情 報 保 護 學 會 誌
第17卷 第2號, 2007. 4

윈도우 비스타 보안기술 분석 : 포렌식 관점을 중심으로

김영백*, 김영직*, 김우한*

요 약

마이크로소프트(MS)의 윈도우 비스타(Vista, 이하 비스타)는 윈도우 XP의 뒤를 잇는 버전으로 06년 11월말 기업용이 출시되었고 2007년 1월 31일 개인사용자용이 출시되었다. 비스타는 이전 버전인 윈도우 XP에 비하여 한층 강화된 보안기능을 탑재하고 있어 인터넷 사용시 악성코드 감염 등의 위험이 많이 줄어들 것으로 예측되고 있다. 그러나 비스타에서는 하드디스크 전체를 암호화 할 수 있는 BitLocker 기능 등이 추가되어 포렌식의 관점에서 보면 기존 XP와 달라진 점이 다수 존재한다. 본고에서는 기존 XP와 비교하여 비스타에서 변경된 부분을 포렌식 관점을 중심으로 기술하고자 한다.

Ⅰ. 서 론

비스타는 사용 용도에 따라 일반사용자용과 기업사용자용으로 구분되며 5가지 제품으로 출시된다. 일반사용자용은 HDTV 지원 기능 등 대부분의 일반사용자들이 가정에서 활용하는 기능들을 중심으로 구성되어 있으며, 기업용은 기업정보 유출을 방지하기 위한 데이터 암호화 기능, 인터넷정보서비스(IIS)등의 기능 등 기업 환경에서 활용하기 위한 기능들을 강화하여 구성된다. 또한 윈도우 비스타는 32비트 버전이외에 최근의 하드웨어 발전을 반영하여 64비트 버전도 함께 발표되었다.

국내에 출시되는 비스타는 버전별로 5가지로 출시되며 크게 가정용과 기업용으로 구분된다. 가정용인 홈 베이직 및 홈 프리미엄에는 강화된 보안 기능, HDTV 지원, 미디어센터 지원 기능 등이 있으며, 기업용인 비즈니스 및 엔터프라이즈에는 IIS, 원격 데스크톱, BitLocker 암호화 기능 등이 들어있고, 최상위 버전인 얼티메이트 에디션이 있다.

특히 기업용 버전에서부터 지원되는 BitLocker는 운영체제가 설치된 하드디스크 전체를 암호화 하는 기능으로 노트북등을 분실하였을 경우 기업의 민감한 정보를 보호할 수 있다. 그러나 포렌식 관점에서 보면 사용자 계정 정보를 알지 못하면 암호 해독을 할 수 없는 등 기존 XP와는 다른점들이 다수 존재하므로 이러한 부분들을 살펴보고자 한다

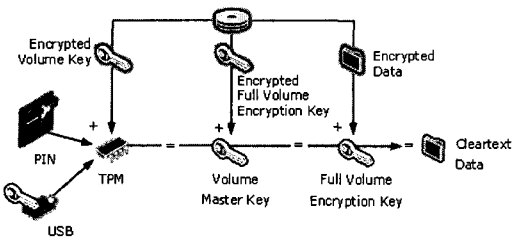
Ⅱ. BitLocker 암호화

2.1. BitLocker 드라이브 암호화 개요

BitLocker는 하드드라이브를 암호화 하는 기능으로 비스타 버전 중 Enterprise 버전과, Ultimate 버전에서 제공되는 기능이다. 이 기능은 하드웨어 암호화를 위한 TPM(신뢰할 수 있는 플랫폼 모듈) 칩 버전 1.2 이상에서 동작한다. BitLocker 기능은 윈도우 XP에서 제공하던 암호화파일 (EFS, Encrypted File System)이 파일이나 폴더 단위로 암호화하는데 비하여 디스크 자체를 암호화할 수 있도록 하였다. 이 기능을 사용하여 하드드라이브를 암호화 하면 사용자가 분실하거나 도난당한 컴퓨터에서 침입자가 데이터 절취를 위하여 무단으로 디스크에 접근할 수 없도록 할 수 있다. 또한 BitLocker가 적용된 경우 하드디스크를 PC에서 분리하여 다른 PC에 부착하여도 복구암호가 없으면 디스크의 내용이 나타나지 않는다.

Bitlocker 기능에는 HDD 볼륨 암호화 기능과 무결성 검사 기능이 있으며, 암호화 기능은 Windows OS가

* 한국정보보호진흥원 인터넷침해사고대응지원센터 (ybkim@kisa.or.kr, yjkim@kisa.or.kr, whkim@kisa.or.kr)



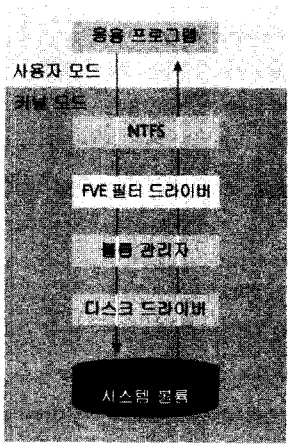
〔그림 1〕 BitLocker 암호화[6]

설치된 OS 파티션을 암호화 하는 기능으로 H/W에 내장된 TPM칩 등을 이용해 파티션의 모든 사용자 파일과 시스템 파일 내용을 암호화 시킨다. 무결성 검사 기능은 초기 부팅 시 암호화된 드라이브가 본래의 시스템에 있는 것을 확인한 후 볼륨의 훼손여부 확인을 통해 데이터 암호 해독을 진행하는 기능으로, 변경으로 인해 접근이 제한될 경우 복구암호를 통해 해제를 진행할 수 있다. 암호화 기능은 TPM 칩이 없어도 동작이 가능하나 무결성 검사 기능은 TPM 칩이 없으면 동작하지 않는다.

BitLocker는 〔그림 2〕와 같이 FVE(전체 볼륨 암호화) 드라이버를 사용하여 볼륨 수준에서 디스크를 암호화 한다. FVE는 NTFS가 볼륨으로 전송하는 모든 I/O 요청을 자동으로 확인하고, 처음에 BitLocker를 사용하도록 볼륨을 구성한 경우 해당 볼륨에 할당된 FVEK(전체 볼륨 암호화 키)를 사용하여 블록을 기록할 때 암호화하고 블록을 읽을 때 암호를 해독한다. 기본적으로 볼륨은 256비트 AES 키를 통해 암호화하며, 암호화 및 암호 해독은 I/O 시스템의 NTFS 아래에서 수행되기 때문에 볼륨은 암호화되지 않은 것처럼 NTFS에 표시된다. 그러나 Windows 외부에서 볼륨에 있는 데이터를 읽으려고 시도하면 해당 데이터는 보이지 않는다.[5]

BitLocker 암호화시에는 다음과 같은 4가지 방법이 존재한다. ①TPM(ver 1.2) only, ②TPM and PIN(개인 ID 번호), ③TPM and USB startup key, ④USB start-up key only(TPM 없는 경우).[6] 일반적으로는 ①번 방식을 지원하고 그룹정책을 적용하는 기업환경 등에서는 ②, ③번도 가능하며, TPM 칩이 없는 경우에는 ④번을 사용할 수 있다. 그러나 ①번을 제외하고는 사용자 입력(PIN 입력, USB 설치)이 필요하다.

BitLocker는 기본적으로 윈도우가 설치된 파티션에 대해서만 설정이 가능하며 BitLocker로 암호화 시에 제공되는 복구암호는 USB 장치나 폴더에 보관할 수도 있

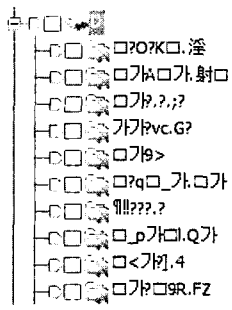


〔그림 2〕 BitLocker 동작원리[4]

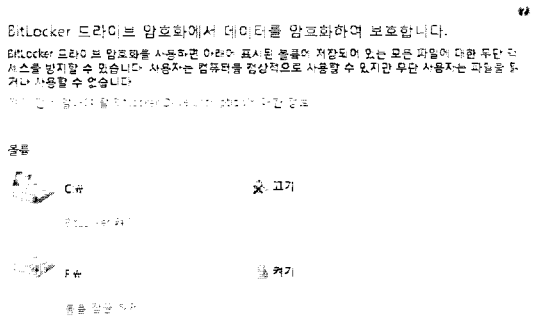
고 Text 형태로 인쇄하여 보관할 수도 있다. 이렇게 암호화된 하드디스크는 다른 컴퓨터에서도 복구암호만 있으면 인식시킬 수 있으나, 자신의 복구암호를 분실하는 경우에는 복구할 수 있는 방법이 없으므로 세 가지 장소에 모두 복구암호를 저장하는 것이 보다 안전하다.

2.2. BitLocker 암호화된 디스크의 포렌식

기존 윈도우 XP/2003 에서 EFS 암호화가 된 경우에는 분석도구에서 계정 패스워드를 이용하여 암호 해독이 가능하였다. 그러나 현재까지 출시된 포렌식 분석도구로는 BitLocker 암호화된 디스크를 암호 해독하여 내용을 볼 수 없다. BitLocker는 오직 윈도우 비스타 OS가 설치된 PC 에서만 암호 해독이 가능한데, 그것도 BitLocker 기능이 없는 Home Basic, Home Premium, Business 버전에서는 불가능하고, BitLocker 기능이 탑재된 Enterprise, Ultimate 버전에서만 복구암호를 통하



〔그림 3〕 BitLocker 암호화된 디스크



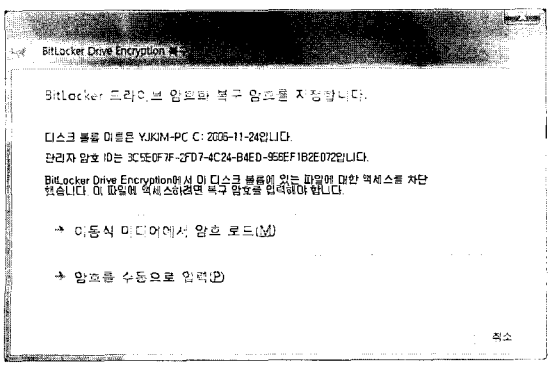
〔그림 4〕 BitLocker 암호화된 디스크 연결

여 암호 해독이 가능하다.

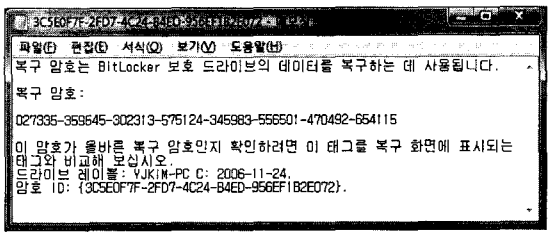
따라서 BitLocker 암호화된 디스크를 분석하기 위해서는 BitLocker 기능이 있는 또 다른 윈도우 비스타 PC에 분석할 하드디스크를 연결하여 복구암호를 통한 "볼륨 잠금 해제" 후 분석하여야 한다. 물론 암호 해독을 하지 않고 Physical 디스크 형태로 분석을 시도 할 수 있지만 〔그림 3〕과 같이 디스크 내용을 확인할 수 없다.

암호화된 디스크의 암호 해독을 위해 BitLocker 암호화된 디스크를 연결하고 제어판의 "BitLocker 드라이브 암호화" 메뉴를 클릭하면 〔그림 4〕와 같은 화면이 나타난다. 〔그림 4〕의 경우 F 디스크가 BitLocker 암호화된 것을 확인 할 수 있으며 "볼륨 잠금 해제"를 클릭하여 〔그림 5〕와 같이 암호화된 볼륨을 암호 해독할 수 있다.

이 때 암호화시에 생성된 복구 암호를 입력하면 디스크가 암호 해독 되는데, 이동식 미디어 나 특정 폴더에 저장한 경우라면 해당 위치에서 직접 로드하면 되고, 그렇지 않은 경우에는 〔그림 6〕과 같은 텍스트 형태의 복구암호를 수동으로 입력하여야 한다. 복구암호는 8개의 그룹으로 구성된 6자리 숫자, 즉 48개 숫자로 구성되어 있으며 BitLocker가 이를 128비트 키로 변환하여 복구



〔그림 5〕 복구 암호 지정



〔그림 6〕 텍스트 형태의 복구 암호

작업을 진행한다. 이러한 복구암호는 PC 업그레이드시 새로운 메인보드에 디스크를 설치하는 경우나, TPM 이나 BIOS에 장애가 발생하였을 경우에도 디스크에 암호화되어 저장된 데이터를 안전하게 복구할 수 있도록 한다.

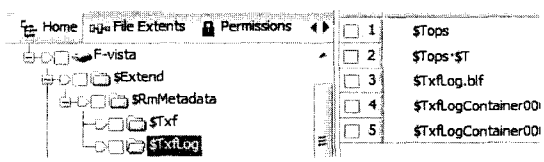
이러한 암호 해독 과정이 끝나면 일반적인 디스크와 같이 연결이 가능하며 디스크 내용도 볼 수 있다. 그러나 이 경우에도 포렌식 툴에서 로드시 Logical 드라이브 형태로 로드하여야 하며 Physical 드라이브 형태로 로드하면 암호화된 형태의 데이터만 보이게 된다.

Ⅲ. 포렌식 관점에서의 윈도우 비스타[1]

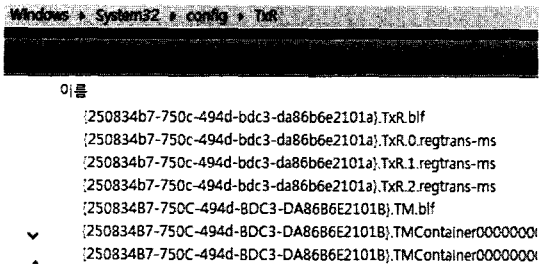
3.1. 비스타에서의 파일 시스템

비스타에서는 Transactional NTFS(TxF)가 적용되어 있다. 이는 기존 NTFS에 transaction logging 기능이 추가된 형태로 파일시스템 변경사항 등이 하나의 "transaction"으로 logging 된다. 이 후에 NTFS는 이러한 파일시스템 변경이 성공적으로 완료되었는지 여부를 확인 후 실제 변경을 완료(commit)함으로써 무결성을 향상시켰다. 응용프로그램은 실제 변경을 완료(commit)하는 단계 이전이라면 언제라도 "transaction"을 rollback 하여 변경을 취소할 수 있다. TxF는 〔그림 7〕과 같이 해당 볼륨의 "\$Extend\RmMetadata"라고 하는 숨겨진 디렉터리에 저장된다.

레지스트리도 마찬가지로 TxR 이라고 하는 확장기



〔그림 7〕 TxF 저장 공간($Extend)



〔그림 8〕 TxR 저장공간

능을 통해 로깅되며, TxR 로깅은 〔그림 8〕과 같이 "%Systemroot%\System32\Config\Txr"에 저장된다.

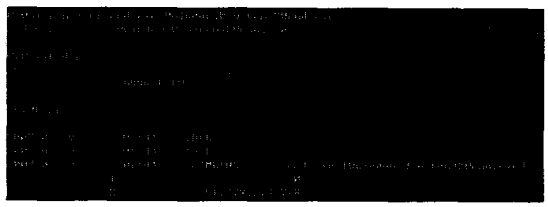
3.2. Symbolic Links

XP에서의 "C:\Documents and Settings" 디렉터리가 비스타에서는 "C:\Users" 디렉터리로 변경되었다. 그러나 기존 응용 프로그램과의 호환성 확보 등을 위하여 비스타에서는 Symbolic Links를 통하여 "C:\Documents and Settings" 디렉터리를 "C:\Users" 디렉터리로 re-direct 하고 있다. 마찬가지로 "\Application Data"를 "\AppData\Roaming"으로, "\My Documents"를 "\Documents"로 redirect 하고 있다.

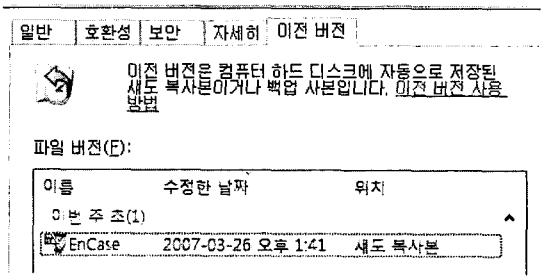
이러한 Symbolic Links는 기존 NTFS의 "디렉터리 교차점"과는 달리 폴더뿐만 아니라 파일에 대해서도 Link가 가능하며, 〔그림 9〕와 같이 mklink 라는 명령어로 새로운 Link를 만들수도 있다.

3.3. 섀도 복사본 및 이전 버전

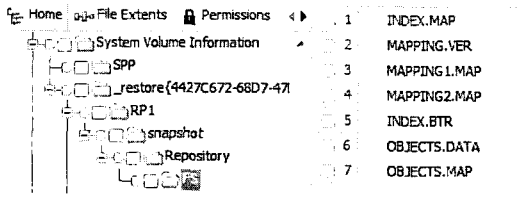
섀도 복사본은 기존 "시스템 복원" 기능에 〔그림 10〕과 같이 각각의 파일별 백업 개념이 추가된 형태이다. 윈도우는 디스크 볼륨을 대상으로 수행되는 작업을 모니터링 하면서 해당 작업이 변경하는 내용을 허용하기 전에 섹터의 백업 복사본을 만들고, 원래 데이터는 〔그림 11〕과 같이 해당 볼륨의 "System Volume Information" 디렉터리에 저장한다. 이러한 백업 과정은 일반적으로 매일 한번씩 발생한다.



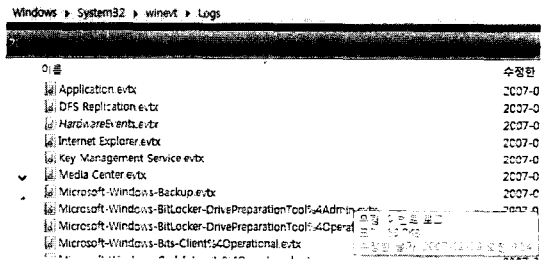
〔그림 9〕 Symbolic Link 생성[4]



〔그림 10〕 섀도 복사본의 예



〔그림 11〕 섀도 복사본 저장 디렉터리



〔그림 12〕 각종 이벤트 로그

섀도 복사본을 이용하여 시스템 전체의 복원뿐만 아니라 특정 파일별로 이전 버전의 파일을 복구할 수 있다.

3.4. Event Logs

비스타에서 이벤트 로그는 기존의 .evt 파일 대신 .evtx 파일형태로 저장되며, 파일의 저장위치도 기존의 "\Windows\System32\config" 디렉터리가 아닌 "\Windows\System32\winevt\Logs" 디렉터리에 저장된다. 또한 기존의 이벤트 로그뿐만 아니라 다양한 로그들이 새로 저장된다.

Ⅳ. 결 론

윈도우비스타는 이전의 윈도우 운영체제에 비하여 강화된 보안기능을 가지고 있으며, 설계단계부터 보안성을 고려하여 개발되었다. 이렇게 강화된 보안기능은 사용자들이 웜/바이러스, 트로이전 등의 악성코드 위협으로부터 보호될 수 있는 장치로 사용될 수 있으므로 이런 기능들을 적절히 활용하면 사용자 PC가 해킹에 악용되는 것을 방지할 수 있을 것으로 기대된다.

또한 비스타에서는 기업의 민감한 정보가 유출되는 것을 막기 위하여 BitLocker 라는 디스크 전체 암호화 기능을 제공한다. 이러한 기능은 노트북 분실과 같은 사고 발생시 정보유출을 방지하는 효과가 있으나, 포렌식 관점에서 보면 복구암호와 같은 정보 없이는 분석을 진행할 수 없어 사고 조사를 어렵게 하는 양날의 칼이 될 수 있다.

국외에서도 윈도우 비스타 포렌식에 대한 논의가 이루어지고 있으나 아직까지 BitLocker 암호화된 디스크를 암호 해독할 수 있는 분석툴은 없으며, 심지어 사용자 계정을 알고 있더라도 분석툴만으로는 암호 해독을 할 수 없어 BitLocker를 지원하는 비스타 OS가 설치된 PC에서만 암호 해독 및 분석이 가능하다. 향후에는 복구 암호를 알고 있는 경우에는 비스타 운영체제 없이 암호 해독 가능한 모듈이 업체에서 출시할 것으로 예상되지만, 복구 암호를 알지 못하는 경우에는 여전히 분석이 어려울 것으로 전망되므로 분석시 복구암호가 저장된 USB 등을 반드시 확보하여야 할 것으로 판단된다.

참고문헌

[1] Troy Larson, "Windows Vista Forensics", *Botnet Task Force* 5, Jan 2007

[2] "BitLocker 드라이브 암호화", http://www. microsoft.com/korea/technet/itsolutions/msit/security/ bde_note.mspx

[3] "윈도우즈 비스타(Vista)의 주요 보안이슈", *2007년 01월 해킹 바이러스 통계 및 분석 월보*, pp. 20-40, Jan 2007

[4] "Windows Vista 커널 속으로", http://www.microsoft.com/technet/technetmag/default.aspx?loc=ko

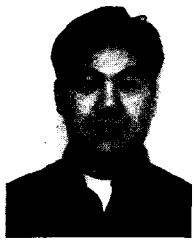
[5] "Windows BitLocker Drive Encryption Frequently Asked Questions", http://technet2.microsoft.com/ WindowsVista/f/?en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx

[6] "BitLocker Drive Encryption Technical Overview", http://technet2.microsoft.com/WindowsVista/f/?en/library/ce4d5a2e-59a5-4742-89cc-ef9f5908b4731033.mspx

[7] "Windows BitLocker Drive Encryption Step-by-Step Guide", http://technet2.microsoft.com/WindowsVista/f/?en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx

〈著者紹介〉

김영백 (Young Baek Kim)
정회원
1995년 2월 : 순천향대학교 정보통신공학과 졸업
1997년 2월 : 순천향대학교 정보통신공학과 석사
1996년 12월~2000년 3월 : 한전 KDN 주임
2002년 9월~현재 : 순천향대학교 정보보호학과 박사과정(수료)
2000년 4월~현재 : KISA 인터넷침해사고대응지원센터 해킹대응팀 선임연구원
관심분야 : 인터넷침해사고대응, 정보보호



김영직 (Young Jik Kim)
정회원
1995년 2월 : 동국대학교 전자계산원 졸업
2003년 2월 : 광운대학교 정보과학교육원 컴퓨터과학과 졸업
2007년 2월~현재 : 전남대학교 정보보호협동과정 석사과정
1998년 6월~2000년 6월 : 두루넷 고객지원실
2000년 7월~현재 : KISA 인터넷침해사고대응지원센터 해킹대응팀 연구원
관심분야 : 인터넷침해사고대응, 정보보호, 포렌식

김우한 (Woo Han Kim)
정회원
1979 넌 2월 : 성균관대학교 전자공학과 졸업
1982년 3월~1982년 12월: 금성사중앙연구소
1983.1월~2003년 8월:: (주) 데이콤, (주) 한솔아이글로브
2003년 8월~현재 : KISA 인터넷침해사고대응지원센터 본부장
관심분야 : 전자공학, 통신공학, 정보보호