



Penetration Testing Windows Vista™ BitLocker™ Drive Encryption

Douglas Maclver

Penetration Engineer
System Integrity Group, Microsoft Corporation



Hack In The Box 2006/09/21

© 2006 Microsoft Corporation. All rights reserved.

Trustworthy Computing

“The security of our customers' computers and networks is a top priority, and we are committed to building software and services to better help protect our customers and the industry.”

Microsoft

- Threats discussed in this presentation are not secrets
- Our customers' adversaries are aware of these attack vectors
- Our customers need this information too, so that they may make informed decisions about the level of data protection that they need

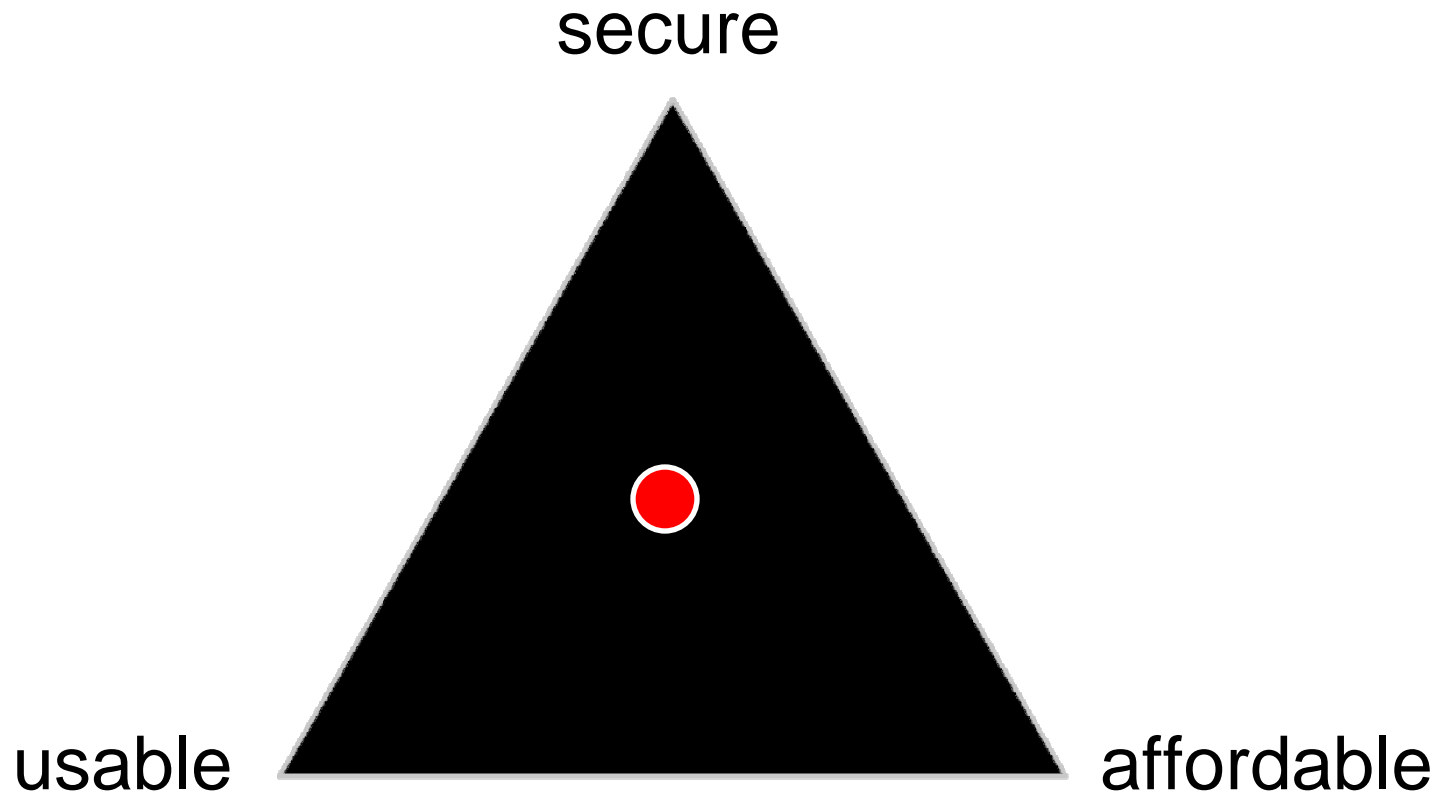
Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - Top Threats Part 1 (basic mode)
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

BitLocker Drive Encryption: Feature Introduction

- Data Confidentiality
 - Encrypts the OS volume
 - Secure decommissioning
- System Integrity
 - Cryptographically validates pre-OS components
- The lost or stolen laptop is the primary threat scenario
- Provides multiple levels of protection with basic and advanced modes

Security Management



Adapted from Jesper M. Johansson, "Security Management", Microsoft TechNet

BitLocker Key Points

- BitLocker in its basic mode provides a higher-level of data security with no additional security burden on the user
- BitLocker provides a range of options that allows customers to configure BitLocker for their security needs
- BitLocker should be deployed on platforms that have the “Designed for Windows” logo

Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - Top Threats Part 1 (basic mode)
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

Trusted Platform Module v1.2

- BitLocker uses TPM v1.2 (not v1.1)
 - Similar to the functions and security properties of Smart Cards
 - Fastened onto motherboard
 - Platform Configuration Registers (PCRs)
 - Can have Tamper Resistance / Reaction / Evidence
 - Trusted Computing Group (TCG) specification
- BitLocker can be used without TPM
 - But this mode does not include BitLocker's pre-OS integrity validation

BitLocker Modes

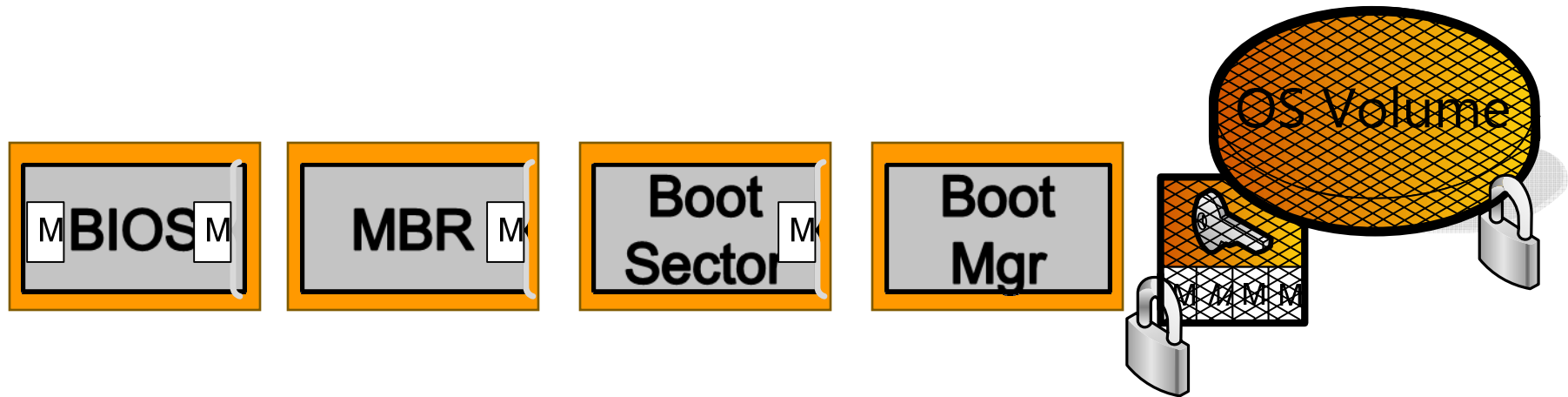
- Basic
 - TPM
- Advanced
 - TPM + PIN
 - TPM + USB Dongle
 - USB Dongle

Trusted Computing Base (TCB)

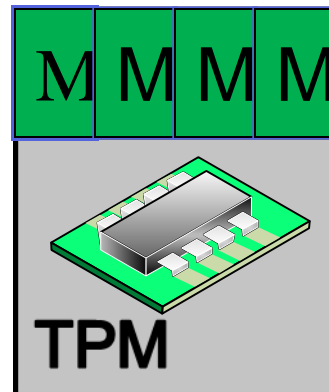
“The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.” [INFOSEC glossary]

- BitLocker’s use of a TCB:
 - Trusted identification of code and data loaded during boot
- Foundation that OS builds on
 - OS Code Integrity
 - x64 platforms: digital signatures for kernel-mode software

TCB Validation



TPM's Platform Configuration Registers (PCRs)



M: Measurement
MBR: Master Boot Record
Boot Mgr: Boot Manager

Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - **Top Threats Part 1 (basic mode)**
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

Adversary Objectives

- Read plaintext data off of the disk
- Gain access to encryption keys
- Gain control of privileged threads

Physical Memory Ghosts: Warm

- Warm ghosting
 1. Attacker boots system
 2. Attacker warm reboots into OS which avoids destruction of RAM image
 3. Attacker then can access ghost secrets in memory
- **Mitigations:**
 - Platforms where BIOS clears memory on reboot
 - BitLocker advanced modes

Physical Memory Ghosts: Cold

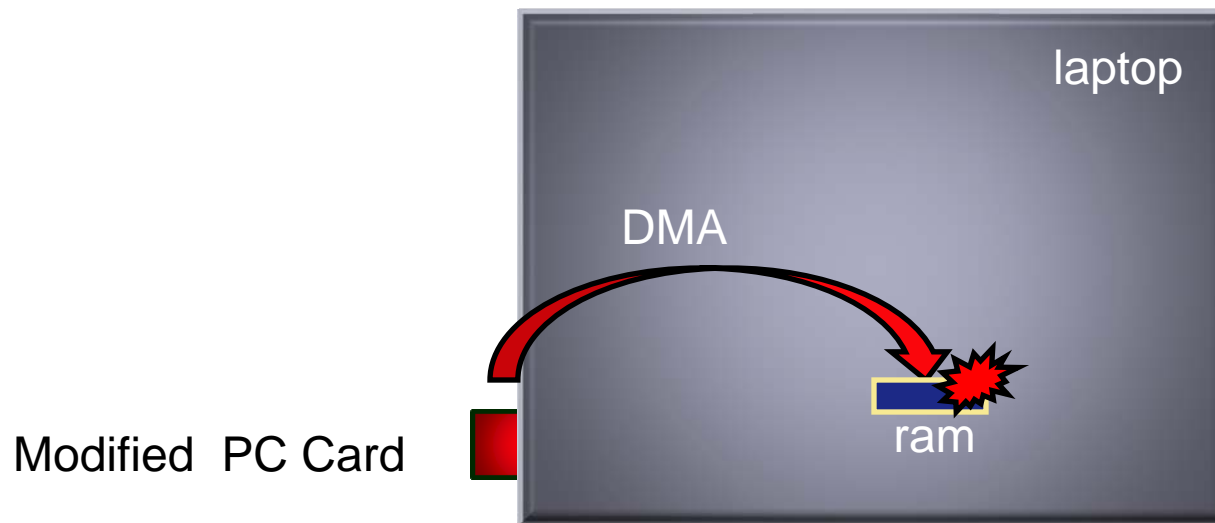
- Cold ghosting
 - Physical memory cells may retain charge long enough to be copied
 - Iceman attack



- Battery-backed DIMMs make this even easier
- Mitigations: BitLocker advanced modes

Cheap, Easy, & Distributable HW-oriented Attacks

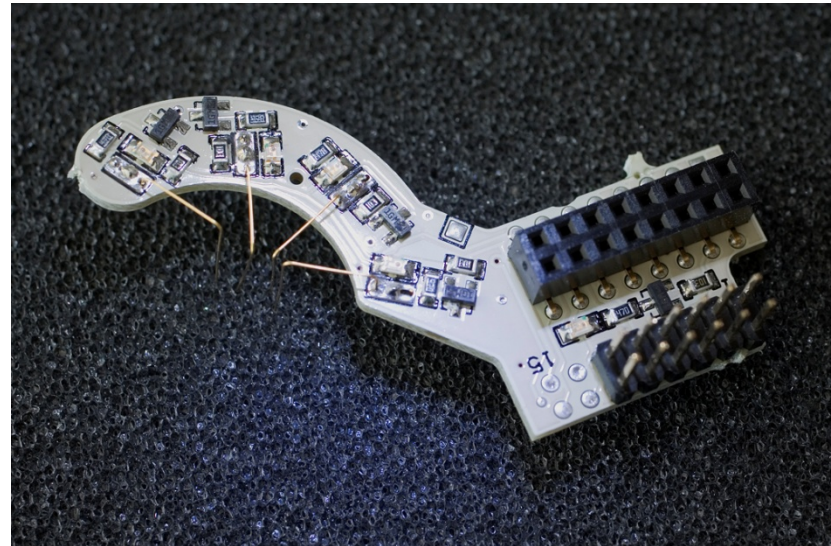
- PCI bus exploit with repurposed PC Card device and DMA (direct memory access)
 - e.g. CardBus DMA technique demoed by David Hulton at ShmooCon, 2006



Mitigation: BitLocker advanced modes

Cheap, Easy, & Distributable HW-oriented Attacks

- Xbox v1-style attacks
 - LPC bus, HyperTransport bus, etc.
 - Hacking the Xbox, by Andrew “bunnie” Huang



- Mitigation: BitLocker advanced modes

Threats against the TCB

- Executing code-of-choice within the TCB
 - Controlling the instruction pointer
 - Potential pre-OS component vulnerabilities (bootmgr, winload, winresume, etc.)

- Mitigation: MS Security Development Lifecycle
- Mitigation: BitLocker advanced modes

Threats against the TCB

- Core Root of Trust for Measurement (CRTM) is intended to be 'immutable' portion of BIOS
- Attacking the CRTM
 - Execute chosen-code in CRTM
 - Control / prevent measurements
 - Physically remove it
 - Attack existing CRTM (e.g. buffer overrun)
 - Attack secure update-mechanism to inject unauthorized code into CRTM
- Mitigation: BIOS meets BitLocker requirements
- Mitigation: BitLocker advanced modes

Ciphertext Manipulation Threats

- Attacker can alter disk sectors offline, which will subsequently be decrypted during boot
- AES-CBC allows attacker to make known deltas in the decrypted data
- These deltas could be used to alter the security posture of the stolen laptop

- Mitigation: AES-CBC + Diffuser
- Mitigation: BitLocker advanced modes

Encryption without Diffuser

Plaintext

```
a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa  
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba  
c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca  
d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da  
00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00
```

Encrypt with
AES-CBC

Encrypted data (AES-CBC)

```
6e f8 7b 69 25 5d e0 19 fb ab ca f4 f8 b5 4b 58  
ad 99 e6 ef e2 f7 8e 1d 9d 91 a8 61 fc 81 5d c8  
60 b0 dc 81 5e 4e ed 2e c9 aa e9 63 40 a2 a8 c5  
d5 7c 42 d0 84 f8 a2 c2 ad 56 8b 35 4f ea 2a e7  
2e 32 70 f8 48 08 d0 b5 1f 81 40 69 7b 00 8c 03  
f0 60 74 15 62 d5 c8 14 fb 7b 66 e5 4e df 18 aa  
8e 26 a2 39 76 9a f6 ba c5 ef 8d e3 b2 ce b3 87  
05 d1 60 fe a1 4c 33 31 9b 24 1b 3f 4f 6a 29 e8  
c4 50 82 07 f4 b2 bf 03 66 8b 73 9d a7 13 3f 69  
29 a7 ae c5 28 a6 48 15 86 76 bd 4d 7e 91 b4 69  
e2 bc 4b 9b 23 9a 10 35 7f 21 73 46 4c 27 a7 a3  
cd 63 86 d1 54 b6 b1 56 33 5e cf b1 59 2d c6 6a  
0f 62 a5 51 8d d6 3e 4e b5 3c 7e c0 a6 65 fa 11  
9a 2c 90 c3 e4 b2 87 ab be d0 9a e7 62 ea 22 75  
a6 46 67 05 35 4b 81 bb 87 e1 fc 84 10 8c 26 2b  
13 ad 7e 4b 4f 15 4d f9 c1 53 0e b9 8f 88 63 da  
46 bd 88 4e 2b 4b 0f 3e b7 7b 1c 10 3f be 76 98  
54 fe 0c 08 5e 5a 80 04 eb 1f d6 53 e5 7a fd 55  
47 af 9d 8b 75 a0 e3 a5 82 21 c1 5a 62 75 e6 9a  
3d e6 6e 77 ae de 1f 06 60 6d df 8f d6 5b 4d 22  
44 5a 89 9f a7 04 35 8a 30 43 e0 03 0c a7 f3 02  
f5 ba 0d c4 bb 5a 82 74 f2 27 b7 25 e8 2a 61 0d  
a9 ed 4c 3d a9 88 3f bb 7e e9 d9 87 d2 b3 e8 35  
8d 0d 2b 2a e6 97 42 27 75 a2 a6 2d 8f 94 3c 1f  
44 26 27 00 d7 fc 05 1d 6e e9 af  
66 80 3f a6 4d f1 36 20 4e 05 2c  
e8 22 99 12 e5 7b 10 e0 38 fe f6  
2c 7e cb 5d 20 a0 c5 cb 08 9a 19  
68 2d f7 36 3d e4 5f 98 05 83 16  
37 84 4a 5a 35 11 c4 d4 7b 48 4b  
98 58 b6 6d 57 88 0c dd b1 37 f4  
2d 6a 6c dd 17 12 ce d8 54 6e bf
```

Decrypt with
AES-CBC

Decrypted Data

```
a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af  
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf  
c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf  
d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```


AES-CBC + Diffuser

Attacker flips a single bit in ciphertext (0x58 to 0x59)

Entire sector is randomized

```
Encrypted data (AES-CBC + Diffuser)
60 db c0 eb ad 22 45 9e 15 3e a8 24 1c 9a 54 00
21 84 66 df 13 30 0b 04 80 71 5d 47 57 f5 68 ec 71 3c
44 b9 e2 6c 31 33 6f 58 81 47 57 f5 68 ec 71 3c
f1 e0 94 b5 53 59 81 47 57 f5 68 ec 71 3c
ff 01 a2 78 55 c9 c0 70 cd 18 2f 55 7c 1e eb 1f
90 ea 0f de 89 01 74 b9 70 58 77 68 ce 1d 8a 98
2d 06 c5 66 70 73 87 81 fb 63 45 67 18 e2 b9 af
1c 60 10 ea 70 72 70 96 57 c8 44 ac 2d 79 94 c4
68 66 36 38 9d 31 ae 78 d8 81 cf 1e 96 48 13 dc
f8 f6 2e f7 0b ee 55 85 97 95 24 41 72 f9 38 b8
a3 1e 78 4c 4e a1 02 0a 12 d3 61 33 dd cd 78 75
ee d5 e1 ba b0 c9 2f b8 85 90 81 72 91 04 ff 35
4f 6c 21 3b d6 cf 72 0e 16 68 a2 cc b2 3e bd 16
b3 24 5c 7e ef 77 d6 ed 03 0c e5 0f 9a e1 51 a2
ba 62 36 b8 fb 54 4b a6 78 c5 9a b3 53 9a 14 3a
6d ea 6f ad 0d 25 2e 98 a9 7a e2 3d f0 41 e3 23
55 e3 39 34 df 15 b3 bd b6 54 49 d1 b5 97 75 2b
0f 34 c8 2e 74 e6 f7 98 22 aa 24 2e c0 39 74 c2
30 d3 9f 41 75 cb f3 59 a5 8c 4b b9 89 57 d9 c2
5d ef f1 da 98 71 c6 be c5 3d 35 a1 43 0f 86 48
29 4b 05 2a c0 67 28 2f 91 4d c8 aa 87 fb 35 1d
7b ed e9 81 4b 75 41 2b 72 76 ae 48 77 fb f5 55
87 49 f3 1b d2 3a e4 21 11 2b 12 0f e6 3e b6 99
eb fd 0a ad 33 da 6c 88 50 53 3a 4a a1 da 5c 7e
f8 9e 48 be 5d b9 83 4e bb 39 fb c0 b4 00 85 d1
e4 bd 52 df fe cc 44 72 33 e3 3e aa 49 f5 5f 17
4c 95 2b 1b 22 5c 2f 62 50 53 76 73 47 d3 2b 43
```

Decrypt with
AES-CBC + Diffuser

```
Decrypted Data
de 4d 7b 4a d0 f6 b7 1 3b 3a 6d 4f e8 52 a2
87 79 dd 7b c3 1b 51 1e d1 27 a1 73 b4 d4 16
74 47 87 a7 b1 57 9f df da bb 43 90 4e 7a 23 fe
06 d3 15 76 a8 8e 8c cf 51 ff 56 26 0e 6e 46 4d
ef 42 7e 60 4c cf 8f 3d 19 71 5a e4 df b1 40 f0
5a 1d b0 a6 04 83 29 51 72 6b 32 08 36 12 ff c5
23 b8 5d 93 b0 51 6a 59 55 d7 4c 9e f0 e8 25 ad
63 df 94 db 72 d3 f5 56 dd f0 5b e8 3a 16 61 70
5f 17 99 25 76 84 09 41 2b 0d f4 67 34 0f 63 f8
2f ff 68 52 9c 61 38 7f b1 ae 1d 43 61 0a e0 5a
c5 e7 da 1c 63 0a d1 6f 1b db f8 64 b4 9e d0 52
32 0f 25 12 1a b4 6f bf 68 c7 dc 46 9b c3 42 a3
d7 3b 4d b2 d6 ca 55 11 33 10 4e 9d 2a e8 ca 43
d0 2b d4 0b ea 9f 57 84 e0 63 05 da c6 b1 4b 66
2e 1b 39 ab 5a d0 26 bf 87 1a fa 02 62 6f c7 cb
cc 24 f7 b7 40 4e 24 ab cd 43 7b 75 47 60 12 c6
36 5a 63 6d 12 fd 88 3b 50 5c 95 77 7a f0 13 dd
80 76 c3 fe f6 ad ee 9e da 45 16 16 8a e3 6e 32
1c 75 bd c5 e7 e5 f9 df 7b 3d cd d2 4f 6e 06 73
98 7c 3c 06 b0 7d 05 41 40 fe d7 05 f9 56 c2 65
43 a5 86 99 44 3c 83 58 38 51 75 fc d7 ee 80 50
8b a1 c7 e6 f8 b2 d0 d1 1d f7 1a 1b 24 b8 01 23
```

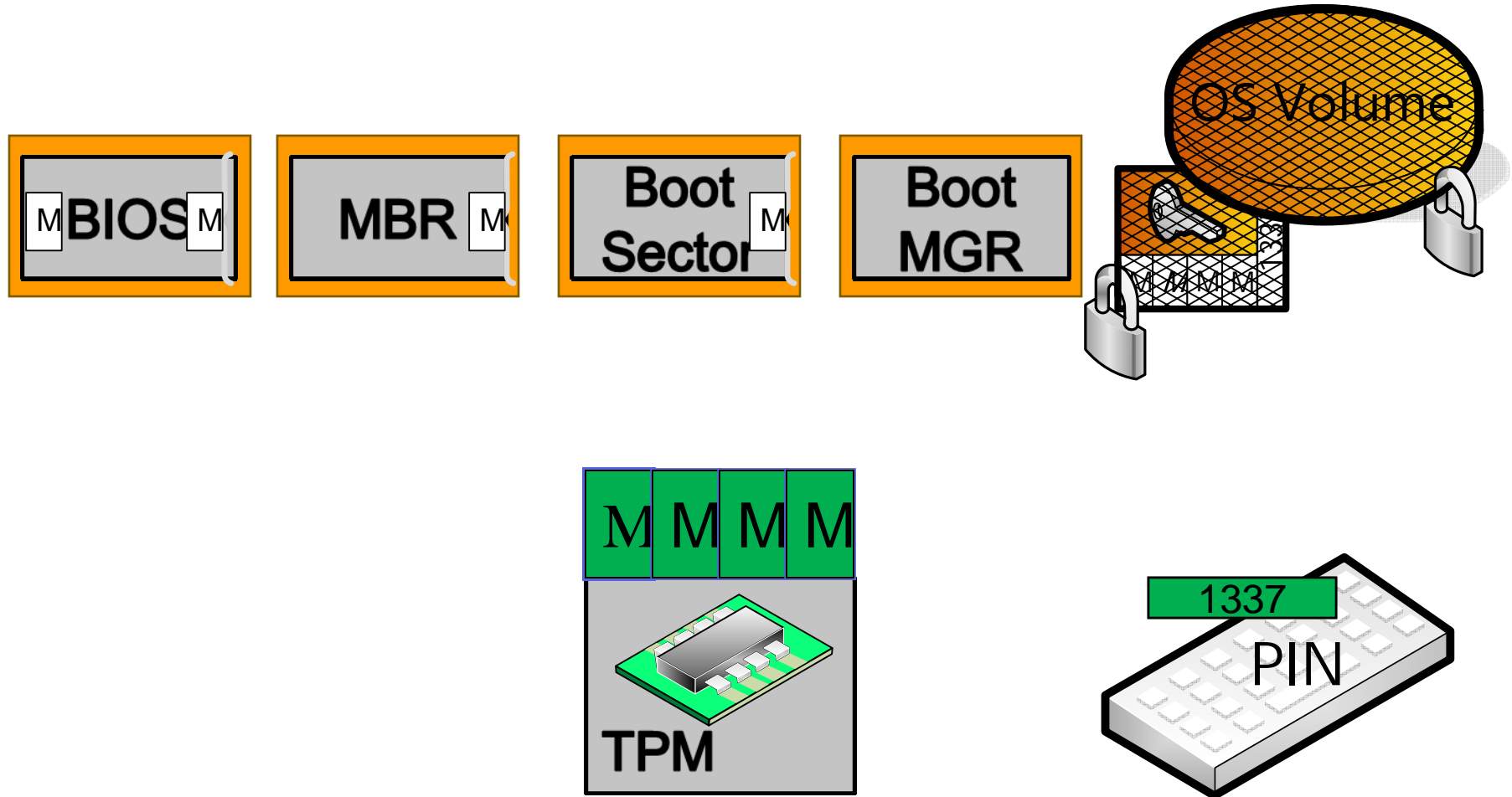
Ciphertext Manipulation Threats

- AES-CBC + Diffuser helps, but there are still threats
 - Cost: randomize entire sector (512+ bytes)
 - Result: limited control of where data changes occur
 - Effects:
 - denial of service
 - critical services fail to load?
- AES-CBC 128 + Diffuser 128 is default mode of BitLocker
- **Mitigation: BitLocker advanced modes**

Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - Top Threats Part 1 (basic mode)
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

Advanced Mode: TPM + PIN



TPM + PIN Threats

- For 'unseal' to succeed:
 - TPM Authdata value correct
 - TRUNC(SHA256(PIN), 20B)
 - TPM PCR values correct
- Attack: Brute-force PIN
- Mitigation: TPM Anti-hammering: TPM Authdata failure lockout geometrically increases
- Mitigation: Use platforms that meet BitLocker requirements

TPM + PIN Key-wear Analysis

- Function keys used for input F1..F10... these are not commonly used
- Speculation: an adversary may be able to determine which keys occur in the PIN



- Mitigation: longer pins (via group policy), diverse pins; numeric keys will work on many keyboards

Boot Rootkits

- BitLocker detects boot rootkits installed *offline*
- BitLocker detects *online* boot rootkits that are *BitLocker-unaware*
- BitLocker does *not* protect against boot rootkits that are *BitLocker-aware* and travel through the OS.

- Mitigation: MS Security Development Lifecycle
- Mitigation: Windows Vista OS Security, Config, Best Practices

Multi-visit / Premeditated Attacks

- Attacker hobbles BitLocker protection *prior* to laptop loss or theft
- There are many advance-strikes

- Mitigations: Windows Vista OS Security, Best Practices

Cryptographic Threats

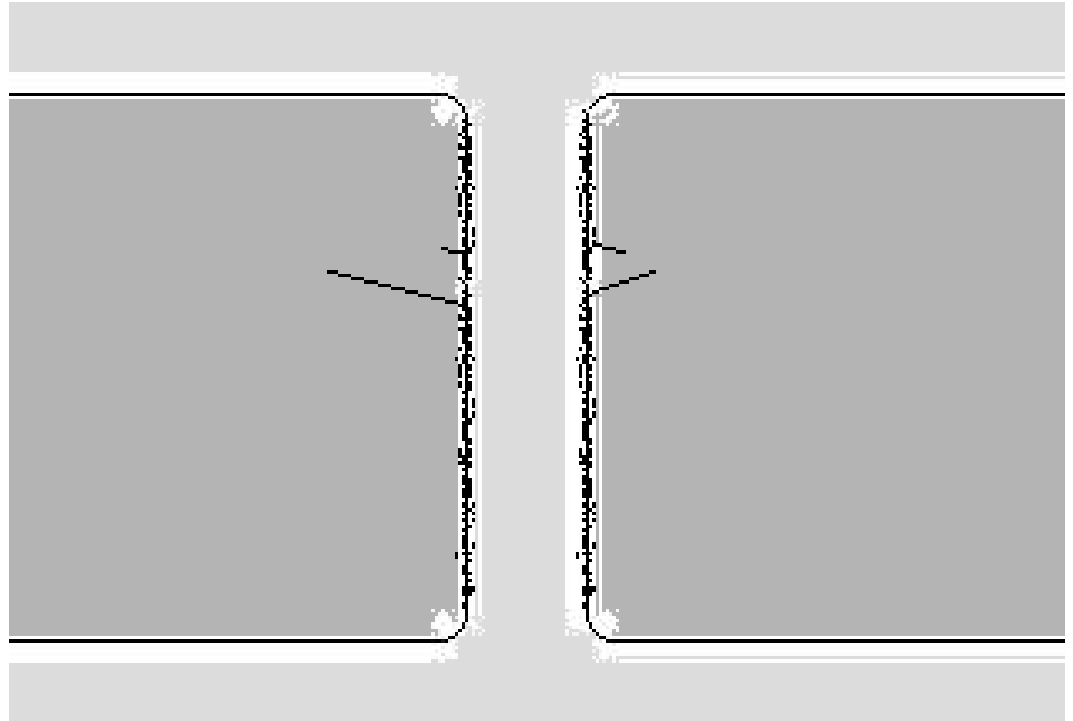
- Diffuser is a new algorithm and implementation
- BitLocker's AES-CCM is a new implementation of the AES-CCM standard
- Correct use of cryptographic APIs, counters, IVs, nonces, etc.
- Chosen- & Known- plaintext threats
- Ciphertext modification threats
- Mitigations: MS SDL, internal crypto review & validation
- Mitigations: external crypto review & validation, Crypto 2006, FIPS, Common Criteria

Lost While Unlocked

- Device is found, stolen, or illicitly accessed after the authorized user has authenticated, but before the device reaches the off state
 - Also known as “One Chance” attacks
 - Physical Memory Threats
 - Cheap, Easy, & Distributed HW-based Threats
-
- Mitigations: Best Practices, Group Policy for Hibernate

Data Remanence: Electromigration

- Relocation of metal atoms due to high current densities
- Detection:
 - OEM ports
 - Mechanical probing
 - Focused ion beam devices



Peter Gutmann, "Data Remanence in Semiconductor Devices", August 2001

Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - Top Threats Part 1 (basic mode)
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

Pen Testing BitLocker: The Team

- Team of several dedicated Microsoft penetration engineers
- Collaborated with the Microsoft Secure Windows Initiative (SWI) team
- Engagements with several external security vendors
- Engagements with many partners
- Engagements with security researchers

Pen Testing BitLocker : The Process

- Microsoft Security Development Lifecycle (SDL)
- Threat Modeling / Threat Storming
- Component data flows
- Large feature spanning hardware and software
- Broad and deep analysis
- Security code review
- Software and hardware pentests
- Trust-boundary Fuzzing
- Automated Analysis Tools

Presentation Outline

- BitLocker Introduction
 - BitLocker Technical Highlights
 - Pen Testing BitLocker
 - Top Threats Part 1 (basic mode)
 - Top Threats Part 2 (advanced modes)
 - Summary
-
- Questions (at the end, please)

Hardware platform is the new attack perimeter

- As some cracks are filled, other surfaces become interesting
- OS and Network are being hardened
- Data / Device mobility is prevalent
- The user and his devices have become the attack vectors
- Widely-deployed disk encryption will result in an increased attack effort against hardware

Adapted from David Maynor, "You are the Trojan!", ToorCon 7, 2005

BitLocker Key Points

- BitLocker in its basic mode provides a higher-level of data security with no additional security burden on the user
- BitLocker provides a range of options that allows customers to configure BitLocker for their security needs
- BitLocker should be deployed on platforms that have the “Designed for Windows” logo

More Information

Microsoft Trustworthy Computing

<http://www.microsoft.com/mscorp/twc>

BitLocker™ Questions

e-mail [bdeinfo\[at\]microsoft.com](mailto:bdeinfo[at]microsoft.com)

BitLocker™ Blog

blogs.msdn.com/si_team

Microsoft Security Development Lifecycle (SDL)

msdn.microsoft.com/security/sdl

Trusted Computing Group (TCG)

www.trustedcomputinggroup.org

Windows Hardware & Driver Central (WHDC)

www.microsoft.com/whdc



Thank you for attending.

Questions?

© 2006 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



© 2006 Microsoft Corporation. All rights reserved.