# 가상 차량에서의 임베디드 보안 테스트

**XiL 테스트 환경을 통한 다양한 해킹 시뮬레이션**

오늘날 소프트웨어 차량 제어 시스템은 기능적으로 안전해야 하는 것은 물론, 사이버 범죄 위협으로부터도 안전해야 합니다. 그래서 이타스와 에스크립트는 가상화 (Virtualization) 및 XiL (Model-, Software-, Hardware-in-the-Loop) 기술을 통해 ECU가 해킹될 수 있는 다양한 상황에서 차량의 안전성을 테스트합니다.

저자

**유르겐 크레핀 (Jürgen Crepin),**
이타스,
마케팅 커뮤니케이션 전문가

**토비아스 크루진저 (Tobias Kreuzinger)**
박사,
이타스, 테스트 및 검증 매니저

해커가 차량 시스템에 침입해 센서 신호를 가로채고 조작된 데이터를 ECU 인터페이스에 입력한다고 가정해봅시다. 그렇게 되면 운전자는 갑작스럽게 외부에서 제어된 차에 갇혀 아무것도 할 수 없게 됩니다. 이러한 시나리오가 현실이 되지 않도록 하기 위해서는 신뢰할 수 있는 보안 솔루션이 필요합니다. 하지만 해커의 공격을 테스트하는 것이 가능할까요? 보안 대책들이 차량 시스템을 안전하게 보호할 수 있다는 것을 입증할 수 있을까요? 기능적 안전성 측면에서는 HiL (Hardware-in-the-Loop) 시스템을 이용해 정상 작동될 때와 작동이 중단되었을 때 기능이 제대로 실행되는 지를 확인할 수 있습니다. 개발자는 모든 ECU와 데이터 네트워크를 포함한 차량 전체 시뮬레이션에서 소프트웨어와 분산된 센서 시스템 및 차량 도메인의 상호작용을 테스트합니다. 그리고 이타스 LABCAR, 통합 시뮬레이션 솔루션인 이타스 COSYM, 또는 이타스 ISOLAR-EVE가 생성한 가상 ECU와 같은 리얼타임 HiL 시스템은 이러한 테스트의 기술적 기반을 제공합니다.

## 새로운 옵션: Security-in-the-Loop

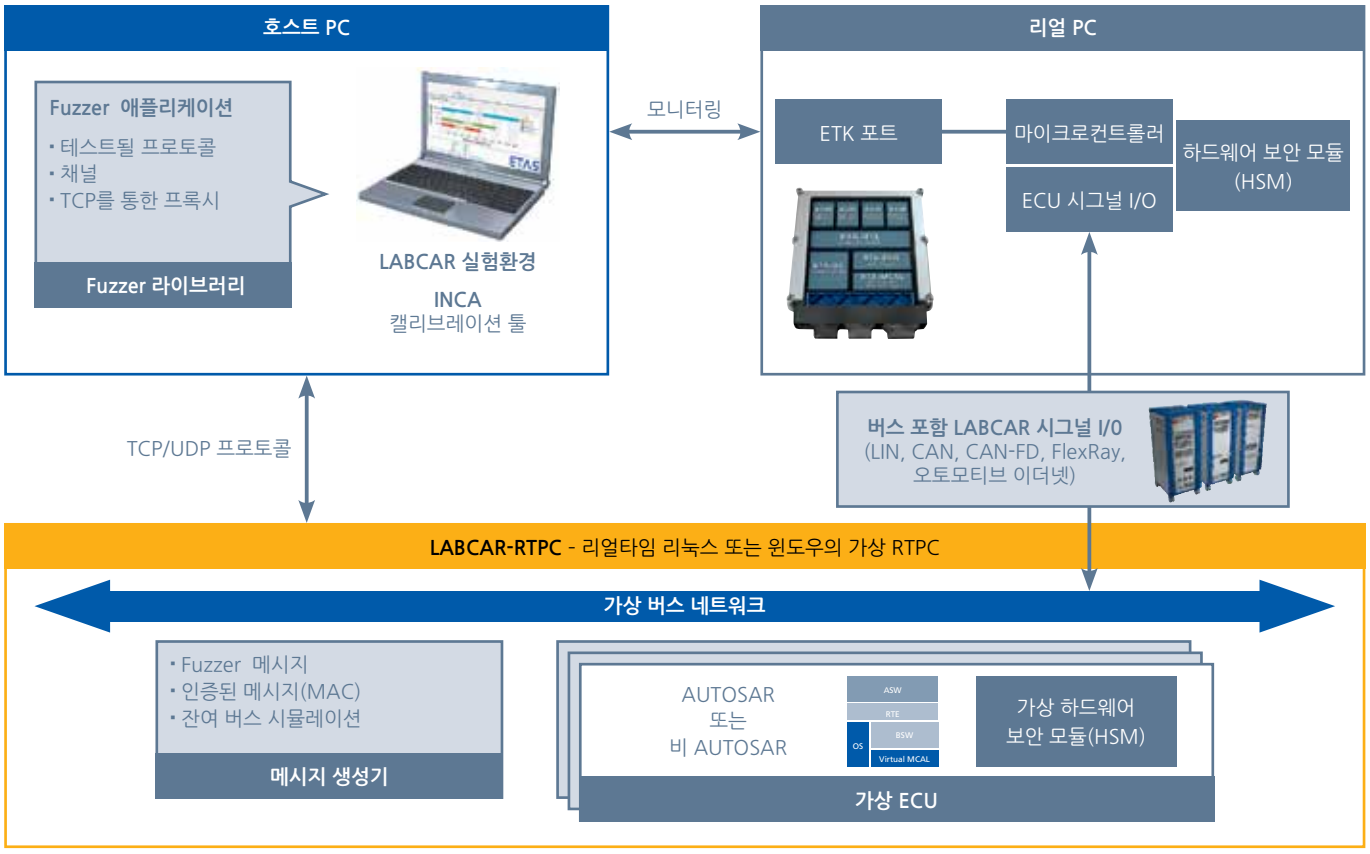
보안 테스트의 경우 true-positive 기법, 즉 예상되는 공격 행태를 테스트하는 것은 크게 효과적이지 않습니다. 개발 시점에 공격 시나리오가 알려져 있지 않거나, 혹은 알려진 경우 곧바로 취약점이 보완되기 때문입니다. 따라서 공격 행위보다는 공격에 취약한 부분을 체계적으로 찾는 데 중점을 둬야 하며, 이러한 보안 테스트에 SiL (Software-in-the-Loop) 또는 HiL 테스트 환경이 적합합니다. 여기서 문제는 서로 다른 영역의 역량을 결합하는 것입니다. 보안 전문가는 XiL 테스트 방법에 익숙해져야 하며, XiL 테스트 엔지니어는 전통적인 IT 환경에서의 방법에 익숙해져야 합니다. 이처럼 역량을 결합해야 임베디드 시스템의 잠재적 취약성을 찾아낼 수 있습니다. 무엇보다 보안과 관련된 차량 기능에 초점을 맞춘 보안 테스트는 시작부터 일관된 계획과 효율적인 실행을 수반해야 합니다. 이타스와 에스크립트는 이 문제를 일찍이 파악하여 XiL 방법과 자동차 보안 분야에 대한 노하우를 접목하고 두 분야의 강점을 결합한 솔루션을 제시하고 있습니다 (그림 참조). LABCAR 하드웨어, Linux 기반 시뮬레이션 타깃 LABCAR-RTPC (Real-Time PC), 가상 ECU 솔루션 ISOLAR-EVE를 기반으로 한 가상 테스트 영역에서는 개별 ECU 인터페이스에 대한 공격을 시뮬레이션하고 전체 차량 상황에 따라 ECU 기능을 조작하는 것이 가능합니다.

## 보안 테스트를 위한 LABCAR

이타스는 테스트 시스템을 담당하며, 에스크립트는 적절한 테스트 방법 등에 대해 보안 전문지식 및 기술을 제공합니다.

- 침투 (PEN, Penetration) 테스트:

* XiL = Model-, Software-, and Hardware-in-the-Loop (MiL, SiL, HiL)




테스터는 ECU의 동작을 외부에서 조작하거나, 인가 없이 데이터를 읽거나, 임베디드 시스템을 손상시키려고 시도합니다. 이타스와 에스크립트의 일부 자동화된 PEN Testing-in-the-Loop는 완벽한 테스트 커버리지 보장을 위해 에스크립트 컨설팅 프로젝트에서 얻은 경험을 바탕으로 지속적으로 확장되는 '공격 라이브러리'를 사용합니다.

▪ Fuzzing: 테스트 소프트웨어, fuzzer는 ECU 포트를 가득 채우는 임의 입력이나 의도적으로 조작된 명령을 자동으로 생성합니다. 그리고 해커의 침입이나 조작을 시뮬레이션할 때 테스트 대상 ECU의 프로토콜, 소프트웨어 시스템, 암호 보안에 대한 지식은 테스트 효율성 향상을 위해 일반적으로 신호 생성에 통합됩니다.

▪ 메시지 인증 (MAC, Message Authentication) 테스트는 인증된 출처의 입력을 통해 시스템의 액세스 가능 여부를 확인합니다. 이를 위해 테스트 시스템은 암호화 키와 카운터를 생성할 수 있는 기능뿐만 아니라 암호 해독 중에 해독된 암호를 해석할 수 있는 메커니즘을 제공합니다.

테스트를 통해 개별 ECU 또는 여러 개가 상호연결된 ECU의 반응을 기반으로 차량 IT 시스템의 취약성을 체계적으로 탐지할 수 있습니다. 이론적으로 거의 무한한 수의 테스트 벡터가 존재하기 때문에 실제로는 테스트 케이스를 제한해야 합니다. 따라서 이타스와 에스크립트는 시뮬레이션 및 테스트 툴 제공과 더불어 테스트 계획 준비와 LABCAR 테스트 환경 구성을 지원합니다. 또한 통합적인 보안 테스트를 위해서는 ECU 액세스 관련 이타스의 XiL 기술 및 툴 (예를 들어, ETK)이 전제되어야 합니다. 이를 통해 테스터는 테스트 대상 ECU의 메모리 및 내부 데이터를 처리할 수 있는 시간 동기식 전체 액세스 권한을 가지며 PEN, fuzz, MAC 테스트가 실행되는 동안 기능 및 프로세스를 정확하게 추적할 수 있습니다. 이러한 실시간 메커니즘과 확장된 모니터링 기능으로 필요한 분석의 범위와 깊이만큼 분석을 수행할 수 있습니다.

## 요약

이타스와 에스크립트는 수년간 자동차 보안 및 XiL 기반 테스트 분야에서 전문성을 갖춰왔으며, 최근에는 이 역량들을 접목하여 ECU 네트워크를 통합적으로 보호하는 솔루션을 개발하고 있습니다. 적절한 보안 테스트 절차가 더해진 XiL 시스템은 보안 메커니즘을 확인하고 보안 취약성을 탐지하는 데 매우 적합하기 때문에 향후 안전한 커넥티드카 구현에 중요한 역할을 할 것으로 기대됩니다.

ON THE NEXT PAGE YOU WILL FIND OUT WHAT POSSIBILITIES THE ESCRYPT TESTING LABORATORY OFFERS.