情 報 保 護 學 會 誌
第17卷 第2號, 2007. 4

윈도우 비스타의 향상된 보안 기능

조 원 영*

요 약

2007년 1월 국내 정식 출시된 윈도우 비스타, 그 안에는 수많은 최신 기술과 새로운 기능이 들어있지만 이번에는 특히 보안과 정보 보호라는 면에서 달라진 기능을 살펴보기로 한다

Ⅰ. 윈도우비스타의 4대 보안 사상

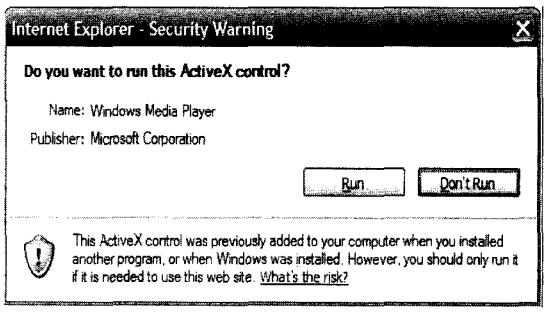
Windows Vista의 보안 사상	
기술적 우수성 (Engineering Excellence)	설계, 구축 그리고 테스트까지 보안을 최우선 Security Development Lifecycle (SDL)을 바탕으로 한 개발
근원적 방어 (Foundational Protection)	위협으로부터의 보호 및 비즈니스의 가용성 보장 Secure Startup 및 FVE(Full Volume Encryption) 윈도우 서비스 하드닝 양방향 방화벽 관리자 권한 제한
안전한 접근 (Secure Access)	PKI 및 각종 인증서비스를 통한 쉽고 안전한 접근
통합한 제어 (Integrated Control)	효율적 중앙관리 관리도구 제공

Ⅱ. 윈도우 비스타의 모든 사용자를 위한 진보된 보안기능

윈도우 방화벽, 윈도우 업데이트, 사용자 계정 컨트롤, 인터넷 익스플로러 7 보호 모드(IE7 Protected Mode), 윈도우 디펜더(Windows Defender)와 같은 기능뿐만 아니라, 악성 소프트웨어 제거 도구(Malicious Software Removal Tool), Windows Live OneCare Safety Scanner, 피싱필터 등 그 밖의 마이크로소프트의 서비스 또는 보안 관련 회사에서 제공하는 바이러스 백신 프로그램과 함께 윈도우 비스타를 사용하면 각종 악성 소프트웨어를 더욱 철저히 차단할 수 있으며, 잠재된 위험으로부터의 공격과, 전자거래 사기 피해 방지, 개인정보보호를 위한 매우 강력한 PC 환경을 사용 할 수 있다. 지금부터 모든 사용자가 강화된 보안의 혜택을 누릴 수 있는 각종 기능들을 알아 보기로 한다.

2.1. 악성프로그램으로부터의 보호 (Malware protection)

악성 소프트웨어는 웹 사이트를 볼 때 갑자기 나타나는 팝업 광고처럼 그저 짜증날 뿐인 정도가 아니라 심각한 문제를 일으켜 PC 성능이 저하되거나 개인 정보와 관련된 ID 도용을 초래하는 등 다양한 영향을 미칠 수 있다. 여러 단계를 통해 체계적인 보안을 유지하고자 노력하는 마이크로소프트의 정책에 따라 윈도우 비스타에는 컴퓨터에 악성 소프트웨어가 설치되지 않도록 도와주고, 감염된 컴퓨터에서도 악성 코드로 인한 피해를 줄여 주고, 이미 설치된 악성 코드를 제거해 주는 새로운 기능이 있다.



또한 그간 사용상의 편리함으로 널리 사용되어 왔던 ActiveX 프로그램이 악성코드의 손쉬운 설치 경로로

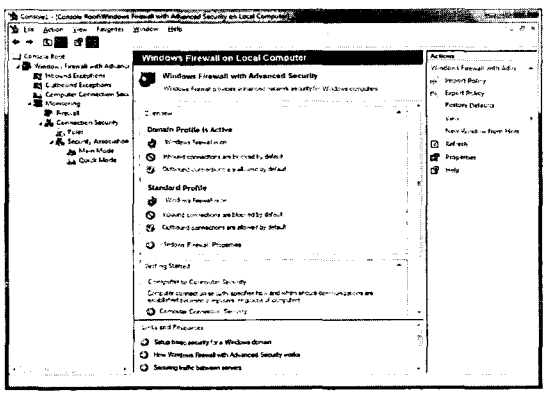
* 한국마이크로소프트 보안담당이사(wycho@microsoft.com)

도 악용되어 온 만큼, Active X의 장점은 그대로 사용할 수 있도록 하되 사용자도 모르는 ActiveX 프로그램의 자동 설치를 방지하기 위해 ActiveX Opt-in 을 도입하였다. 애플리케이션에 포함된 ActiveX 컨트롤이라 하더라도 기존에 없던 새로운 컨트롤이 실행되려 할 경우 반드시 사용자의 개입이 있어야 진행이 가능하게 되었다.

2.2 윈도우 방화벽(Windows Firewall)

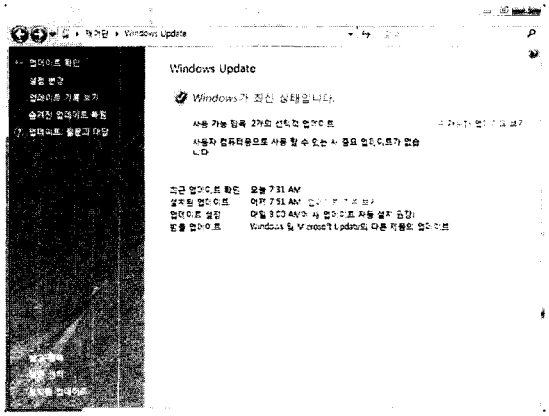
방화벽은 여러 유형의 악성 코드를 맨 처음 차단하는 방어막이다. 방화벽을 알맞게 구성하면 사용자 PC나 네트워크상의 다른 PC가 감염되기 전에 다양한 악성 코드를 막아낼 수 있다. 윈도우 비스타의 방화벽은 기본으로 켜져 있으므로(*On-by default*) 윈도우를 시작하는 즉시 컴퓨터 보호 기능이 작동한다. 일반 사용자가 보게 되는 방화벽 설정 화면은 윈도우 XP의 방화벽과 크게 다르지 않으며, 몇 가지 구성 옵션과 간단한 인터페이스를 통해 기본적으로 필요한 설정을 할 수 있다.

이전 버전에 비해 기능이 강화된 비스타의 방화벽은 악성 코드 감염으로 인해 비정상적으로 작동하는 다른 운영 체제 리소스를 제한하여 사용자를 보호한다. 예를 들어 PC에 있는 포트를 통해 네트워크 메시지를 보내는 윈도우 구성 요소가 공격을 받은 경우 미리 정해지지 않은 다른 포트를 통해 메시지를 보내려고 하면 방화벽이 컴퓨터에서 메시지를 보내지 못하게 하여 악성 코드가 다른 사용자에게 전파되는 것을 막는다. 엔터프라이즈 버전에서는 양방향 방화벽을 지원하므로 내부로부터 외부로의 의도된 또는 의도되지 않은 보안사고 위험을 방지 할 수 있다.



2.3 윈도우 업데이트(Windows Update)

최신 보안 및 기능 업데이트를 자동으로 다운로드 및 설치하는 옵션을 통해 컴퓨터를 최신 상태로 유지할 수 있도록 해 주는 윈도우 업데이트도 윈도우 비스타의 중요한 기능이다. 백그라운드로 진행되며 편리한 시간에 컴퓨터를 다시 시작하여 완료할 수 있는 이 업데이트 과정은 간단하고 자연스럽게 진행된다. 정품 인증을 거치지 않은 경우에는 윈도우 업데이트를 사용할 수 없지만 그 경우에도 자동 업데이트를 이용한 보안 패치 설치는 정상적으로 진행된다.



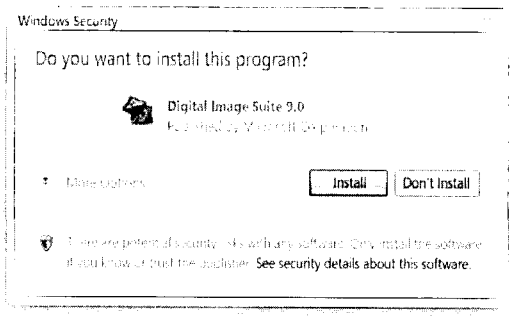
2.4 사용자 계정 컨트롤 (UAC, User Account Control)

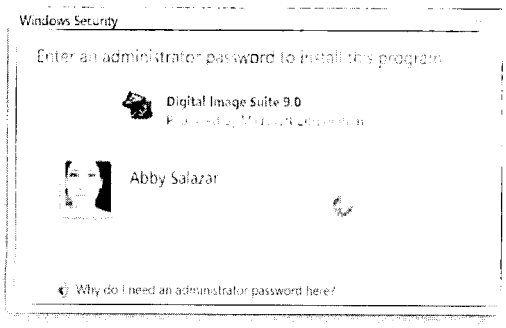
웹 탐색, 전자 메일 전송, 응용 프로그램 사용 등의 일반적인 사용자 작업을 할 때는 시스템의 관리자 권한이 필요 없지만 대부분의 사용자가 모든 관리 권한이 있는 계정으로 가정용 PC에 로그온하기 때문에 PC는 바이러스, 스파이웨어 및 그 밖의 위협에 쉽게 노출된다. 사용자가 부주의하게 실행하는 악성 코드 역시 많은 시스템 권한을 갖기 때문이다. 이와 같이 불필요 하게 높은 권한으로 인한 위험성을 대폭 줄이고자 일반 사용자의 권한으로 대부분의 작업이 가능한 환경으로 바꾸고 관리자의 권한이 반드시 필요한 경우는 반드시 별도의 권한상승과정을 거치도록 하였다.

즉, 윈도우 비스타의 사용자 계정 컨트롤(UAC, User Account Control)을 사용하면 표준 사용자 권한으로 손쉽게 PC를 사용할 수 있다. 가족 구성원마다 별도의 사용자 계정을 만들어 각자 사용하고, 그 사용자마다 설치

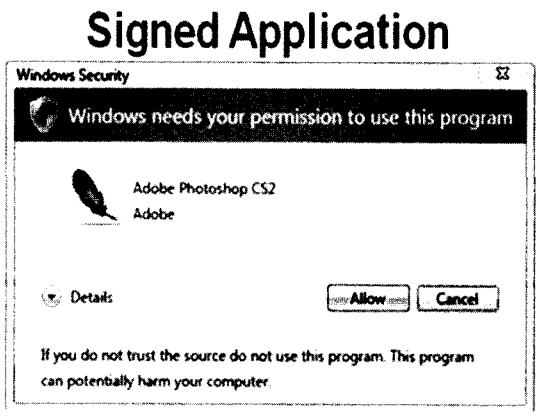
할 수 있는 웹 사이트 애드온, 프로그램, 게임 등을 제어할 수 있다. 어린 자녀가 있는 가정에서는 UAC를 사용하여 아이들이 좋아하는 프로그램에 숨어 있는 바이러스, 웜, 스파이웨어 등의 악성 코드로부터 PC를 보호할 수도 있다. 아이들이 소프트웨어를 새로 설치하려고 하면 관리자 계정 암호를 입력하라는 메시지가 표시되도록 UAC를 통해 어린이용 표준 사용자 계정을 만들 수 있다.

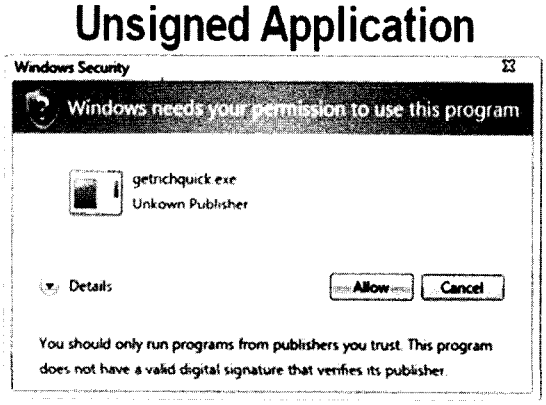
UAC는 관리자 계정을 사용할 때도 추가적인 보호 기능을 제공한다. UAC가 실행되는 기본 환경에서는 대부분의 프로그램이 잠재된 피해를 막기 위해 관리자라 할 지라도 표준 사용자 권한으로 실행된다. 프로그램 설치나 실행 시 그것이 안전한 작업인지, 또 사용자가 실제로 원하는 작업인지 확인할 기회를 제공하여 악성 코드가 실행될 가능성을 최소화한다. 즉, 반드시 관리자 권한이 필요한 시점에서만 관리자 권한을 행사 할 수 있도록 하는 것이다. 이는 운영체제의 취약점을 이용하여 관리자 권한을 탈취한 악성프로그램이 자동적으로 관리자 권한을 수행하는 것을 막을 수 있다. 기업에서는 직원들의 PC에 불필요한 프로그램이 설치되는 일을 차단함으로써 회사의 자산을 안전하게 지킬 수 있다.





또한 프로그램 설치 시 신뢰할 수 있는 기관으로부터의 서명(Signed) 이 들어가 있는 것과 그렇지 않은 것을 명확하게 구분 하여 줌으로써 의심이 가거나 출처가 불분명한 프로그램의 잠재 위험성에 대한 경각심을 높이는 과정을 제공한다.





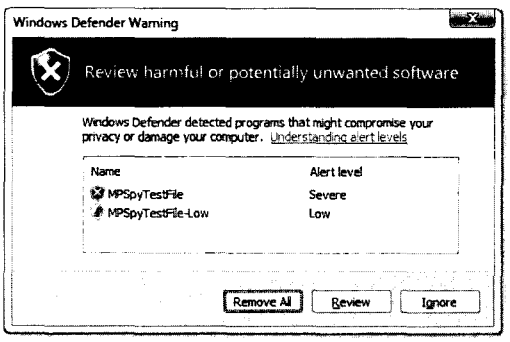
2.5 인터넷 익스플로러 7(IE7) 보호 모드

해커들은 웹 브라우저를 통로로 삼아 악성 코드를 유포하고 사용자 컴퓨터를 손상시켜 왔다. 윈도우 비스타에 기본 탑재된 인터넷 익스플로러 7에는 여러 가지 향상된 보안 기능이 내장되어 있어 이러한 공격을 막는다. 예를 들어 보호 모드(Protected Mode) 기능은 브라우징 기능 이상의 권한을 제한 한다. 즉, 해커가 브라우저를 점령하고 사용자 간섭을 피해서 코드를 실행하거나 프로그램을 설치 하는 등의 행위를 방지한다. 그 이상의 작업이 필요할 때에는 반드시 사용자의 권한상승 과정을 요구하게 하고 브라우저 자체의 실행 권한이 대폭

축소됨으로써 ActiveX를 통해 시스템 자원을 함부로 변경할 수 없게 되었다.

2.6 윈도우 디펜더(Windows Defender)

전에는 '윈도우 안티스파이웨어'라는 이름으로 베타 제품으로 별도로 무료 배포되었지만 이제 정식 제품 이름인 윈도우 디펜더라고 불리우며, 윈도우 비스타에 기본 탑재된다. 이전 이름에서 볼 수 있듯이 스파이웨어를 탐색, 제거하는 것이 주 목적이다. 컴퓨터 하드 드라이브를 정기적으로 검사하고 발견된 스파이웨어나 다른 원치 않는 소프트웨어 제거 옵션을 통해 PC를 보호하는 윈도우 비스타 기능이다. 뿐만 아니라 주요 시스템 위치를 모니터링함으로써 변화를 감시하여 스파이웨어가 있는지 파악하고 알려진 스파이웨어와 관련하여 지속적으로 업데이트되는 데이터베이스에 따라 파일을 검사한다.



2.7 보다 안전한 온라인 환경지원

인터넷은 탐색, 통신, 쇼핑, 학습에 이용할 수 있는 방대한 자원이다. 반면, 규모와 사용자가 증가함에 따라 인터넷은 사용자의 귀중한 개인 정보를 캐내려는 ID 도용꾼, 인스턴트 메시지 대화 내용을 엿보는 정보 사냥꾼, 보호 장치가 없는 PC에 바이러스를 감염시키려는 공격자들의 놀이터가 되었다. 더군다나 최근 들어 악성 코드 유포의 목적이 실질적인 경제적 이익으로 점차 바뀌어가고 파급 효과가 커지면서 인터넷에서의 정보 보호는 국가적인 관심사가 되고 있다.

사용자를 보호하고 안전한 온라인 환경을 제공하기 위해 윈도우 비스타에는 피싱 필터, 보안 상태 표시줄, 윈도우 카드스페이스, 네트워크접근제어(NAP), 보호자 통제와 같은 새로운 기능이 도입되었다.

2.8 피싱 필터(Phishing Filter)

인터넷 익스플로러 7에는 피싱으로부터 사용자를 보호하는 기능이 있다. 온라인 사기꾼들이 신용 카드 번호, 암호, 기타 계정 데이터 등 사용자의 귀중한 개인 정보를 불법으로 수집하는 것을 원천적으로 차단하기 위해 피싱 필터 기능은 일련의 확인 과정을 통해 피싱 사기를 방지한다. 피싱 필터를 사용하면 의심스러운 피싱 사이트에 대한 경고가 나타나기도 하고, 이미 알려진 피싱 사이트일 경우 페이지 내용을 표시하는 대신 다음과 같은 경고 메시지를 표시한다.

또한 Cyota Inc., Internet Identity, MarkMonitor Inc. 와 같은 업체와 블랙 리스트 목록을 공유하여 정기적으로 업데이트하고 있으며 각국 정부와 APWG(Anti Phishing Working Group)등과의 긴밀한 협력을 통하여 피싱정보를 공유 하고 있다.

2.9 보안 상태 표시줄

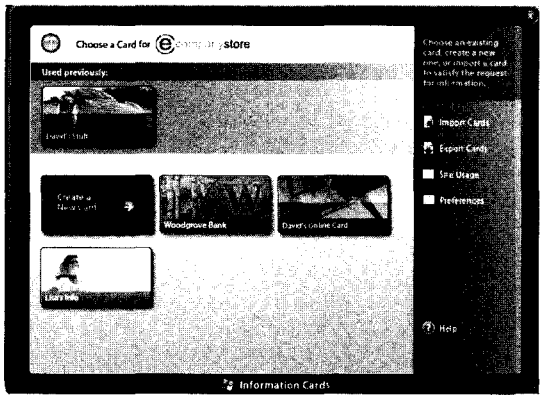
주소 표시줄 옆에 보이는 보안 상태 표시줄을 통해, 인증된 웹 사이트와 의심스럽거나 유해한 웹 사이트를 바로 구별할 수 있다. 이 기능을 사용하여 클릭 한 번으로 유효한 웹 사이트의 합법성을 인증하는 인증서에 액세스할 뿐 아니라 웹 사이트의 안전성과 신뢰도를 직접 확인할 수 있다. 새로운 보안 상태 표시줄에는 웹 사이트의 신뢰도와 보안 수준을 나타내는 자물쇠 아이콘이 있다. 또한 특수한 색 구분이 표시되어 사이트의 합법성을 한 눈에 알아볼 수 있다.

2.10 윈도우 카드스페이스(Windows CardSpace)

윈도우 카드스페이스는 사용자의 디지털 ID를 구성 및 관리하고 필요한 암호 개수를 줄임과 동시에 인터넷을 통해 공유하는 개인 정보를 효과적으로 제어할 수 있는 새로운 기술이다. 윈도우 카드스페이스를 지원하는 웹 사이트를 방문하면 로그인 사용자 이름과 암호 대신 정보 카드를 전송할 수 있다. 정보 카드는 윈도우

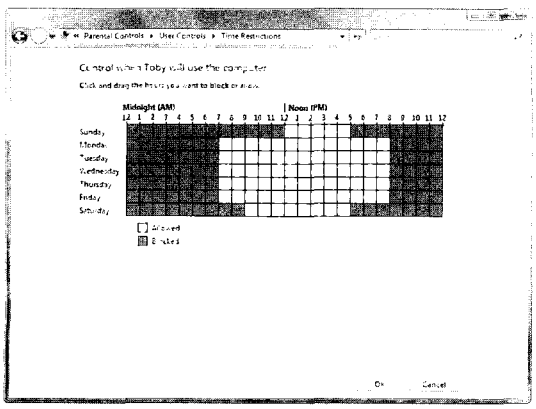
비스타에 기본 제공된 새 인터페이스를 통해 쉽게 전송할 수 있다.

정보 카드에 저장된 개인 정보는 암호화되어 PC에 안전하게 저장되거나 은행, ISP, 정부 기관 등 신뢰할 수 있는 ID 공급자를 통해 관리되므로 사용자 이름 및 암호 방법보다 윈도우 카드스페이스가 안전하다고 볼 수 있다.



2.11 보호자 통제

자녀가 컴퓨터로 접할 수 있는 내용을 제어하는 포괄적인 보호자 통제 기능이 도입되어 부모가 안심하고 자녀에게 컴퓨터 사용을 허락할 수 있다. 보호자는 통제 패널을 사용하여, 자녀가 컴퓨터를 사용할 수 있는 시간과 기간 제한이나 자녀가 방문할 수 있는 웹 사이트와 사용할 수 있는 소프트웨어 응용 프로그램 제어를 할 수 있다.



Ⅲ. 기업사용자를 위한 향상된 보안 기능

3.1 강화된 개인 방화벽

IT 부서에서 보안 위험을 완화시키는 가장 중요한 방법 중 하나는 네트워크에 액세스할 수 있는 응용 프로그램을 제한하는 것이다. 윈도우 비스타에 기본 제공되는 개인 방화벽은 양방향 트래픽 필터링을 제공한다. 관리자는 응용 프로그램이 네트워크를 통해 통신하지 못하도록 할 수 있다. 예를 들어 관리자가 미디어 플레이어 같은 응용 프로그램이 다른 컴퓨터에 연결하거나 응답하지 못하도록 차단할 수 있다. 로컬 컴퓨터에서 음악이나 비디오를 재생하는 용도로 이 응용 프로그램을 사용할 수는 있지만 인터넷 콘텐츠에 액세스하지 못하도록 응용 프로그램이 차단된다. 또한 이러한 방화벽 설정을 그룹 정책 개체별로 구성하여 간편하게 관리하고 제어할 수 있다.

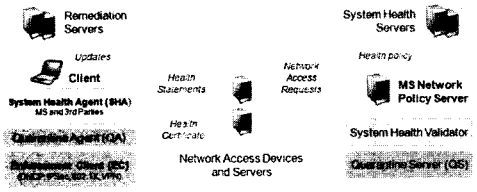
3.2 윈도우 서비스 보안 강화

윈도우 서비스 보안 강화(Windows Service Hardening)라는 새로운 플랫폼 관리 방식을 사용하여, 윈도우의 중요한 서비스가 파일 시스템, 레지스트리 또는 네트워크에서 비정상적인 작업에 사용되지 않도록 할 수 있다. 방화벽은 인바운드 및 아웃바운드 필터링을 모두 지원하며 서비스 보안 강화 네트워크 규칙을 적용하는 데 사용된다. 또한 ACL(액세스 제어 목록)을 기반으로 파일 시스템이나 레지스트리의 특정 영역에만 쓸 수 있도록 서비스를 제한할 수도 있다. 이렇게 하면 파일 시스템이나 레지스트리에서 손상된 서비스로 인해 중요한 구성 설정이 변경되거나 네트워크의 다른 컴퓨터가 영향을 받지 않도록 하는 데 도움이 된다. 예를 들어, RPC(원격 프로시저 호출) 서비스가 시스템 파일을 바꾸거나 레지스트리를 수정하지 못하도록 제한할 수 있다.

3.3 NAP(네트워크 액세스 보호)

윈도우 비스타의 NAP 클라이언트는 기업 내에서 소프트웨어 패치 상태 및 최신 바이러스 시그너처와 같은 클라이언트 상태에 대한 요구 사항을 설정할 수 있도록 하고 클라이언트가 네트워크에 연결될 때 이러한 요구 사항을 확인할 수 있도록 한다. 상태 요구 사항을 만족

하지 않는 클라이언트는 네트워크에서 접근이 허용되지 않는다.



Client
- SHA – Health agents check client state
- QA – Coordinates SHA/EC
- EC – Method of enforcement

Remediation Server
- Serves up patches, AV signatures, etc.

Network Policy Server
- QS – Coordinates SHV
- SHV – Validates client health

System Health Server
- Provides client compliance policies

3.4 통합 IPSec/방화벽 관리

윈도우 비스타에서는 IPSec(인터넷 프로토콜 보안) 및 방화벽 관리가 "고급 보안이 포함된 Windows 방화벽"이라는 하나의 콘솔로 통합되었다. 이 콘솔은 IPSec 서버 및 도메인 격리 설정과 함께 인바운드 및 아웃바운드 트래픽 필터링을 사용자 인터페이스에서 중앙 집중화하므로 보안 설정을 보다 확실하게 확인할 수 있다.

3.5 커널 패치 보호(Kernel Patch Protection)

64비트 버전은 커널 패치 보호 기술도 지원한다. 이 기술은 프로그램이 무단으로 윈도우 커널을 패치하지 못하도록 한다. 커널 패치 보호는 지원되지 않는 커널 후크를 중지하여 운영 체제의 안정성을 개선한다. 커널 후크는 안정성과 성능 문제를 일으킬 수 있으며 시스템에 잠재적인 보안 문제를 일으킬 수 있기 때문이다.

3.6 사용자 인증

현재 가장 일반적인 인증 방법은 암호를 사용하는 것이다. 그러나 이와 같은 단일 요소 인증에는 여러 가지 제한 사항이 있다. 암호가 짧거나 기억하기 쉬우면 공격자가 쉽게 추측할 수 있으며, 반대로 길이가 길고 복잡한 암호는 기억하기 어렵기 때문에 사용자들이 적어 두는 경우가 많다.

윈도우 비스타에는 생체 인식 또는 토큰 같은 대체 인증 방법을 추가하기 위한 수정된 아키텍처 가 도입되었다. Winlogon 수정 아키텍처에서는 소프트웨어 개발 업체나 조직이 자격 증명 공급자 CSP(Credential Service Provider) Interface 를 작성하여 생체 인식이나 토큰 같은 자체 인증 방법을 구현할 수 있다. 자격 증명 공급자 모델은 기존의 GINA 교체 방법에 비해 훨씬 간단하며 여러 공급자가 함께 작동할 수 있어 다중인증(Multi factor Authentication) 을 구현할 수 있다.

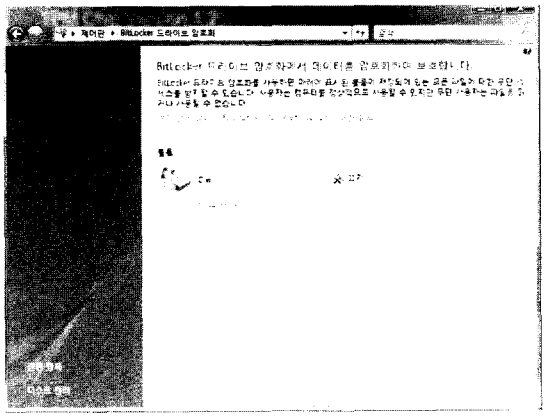
3.7 세분화된 감사

윈도우 비스타의 감사 기능을 사용하면 사용자가 수행하는 작업을 보다 쉽게 추적할 수 있다. 감사 범주에는 다양한 하위 범주가 포함되어 있어 관련 없는 이벤트의 수가 줄어든다. IT 전문가는 별도의 컴퓨터에서 이벤트를 감사할 수 있으며 분석을 위해 이벤트를 중앙 위치에 수집할 수 있다.

3.8 BitLocker 드라이브 암호화

BitLocker는 윈도우 운영 체제에 완벽하게 통합된 솔루션 개발을 통해 하드웨어 손상, 도난, 오작동 등으로 인한 데이터 도용 또는 공개 같은 실제 위협을 해결해 달라는 고객의 요청을 반영한 기능이다. 부당한 방법으로 노트북 컴퓨터를 습득한 사람이 다른 운영 체제 시스템으로 부팅하거나 소프트웨어 해킹 도구를 실행하여 시스템에 침입하거나 보호된 드라이브에 저장된 파일을 오프라인으로 보는 것을 방지한다. 이 기능은 TPM 1.2 칩과 USB 이동 저장 장치등를 사용하여 사용자 데이터를 보호하고 시스템이 오프라인일 때 변조되는 것을 차단한다.

이 보호 기능은 전체 윈도우 볼륨(시스템 파티션)을 암호화하여 수행된다. BitLocker로 페이지 파일 및 최대 절전 모드(Hibernation Mode) 파일을 포함하여 모든 사용자와 시스템 파일파티션을 암호화한다. 구성 요소가 손상되지 않고 암호화된 드라이브가 원래의 컴퓨터에 위치한 경우에만 데이터 해독이 수행되도록 무결성을 확인한다. 기업 보안 관리자는 Recovery Key를 보안 정책에 따라 Active Directory등을 이용하여 통합 관리 할 수 있으며, Recovery Key 가 없이는 데이터 복구가 불가능 하므로, 이 기능을 활용하여 매우 간단히 정보 파기(Data Delete)및 자산 재활용에도 이용할 수 있다.



3.9 장치 드라이버 설치 제어

IT 관리자는 그룹 정책을 사용하여, USB 플래시 드라이브 및 외부 하드 드라이브와 같은 이동식 저장 장치의 설치를 차단할 수 있다. 이렇게 함으로써 회사의 지적 재산이나 중요한 데이터가 손상되거나 도용당하는 사례를 막을 수 있다.

Ⅳ. 맺음말

이상 다양한 비스타의 향상된 보안기능에 대해 간단하게나마 소개 하였다. 비스타의 보안기능을 이해하는데 조금이나마 도움이 되었으면 하는 바람이다.

추가적으로 보다 자세한 정보는 다음의 사이트를 통해 얻을 수 있다.

http://msdn2.microsoft.com/en-us/windowsvista/default.aspx
http://www.microsoft.com/windows/products/windowsvista/default.mspx
http://www.microsoft.com/korea/windows/products/winfamily/ie/default.mspx
http://www.microsoft.com/security/default.mspx
http://technet.microsoft.com/en-us/default.aspx
http://www.microsoft.com/korea/security/default.mspx

〈著者紹介〉

조 원 영 (Wonyoung Cho)
한국마이크로소프트 보안총괄임원(Chief Security Advisor)