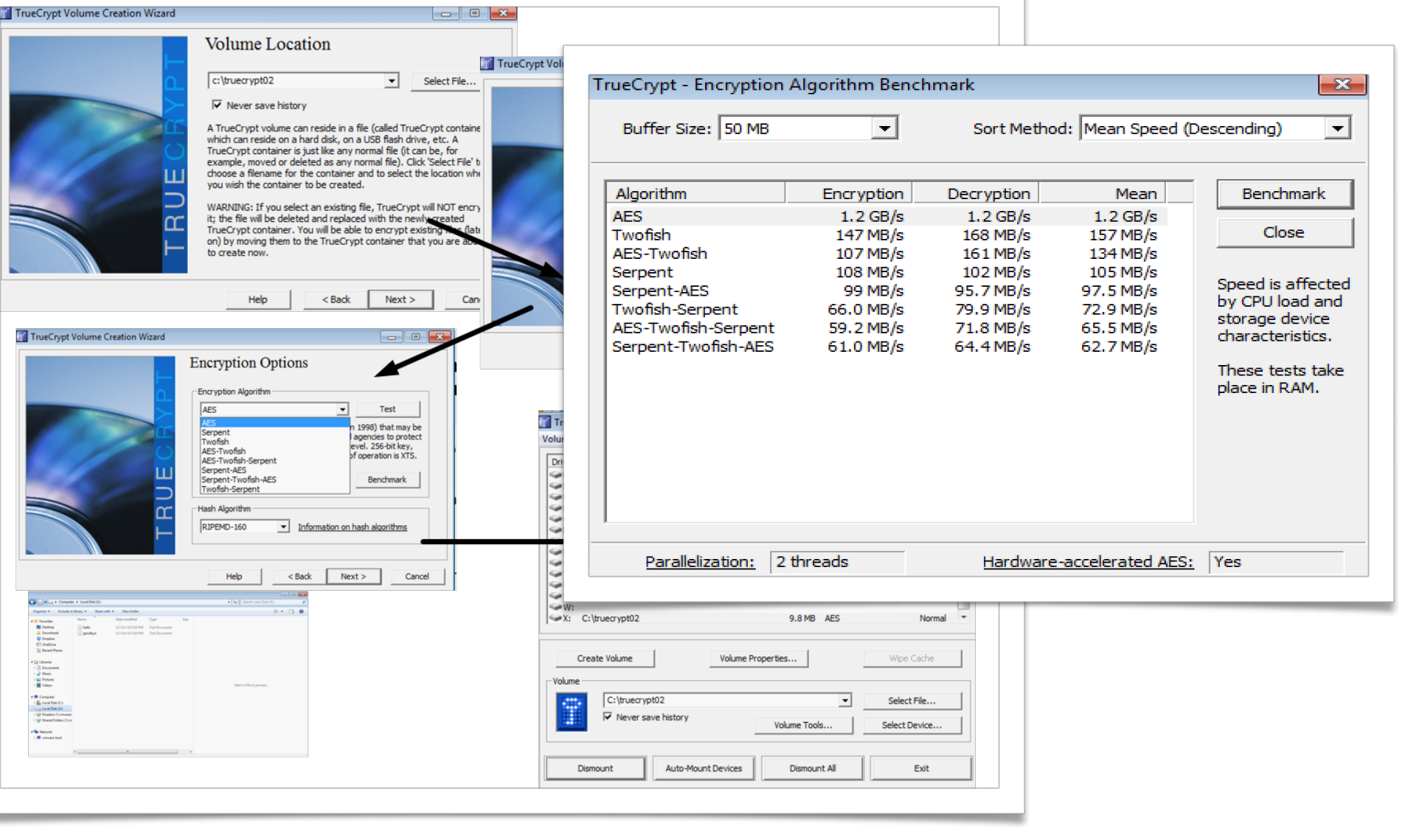


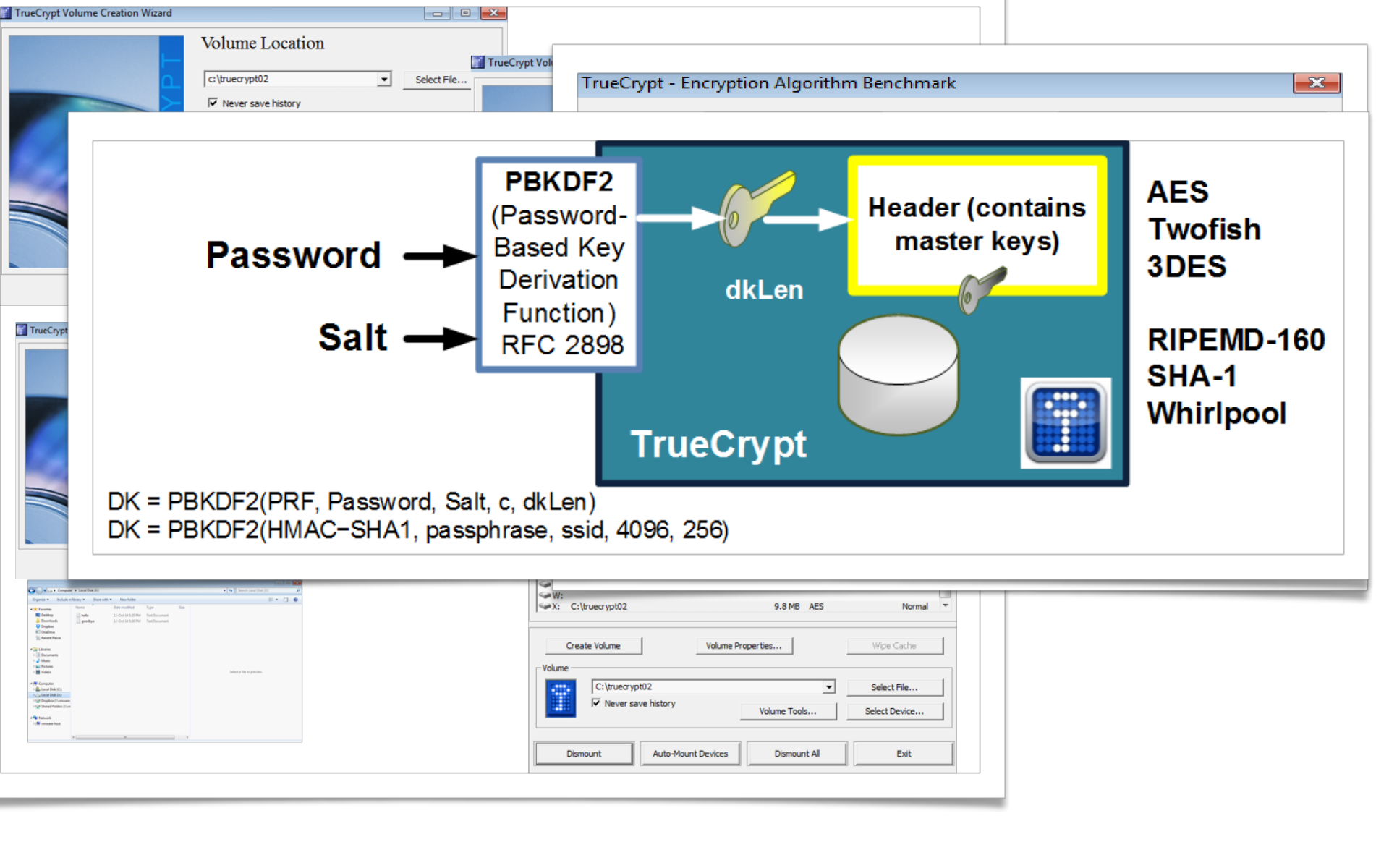
DK = PBKDF2(PRF, Password,Salt, c, dkLen)
DK = PBKDF2(HMAC-SHA1, passphase, ssid,4096,256)

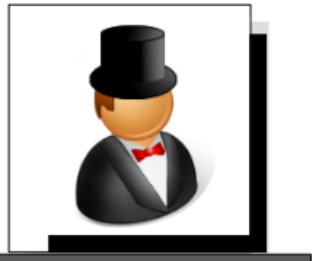
- **Serpent**. Ross Anderson et al. 1998. 256-bit key. 128-bit block (one of the AES finalists).
- **Twofish**. Bruce Schneier et all. 1998. 256-bit key. 128-bit block (one of the AES finalists).
- **AES**. FIPS-approved (Rijndael). 1998. 256-bit key. 128-bit block.

Author: Prof Bill Buchanan


TrueCrypt Volume Creation Wizard
Volume Location
c:\truecrypt02
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt containe
which can reside on a hard disk, on a USB flash drive, etc. A
TrueCrypt container is just like any normal file (it can be, for
example, moved or deleted as any normal file). Click 'Select File' t
choose a filename for the container and to select the location wh
you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encry
it; the file will be deleted and replaced with the newly created
TrueCrypt container. You will be able to encrypt existing files (
on) by moving them to the TrueCrypt container that you are ab
to create now.
Help
< Back
Next >
TrueCrypt Volume Creation Wizard
Volume Size
10
KB
MB
GB
Free space on drive c:\ is 9.62 GB
Please specify the size of the container you want to create.
If you create a dynamic (sparse-file) container, this parameter will
specify its maximum possible size.
Note that the minimum possible size of a FAT volume is 292 KB.
The minimum possible size of an NTFS volume is 3792 KB.
Help
< Back
Next >
Cancel
TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
AES
Serpent
Twofish
AES-Twofish
AES-Twofish-Serpent
Serpent-AES
Serpent-Twofish-AES
Twofish-Serpent
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel
TrueCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption algorithm
Type
X:
C:\truecrypt02
9.8 MB
AES
Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\truecrypt02
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit


TrueCrypt Volume Creation Wizard
Volume Location
c:\truecrypt02
Select File...
Never save history
Help
< Back
Next >
TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Serpent
Twofish
AES-Twofish
AES-Twofish-Serpent
Serpent-AES
Serpent-Twofish-AES
Twofish-Serpent
Test
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel
TrueCrypt - Encryption Algorithm Benchmark
Buffer Size: 50 MB
Sort Method: Mean Speed (Descending)
Algorithm | Encryption | Decryption | Mean
AES 1.2 GB/s 1.2 GB/s 1.2 GB/s
Twofish 147 MB/s 168 MB/s 157 MB/s
AES-Twofish 107 MB/s 161 MB/s 134 MB/s
Serpent 108 MB/s 102 MB/s 105 MB/s
Serpent-AES 99 MB/s 95.7 MB/s 97.5 MB/s
Twofish-Serpent 66.0 MB/s 79.9 MB/s 72.9 MB/s
AES-Twofish-Serpent 59.2 MB/s 71.8 MB/s 65.5 MB/s
Serpent-Twofish-AES 61.0 MB/s 64.4 MB/s 62.7 MB/s
Benchmark
Close
Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.
Parallelization: 2 threads
Hardware-accelerated AES: Yes
X: C:\truecrypt02 9.8 MB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\truecrypt02
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

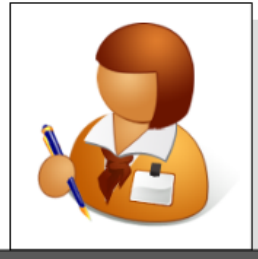

TrueCrypt Volume Creation Wizard
Volume Location
c:\truecrypt02
Select File...
Never save history
TrueCrypt - Encryption Algorithm Benchmark
Password
Salt
PBKDF2
(Password-Based Key Derivation Function)
RFC 2898
dkLen
Header (contains master keys)
TrueCrypt
AES
Twofish
3DES
RIPEMD-160
SHA-1
Whirlpool
DK = PBKDF2(PRF, Password, Salt, c, dkLen)
DK = PBKDF2(HMAC-SHA1, passphrase, ssid, 4096, 256)
X: C:\truecrypt02 9.8 MB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\truecrypt02
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit



Bob

TrueCrypt is an open source disk cryptography package - February 2004 - TrueCrypt Foundation.

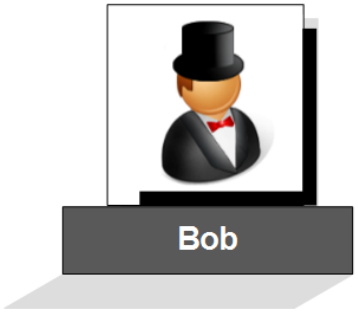
David Tesařík registered the TrueCrypt trademarking the US and Czech Republic, and Ondrej Tesarik registered the not-for-profit TrueCrypt company in the US.



Alice (Web)

Trent

Version 7.1a, there had been an audit on the code, with an announcement on 28 May 2014 that there was a discontinuation of TrueCrypt, along with the release of version of 7.2 (which was intentionally crippled and contained lots of warnings in the code). The updated licence (TrueCrypt License v 3.1) contained the removal of a specific language that required attribution of TrueCrypt.



WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

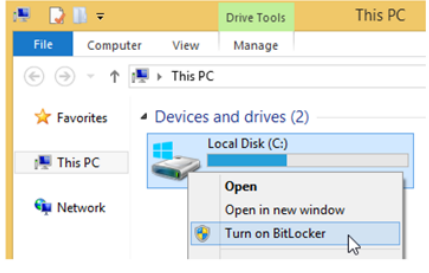
The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

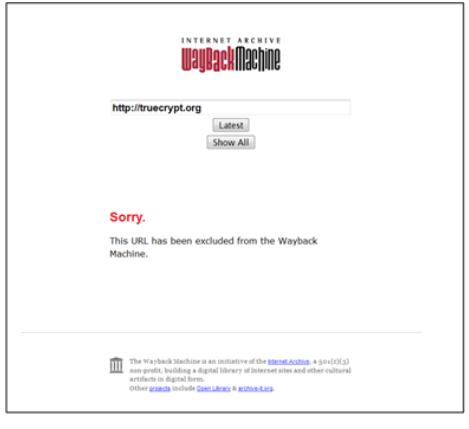
1. Decrypt the system drive (open **System** menu in TrueCrypt and select **Permanently Decrypt System Drive**). If you want to encrypt the drive by BitLocker before decryption, disable Trusted Platform Module first and do not decrypt the drive now.
2. Encrypt the system drive by BitLocker. Open the Explorer:

3. Click the drive C: (or any other drive where system encryption is or was used) using the right mouse button and select **Turn on BitLocker**:



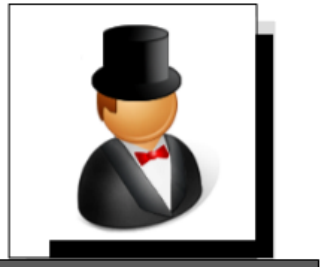
Within the code, "U.S." has been changed to "United States", which could point to an automated search and replace method of changing the code to reflect a possible change of ownership of the code

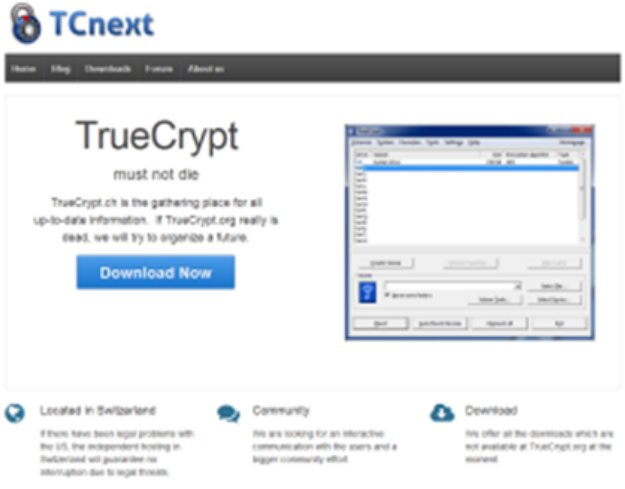
Novice Web page. Very poor layout of message.



Code bug? Generation of a pseudo random number, randomly use the time between key strokes for users.

Binary code exploit? Binary distribution could have been modified.



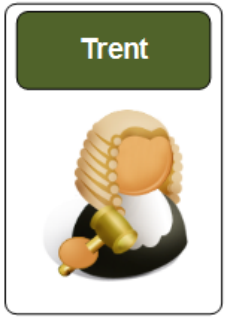


Truecrypt.ch

TrueCrypt must not die

TrueCrypt.ch is the gathering place for all up-to-date information. If TrueCrypt.org really is dead, we will try to organize a future.

@TrueCryptNext



Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity

An example of the first few bytes of TrueCrypt volume is:

```
4c 43 dd 86 cf 1f 69 eb 86 14 80 66 c9 2f 4b e2
f9 5a 01 c2 82 f4 bc c8 8b 71 59 3c 23 9b cc 40
ad 46 a7 b7 4e 00 45 98 d2 ea d2 32 26 a0 10 1c
67 80 2d 8a 08 61 ba c9 f6 d9 57 84 f2 93 11 18
```

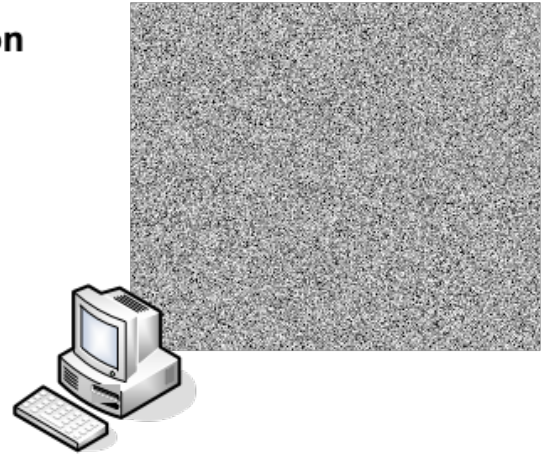
```
C:\Python27>python en.py "c:\Campus&DL - WB.tc"
File size in bytes:
3145728

Shannon entropy (min bits per byte-character):
7.99994457357

Min possible file size assuming max theoretical compression
efficiency:
25165649.6435 in bits
3145706.20544 in bytes

File size in bytes:
318724

Shannon entropy (min bits per byte-character):
7.98787618412

Min possible file size assuming max theoretical compression
efficiency:
2545927.84891 in bits
318240.981113 in bytes

File size in bytes:
62464

Shannon entropy (min bits per byte-character):
4.64286159485

Min possible file size assuming max theoretical compression
efficiency:
290011.706661 in bits
36251.4633326 in bytes
```

File Compression

PKZIP: 50 4B 03 04 [PK]
GZIP: 1F 8B 08
Tar: 75 73 74 61 72
Zlib: 78 01, 78 9C or 78 DA

```
[00000000] 50 4B 03 04 14 00 02 00 08 00 80 9D 6C 39 DA 4D   PK..........l9.M
[00000016] B8 0F 90 01 00 00 27 06 00 00 09 00 00 00 61 6E   ......'.......an
[00000032] 69 6D 2E 78 61 6D 6C ED 54 D1 4E 83 30 14 7D 37   im.xaml.T.N.0.}7
[00000048] F1 1F 9A 7E 00 C5 69 4C 24 B0 C4 CD A9 0F 6A 96   ...~..iL$.....j.
[00000064] 8D 64 CF 15 EE A0 B1 B4 A4 2D 8A 7F 6F 2D 6C 63   .d.......-..o-lc
[00000080] CA 14 13 1F 7C 90 A7 02 E7 9C 7B EF 39 E9 0D 57   ....|.....{.9..W
[00000096] 4C A4 F2 05 D5 C1 94 53 AD 23 BC 2A D7 97 65 C9   L......S.#.*..e.
```

File Encryption



```
47 c3 dd 4e 94 15 ce af 76 d6 94 9d 5d 82 88 99
34 d3 db 0d e4 ae af 57 e3 87 62 fd 14 7e f5 7d
02 7a 67 40 2b 2c 71 41 24 92 9d 54 1c 75 bb 54
0b f8 95 a9 92 d7 33 ad 2f 00 cb 8c 9f 90 66 49
b2 bd 0f 90 52 e3 aa 0a 59 6b 78 65 1f 5b 35 19
0f e3 32 ed c3 f0 04 88 67 51 33 cb 03 40 9f 3b
```

Host Security

TPM Chip.
Apple T2 Chip.
Disk Encryption: BitLocker.
Disk Encryption: TrueCrypt.
Entropy.

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity