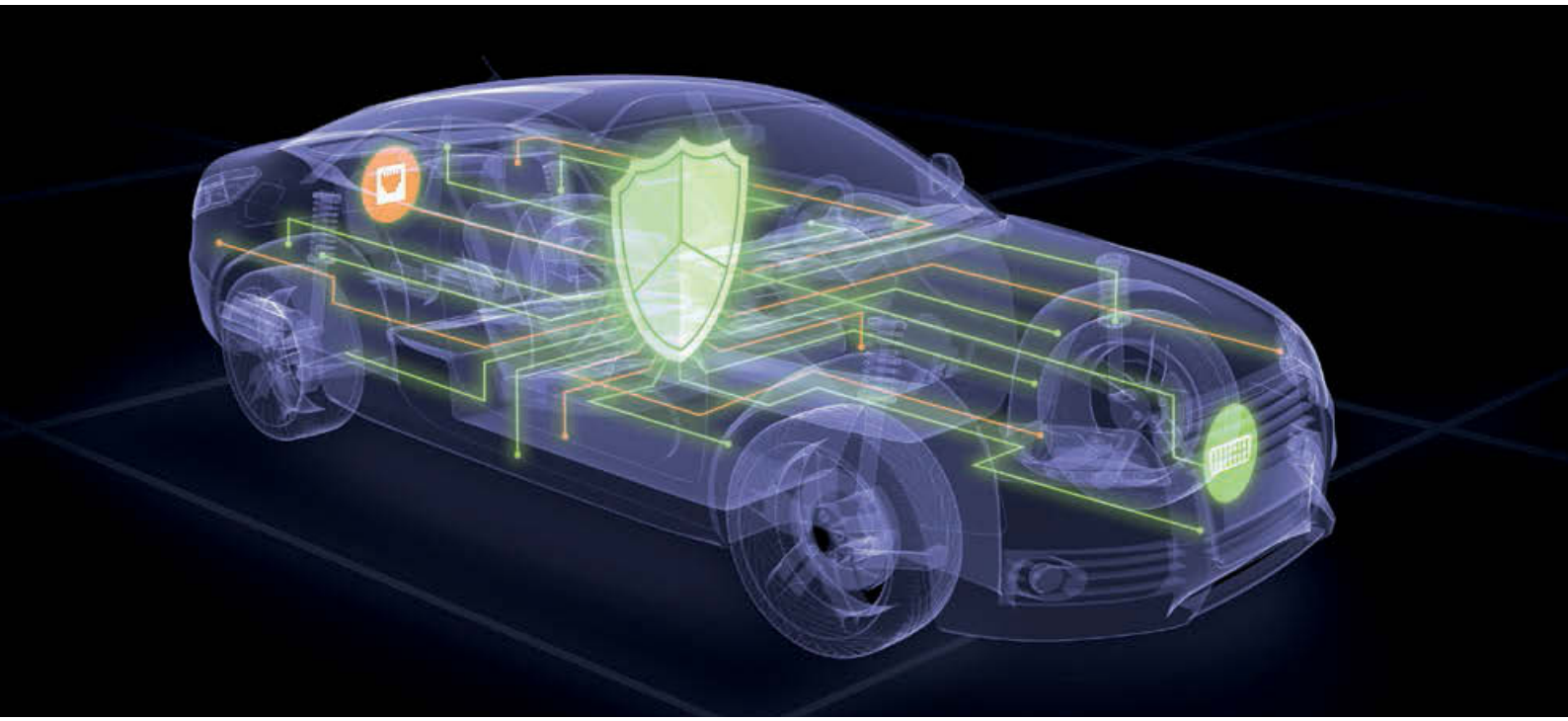
하이브리드 CAN-Ethernet 네트워크를 위한 침입 탐지

CAN과 Ethernet에 최적화된 보안 방안



오늘날의 분산된 E/E 아키텍처로는 커넥티드카와 자율주행 차량 관련 보안 문제들을 모두 해결할 순 없습니다. 그래서 차량 컴퓨터(Vehicle Computer, VCs)와 자동차 Ethernet이 기존의 ECU와 CAN 버스를 보완해주어야 합니다. 또한, 이러한 차량 네트워크들은 데이터 트래픽 관점의 모니터링과 공격 탐지와 같은 보안 조치들을 필요로 합니다.

차량 네트워크의 개발 방향은 명확합니다. 오늘날 차량 E/E 시스템은 CAN, LIN, FlexRay 데이터 버스로 연결된 수십 개의 ECU로 구성되어 있습니다. 이러한 차량 E/E 시스템은 차량 컴퓨터(VCs)와 광대역 차량 Ethernet으로 기존의 CAN, LIN, FlexRay를 보완할 것입니다. 현재 CAN, LIN, FlexRay는 높은 실시간 처리를 요구하는 기능과 주기적으로 반복되는 기능에 사용되고 있습니다. 그 외, 차량 기능에 따라 커넥티드카와 자율주행 차량에서의 여러 문제들을 해결하기 위해 가상 머신으로 분할된 마이크로프로세스 기반의 중앙 컴퓨터를 사용하고 있습니다.

그렇다면, CAN-Ethernet이 혼합된 하이브리드 아키텍처의 차량 네트워크는 어떻게 효과적으로 보호할 수 있을까요?

여기에는 2가지 원칙이 있습니다. 그것은 바로 통신 쉴딩(shielding)과 파티셔닝(partitioning)입니다. 즉, 사이버 공격을 초기에 탐지하기 위해서는 빈틈없는 모니터링이 수행되어야 하고, 공격자의 침투 정도를 최소화 하기 위해서는 각 도메인 별로 VLANs을 적용해야 합니다. CAN/Ethernet 하이브리드 네트워크 환경에서도 앞서 말한 2가지 원칙을 모두 적용할 수 있지만, CAN과 Ethernet 각각의 특성을 고려하여 서로 다른 접근 방식으로 구현해야 합니다.

CAN을 위한 효율적인 침입 탐지

침입 탐지 시스템(IDS)은 CAN 버스를 모니터링 하기 위해 게이트웨이 또는 ECU에 통합될 수 있습니다. IDS는 OEM에서 명시한 '정상 동작' 조건과 CAN 데이터 트래픽을 비교하여 이상 징후를 탐지합니다. 예를 들어, ECU 또는 게이트웨이에 내장된 보안 컴포넌트는 주기적인 메시지와 악의적인 진단 요청 메시지 내의 이상 징후를 탐지합니다. 보안 컴포넌트에서 탐지된 이상 징후는 잠재적인 공격으로 분류되어 로그로 남겨지거나 보고됩니다.(그림 1)

CycurIDS (CAN IDS) 성능은 IDS 설정에 따라 크게 좌우됩니다. 그렇기 때문에 가능한 오탐을 줄이고, 탐지 성능을 높이기 위해서는 지속적인 관리와 새로운 탐지 매커니즘 업데이트가 필요합니다. 새로운 탐지 매커니즘은 처음 OEM에서 설정한 탐지 규칙 뿐만 아니라 새롭게 나타나는 공격 패턴을 분석하여 이를 기반으로 탐지 규칙들이 업데이트됩니다. IDS를 구현하기 위해서는 툴박스(toolbox)가 필요하며, 툴박스 품질에 따라 IDS 성능이 달라지게 됩니다. 툴박스는 IDS를 구현할 때에 초기 설정 등을 구성하는 데에 사용되며, IDS의 탐지 규칙 세트(rule sets) 추가에도 활용됩니다. CycurIDS는 하이브리드 CAN/Ethernet 네트워크 환경에서의 CAN 공격 탐지 시스템으로 언제든 사용 가능한 소프트웨어입니다.

Ethernet 스위치를 위한 차량 방화벽

CycurGATE는 하이브리드 CAN/Ethernet 네트워크 환경에서의 안전하고 원활한 자동차 Ethernet 통신에 적합합니다. CycurGATE는 이더넷 스위치에 직접 구현되어 ECU와 호스트 컨트롤러 간의 노이즈(noise)로 인한 손실(loss)없이 전체 패킷 흐름을 모니터링 할 수 있습니다. 더불어 하드웨어와 소프트웨어의 호환성을 고려하여 설계했기 때문에 스위치의 하드웨어 가속(H/W acceleration)을 사용할 수 있습니다. 그 결과, CycurGATE는 통신 속도의 저하없이 기존의 유선 속도로 데이터 패킷들을 처리할 수 있습니다. 또한, CycurGATE는 모든 네트워크 계층의 파티셔닝을 지원하기 때문에 서비스 거부 공격과 같은 리소스 고갈 공격에 대응할 수 있습니다. CycurGATE의 패킷 필터는 오고 가는 모든 데이터 패킷들을 스테이풀(stateful) 방식과 심층(deep) 방식으로 검사하기 때문에 분리된 도메인 간의 안전한 데이터 교환을 보장합니다.

자동차 Ethernet 방화벽(CycurGATE)은 공격자의 인가되지 않은 접근과 데이터 변조로부터 차량 네트워크를 보호하고, 온보드 통신을 제어하는 역할을 합니다. 또한, Ethernet 방화벽은 SOME/IP와 같은 일반적인 프로토콜을 포함한 Ethernet/IP까지 데이터 처리가 가능하며, MAC 수준에서의 VLANs과 네트워크의 모든 접근을 모니터링 할 수 있습니다. 방화벽의 필터 방식은 화이트리스트 또는 블랙리스트 방식으로 필터링 됩니다. 필터에 사용되는 화이트리스트와 블랙리스트는 상시 업데이트가 가능하기 때문에 새로운 공격 패턴에 대해 신속하고 효과적인 대응을 보장합니다.

지능적 부하 분산

```
…
0.010000 1  100  Rx  d 8 8A FF FF 0C 42 5F FD 97
0.011000 1  110  Rx  d 8 03 3E 3E E2 10 FF 4A 3F
0.012000 1  120  Rx  d 8 03 F7 30 27 C7 7E D9 9C
0.020000 1  100  Rx  d 8 11 F4 00 3E E2 60 6C B9
0.021000 1  110  Rx  d 8 1F AA 00 00 00 00 C0 00
0.022000 1  120  Rx  d 8 02 AA 00 00 00 00 C0 00
0.031000 1  110  Rx  d 8 86 4A 2F 01 81 05 80 7F
0.031500 1  110  Rx  d 8 E5 2B 41 0C 00 00 00 00
0.032000 1  120  Rx  d 8 02 04 78 00 FF 00 00 30
0.041000 1  110  Rx  d 8 6E 7B FF FF 3F FF 1F 8B
0.042000 1  120  Rx  d 8 00 5A 00 00 0F 55 02 00
0.043000 1  7DF  Rx  d 8 02 10 03 00 00 00 00 00
0.044000 1  7E8  Rx  d 8 02 50 03 AA AA AA AA AA
0.051000 1  110  Rx  d 8 FE 4B 2F 01 81 07 80 7F
0.052000 1  120  Rx  d 8 68 05 78 00 FF 00 00 30
…
```

타이밍
- 주기 이탈
- 메시지 침투
- 타임 아웃

진단
- 서비스 유형
- 서비스 상태

그림 1: CAN IDS는 주기적 메시지 내의 이상 징후 및 악의적인 진단 요청을 탐지합니다.

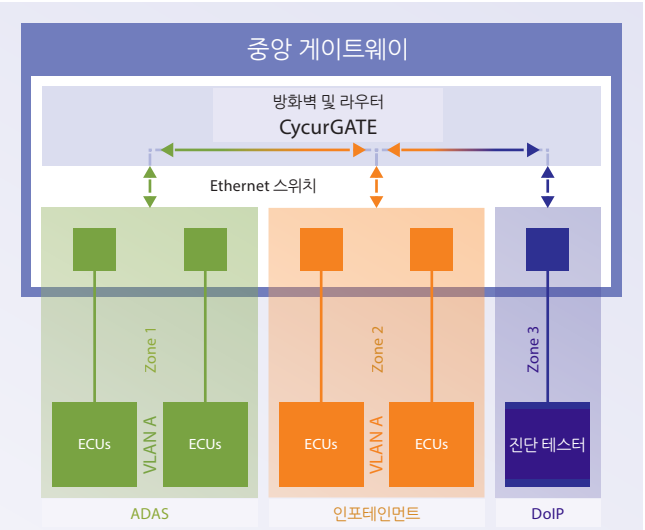


그림 2: 차량 이더넷 방화벽은 게이트키퍼 및 라우터 기능을 담당합니다.

CycurGATE(Ethernet 방화벽)는 중앙 Ethernet 스위치에 구현하는 방식 이외에도 호스트 기반으로 ECU에 직접 통합할 수 있습니다. 그러기 위해서는 ECU가 고성능의 하드웨어 스펙을 지녀야 합니다. 그래야만 ECU에서 실시간 데이터 처리가 가능하고, 각각의 데이터 패킷들의 라우팅 여부와 라우팅 위치를 결정할 수 있습니다. 그러나, SOME/IP 통신의 빈도를 스테이풀(stateful) 방식으로 탐지하는 등의 복잡한 공격 탐지 패턴은 이에 해당되지 않습니다. 위와 같이 복잡한 공격 탐지 패턴을 탐지하기 위해서는 추가적인 Ethernet IDS가 필요합니다. Ethernet IDS는 메시지 빈도(frequency), 시퀀스(sequence), 페이로드(payload), 데이터, 서비스 기반의 이상 징후 탐지하고 이를 로그로 남기거나 보고하는 역할을 합니다. 그러면, 추가한 Ethernet 스위치(IDS)와 마이크로컨트롤러(방화벽) 간의 최적의 성능을 내기 위한 효율적인 로드 분배가 필요하게 됩니다. 이 작업은 스위치와 컨트롤러에서 각각 처리하게 됩니다.

CAN IDS, 차량 Ethernet 방화벽, 차량 Ethernet IDS가 모두 갖춰지면, 어떠한 지연없이 빠르고, 안정적으로 하이브리드 E/E 아키텍처를 보호할 수 있게 됩니다. 위와 같이 보안 기능이 통합적으로 내장된 임베디드 시스템은 미래의 커넥티드카와 점차 증가하는 자율주행 차량에서의 위험을 예방하고, 기능 안전에 반드시 필요한 핵심적인 컴포넌트가 될 것입니다. ■

저자

얀 홀레(Jan Holle) 박사, 에스크립트, 침입 탐지 시스템 프로덕트 매니저
시드하스 슈클라(Siddharth Shukla), 에스크립트, 차량 방화벽 프로덕트 매니저

영문 원문으로 보기