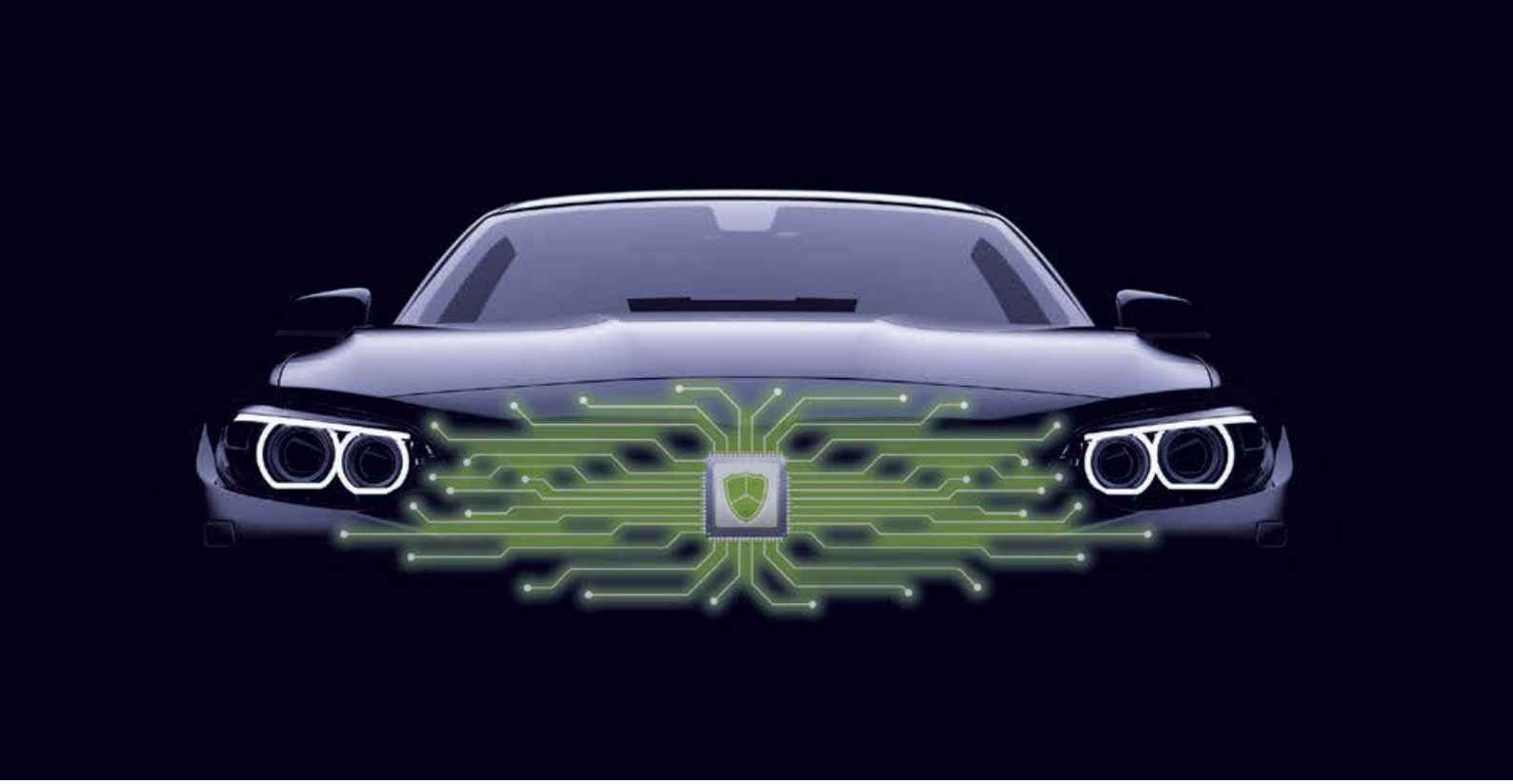

하드웨어 보안 모듈의 성능 강화

서비스 기반 HSM 소프트웨어가 미래형 전기 시스템 아키텍처의 보안을 책임진다.

미래의 자동차 아키텍처에서 소프트웨어의 상당 부분은 도메인 컨트롤러를 중심으로 집중되고 차량 이더넷은 광대역 온보드 통신을 제공할 것입니다. 이러한 변화는 IT 보안에 대한 새로운 접근방식을 요구합니다. 차세대 하드웨어 보안 모듈(이하 'HSM')은 멀티 애플리케이션 역량과 실시간 통신을 결합함으로써 중심 컴포넌트로 부상하고 있습니다.

머지않아 Vehicle computer(VC)가 차량 도메인 및 소프트웨어로 제어되는 도메인 기능을 통합할 것입니다. 주변장치의 ECU는 점차 입출력 장치로 변모하고, 이러한 ECU의 실제 애플리케이션은 VC에서 구현될 것입니다. 이러한 변화가 차량 제조사에 가져다 줄 혜택은 매우 광범위합니다. IP는 중앙 컴퓨터로 이동합니다. E/E 아키텍처와 엔지니어링 과정의 복잡성이 완화됩니다. 또한 차량 제조사는 각 세대의 차량 별로 특수한 ECU 및 소프트웨어를 구매하는 대신 소프트웨어 애플리케이션들이 VC 상에서 발전하고 상호작용하는 과정을 활용할 수 있게 됩니다.

그러나 중앙집중화는 온보드 통신을 증가시킵니다. 도메인 컨트롤러는 ECU에 분산 처리를 맡기는 대신 데이터를 수집 및 처리하고 차량에 배포해야 합니다. 실시간 구현에 대한 요구가 자주 발생함에 따라 데이터 트래픽은 차량 이더넷을 통해 이동합니다. 그러나 하부 네트워크에서는 여전히 CAN 버스를 통해 신호가 전송됩니다. IT 보안은 이러한 하이브리드 아키텍처에 적응해야 합니다.

보안 내재화

보다 심화될 연결성에 대비하여 보안 내재화 및 업데이트 내재화는 차량 내 하이브리드 네트워크에 단단히 뿌리를 두고 계획되어야 합니다. 이러한 내재화 계획은 특히 하드웨어와 소프트웨어의 분리 추세 및 여러 소프트웨어 애플리케이션의 배치 변화에 따라 새롭게 나타날 가능성을 염두에 두고 진행되어야 합니다. IT 보안 기능은 차량내 중앙집중형 네트워크에서 중앙집중형으로 관리될 수도 있습니다. 동시에 주변장치에서의 ECU 보안도 보장되어야 합니다.

HSM은 온보드 통신의 완벽 보안(SecOC)에 필수불가결한 요소입니다. HSM은 자동차에 모이는 모든 데이터의 진위를 확인하고, 공격자가 보안 관련 ECU 인터페이스를 우회하여 중앙 프로세서나 심지어는 차량내 네트워크에 접근하지 못하도록 합니다. 그러나 중앙집중형 차량 네트워크의 경우 HSM는 훨씬 복잡한 과제를 해결해야 합니다. 종종 다수의 가상 머신에

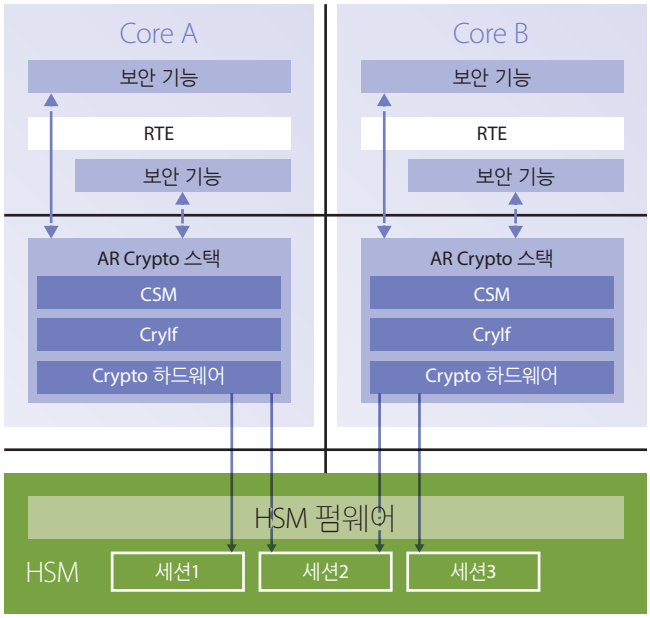

그림 1: HSM 펌웨어는 복수의 호스트 코어에서 발생한 요청을 병렬 세션에서 처리합니다.

분리 구획되어 있는 중앙VC가 여러 ECU의 소프트웨어 애플리케이션 및 기능을 담당할 때마다 보안 컴포넌트에 대한 수요도 증가하기 때문입니다. 차세대 HSM은 이미 이러한 새로운 요구에 대한 준비를 마쳤습니다.

작업의 우선순위 및 실시간 운영체제

HSM의 IT 보안 기능은 각 프로세서 마이크로컨트롤러의 HSM 코어에 물리적으로 단절된 상태로 존재합니다. 여기에서 IT 보안 기능은 HSM 소프트웨어 스택을 통해 활성화되고 실행됩니다. 그 결과 컴퓨터의 호스트 컨트롤러는 본연의 작업에 집중할 수 있고, 그 동안 HSM 코어는 온보드 통신 보안, 런타임 조 작 탐지 및 부팅, 플래싱, 로깅, 디버깅 보안 등 보안상의 요구사항을 처리합니다. 이러한 장점 덕분에 HSM은 소프트웨어에만 기반한 IT 보안 솔루션보다 보다 강력한 성능을 갖게 됩니다.

소프트웨어 애플리케이션과 ECU 기능이 VC에서 결합된다면 아마도 다수의 애플리케이션이 HSM의 보안 기능을 놓고 동시에 경쟁하는 순간이 때때로 발생할 것입니다. 이러한 경우 HSM은 필요한 IT 보안 기능을 제공하면서도 여러 애플리케이션의 데이터 스트림을 실시간으로 관리해야 합니다. 일반적인 HSM라면 한계에 다다를 수 있으며, 소프트웨어에만 기반한 보안 솔루션이라면 더욱 그러할 것입니다. 그러나 실시간 운영체제와 지능적이고 유연한 세션 컨셉이 포함된 차세대 HSM이라면 이러한 작업에도 무리가 없습니다.

멀티 코어/멀티 애플리케이션 지원

미래형 아키텍처에서는 수 개의 코어로부터 병렬 요청이 있는 경우, HSM 코어가 최대 16개의 병렬 세션에서 요청을 처리하도록 HSM 펌웨어가 확인합니다. HSM 소프트웨어 스택에서 세션 수를 설정할 수도 있습니다. 이처럼 멀티 코어 및 멀티 애플리케이션 지원이 가능한 것은 HSM 펌웨어 드라이버의 특수한 아키텍처가 있기 때문입니다. 이러한 아키텍처 덕분에 서로 다른 가상화 애플리케이션은 독립적으로 드라이버를 통합할 수 있고, 그 결과 다양한 소프트웨어 부분을 독립적으로 개발할 수 있습니다. 드라이버 통합 과정에서 'linker' 단계는 드라이버의 다양한 인스턴스가 하드웨어의 공유 RAM에 있는 공통 구조를 사용할 수 있게 합니다. 이 때 각 인스턴스는 개별 구조(세션)를 생성하여 드라이버는 엄격히 단절된 애플리케이션에서 발생한 다수의 요청을 언제나 병렬적으로 관리할 수 있게 됩니다(그림 1).

이러한 셋업의 핵심 보안 컴포넌트는 호스트와 HSM 사이의 브릿지입니다. 하드웨어 보안과 호스트를 분리하는 브릿지는 HSM을 향한 '유입 제어'를 담당합니다. 브릿지 레지스터에서는 호스트 코어로부터 발생한 일련의 요청을 정리 및 처리하는데, 이 과정에서 한정된 리소스인 HSM을 최적으로 활용하면서 요청된 보안 기능을 최대한 신속하게 수행할 수 있는 방식을 따릅니다. 차세대 HSM 소프트웨어는 HSM의 멀티 애플리케이션 및 멀티 코어 역량을 실현합니다. 차량 제조사는 완전 검증을 거친 양산 가능 형태의 HSM 소프트웨어를 만나볼 수 있습니다(그림 2).

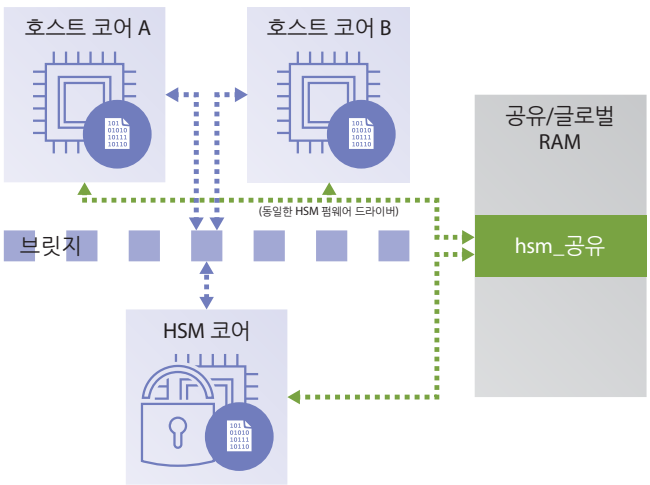

그림 2: 멀티 코어/멀티 애플리케이션 지원 – 브릿지 레지스터 및 공유 RAM을 통해 작업 요청을 처리합니다.

일괄적 MAC 인터페이스로 실시간 성능 지원

다음 과제는 급증한 통신에 대한 보안입니다. 중앙집중형 전기 시스템에서는 CAN 버스와 차량 이더넷이 공존하고 있고, 차량 내에서는 모든 통신 프로토콜에 대해 데이터 교환을 보호해야 합니다. 이러한 과제는 매우 까다로울 수 밖에 없습니다. 혁신적인 HSM은 이러한 까다로운 과제에도 솔루션을 제공하지만, 그 성능은 한정적입니다. HSM의 하드웨어 암호화 엔진은 모든 용량과 속도에서 데이터 교환을 허용하지는 않기 때문에 브릿지 레지스터보다 성능 한계를 더 낮게 설정합니다. 이러한 문제에 대한 솔루션으로 알려진 것이 일괄적 MAC 인터페이스입니다. 첫째, 호스트는 사전에 정해

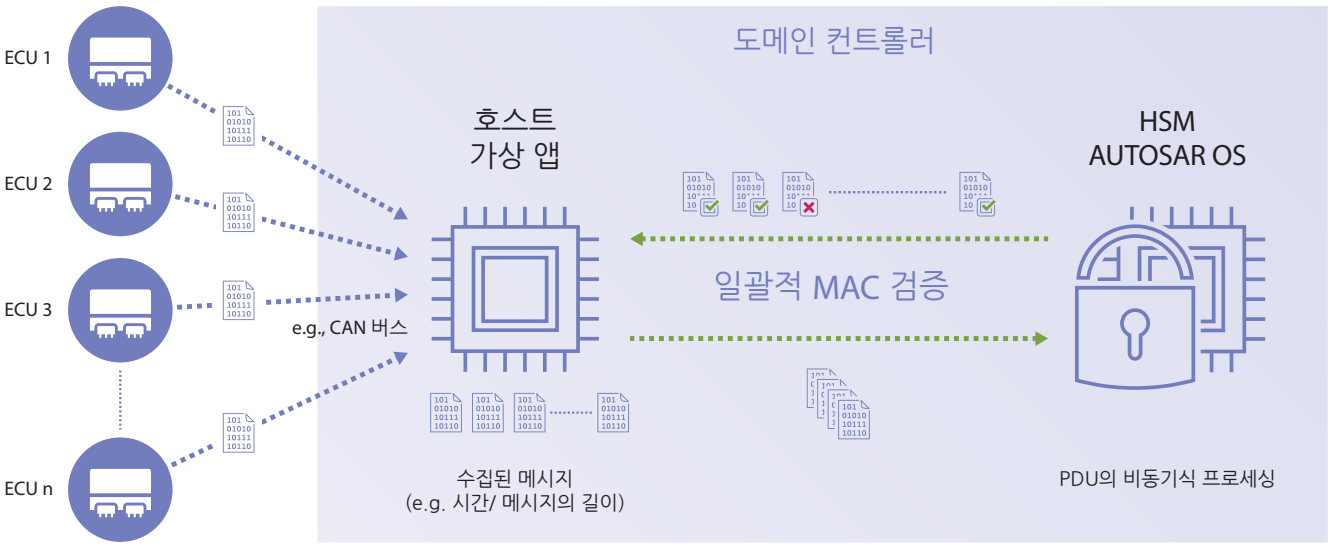

그림 3: 일괄적 MAC 인터페이스는 실시간 통신에 대한 보안을 제공합니다.

진 시간 동안 모든 메시지를 수집합니다. 그 다음 브릿지 레지스터를 통해 이 메시지를 일괄적으로 HSM에 대한 요청으로 게시합니다. 단 건의 데이터 교환만으로도 충분합니다. HSM 펌웨어는 HSM 하드웨어 단위에서 모든 수집 메시지를 한꺼번에 처리하여 그 결과를 호스트에 전송합니다(그림 3).

이러한 방식은 엄청난 성능 개선을 가져옵니다. 호스트와 HSM 간의 데이터 교환 한 건 당 단 10 마이크로초가 소요된다 하더라도 메시지 백 건이 모이면 지연시간도 1 밀리초로 늘어납니다. 실시간 시스템에 있어서는 이러한 지연이 큰 문제입니다. 그러나 일괄적 MAC 인터페이스를 사용하면 백 건의 메시지를 기존 소요시간의 1/100만에 처리할 수 있습니다. 중앙 컴퓨터 및 도메인 컨트롤러로 구성된 네트워크를 설정하고 그 과정에서 여러 PDU를 정의해 놓은 차량 제조사 입장에서는 일괄적 MAC 인터페이스의 장점이 매우 큽니다. 일괄적 MAC 인터페이스는 다양하고 수많은 메시지를 충분히 신속하게 인증함으로써 차량 네트워크의 실시간 통신에 대해 보안을 유지합니다. 일괄적 MAC 인터페이스는 차세대 HSM 소프트웨어에 이미 통합되어 양산 준비를 마쳤습니다.

미래에도 사용 가능한 하드웨어 보안 펌웨어

차량 내 네트워크가 중앙집중형 플랫폼으로 변모하면서 하드웨어와 소프트웨어의 분리 현상이 일어나고 있습니다. HSM은 이러한 플랫폼의 IT 보안에 핵심적인 역할을 수행합니다. HSM은 CAN 버스가 여전히 지배적인 역할을 수행하는 주변장치에서부터 중앙 컨트롤러에 이르는 데이터 스트림을 무단 접근 및 조작으로부터 보호(SecOC)할 뿐만 아니라, 최상위 네트워크 수준의 보안 유스케이스를 커버하고, 높은 데이터 부하와 실시간 요구사항이 많은 소프트웨어 애플리케이션이 구현될 때 보안을 확보합니다. 멀티 코어 및 멀티 애플리케이션 작업을 위해 설계된 차세대 HSM은 데이터 부하가 높고 일괄적 MAC 인터페이스를 사용하는 이종 포맷에 대해서도 실시간 통신을 보장합니다.

연결성 강화 및 자동화 주행 트렌드에 대응하여 차량 제조사들은 점차 자신만의 E/E 아키텍처 보안 표준을 정하고 있습니다. 차세대 하드웨어 보안 펌웨어는 차량 제조사만의 고유한 제품에 맞게 매핑될 수 있으며, 중앙 보안 컨셉에 유연하게 통합될 수 있습니다. 차세대 하드웨어 보안 펌웨어는 최신 마이크로컨트롤러에서 실행되면서 호스트 드라이버를 소스코드로 제공합니다. 그 결과 차량 제조사 및 1차 공급업체는 재사용 및 맞춤 설계를 할 수 있는 무궁무진한 기회를 얻게 됩니다. 이러한 유연성 및 성능에 기초하여 최신 펌웨어가 포함된 HSM은 미래의 중앙집중형 하이브리드 네트워크 보안에 필수적인 컴포넌트로서 자리매김합니다. ■

차세대 하드웨어 보안 펌웨어는 차량 제조사만의 고유한 제품에 맞게 매핑 될 수 있습니다.

저자

토비어스 클라인(Tobias Klein): 에스크립트, HSM 수석 제품 책임자
프레데릭 스텀프(Frederic Stumpf) 박사: 에스크립트, 사이버보안 솔루션 제품 관리 총괄

영문 원문으로 보기