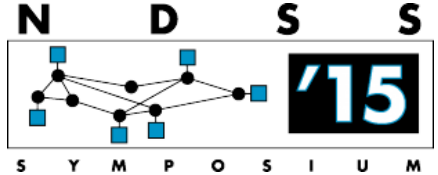
Gracewipe: Secure and Verifiable Deletion under Coercion

Lianying Zhao (Viau) Mohammad Mannan

Concordia University, Montreal, Canada

February 10, 2015



This is not a corner case ...

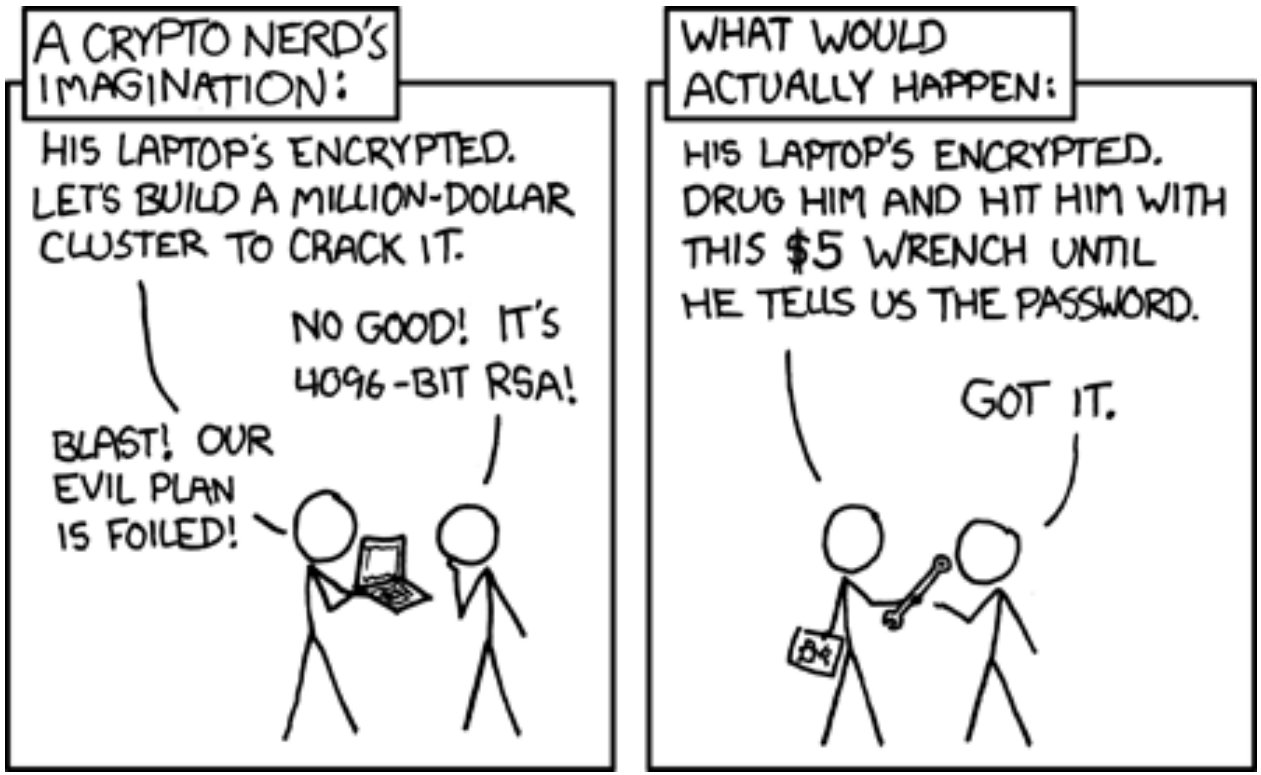


Image source: `http://xkcd.com/`

Confidentiality under coercion

- Coercive threats:
  - Law enforcement
  - Hostile country
- What makes the situation different?
  - Forced cooperation
  - Physical control

Confidentiality under coercion

- Coercive threats:
  - Law enforcement
  - Hostile country
- What makes the situation different?
  - Forced cooperation
  - Physical control

Rational adversary!

Existing mitigations - Hiding it?

- Plausibly Deniable Encryption (PDE)
  1. TrueCrypt
  2. StegFS: multi-level hidden file system

Existing mitigations - Hiding it?

- Plausibly Deniable Encryption (PDE)
  1. TrueCrypt
  2. StegFS: multi-level hidden file system

The adversary will find it!

Existing mitigations - Deleting it?

- Various secure deletion schemes
  1. ATA secure erase: overwriting-based deletion
  2. Cryptographic deletion

Existing mitigations - Deleting it?

- Various secure deletion schemes
  1. ATA secure erase: overwriting-based deletion
  2. Cryptographic deletion

Will you get the chance?

Existing mitigations - Deleting it?

- Various secure deletion schemes
  1. ATA secure erase: overwriting-based deletion
  2. Cryptographic deletion

Will you get the chance?

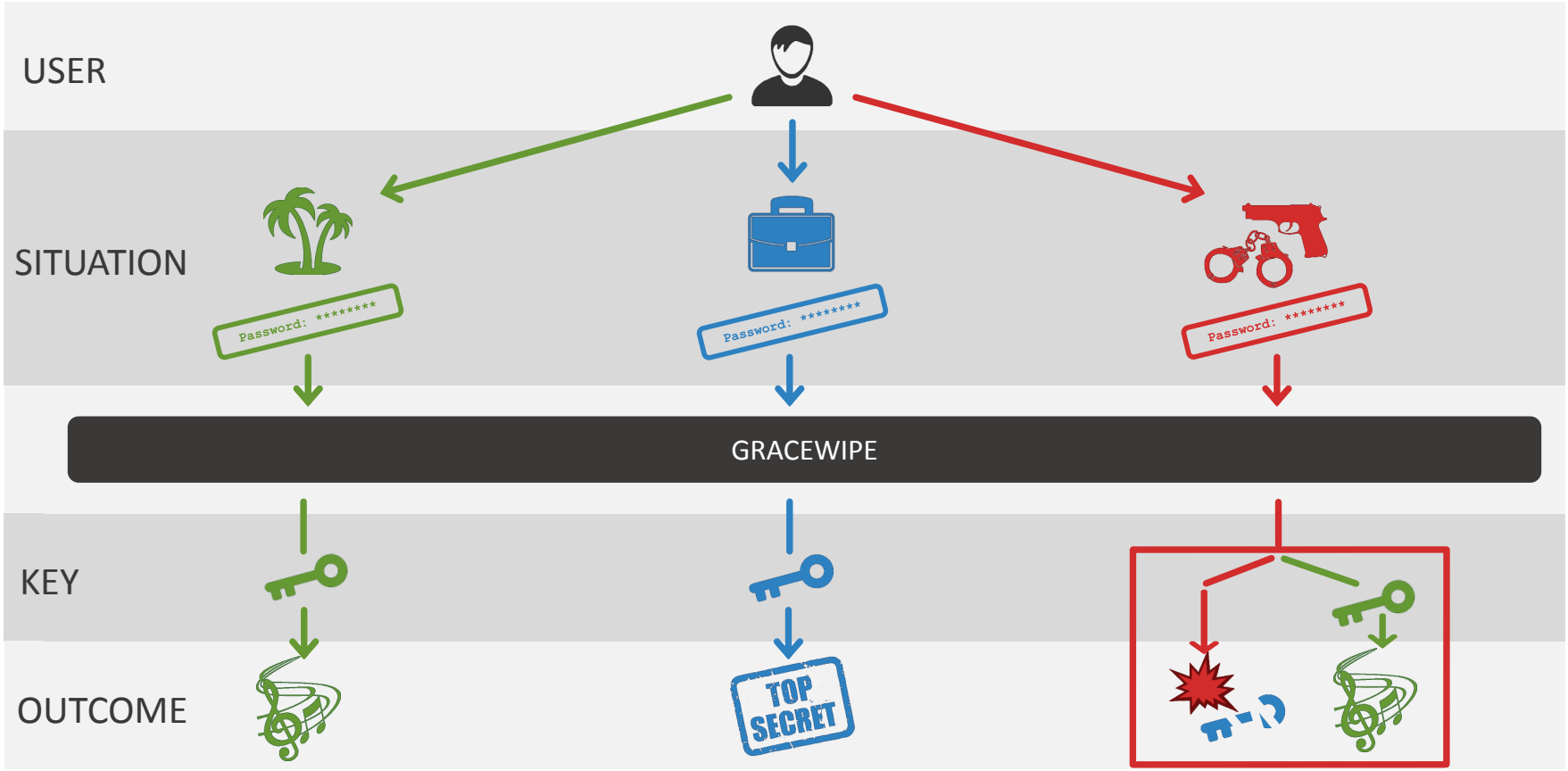
The adversary does NOT believe you!

Our goals

1. **Deletion triggering**: undetectable
2. **Deletion process**: uninterruptable
3. **Deletion outcome**: cryptographically verifiable
4. **Risk of guessing**: unavoidable

Image source: `http://security-is-just-an-illusion.blogspot.ca/`

Gracewipe: A simplified overview



Icon source: `www.shutterstock.com`

What is Gracewipe?

1. A small pre-OS system
2. Acts upon user-entered password (destroy? decrypt?)
3. Attests to what happened cryptographically

Gracewipe terminology

1. Two systems:
   - Decoy (protected by key KN)
   - Hidden (protected by key KH)
2. Three (sets of) passwords:
   - Normal password (PN) that decrypts KN
   - Hidden password (PH) that decrypts KH
   - Deletion password (PD)

Building blocks

1. Trusted Platform Module (TPM)
   - Onboard secure storage

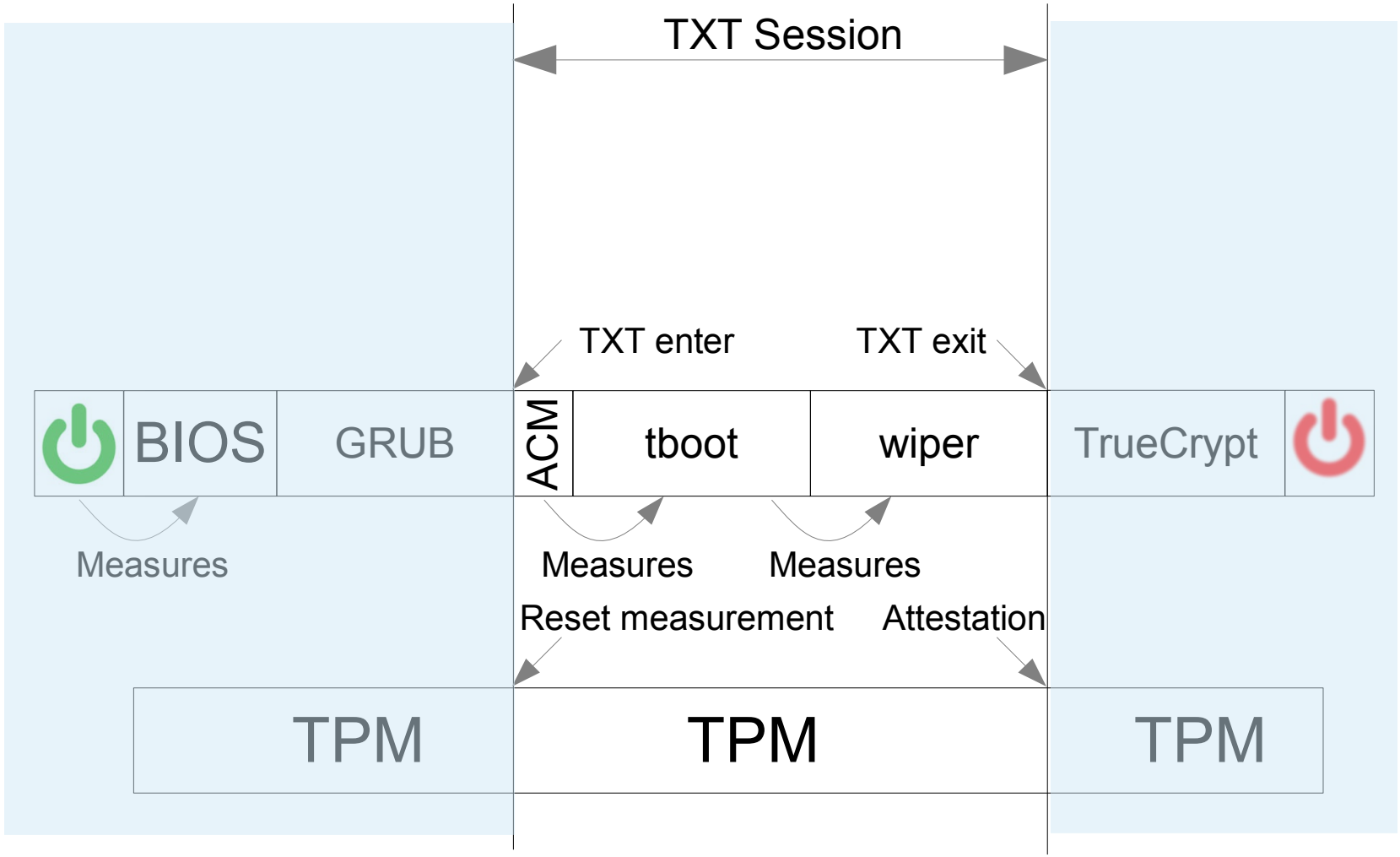
2. Intel TXT late launch
   - CPU execution mode
3. TrueCrypt
   - Encryption tool with PDE

4. Self-Encrypting Drive (SED)
   - Disks with internal encryption engine

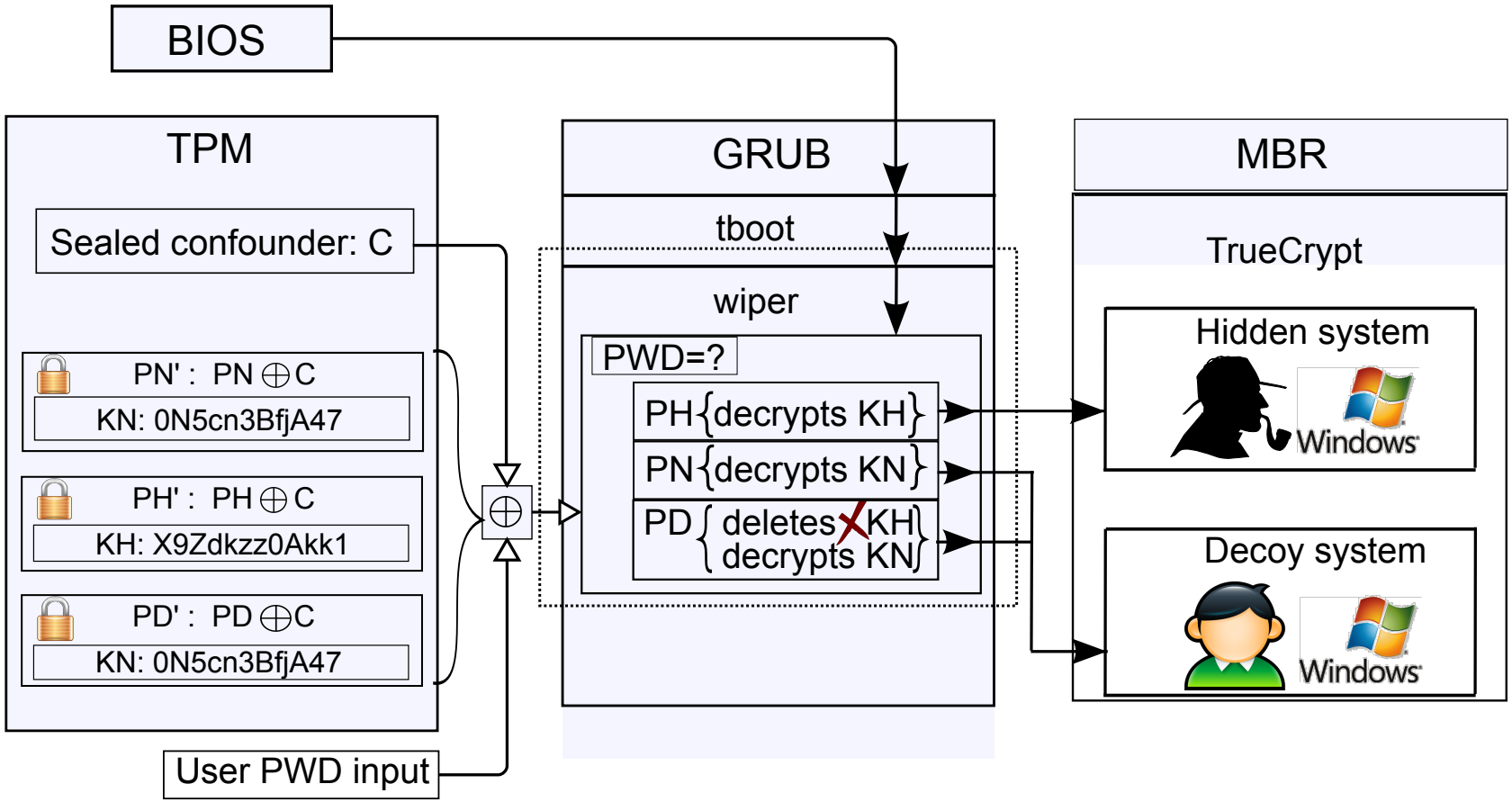
How are goals achieved?

1. Deletion triggering:
   deletion password
2. Deletion process:
   cryptographic deletion
3. Deletion outcome:
   chained measurement (TXT + TPM)
4. Gracewipe uncircumventable:
   keys only in TPM

How is the chain of trust established?



The design and workflow



Key features

1. TPM-bound protection
   (bypassing Gracewipe is difficult)
   - The user does not know the key secured in TPM
2. Environment integrity-bound secret
   (brute-forcing to access TPM is hard)
   - A sealed high-entropy C protects TPM storage
   - Alternative options also available

SED-based Gracewipe

- Only one regular volume is considered
- Similar design and workflow apply
- ATA security API compliant mode is used for compatibility
- The hidden key (KH, sealed in TPM) replaces the ATA password, but with higher entropy

Implementation challenges

- Pre-OS environment
  (context switch, device access etc.)
- Inherent technical restrictions
  (Intel TXT with Microsoft Windows)
- Effort to bridge all components
  (for minimum changes to maintain)

Remaining limitations

- TPM deadlock
- Limited number of PDs
- Degraded disk I/O without DMA

Other application scenarios

1. Emergency data deletion
2. Pre-OS isolated and verifiable execution of sensitive operations (e.g., OS integrity check)

Recap:

1. Coercion poses special challenges:
   Forced cooperation + Physical control
2. Gracewipe initiates verifiable deletion of data via deletion password(s)
3. Verifiability comes from hardware features available on commodity computers

Recap:

1. Coercion poses special challenges:
   Forced cooperation + Physical control
2. Gracewipe initiates verifiable deletion of data via deletion password(s)
3. Verifiability comes from hardware features available on commodity computers

Thank you! Questions?

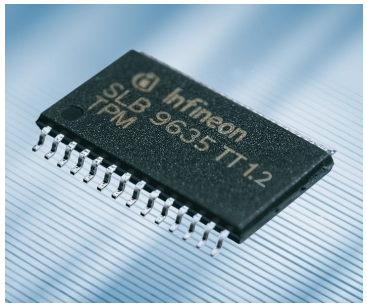
For more information:

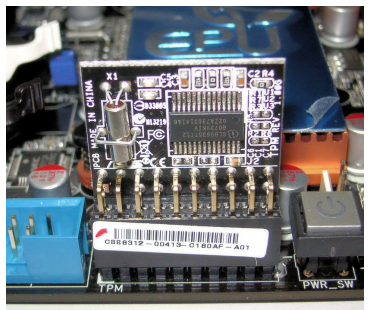
`https://madiba.encs.concordia.ca/software.html`

Backup foils

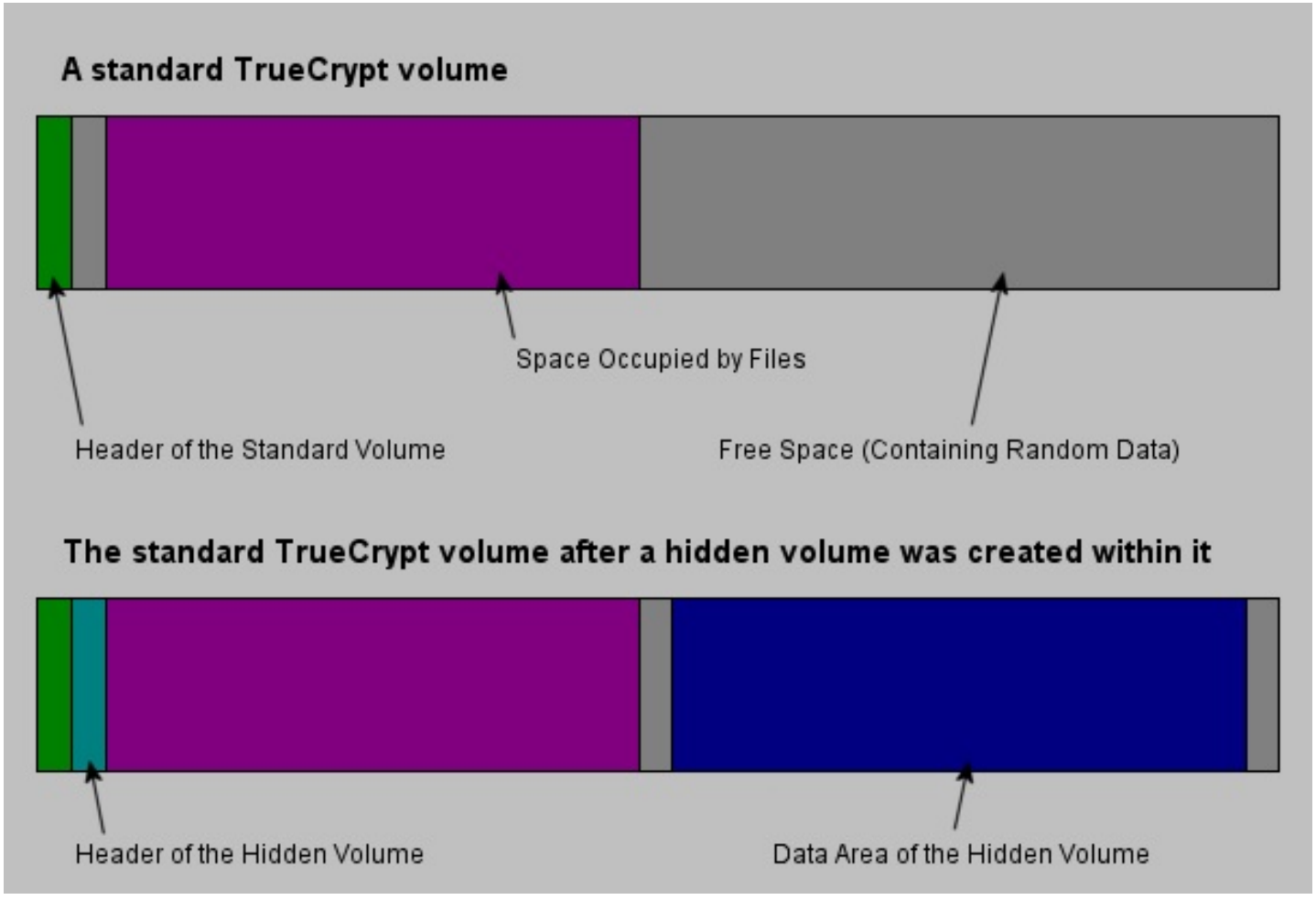
Trusted Platform Module (TPM)

1. Cryptographic processor + RAM + NVRAM + secured I/O
2. Platform Configuration Registers (PCRs as RAM)
3. Security-enabling operations
   - Extend: chaining measurements to PCRs
   - Seal: binding data to platform in a given state
   - Secure storage: protected NVRAM





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

Programming TPM communication

```
TCSD TCS rpc/tcstp/rpc.c:580 Dispatching ordinal 91 (NVReadValueAuth)
TCSD TCS tcsi_nv.c:202 TCSP_NV_ReadValueAuth_Internal: Enter
TCSD TCS tcsi_nv.c:212 req_mgr_submit_req  (oldOffset=67)
To TPM: 00 C2 00 00 00 43 00 00 00 D0 80 00 00 00 00 00
To TPM: 00 00 00 00 00 80 00 8B B4 4D 29 B2 61 E6 0E 88
To TPM: 75 AD D9 19 23 81 1F EE 6D CB 07 F2 B5 04 00 90
To TPM: 42 5A F1 35 63 63 FC 60 45 85 03 02 E6 61 F1 8D
To TPM: D9 4E B3
TCSD TDDL tddl.c:171 Calling write to driver
From TPM: 00 C5 00 00 00 B7 00 00 00 00 00 00 00 80 61 62
From TPM: 63 31 32 33 00 FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
From TPM: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FC BA
From TPM: D8 74 32 6C BB A3 4C 65 88 BF 21 71 7B 3F 84 25
From TPM: 08 9A 00 A6 2C 3E 5D FB B9 B4 FF DE 08 58 C8 D7
From TPM: 0B 4F 4D 3A DE BB 20
TCSD TCS tcsi_nv.c:217 UnloadBlob  (paramSize=183) result=0
TCSD TCS tcsi_nv.c:223 Leaving NVReadValueAuth with result:0
```

- TPM_TAG_RQU_AUTH1_COMMAND: 00 C2
- Total number of input bytes including paramSize and tag
- Ordinal, TPM_ORD_NV_ReadValueAuth
- The index of the area to set
- The offset from the data area
- The size of the data area
- authThe auth handle for the NV element authorization
- Nonce generated by system associated with authHandle (Odd)
- The continue use flag for the authorization session handle
- HMAC key: nv element authorization

- TPM_TAG_RSP_AUTH1_COMMAND
- Total number of output bytes including paramSize and tag
- The return code of the operation
- The size of the data area
- The data ("abc123")
- Even nonce newly generated by TPM to cover outputs
- Continue use flag, TRUE if handle is still active
- HMAC key: nv element authorization

BIOS is working overtime in Windows protected mode

```
nt!RtlpBreakWithStatusInstruction:
81cb87b8 cc              int     3
kd> kv
ChildEBP RetAddr  Args to Child
82386958 81cb87b0 00000001 81cb8782 00000000 nt!RtlpBreakWithStatusInstruction (FPO: [1,0,0])
82386960 81cb8782 00000000 00000000 00000002 nt!KdCheckForDebugBreak+0x22 (FPO: [0,0,0])
82386990 81cb8610 81c2009b 03923b00 00000000 nt!KeUpdateRunTime+0x164
823869ec 81cb7e13 00000000 00000000 000000d1 nt!KeUpdateSystemTime+0x613
823869ec 81c2009b 00000000 00000000 000000d1 nt!KeUpdateSystemTimeAssist+0x13 (FPO: [0,2] TrapFrame @ 82386a00)
82386a70 81c1ba50 00000042 82386a90 81c1c82c hal!READ_PORT_UCHAR+0x7 (FPO: [1,0,0])
82386a7c 81c1c82c 00000000 00000042 81c25100 hal!x86BiosReadIoSpace+0x76 (FPO: [Non-Fpo])
82386a90 81c1bee8 81c25100 81c244bc 82386ab8 hal!XmInOp+0x36 (FPO: [Non-Fpo])
82386aa0 81c1bfb5 81c25100 0000c000 00000014 hal!XmEmulateStream+0xb9 (FPO: [Non-Fpo])
82386ab8 81c1b61f 00000010 82386b00 81c244bc hal!XmEmulateInterrupt+0x89 (FPO: [Non-Fpo])
82386acc 81c15267 00000010 82386b00 00000000 hal!x86BiosExecuteInterruptShadowed+0x43 (FPO: [Non-Fpo])
82386aec 81c152af 00000010 82386b00 00000400 hal!x86BiosCall+0x45 (FPO: [Non-Fpo])
82386b20 8b09f680 8080ad70 80811dc8 00000000 hal!HalpBiosDisplayReset+0x25 (FPO: [Non-Fpo])
82386b48 81fd375e 00000000 8468e001 00000000 BOOTVID!VidInitialize+0x142 (FPO: [Non-Fpo])
82386b60 81ff3627 00000001 8080ad70 845c87b8 nt!InbvDriverInitialize+0x75
82386c48 81dca4d8 82386c90 81e4713d 8080ad70 nt!Phase1InitializationDiscard+0x126
82386c50 81e4713d 8080ad70 3161fd63 00000000 nt!Phase1Initialization+0xd
82386c90 81cee559 81dca4cb 8080ad70 00000000 nt!PspSystemThreadStartup+0x9e
00000000 00000000 00000000 00000000 00000000 nt!KiThreadStartup+0x19

kd>
```