4-12-2006

# BitLocker - the end of digital forensics?

Andrew Woodward
*Edith Cowan University*

# BitLocker - the end of digital forensics?

Andrew Woodward

School of Computer and Information Science

Edith Cowan University

Perth Western Australia

a.woodward@ecu.edu.au

## Abstract

*Microsoft's upcoming operating system release, Windows Vista, contains the option to encrypt all information on a hard drive. Previous versions of Windows have used the encrypting file system (EFS), allowing users to selectively encrypt files and folders on a drive. The technology is called BitLocker, and poses a problem for forensic investigators, as all information on the drive will be encrypted, and therefore unreadable. The technology has some limitations, such as only 2 versions out of the 5 available contain this technology and it also requires a trusted platform module (TPM) in order to operate. Other inherent limitations, along with possible interjection by security agencies, suggest that while this may create problems in some cases, it is unlikely that there will be widespread adoption of this technology. The likely result is that digital forensics will not end with the release of Windows Vista.*

## Keywords

Digital forensics, operating systems, whole of disk encryption

## INTRODUCTION

Other than some proprietary systems which currently exist, there are no operating systems which by default provide whole of disk encryption. By the time that this paper is published, Microsoft's latest operating system, Windows Vista, should already be available to business customers, with the consumer versions being available in January (ZDNet 2006). This new operating system will see the introduction of a new security technology known as BitLocker. The aim of BitLocker is to provide for greater data security by encrypting the entirety of a hard drive, as opposed to the current systems available which only provide limited encryption. The encrypting file system (EFS) was introduced with Windows 2000, and was also available in Windows XP professional, but not with the home and version. Used with current versions of Windows, EFS allows for selective encryption of files or folders or both, but it is not capable of encrypting entire volumes or disks (Microsoft TechNet 2003). The other limiting feature of EFS is that it needs to be selectively enabled by a user and is not switched on by default (Schneier 2006). Current digital forensics, or electronic evidence, practitioners rely on at least some part of the hard drive being readable. That is to say that other than an initial password protecting logon access, there are no other major barriers preventing a forensic investigator from reading or viewing the contents of a hard drive. Any cracking or brute force attempts are usually made against a password used to restrict access to a system, rather than attempting to decrypt an encrypted file. The introduction of bit locker in Windows Vista will see this situation change, with its whole of disk encryption effectively preventing a hard drive from being read by a forensic investigator (Muradin 2006).

There are however some mitigating factors that work in favour of the forensic practitioner. These relate both to the technology itself, and the way in which it is applied. These include cost, adoption rates, appropriate hardware and implementation. An overview of the bit locker technology itself in terms of the way it functionality, and how it can be applied will be examined. Potential mitigating factors in terms of the pervasiveness of this new technology will are then discussed.

# AN OVERVIEW OF WINDOWS VISTA AND BIT LOCKER

Microsoft's next operating system, Windows Vista, is scheduled to be released sometime within the next two months, at least to volume license users. This discussion will look at bit locker, the way it is implemented and the system requirements for its use.

## System Requirements

Windows Vista has two different desktop modes of operation, the more advanced of which requires a dedicated graphics processor card in order to function. As with most software applications and some operating systems, there is a minimum specification and a recommended specification:

Minimum specification

- A modern processor (at least 800MHz).
- 512 MB of system memory.
- A graphics processor that is DirectX 9 capable.

Recommended specification (Windows Vista premium PC)

- 1 GHz 32-bit (x86) or 64-bit (x64) processor.
- 1 GB of system memory.
- Support for DirectX 9 graphics with a WDDM driver, 128 MB of graphics memory (minimum), Pixel Shader 2.0 and 32 bits per pixel.
- 40 GB of hard drive capacity with 15 GB free space.
- DVD-ROM Drive.
- Audio output capability.
- Internet access capability.

As can be seen from the list of recommended specifications above, Windows Vista will require a fairly substantial amount of system memory; that is 1 GB. It also requires a dedicated graphics card with at least 128 MB of memory on board.

## Windows Vista versions and pricing

Microsoft has stated that there will be five versions of Windows Vista available (Microsoft 2006a). The five versions and their pricing (ZDNet 2006) are:

- Vista home versions
    - home basic ($385 AUD)
    - home premium ($455 AUD)
    - ultimate*($751 AUD)
- Vista business versions
    - business ($565 AUD)
    - enterprise*(unknown)

The only versions of Windows Vista that will have the bit locker technology enabled in them are the Vista home ultimate version and the business enterprise version.

**Security**

Other than bit locker, most of the changes implemented in Windows Vista in relation to security relate to the integration of anti spy ware and antivirus applications. The only change in security which has an impact upon electronic evidence gathering is the bit locker whole of disk encryption technology.

**Bit locker**

A Microsoft White Paper makes the following statement about the bit locker drive encryption (Microsoft 2006b):

> "BitLocker Drive Encryption is a hardware-enabled data protection feature in Windows Vista that helps protect data on a PC when the machine is in unauthorized hands. By encrypting the entire Windows volume, it prevents unauthorized users from accessing data by breaking Windows file and system protections or attempting the offline viewing of information on the secured drive."

Bit locker functionality

Microsoft's stated purposeful bit locker is that its intention is to protect user data which is present on the operating system volume. It does not protect any other information found on any other volume or drive in the computer. Bit locker's main two features are that it not only provides full drive encryption it also verifies the integrity of early boot components.

Microsoft makes the following statement about BitLocker's purpose and functionality:

> BitLocker Drive Encryption:
>
> • Protects data while the system is offline because it:
>
> > • Encrypts the entire Windows volume, including both user data and system files, the hibernation file, the page file, and temporary files.
>
> > • Provides umbrella protection for third-party applications. Third-party applications benefit automatically when installed on an encrypted volume.
>
> • Ensures boot process integrity because it:
>
> > • Provides a method to check that early boot file integrity has been maintained, and there has been no adversarial modification of those files, such as with boot sector viruses or root kits.
>
> > • Protects the system from offline software-based attacks: any alternative software which might boot the system will not have access to the root keys that protect this Windows volume.
>
> > • Locks the system when tampered with: if any monitored files are tampered with, the system will not boot. This alerts the user to the tampering, since the system will fail to boot as usual.
>
> • Eases equipment recycling by:
>
> > • Reducing the time to permanently and safely delete all data on the drive. Data on the encrypted volume can be rendered useless by simply deleting the keys that are required to access the drive.

(Microsoft 2006c)

The BitLocker Architecture

Figure 1 shows the basic architecture in terms of what components are used and required by BitLocker.
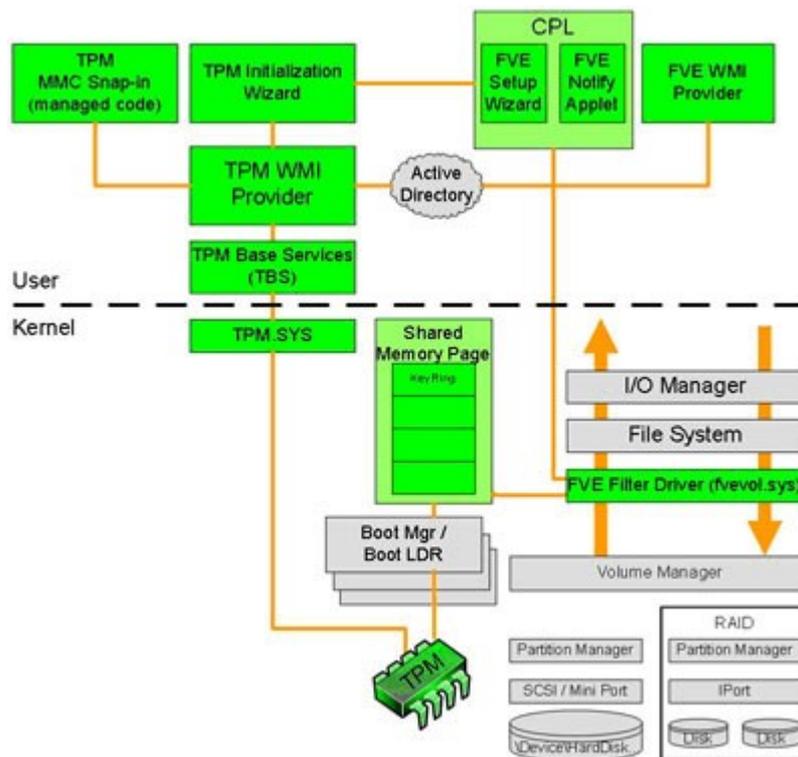
*Figure 1: the overall BitLocker architecture (Microsoft 2006c)*

Hardware, software and firmware requirements.

Bit locker will require the following specifications in order to function:

- The system must have a Trusted Platform Module (TPM) v1.21.

    - The TPM provides system boot process integrity measurement and reporting.

- The system must have v1.2 TCG-compliant (Trusted Computing Group) BIOS.

    - The BIOS establishes chain of trust for pre-OS boot.

    - The system must include support for TCG specified Static Root Trust Measurement (SRTM)

- The system BIOS must support the USB Mass Storage Device Class, including both reading and writing small files on a USB flash drive in the pre-operating system environment.

- The computer must have at least two volumes to operate:

    - The "Operating System (OS) volume" (or boot volume) is the volume that contains the Windows operating system and its support files; it must be formatted with NTFS. Data on this volume is protected by BitLocker.

    - The "system volume" is the volume that contains the hardware-specific files that are needed to load Windows computers after the BIOS has booted the platform. For BitLocker to work, the system volume must not be encrypted, must differ from the operating system volume, and must be formatted with NTFS. Your system volume should be at least 1.5 gigabytes (GB). Data, including additional user data, written to this volume is not protected by BitLocker.

(Microsoft 2006c)

### Note in relation to encryption specifics

This paper does not discuss the exact mechanisms by which BitLocker boots a protected system, or which encryption methods are used, as it is not relevant to this discussion. These aspects will be covered in future research which will examine any flaws or vulnerabilities present in BitLocker.

## MITIGATING FACTORS

On the surface it appears that the introduction of bit locker may have severe repercussions and ramifications for examining hard drives for the purposes of forensic investigation. However, there are a number of mitigating factors that are working in the favour of the electronic evidence practitioner. These are a combination of: limitations of the technology itself, the way in which it is implemented and social aspects such as user apathy. These mitigating factors are listed below and discussed in terms of their potential to reduce the impact of bit locker on the ability of digital forensics practitioners to read information from hard drives.

### Availability and cost

Of the five different versions of Windows Vista that will be available upon its release, only two of them contain the bit locker technology. Additionally, the two versions of Windows Vista that will contain this technology are also the most expensive, with the ultimate home version costing in excess of $700. Information supplied by the West Australian police force indicates that encryption usage by offenders is minimal: certainly in the order of less than 10% (Taylor 2006). It is not possible to say with certainty that paying double the cost to obtain the Ultimate version as opposed to the Basic version will prevent people from obtaining the version containing bit locker. However when added to the cost of a new computer the extra $350 to obtain bit locker may be enough to prevent some people from using it.

### TPM

Probably the most significant barrier to the use or adoption of bit locker is its requirement of a dedicated hardware chip, the trusted platform module or TPM. In particular a version 1.2 TPM is required. Microsoft has clearly stated that earlier versions of the TPM chip will not be supported by bit locker (Microsoft 2006d). In addition, a trusted computing group (TCG) BIOS must also be present on the same computer for bit locker to function correctly. It is difficult to gauge exactly how many PCs may possess this, but a survey of some mainstream web sites indicates that some laptops and desktop computers already contain this chip. What follows is a review of both OEM suppliers, i.e. those companies who produce ready built PCs for the mainstream, and the so-called beige box suppliers, those who assemble their own computers locally from components. This review was conducted in terms of examining whether a TPM was present but did not look at whether a TCG was present. The assumption being made is that if the correct version of the TPM is present then the appropriate TCG would also be found. The implication, if this assumption is incorrect, is that fewer computers are likely to be bit locker compatible and not more. So effectively, the worst-case scenario has been worked from.

OEM suppliers

Information on the Australian web site for Lenovo, formerly IBM, states that "select ThinkPad and ThinkCentre systems also include an embedded chip called the Trusted Platform Module (TPM)." (Lenovo 2006).

A review of the HP/Compaq Australian web site found that the majority of the desktop and notebook PCs designed for business use contained the TPM chip version 1.2 (HP 2006). Computers designed for home use and desktop PCs in particular, did not appear to contain a TPM chip. However, home users are not really the intended market for this particular manufacturer.

The Dell web site was more forthcoming with information. A list of the systems offering the TPM chip was found on their web site. However, the date on this particular web site was shown as being June of 2005. The list was as follows (Dell 2005):

The TPM security feature will be offered on the following platforms:

- OptiPlex™ GX280 (Desktop and Tower chassis only)

- Dell Precision™ Mobile WorkStation M20

- Dell Precision™ Mobile WorkStation M70

- Latitude™ D410

- Latitude™ D610

- Latitude™ D810

Future platforms will also support the TPM security feature.

A more thorough search of their web site revealed that a larger number of systems now ship with the TPM. Again, as with HP, the majority of systems that ship with a TPM are business oriented models and not computers intended for a home user (Dell 2006).

What is clear from the review of the major preassembled PC manufacturers, is that the TPM is aimed more at business users than it is at home users: computers destined for the home market appear not to be incorporating the TPM. It is likely then that anyone purchasing a computer for home use is unlikely to be obtaining a machine which is capable of running bit locker. In summary, it does appear that as the TPM's are destined more for business machines rather than home users, this may be a further mitigating factor in the uptake or prevalence of bit locker.

Beige box component suppliers

The latest range of motherboards from Asus, a major manufacturer of PC components used in beige boxes, state that they are all Windows Vista Premium ready (Asus 2006a). However, a review of the specifications for these motherboards fails to reveal the presence of a TPM (Asus 2006a). A search of the website failed to produce any information relating to the use of TPMs by Asus on their motherboards. This was also the case for another major manufacturer in the motherboard market, Gigabyte, with a press release indicating that some of their motherboards are Windows Vista Premium ready (Gigabyte 2006a), but with no evidence of a TPM in the specifications (Gigabyte 2006b). Abit also had no mention of a TPM module being used on their motherboards (Abit 2006).

These manufacturers also produce their own range of notebooks, and a review of the specifications for these devices was also undertaken to determine whether their notebooks contained a TPM. A review of the notebooks on the Asus web site revealed that of their notebooks aimed at the home user market, only two out of eight notebooks contained a TPM (Asus 2006b). The notebooks intended for the business market did have increased availability of the TPM. However, of the nine notebooks examined, five did not contain at TPM at all three of them had a TPM, with one other listing it as optional (Asus 2006c). Whilst some of these notebooks indicated that they contain a TPM, only one notebook stated that it was a version 1.2 TPM, which is required for bit locker to function. Where at TPM was listed in the specification, no version was specified. It is possible that these are not version 1.2 TPM's, but without direct contact with the manufacturer this is difficult to confirm.

Intel, who also manufactures their own motherboards as well as CPUs, did have a range of motherboards which included a TPM. Some of the "executive" range of motherboards from Intel contains a TPM V1.2 chip, which is required by BitLocker (Intel 2006a). As with the OEM boxes form the major manufacturers, these boards are designed for and aimed at the business rather than the home market. Specifically, those boards which use the Intel 965 chipset also had a TPM, while those with 945 chips did not (Intel 2006a). However, motherboards in other ranges aimed at the home and gaming user did not contain a TPM, regardless of which chipset they contained (Intel 2006b). Of all of the current Intel desktop motherboards available, only 6 out of 31 contained a BitLocker compatible TPM (Intel 2006c).

In summary, it appears that whilst TPM's are available from both OEM suppliers and component suppliers, prevalence of devices with these chips is not high. The exact number would be difficult but an approximation would place a percentage at somewhere around 30-40%. What is clear is that business, and not home models,

are the target for TPM inclusion. Also, whilst the proportion of OEM computers containing TPM's is higher than that of beige boxes, information supplied by the Western Australian police force indicates that only 30% of the computers they examine fall into this category: most of the computers they examine are of the component type (Taylor 2006).

**Off by default and backdoors**

Initially, the BitLocker technology was set to be enabled by default (Schneier 2006). It seems that whilst encrypting technologies are available they are simply not being used by offenders. Information supplied by the Western Australian police force indicates that use of encryption by offenders is less than 10% (Taylor 2006). As to whether this is user apathy, or whether it has some impact upon the availability and speed with which users can access images and videos, is unclear. The point of interest is that although these encryption technologies are available they are not being used. It is difficult to state with any certainty that this will translate into users not turning on or using BitLocker. However, as is a process which does require some user intervention and input, it is possible that not all users will enable this feature even if they have a system and the correct version of the operating system capable of running it.

There have already been concerns were voiced in other countries in relation to the ability of security agencies to be able to view information on hard drives, and how this will be impacted upon by the use of bit locker. Concerns about the BitLocker effect on the ability to read information on terrorism suspect's computers was raised at the UK's Commons home affairs committee (Muradin 2006). The government was advised that it would be a good idea to look at implementing a back door so that information could still be read from a suspect's computer even if they are using BitLocker encryption. It is also possible to speculate that US security agencies already have some means of circumventing the technology, or will pressure Microsoft into allowing them to do so.

**Adoption rate**

The computer crime squad of the Western Australian police force have indicated that it was approximately 2 years after the release of Windows XP before they started to see Windows XP as a majority operating system for PCs that they examined (Taylor 2006). When Windows XP was released, it represented a fairly significant increase in performance functionality and a security over the Windows 9x operating systems that it replaced. There were quite significant incentives and justification to upgrade from either Windows 98 or Windows ME, to Windows XP. In this case, there appear to be more barriers than incentives to upgrade from the Windows XP to Windows Vista. Due to Windows XP having been thoroughly tested by millions of users since its release, most of the flaws and bugs have now been found and patched: at this point it is a reasonably stable operating system. In terms of security, the changes introduced by Microsoft through service Pack 2, such as an integrated firewall and the facility to actively monitor an antivirus application, made Windows XP a reasonably secure operating system. Both of these were fairly major reasons to upgrade from Windows 9x to Windows XP. This disincentive to upgrade is given further impetus by the fairly significant cost factor that needs to be considered in terms of purchasing the new Windows Vista operating system. Also, it is quite likely that most users will not possess the hardware required in order to run this day itself, regardless of whether bit locker is to be used. The operating system requires a minimum of 1 GB of memory, something which most users are unlikely to have.

**Bit locker only encrypts the operating system (OS) volume**

Another aspect which needs to be considered is bit locker only encrypts the operating system volume and any information contained on it. It does not encrypt the system volume or any other volumes, and in fact it is a requirement that the system volume and the files thereon are not encrypted. In relation to encrypting other volumes, a Microsoft FAQ states that this is not possible:

> Q. Will we be able to encrypt more than just the OS volume at Windows Vista RTM?
>
> A. When released BitLocker will provide encryption for the entire operating system volume, including Windows system files and the hibernation file, which helps

protect data from being revealed from a lost or stolen PC asset. A user can optionally use the Encrypting File System (EFS) feature within Windows Vista to protect other volumes. The root secrets of EFS are stored by default on the O/S volume, so therefore if BitLocker is enabled for the OS volume all data protected by EFS will be additionally protected by BitLocker.

(Microsoft 2006d)

This provides another avenue for finding information that is not encrypted, as it is common practice among users to partition large drives. With 250 GB hard drives costing approximately $100, and with people adding additional hard drives into systems as their existing space fills, it is likely that there will be at least some information that does not get placed on the encrypted volume. Not only does this provide the potential for finding information that which is not protected by bit locker, it also provides the potential for a back door into the system with the files used to boot the operating system needing to be placed on the unencrypted system volume.

## CONCLUSION

At face value it would appear that Microsoft Windows Vista, in particular the bit locker technology, presents a significant challenge for digital forensics investigators. However, analysis of the particulars of bit locker and other mitigating factors in relation to Windows Vista availability and pricing indicated that the problem may not be as significant as first thought. Firstly, is that only the most expensive versions of Windows Vista will even contain the technology. Secondly, is that specific hardware is required to run Vista, both the operating system itself and the TPM which is required for bit locker. These combined with the other factors as discussed in this paper such as price, suggest that even if bit locker is adopted by those who wish to encrypt or hired their files from others, it is likely to be some time until we see bit locker in wide use, if at all. There may be other factors which also restrict its update. At the time of writing, it is still unclear as to whether United States security agencies, such as the NSA, are likely to place any restrictions on or watering down of the bit locker technology. There is also the question of what sort of impact the technology has on the speed of the system. Microsoft claims that it is minimal, but this is yet to be tested.

If implemented correctly, and if it performs as Microsoft claims, then this technology will present a significant problem for security agencies. As has occurred with previous Microsoft operating systems, it is possible that a back door or other work around may be forced upon the operating system before its release. Further research in this area may look at ways in which the technology can be defeated, or any flaws that may be present in the system.

## REFERENCES:

Asus (2006a). ASUS Launches World's First 64-bit and 32-bit Vista Premium Certified Motherboard URL http://www.asus.com/news_show.aspx?id=4565 accessed 28 October 2006

Asus (2006b). Asus notebooks - digital home, URL http://www.asus.com/products2.aspx?l1=5&l2=22 accessed 31 October 2006

Asus (2006c). Asus notebooks - business, URL http://www.asus.com/products2.aspx?l1=5&l2=24 accessed 31 October 2006

Dell (2005) What is the Trusted Platform Module (TPM) security feature? URL http://support.ap.dell.com/support/topics/global.aspx/support/dsn/en/document?docid=E75E35123E8AC4D0E030030ABD623A10&c=au&l=en&s=dhs#2 accessed 27 October 2006

Dell (2006)

Gigabyte (2006a) GIGABYTE GA-945P-DS3 Certified for Windows® Vista™ Premium WHQL Logo - Wide Range of GIGABYTE Vista Premium Motherboards to Follow URL

http://www.gigabyte.com.tw/News/Motherboard/News_List.aspx?NewsID=1301 accessed 28 October 2006

Gigabyte (2006b) Motherboard overview GA-965G-DS3
URL http://www.gigabyte.com.tw/Products/Motherboard/Products_Overview.aspx?ProductID=2361 Accessed 28 October 2006

Intel (2006a). Intel executive desktop boards - designed for business. URL
http://www.intel.com/products/desktop/motherboard/executive.htm accessed 28 October 2006

Intel (2006b). Intel classic desktop boards.
http://www.intel.com/products/desktop/motherboard/classic.htm

Intel (2006c). Desktop Boards Comparison Chart URL
http://indigo.intel.com/compare_cpu/showchart.aspx?mmID=24744,22631,22185,22642,22641,22639,22638,22637,22186,24743,22634,22633,22640,24779,24672,7675,141,23891,23504,23503,111,110,22627,112,7672,24972,113,22623,7670,7669,22622&familyID=12&culture=en-US

Lenovo (2006) Thinkvantage client security solution, URL http://www-8.ibm.com/lenovoinfo/au/innovation/css.html?cntry=au accessed 27 October 2006

Muradin, A. (2006) Windows Vista might have backdoor capabilities, URL
http://news.softpedia.com/news/Vista-Might-Have-Back-Door-Capabilities-18188.shtml accessed 1 November 2006

Microsoft (2006 a) Microsoft unveils Windows Vista product line-up, URL
http://www.microsoft.com/presspass/press/2006/feb06/02-26WinVistaProductsPR.mspx accessed 26 October 2006

Microsoft (2006 b) Windows Vista Security advancements, URL
http://download.microsoft.com/download/c/2/9/c2935f83-1a10-4e4a-a137-c1db829637f5/WindowsVistaSecurityWP.doc , accessed 26th October 2006

Microsoft (2006c). BitLocker Drive Encryption: Technical Overview, URL
http://www.microsoft.com/technet/windowsvista/security/bittech.mspx , accessed 21 October 2006

Microsoft (2006d).  Bit locker Drive encryption frequently asked questions, URL
http://www.microsoft.com/technet/windowsvista/security/bitfaq.mspx accessed 31 October 2006

Microsoft TechNet (2003).  Encrypting file system in Windows XP and Windows Server 2003, URL
http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx accessed 26 October 2006

Schneier, B (2006) Microsoft's BitLocker, URL http://www.schneier.com/blog/archives/2006/05/bitlocker.html accessed 1 November 2006

Taylor, D. (2006) Personal communication, October 27th 2006

ZDNet (2006) Microsoft details Aussie Vista pricing, URL
http://www.zdnet.com.au/news/software/soa/Microsoft_details_Aussie_Vista_pricing/0,130061733,339271542,00.htm accessed 26 October 2006

## COPYRIGHT