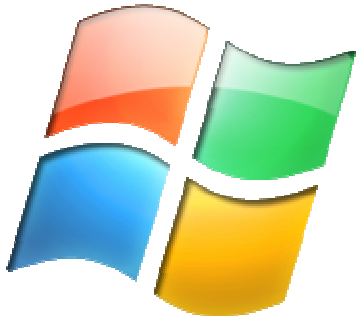


Penetration Testing Windows Vista™ BitLocker™ Drive Encryption

Douglas MacIver

Penetration Engineer
System Integrity Group, Microsoft Corporation

Microsoft Windows Vista™

Hack In The Box 2006/09/21

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

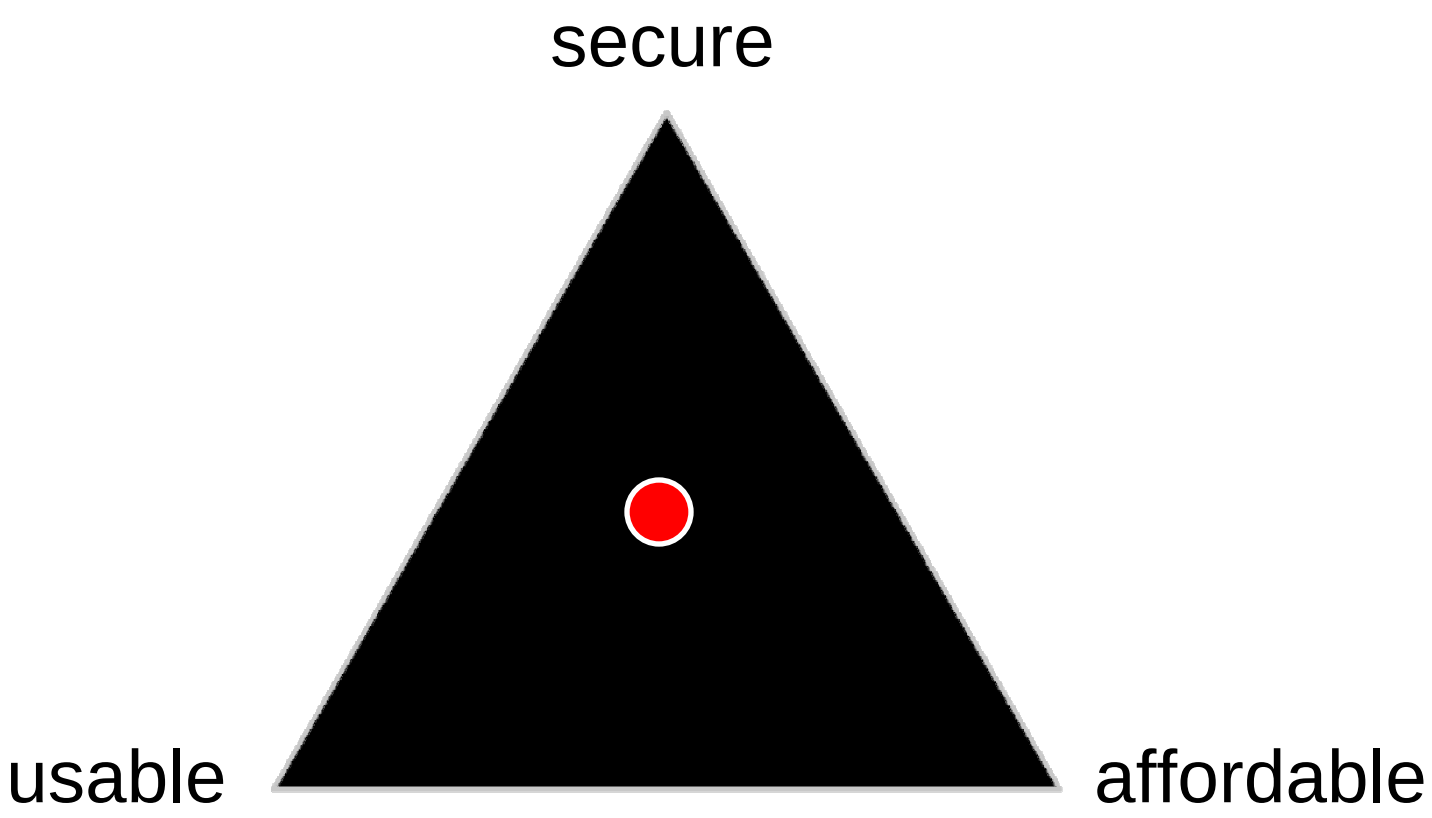
- BitLocker Introduction
- BitLocker Technical Highlights
- Pen Testing BitLocker
- Top Threats Part 1 (basic mode)
- Top Threats Part 2 (advanced modes)
- Summary

- 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

Microsoft Windows Vista™

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

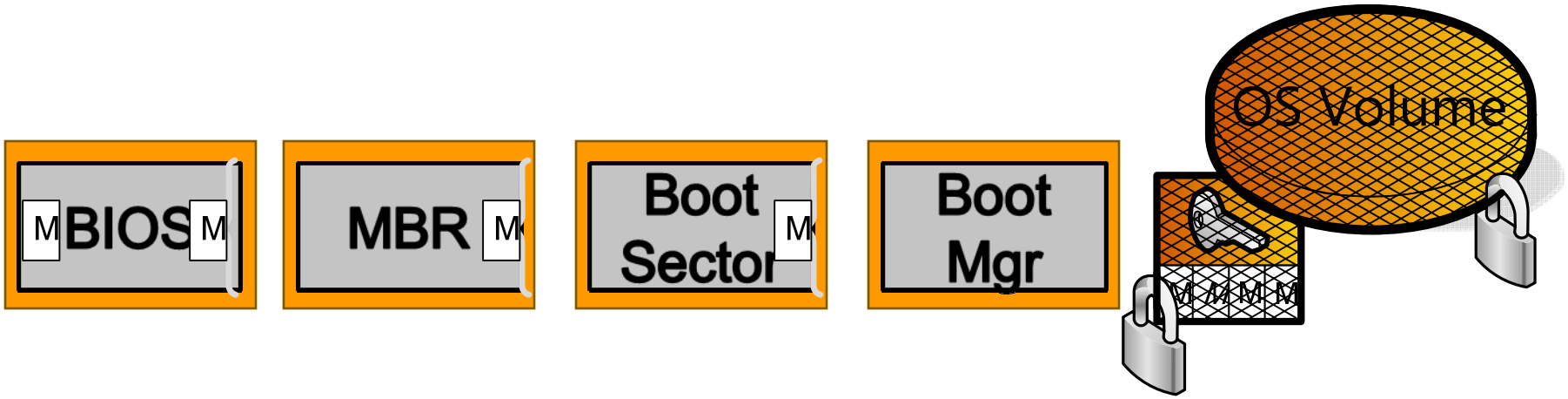
- Basic
  - TPM
- Advanced
  - TPM + PIN
  - TPM + USB Dongle
  - USB Dongle

Trusted Computing Base (TCB)

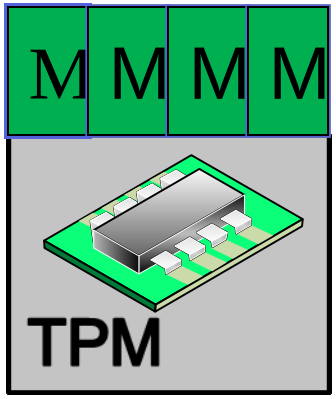
"The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy." [INFOSEC glossary]

- 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

Microsoft Windows Vista™

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

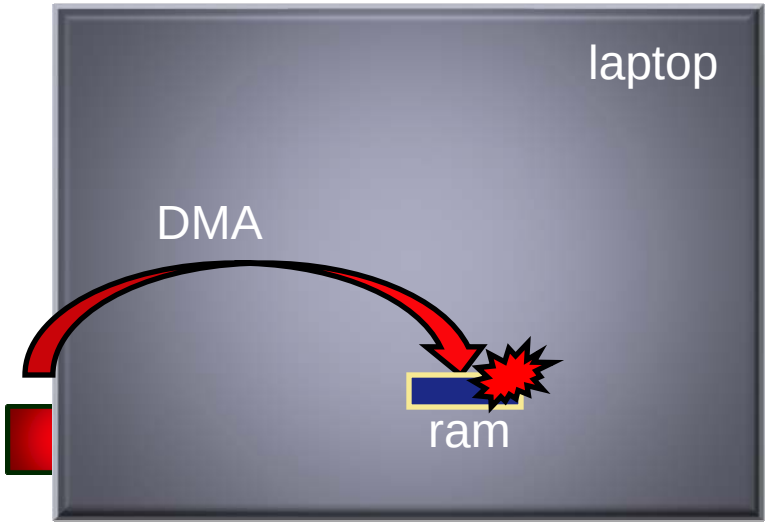
- Cold ghosting
  - Physical memory cells may retain charge long enough to be copied
  - Iceman attack

  - 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

Modified PC Card

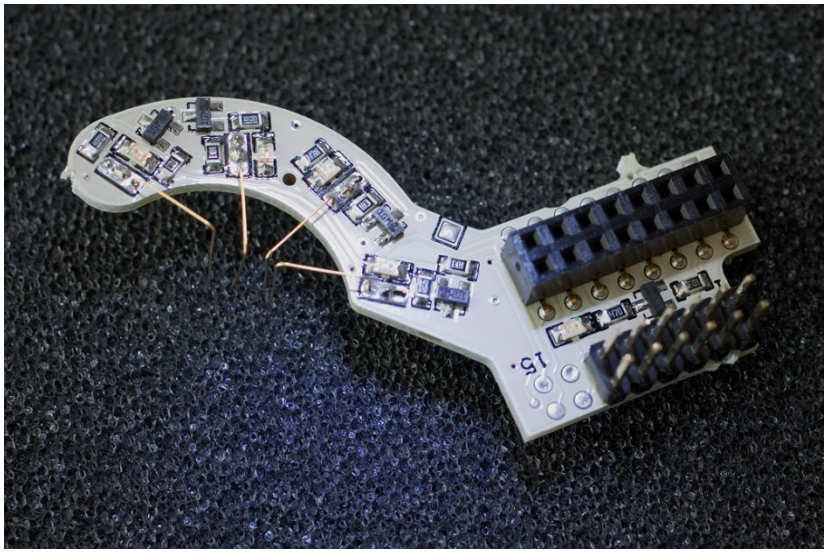


Mitigation: BitLocker advanced modes

Microsoft Windows Vista™

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

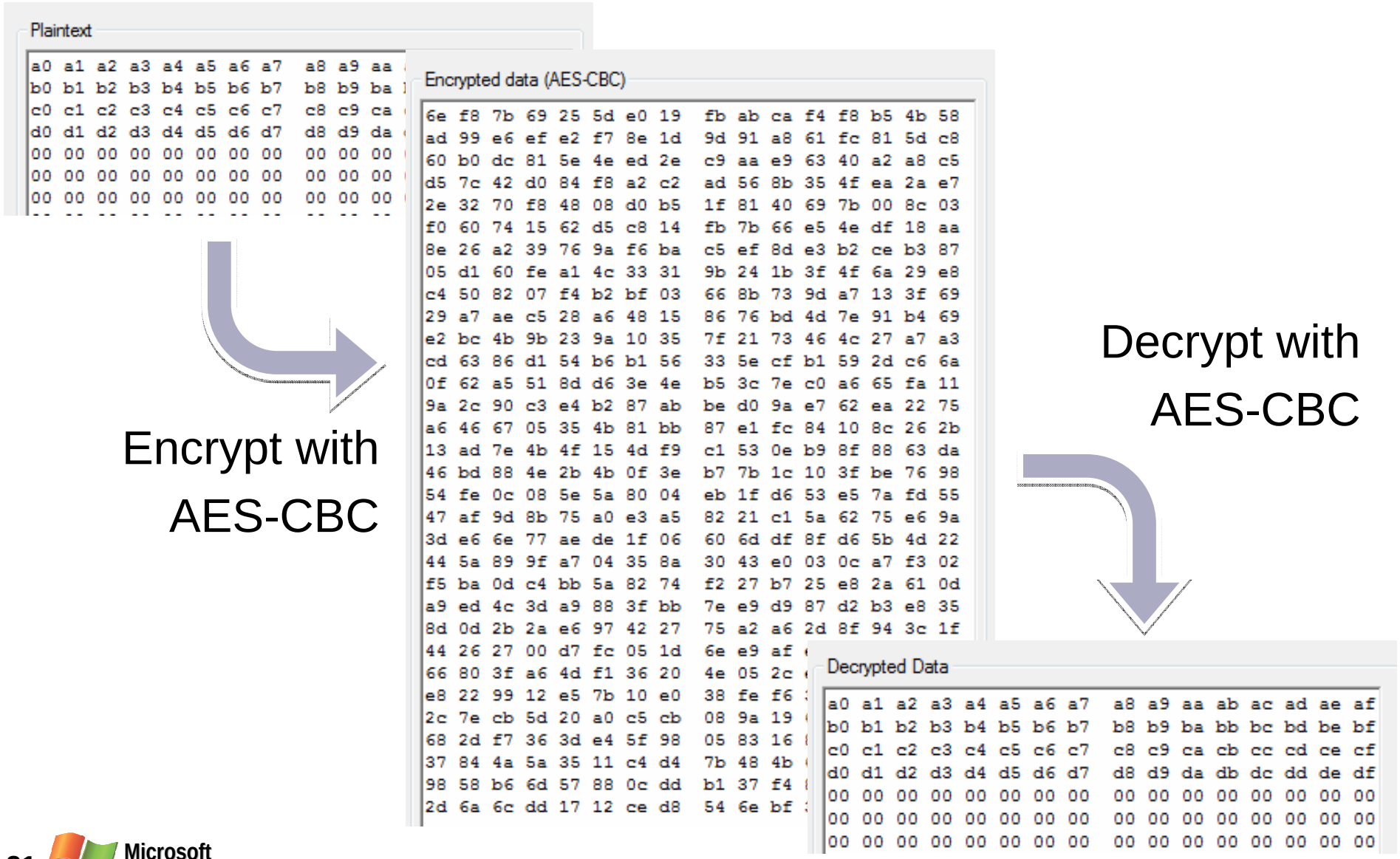
- Core Root of Trust for Measurement (CRTM) is intended to be ‘immutable’ portion of BIOS
- Attacking the CRTM
  - Execute chosen-code in CRTM
  - Control / prevent measurements
  - Physically remove it
  - Attack existing CRTM (e.g. buffer overrun)
  - Attack secure update-mechanism to inject unauthorized 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

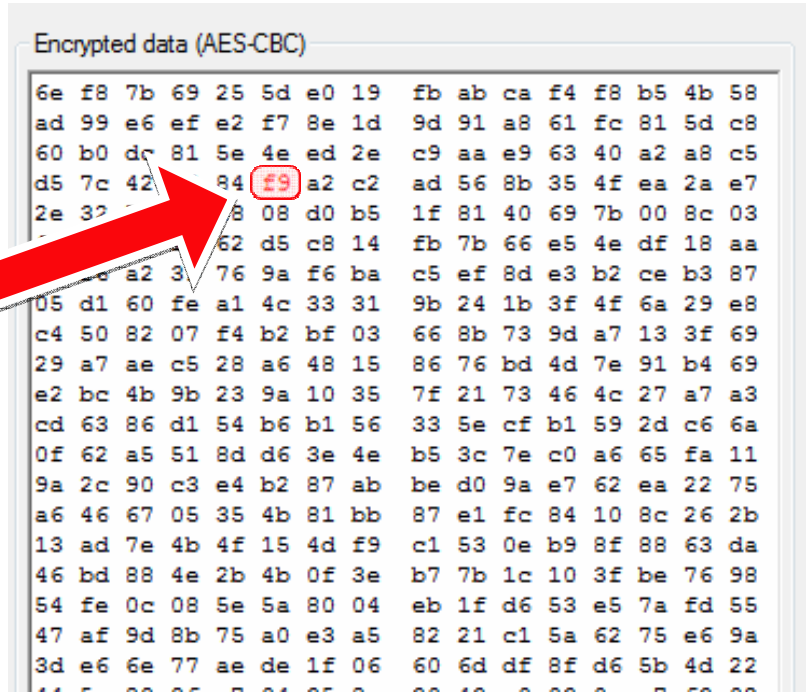
- Mitigation: AES-CBC + Diffuser
- Mitigation: BitLocker advanced modes

Encryption without Diffuser



Modification of AES-CBC Ciphertext

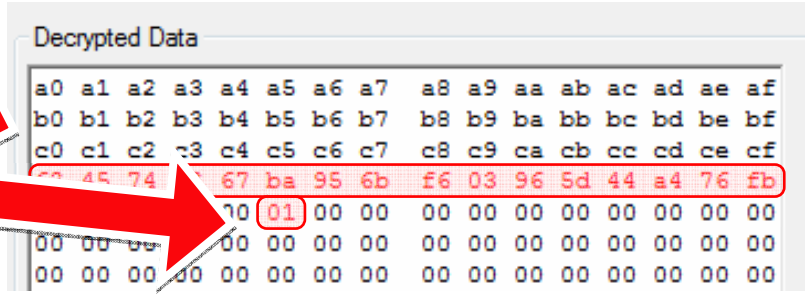
Attacker flips a single bit in the ciphertext (0xf8 to 0xf9)



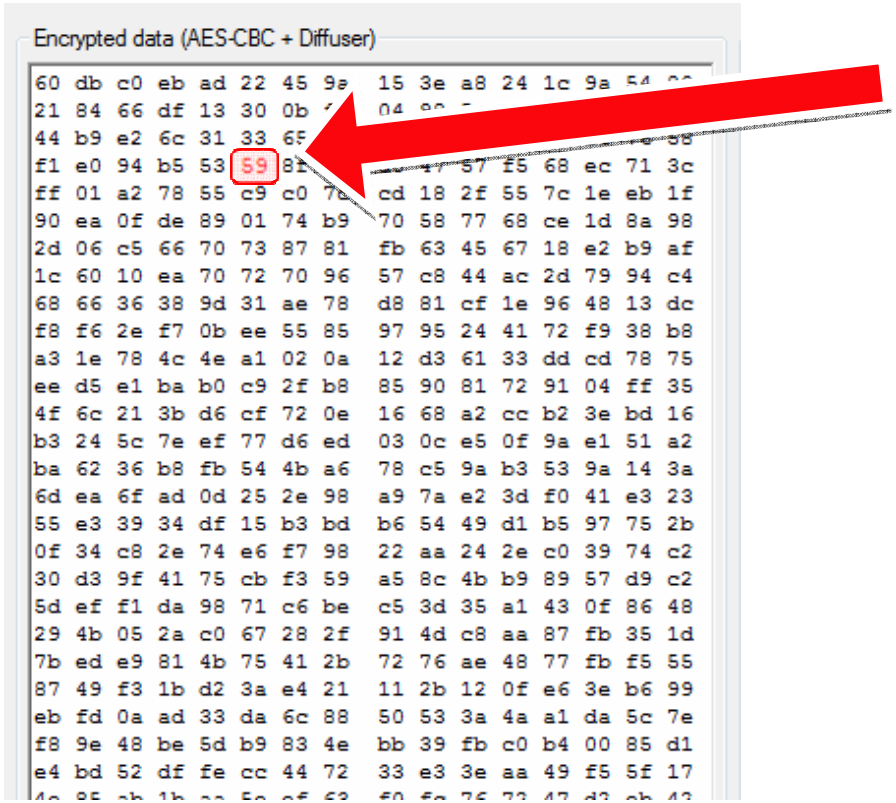
Decrypt with AES-CBC

One block randomized

Known delta in next block

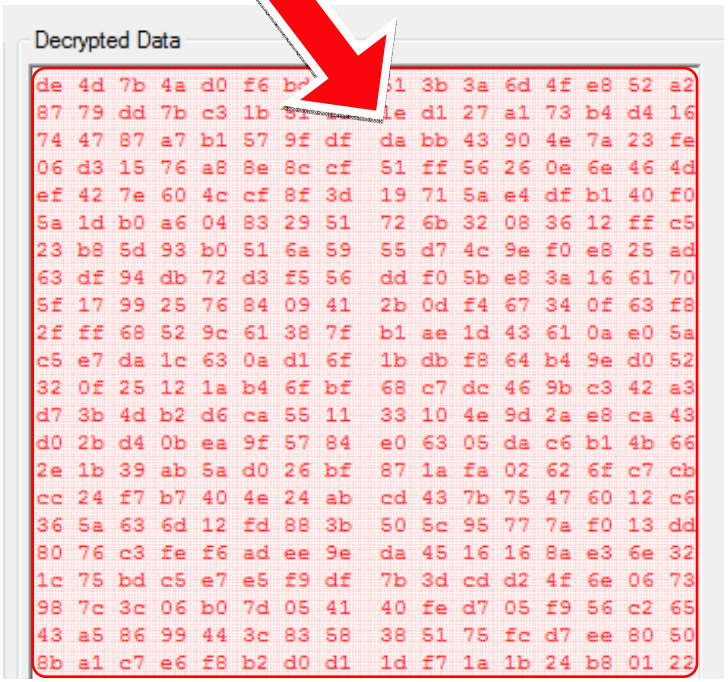


AES-CBC + Diffuser



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

Entire sector is randomized



Decrypt with AES-CBC + Diffuser

Microsoft Windows Vista™

Ciphertext Manipulation Threats

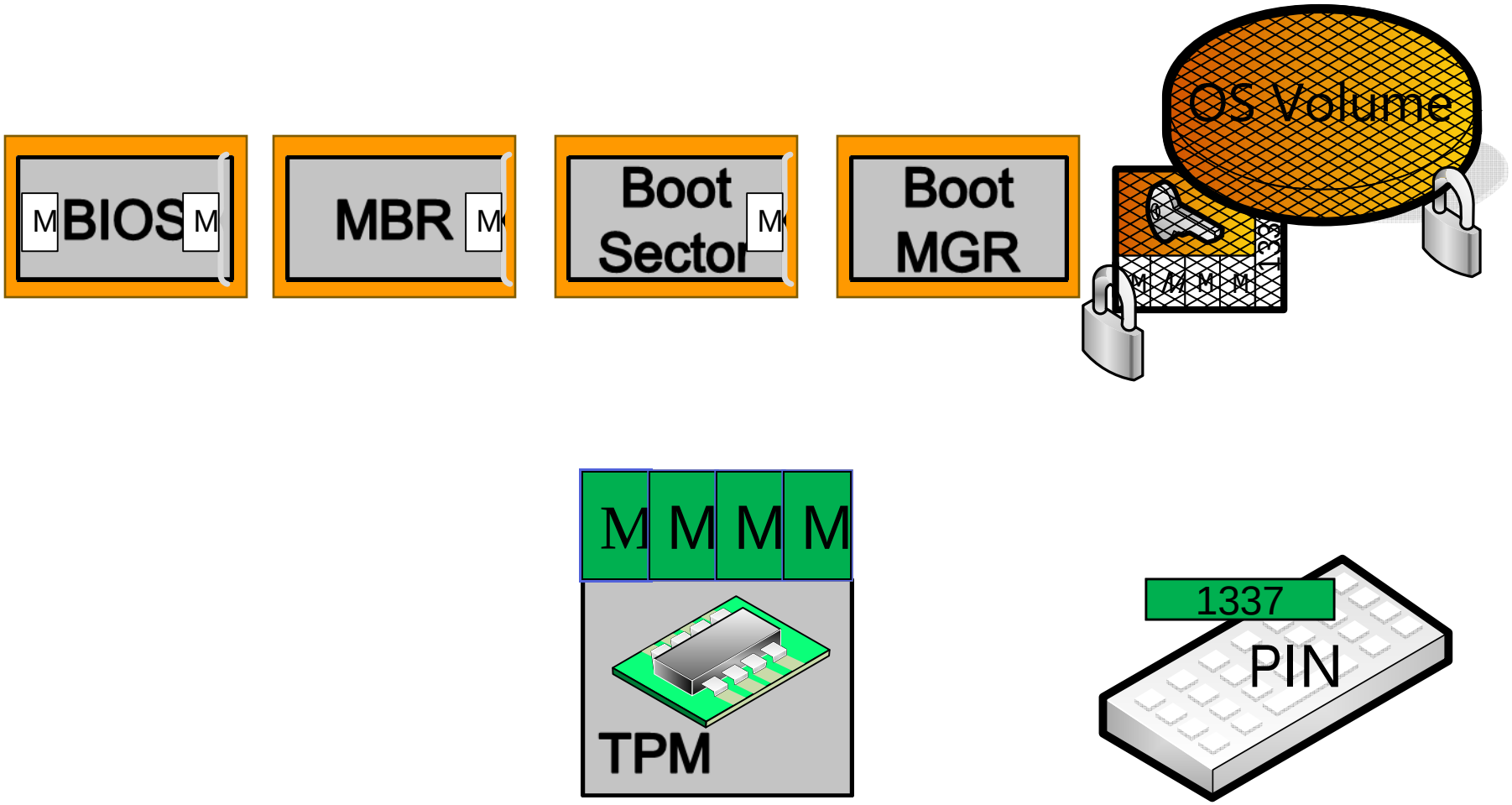
- AES-CBC + Diffuser helps, but there are still threats
  - Cost: randomize entire sector (512+ bytes)
  - Result: limited control of where data changes occur
  - Effects:
    - denial of service
    - critical services fail to load?
- AES-CBC 128 + Diffuser 128 is default mode of BitLocker
- Mitigation: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



Microsoft Windows Vista™

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

Microsoft Windows Vista™

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

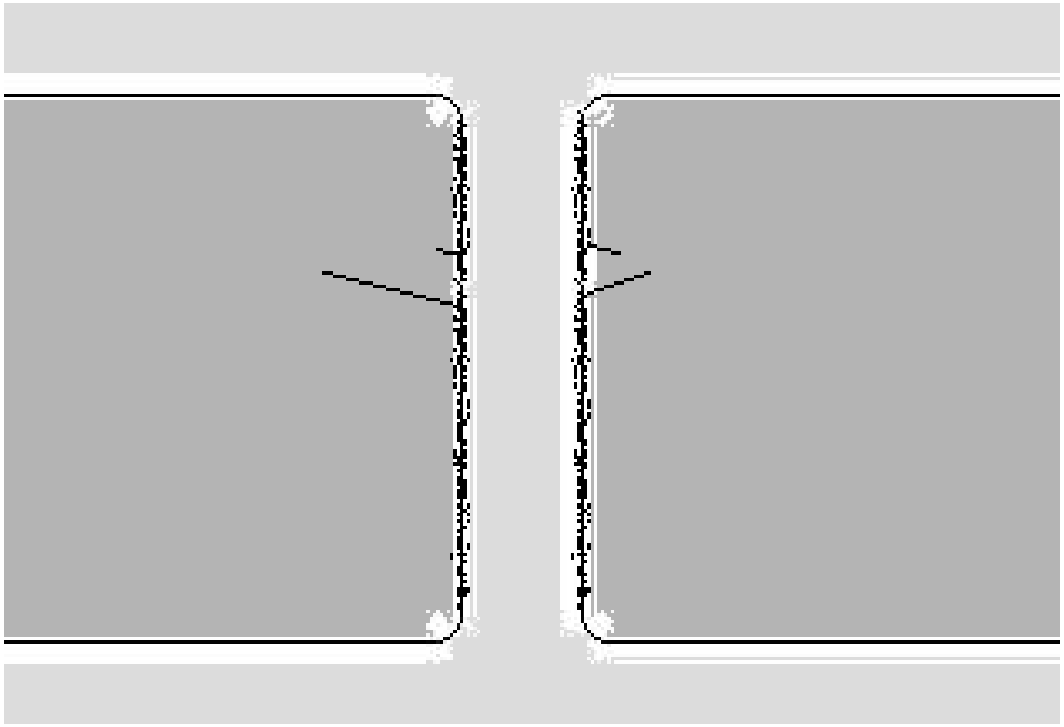
Lost While Unlocked

- 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

BitLocker™ Blog

blogs.msdn.com/si_team

Microsoft Security Development Lifecycle (SDL)

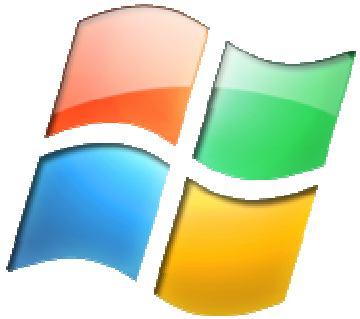
msdn.microsoft.com/security/sdl

Trusted Computing Group (TCG)

www.trustedcomputinggroup.org

Windows Hardware & Driver Central (WHDC)

www.microsoft.com/whdc



Thank you for attending.

Questions?

Microsoft
Windows Vista™

© 2006 Microsoft Corporation. All rights reserved.