

Micron Technology, Wave Systems, Lenovo 및 American Megatrends Inc., 새로운 업계 표준 마련하여
글로벌 보안 요건 강화에 공동 대응

엔터프라이즈 공급망에 필요한
CTRM (Core Root of Trust for Measurement) 강화에 협력

2014년 10월 29일, 아이다호주 보이시(글로브 뉴스와이어) -- 고급 반도체 시스템의 글로벌 리더인 Micron Technology, Inc.(Nasdaq:MU)와 엔드포인트 보안 선도업체인 Wave Systems Corp.(Nasdaq:WAVX)는 Lenovo(HKSE:992) (ADR:LNVGY) 및 American Megatrends Inc.(AMI)와 함께 협업 관계를 확대한다고 발표했다. 이 회사들은 첨단 엔터프라이즈급 보안 오퍼링을 개발하여 공공 기관 및 다국적 기업의 악화되는 우려사항에 대응해 나갈 방침이다.

소프트웨어 컴포넌트를 검증하고 안전하게 유지하기 위해, 이 솔루션은 CTRM(Core Root of Trust for Measurement)을 크게 강화하여 공급망 내에서 현재 및 향후에도 부팅 전 위협 요소에 대한 최상급 보호 기능을 제공하게 된다. 이 회사들은 이러한 솔루션을 통해 공급망의 무결성을 보장하도록 고안된 새로운 업계 표준의 기반을 형성하게 된다.

2014 Verizon DBIR 보고서에 따르면, 공급망의 취약성과 제 3자 벤더들은 아직도 엔터프라이즈 데이터를 침해하는 선두적인 원인이다(자료출처: Verizon DBIR, 2014). 주요 브랜드들의 민감한 기업 자료가 계속 유출되면서, 연산 디바이스의 제조 단계에서부터 수명 주기를 통해 메모리 콘텐츠를 보호할 수 있는 종합적 엔터프라이즈 보안 스위트를 구축하는 것이 무엇보다 중요해지고 있다. 첫번째 실행되는 BIOS 코드인 CRTM을 검증하면, 기본적으로 내재된 신뢰성에 기반하기보다 시스템 측정의 보안성을 확보하여 공급망 공격의 위험을 줄일 수 있다. 클라이언트의 CRTM과 연동되는 중앙 관리형 보안 솔루션은 공급망 전체에 걸쳐 클라이언트 시스템의 무결성을 제공한다.

Micron, Wave, Lenovo 및 AMI가 공동으로 개발하는 보안 솔루션은 메모리 콘텐츠의 첨단 보호, 침입 탐지 및 메모리 콘텐츠의 복구 기능을 구현하여 클라이언트 보안성의 근본적인 수준을 향상시킴으로써, 공급망부터 기업 환경에 이르기까지 타의 추종을 불허하는 신뢰도를 확보할 수 있다. 이 계획된 소프트웨어 솔루션은 TPM(Trusted Platform Module) 및 기타 하드웨어 소자와 함께 집적되어 통보, 원격 관리 그리고 엔터프라이즈에 필요한 추가 변경 옵션을 제공할 예정이다.

Micron의 컴퓨팅 및 네트워킹 마케팅 담당 부사장인 Robert Feurle은 "기업들은 조직 내부는 물론 외부의 조직적인 공격으로부터 네트워크, 디바이스 및 데이터를 보호해야하는 계속 증가하는 중압에 직면해 있습니다. 컴퓨팅 디바이스의 수명주기에 걸쳐 데이터 보안은 충분조건이 아니라 이제 필요조건입니다"라고 말한다. "Micron은 메모리 수준에서 데이터를 보호하기 위해 시간과 자원을 투자하고 있으며, Wave Systems 같은 엔터프라이즈 보안 리더들과 협력하여 엔터프라이즈 공급망에 걸쳐 강력한 보안성을 제공합니다."

Wave의 CEO인 Bill Solms는 "하드웨어와 소프트웨어 보안성을 결합한 첨단 솔루션을 지속적으로 개발하여 새로운 형태의 공급망 위협 요소들을 차단하거나 제거하도록 Micron, Lenovo 및 AMI와 더욱 긴밀하게 협력하게 되어 기쁩니다"라고 말했다. "Micron, Lenovo 및 AMI는 수년 동안 당사의 핵심 OEM이었기 때문에, 이 회사들은 Wave의 포트폴리오를 직접 액세스할 수 있고 당사는 기존의 소프트웨어 솔루션을 토대로 엔터프라이즈 공급망 보안 그리고 궁극적으로는 NIST 800-155 지원 기능을 한 차원 높일 수 있습니다."

Lenovo Corporation의 보안 담당자 겸 부사장인 Anthony Corkell은 "신뢰의 근원을 하드웨어에 구축하면, BIOS의 실행을 조절하고, 측정하며, 보고하는 데 필요한 불변의 메커니즘을 조성할 수 있습니다"라고 말한다. "이것은 무단 변경 및 변칙으로 공격을 들어오기 전에 이를 탐지하여, 관리자들은 해당 디바이스가 영향을 받지 않게 할 수 있습니다."

American Megatrends의 사장 겸 CEO인 Subramonian Shankar는 "AMI는 파워-온부터 핸드-오프, 운영체제와 모든 관련된 기업 보안 표준을 집적하고 지원하는 안전한 플랫폼을 개발하는 데 주력해오고 있습니다. 따라서, AMI는 당사의 대표 제품인 UEFI 개발 플랫폼용 Aptio(R) UEFI BIOS 펌웨어를 채택하여 Micron, Wave, Lenovo와 함께 공동 작업에 참여하게 되어 기쁩니다. AMI는 앞으로도 파트너 및 OEM 고객들에게 가장 신뢰할 수 있고 안정성 높은 보안 기능을 갖춘 솔루션을 제공해 드릴 것입니다"라고 말했다.

이 회사들은 2015년 전반기를 목표로 제품 개발에 관한 업데이트를 제공할 예정이다.

Micron 소개

Micron Technology, Inc.는 고급 반도체 시스템을 공급하는 글로벌 리더이다. Micron Technology, Inc.는 첨단 반도체 솔루션을 제공하는 세계 선두 업체 중 하나로, 전 세계적으로 최첨단 기술의 컴퓨팅 제품 및 소비재 제품, 네트워킹 제품, 내장 제품 및 휴대용 제품에 사용되는 획기적인 메모리 기술 및 패키징 솔루션과 반도체 시스템은 물론 모든 종류의 DRAM, NAND Flash 및 NOR Flash 메모리를 제조 및 판매하고 있다. 35년이 넘는 기술 리더십을 바탕으로 한 Micron의

메모리 솔루션은 세계에서 가장 혁신적인 컴퓨팅, 소비재, 엔터프라이즈 스토리지, 네트워킹, 모바일, 임베디드 및 자동차 애플리케이션을 구현한다. Micron의 보통주는 NASDAQ에서 MU라는 약어로 거래되고 있다. Micron Technology, Inc에 대한 자세한 정보는 www.micron.com를 참조한다.

Wave Systems Corp. 소개

Wave Systems Corp. (Nasdaq:WAVX)는 디바이스의 내부부터 시작하여 복잡성, 비용 및 데이터 보호의 불확실성을 줄여준다. 소프트웨어 레이어를 추가하여 보안성을 확보하여 정보를 안전하게 유지하려는 여타의 벤더들과 달리, Wave는 엔드포인트 컴퓨팅 플랫폼 자체에 직접 구축된 하드웨어 보안 기능을 활용한다. Wave는 이런 동향을 선도하는 최정예 전문업체 중 하나이며, 여러 가지 최초 솔루션으로 시장을 선도하며, TCG(Trusted Computing Group)의 이사로 참여하여 표준을 만드는 데 기여하고 있다.

Lenovo 소개

Lenovo (HKSE:992) (ADR:LNVGY)는 390억 달러 규모의 개인용 기술 기업으로, 전세계 최대의 PC 제조사이자 PC Plus의 리더로 각광받고 있으며 160여 개국에 고객을 두고 있다. 탁월한 엔지니어링 PC 및 모바일 인터넷 디바이스를 중심으로 한 Lenovo 비즈니스는 제품 혁신, 고효율성의 글로벌 공급망 그리고 강력한 전략 실행력을 갖추고 있다. Lenovo Group에서 IBM 개인용 컴퓨팅 사업부를 인수하여 탄생한 이 회사는 안정성 높은 고품질의 안전하고 사용하기 간편한 기술 제품 및 서비스를 개발, 제조 및 마케팅하고 있다. 이 제품 라인에는 아주 유명한 Think 브랜드의 상용 PC 및 Idea 브랜드의 소비자용 PC는 물론 서버, 워크스테이션 그리고 태블릿 및 스마트폰 등 모바일 인터넷 디바이스 제품군이 있다. 글로벌 Fortune 500대 기업인 Lenovo는 일본 야마토, 중국 베이징, 상하이 및 쉐첸, 노스캐롤라이나 레일리에 리서치 센터를 두고 있다. 보다 자세한 정보는 www.lenovo.com을 참조한다.

AMI 소개

1985년에 설립되어 AMIBIOS(R)로 유명해진 American Megatrends Inc. (AMI)는 최첨단 하드웨어, 소프트웨어와, 최상급 제조사들의 데스크톱, 서버, 모바일 및 임베디드 시스템에 지원 프로그램을 공급한다. AMI의 업계 선도적인 Aptio(R) V UEFI BIOS 펌웨어, 혁신적인 StorTrends(R) 네트워크 스토리지 하드웨어 및 소프트웨어 제품 그리고 MegaRAC(R) 원격 서버 관리 솔루션은 전세계로부터 각종 상을 휩쓸며 업계의 인정을 받고 있다. 기술 및 제품 라인의 다양성과 더불어, AMI는 Unified EFI Forum, Intel(R) Internet of Things/Intelligent Systems Alliance 및 TCG(Trusted Computing Group) 등 다수의 협회 및 표준 그룹에 참여하고 있다. 조지아주 노크로스에 본사를 두고

있는 AMI 는 미국, 중국, 독일, 인도, 일본, 한국 및 대만에 사무소를 열고
고객들을 효과적으로 지원하고 있다.

AMI, 제품 또는 서비스에 관한 자세한 정보는 1-800-U-BUY-AMI 로
문의하거나 www.ami.com 을 참조한다.

연락처: Micron 언론 홍보:

Karl Stetson
Zeno Group
206.297.5943
Karl.stetson@zenogroup.com

Wave 언론 홍보:

Krista Zanolli
Wave Systems Corp.
413.243.7029
kzanolli@wave.com