Windows Vista BitLocker 분석†

황성호*, 남현우*, 박능수*, 홍도원**
*건국대학교 컴퓨터공학과 **한국 전자 통신 연구원
e-mail : seongho.hwang@hotmail.com

Analysis of Windows Vista BitLocker

Seongho Hwang*, Hyunwoo Nam*, Neungsoo Park*,Dowon Hong**
*Dept. of Computer Science & Engineering, Konkuk University
**Electronics and Telecommunications Research Institute

요 약

BitLocker는 2006년에 Microsoft가 새롭게 출시한 운영체제인 Windows Vista에서 처음 사용되는 보안 메커니즘이다. 기존의 다양한 운영체제에서 사용되는 보안 메커니즘은 기본적으로 사용자가 로그인한 후 로그인한 사용자의 데이터를 바탕으로 파일에 대한 암호화, 데이터에 접근에 관한 권한 확인과 같은 방법을 사용하여 데이터를 보호했다. 하지만 이러한 보안 메커니즘은 물리적으로 접근하는 공격방법에는 취약하고, 플랫폼 자체에 대한 신뢰성이 부족하기 때문에 새롭게 Microsoft에서 새롭게 제안하는 보안 메커니즘인 BitLocker는 디스크 자체를 암호화 해서 보호하는 새로운 메커니즘이다. 본 논문에서는 Windows Vista에서 사용되는 새로운 보안 메커니즘인 BitLocker의 운영 메커니즘에 대해서 분석하고 이를 바탕으로 Windows 보안 메커니즘에 대한 취약점을 검증하기 위한 기존 자료로 활용하였다.

1. 서론

Windows 운영체제는 전 세계에서 개인용 컴퓨터 사용자가 가장 많이 사용하는 운영체제이다. 하지만 많은 해커들에 의해서 운영체제의 보안을 위한 메커니즘이 분석 되었고 인터넷에서 배포되는 바이러스나 웜의 경우 윈도우 운영체제를 목표로 하고 있는 비율이 압도적으로 많다.[1]

가정에서 사용하는 개인용 컴퓨터를 제외하고 점점 사용자가 증가 추세인 휴대용 컴퓨터인 PDA(Portable Digital Assistance)나 노트북의 사용인 경우에도 2005년 FBI 보고서에 따르면 매년 휴대용 컴퓨터의 도난 횟수의 증가와 함께 휴대용 컴퓨터 도난에 따른 개인이 부담해야 하는 비용 또한 증가했다.[2] 개인용 휴대 컴퓨터 사용에 따른 위험과 비용의 증가에 대응하기에는 현재의 운영체제에 많은 문제점이 있다.

Microsoft에서는 Windows 2000 운영체제부터 NTFS 파일 시스템을 운영체제의 주 파일 시스템으로 사용하고, NTFS 파일 시스템을 기반으로 저장되어 있는 데이터를 보호하기 위해서 EFS(Encrypting file System)을 사용한다. 하지만 EFS 파일 시스템은 운영체제가 부팅 된 후 파일 각각을 사용자의 정보를 기반으로 암호화 하기 때문에 디스크 자체에 대한 접근을 막을 수 없고 다양한 해킹 방법에 의해서 암호화 된 파일들을 읽는 것이 가능하다.

기존의 Windows 운영체제에서 사용하는 보안 메커니즘에 많은 약점이 노출되었고 이를 보안하기 위해서 Microsoft에서는 64-bit 운영체제인 Windows Vista를 출시하면서 'BitLocker'라고 명명된 새로운 보안 메커니즘을 개발하였다.

본 논문은 2장에서는 관련 연구에 관하여 기술하고 3장에서는 BitLocker에서 사용하는 메커니즘 및 암호화 알고리즘에 대해서 분석하고 4장에서 결론을 맺었다.

2. 연구배경

2.1. Windows 보안 체계

Windows 운영체제에서 사용하는 데이터를 보호하기 위한 메커니즘은 EFS(Encrypting File System)와 RMS(Right Management System)를 사용한다. EFS의 경우 로그인한 사용자의 정보를 바탕으로 사용자가 소유하고 있는 데이터를 암호화해서 저장하는 방법으로 데이터를 보호한다. RMS의 경우 로그인한 사용자 정보를 바탕으로 Windows 운영체제에서 접근할 수 있는 E-mail이나 파워포인트 파일과 같은 정보에 대한 접근을 제한한다.

† 본 연구는 정보통신부 및 정보통신 연구진흥원의 IT 신 성장 동력 핵심 기술 개발 사업의 일환으로 수행하였음[2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발]

2.2. TPM(Trusted Platform Module)

TPM은 TCG(Trusted Computing Group)에서 만든 하드웨어 칩으로써 칩 내부에 하드웨어 형태로 다양한 해시 함수와 암호화 알고리즘이 구현되어 있다.[8] TPM 내부에 PCR(Platform Configuration Register)를 통해서 다양한 플랫폼에서 운영체제가 부팅되기 전의 과정을 검증하고 플랫폼에 대한 안전성에 대한 검증을 하는 것이 가능하다. TPM의 사용으로 물리적으로 접근하는 다양한 공격 방법에 대한 방어가 가능해 진다.

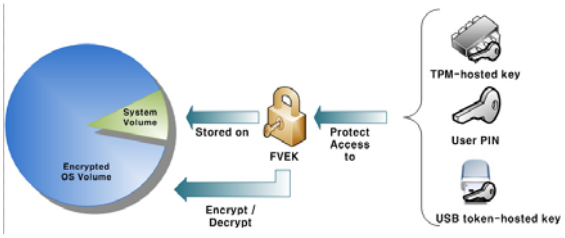
3. BitLocker

BitLocker는 Microsoft사에서 2006년에 공개한 Windows Vista에 포함되어 있는 보안 메커니즘이다. 기존의 Windows에서 사용하는 EFS나 RMS같은 보안 메커니즘은 운영체제가 완전히 부팅이 된 후 로그인한 사용자 정보를 바탕으로 보안 메커니즘을 적용하였다.

하지만 Windows 시스템의 기존 보안 메커니즘들은 디스크의 물리적인 접근을 막지는 못한다. 따라서 휴대용 컴퓨터의 경우 도난, 분실 할 경우 또 기밀 데이터가 저장되어 있는 디스크가 도난 당했을 경우에 저장되어 있는 데이터에 대한 물리적인 접근이 가능하기 때문에 디스크에 저장되어 있는 사용자 개인의 정보나 기업의 기밀 데이터가 노출될 수 있다. 이러한 보안상의 취약점을 보안하기 위해서 Windows Vista 부터 BitLocker라고 명명된 보안 메커니즘을 사용한다.

3.1. BitLocker 개념

BitLocker는 부트로더에 의해서 운영체제가 부팅되기 전에 Windows 운영체제가 저장되어 있는 디스크 자체를 보호하기 위한 메커니즘이다. BitLocker가 적용된 컴퓨터의 경우 Windows를 부팅하기 위해서는 외부로부터 입력되는 키가 필요하다. 이 키는 USB에 들어있는 startup-key, 사용자가 입력할 수 있는 4~20개의 숫자로 이루어진 PIN(Personal Identification Number)이 가능하다. 외부에서 입력되는 키는 FVEK(Full Volume Encryption Key)를 암호화·복호화 하는데 사용되고 FVEK는 OS볼륨과는 별도의 시스템 볼륨에 저장되어 있어 실제 운영체제의 데이터가 저장되어 있는 OS 볼륨을 암호화 하는데 사용된다. 이때 TPM(Trusted Platform Module)을 사용할 경우 BitLocker의 보안 매커니즘을 더욱 강력하게 할 수 있다.

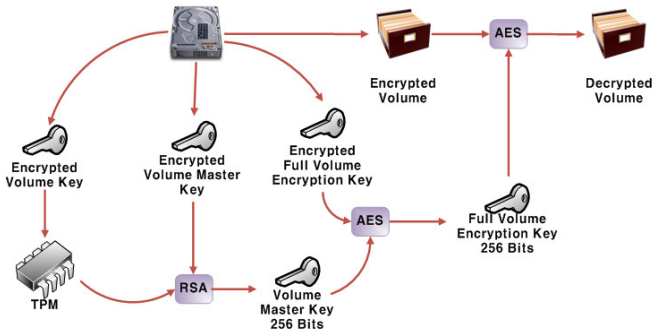


(그림 1) BitLocker 전체 개요

3.2. BitLocker 복호화 과정

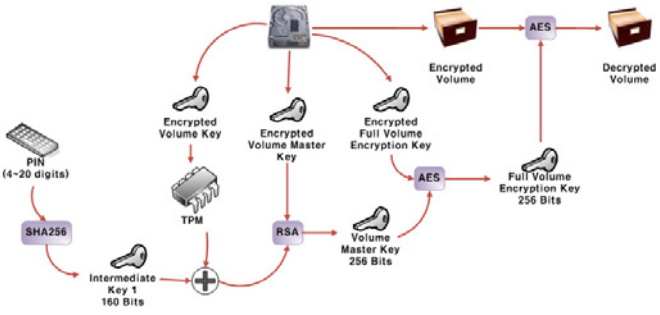
BitLocker를 암호화 되어 저장된 OS 볼륨을 복호화 하기 위해서 TPM을 사용할 경우에는 외부에서 PIN을 입력하거나 USB에 저장되어 있는 startup-key를 이용, 그리고 TPM만을 사용해서 OS 볼륨을 복호화 할 수 있다. 만약 TPM을 사용하지 않을 경우에는 starup-key를 사용하는 방법만을 사용할 수 있다.

첫 번째로TPM 만을 사용하는 경우에는 암호화 된 OS 볼륨이 처음 암호화된 컴퓨터에서 다른 컴퓨터로 옮겨진 것인지 검증하기 위해서 사용한다. 휴대용 컴퓨터나 혹은 개인용 컴퓨터의 저장장치가 다른 컴퓨터로 옮겨졌을 경우 저장되어 있는 데이터를 보호하기 위해서 사용할 수 있다.



(그림 2) TPM 만을 사용할 경우 BitLocker 적용

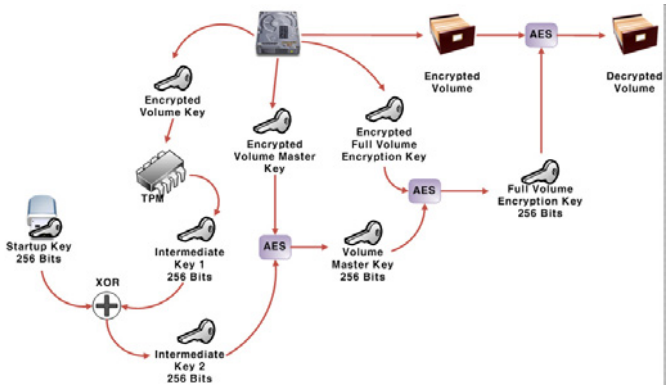
두 번째는 TPM과 PIN을 사용하는 경우이다. 이 경우에는 컴퓨터를 부팅하는 사용자가 '누구' 인가를 확인하는 경우이다. 이 경우에는 사용자가 입력한 PIN과 TPM을 바탕으로 암호화된 OS 볼륨을 복호화 하기 위한 키를 만든다. 이때 PIN은 SHA256 해시 알고리즘을 사용하고 이중 160 bit를 사용하고, TPM으로부터 나온 데이터와 추가적인 연산을 통해서 데이터를 복호화 한다.



(그림 3) TPM+PIN을 사용한 BitLocker 적용

세 번째 경우는 TPM과 startup-key를 사용하는 방법이다. 이 방법은 컴퓨터를 부팅하려 하는 사용자가 '무엇' 을 가지고 있는지 확인하는 방법이다. 이 경우 256-bit의 크기로 USB 저장 장치에 저장되어 있는 starup-key와 TPM을 통해서 나온 256-bit의 키를 XOR

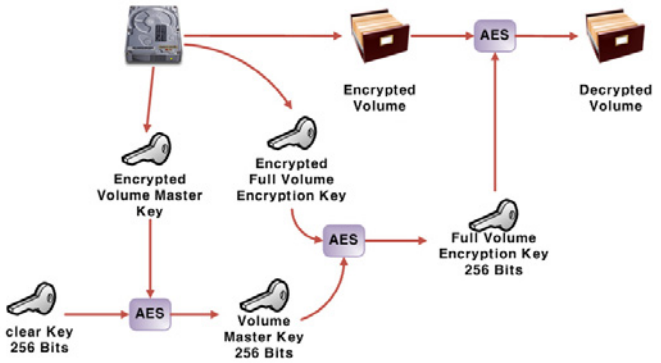
연산을 통해서 만들어진 키가 암호화된 OS 볼륨을 복호화 하기 위해서 사용된다.



(그림 4) TPM+Startup-key를 사용한 BitLocker

3.3. BitLocker를 임시로 불능화

BitLocker를 디스크 자체를 암호화 해서 저장하기 때문에 TPM이 장착되어 있는 컴퓨터에서 BitLocker를 적용 시켰을 경우 이 디스크를 다른 컴퓨터로 옮겨서 사용하기 위해서는 임시적으로 BitLocker를 불능화하는 동작이 필요하다. 이때 임시적인 불능화를 위해서 FVEK가 clear-key로 다시 암호화 되고 clear-key는 디스크에 텍스트파일 형태로 저장이 된다.



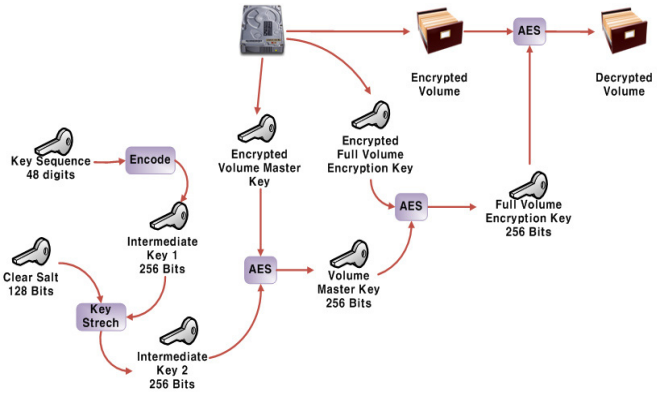
(그림 5) BitLocker의 임시적 불능화

3.4. BitLocker의 복구

BitLocker를 적용한 컴퓨터에서 BIOS의 업데이트, TPM 칩의 교체와 같은 경우와 PIN과 startup-key가 들어 있는 USB 저장 장치를 분실했을 경우에 BitLocker로 암호화 되어 있는 저장장치를 복구하기 위해서는 복구 키나 복구 암호가 필요하다. 복구 키와 복구 암호는 처음 BitLocker를 디스크에 적용시킬 경우 선택할 수 있다.

첫 번째 방법은 복구 키를 사용하는 방법으로 256-bit의 크기이고 startup-key와 마찬가지로 USB 저장장치에 저장한다.

두 번째 방법은 복구 암호를 사용하는 방법으로 복구 암호는 48개의 숫자로 이루어져 있고 입력 시 F1~F9까지의 기능키를 이용해서 입력한다.

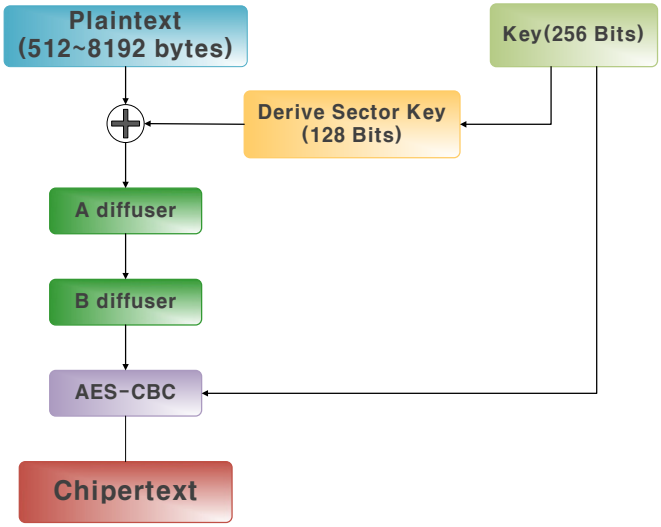


(그림 6) 복구 암호를 이용한 BitLocker의 복원

3.5. BitLocker 볼륨 암호화 알고리즘

BitLocker에서 사용하는 알고리즘은 대칭키를 사용해서 암호화 할 경우에는 AES 암호화 알고리즘을 사용하고 비대칭키를 사용할 경우에는 RSA 암호화 알고리즘을 사용한다.

하지만 OS 볼륨을 암호화 하기 위해서 사용되는 알고리즘은 BitLocker에서 처음 적용된 AES-CBC+diffuser 알고리즘을 사용한다.[4] 이 알고리즘은 기존의 AES-CBC 알고리즘에 추가로 diffuser 알고리즘을 적용해서 더욱 강력한 보안 방법을 사용하게 되고 또한 크기가 큰 OS 볼륨을 암호화·복호화 하기에도 충분한 성능으로 실행된다.



(그림 7) AES-CBC+diffuser 암호화 알고리즘

Diffuser 알고리즘의 경우 A와 B 로 나뉘어진 알고리즘을 적용한다. Diffuser 알고리즘의 경우 복호화 할 때와 암호화 할 때의 속도가 다르고 A, B 방법이 이를 서로 보완해서 복호화와 암호화에 동일한 성능을 보인다.

4. 결론

BitLocker는 Windows Vista에서 처음 사용되는 디스크 자체에 대한 암호화 방법으로 기존의 Windows 시스템에서 사용하던 RMS나 EFS와 같은 데이터를 보호 하기 위한 메커니즘을 보안하기 위해서 사용된다. BitLocker를 적용시킬 경우 사용되는 시나리오를 정리하면 다음의 표와 같다.

<표 1> Windows Vista에서 BitLocker 적용 시나리오

인증 시나리오	VMK 암호문	VMK 암호화 알고리즘
TPM만 사용	SRK(VMK)	RSA
TPM+PIN 사용	(SRK+SHA256(PIN))(VMK)	RSA
TPM+startup-key 사용	SHA256(SRK(DerivedKey), StartupKey)(VMK)	AES
복구키 사용	Recoverykey(VMK)	AES
복구 암호 사용	(Chained-hashing(Password), Salt)(VMK)	AES
Clear-key 사용	ClearKey(VMK)	AES

BitLocker의 사용으로 기존의 보안 메커니즘에서 문제가 되는 물리적으로 디스크에 대한 접근을 제한할 수는 있고 또 TPM 칩과 같이 사용해서 더욱 강력한 보안 메커니즘을 구축하는 것이 가능하다. BitLocker는 휴대용 컴퓨터 뿐만 아니라 개인용 컴퓨터 그리고 추후에 나올 Windows 2008(Longhorn)에서도 사용되므로 앞으로 나올 모든 Windows 운영체제에 사용될 것이다.

참고문헌

[1] 한국정보보호진흥원, 2006 정보시스템 해킹 바이러스 현황 및 대응 보고서, 2006

[2] Computer Security Institute, CSI/FBI Computer Crime And Security Survey, 2005

[3] Mark E. Russinovich, David A. Solomon, Windows Internals, 2006

[4] Niels Ferguson, AES-CBC+Elephant diffuser A Disk Encryption Algorithm for Windows Vista, 2006

[5] Microsoft, BitLocker Drive Encryption Technical Overview, http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx

[6] Shon Eizenhoefer, BitLocker™ Drive Encryption Hardware Enhanced Data Protection, Microsoft WinHEC 2006

[7] Microsoft, Windows BitLocker Drive Encryption Frequently Asked Questions, http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx

[8] Trusted Computing Group, TCG TPM Specification Version 1.2 Revision 103, https://www.trustedcomputinggroup.org/specs/TPM/