Embedded-Security-Tests im virtuellen Fahrzeug

Umfassende Angriffssimulationen mittels XiL-Testumgebung

Moderne softwaregesteuerte Fahrzeugsysteme müssen nicht mehr nur funktional sicher sein, sie brauchen auch Schutz gegen Angriffe von Cyberkriminellen. Um testen zu können, ob angegriffene Steuergeräte im Kontext des Gesamtfahrzeugs sicher bleiben, setzen ETAS und ESCRYPT auf Virtualisierung. Die Vorteile der XiL*-Technologie werden so auch für Security-Tests nutzbar.

AUTOREN

Jürgen Crepin ist Senior Expert Marketingkommunikation bei der **ETAS GmbH**.

Dr.-Ing. Tobias Kreuzinger ist Senior Manager Test and Validation bei der **ETAS Inc.** in Ann Arbor, Michigan, USA.

Ein Albtraum: Hacker verschaffen sich Zugriff aufs Fahrzeugsystem, fangen Sensorsignale ab, speisen stattdessen korrumpierte Daten in Steuergeräteschnittstellen ein. Aus heiterem Himmel wäre der Fahrer machtlos, säße im fremdgesteuerten Fahrzeug. Damit solche Szenarien fiktional bleiben, sind verlässliche Security-Lösungen gefragt.

Doch lassen sich Hackerangriffe testen? Oder präziser: Lässt sich der Nachweis führen, dass Security-Maßnahmen Fahrzeugsysteme zuverlässig abschirmen? Im Bereich der funktionalen Sicherheit sind Hardware-in-the-Loop-(HiL-)Systeme etabliert, um nachzuweisen, dass Funktionen im Normalbetrieb und bei Störungen wie geplant reagieren. Dabei testen Entwickler die Software sowie die Interaktion verteilter Sensorsysteme und Fahrzeugdomänen in Simulationen ganzer Fahrzeuge inklusive aller Steuergeräte und Datennetze. Echtzeit-HiL-Systeme wie ETAS LABCAR, die Co-Simulationslösung ETAS COSYM oder virtuelle, per ETAS ISOLAR-EVE erzeugte Steuergeräte bieten dafür die technologische Basis.

Neue Option: Security-in-the-Loop

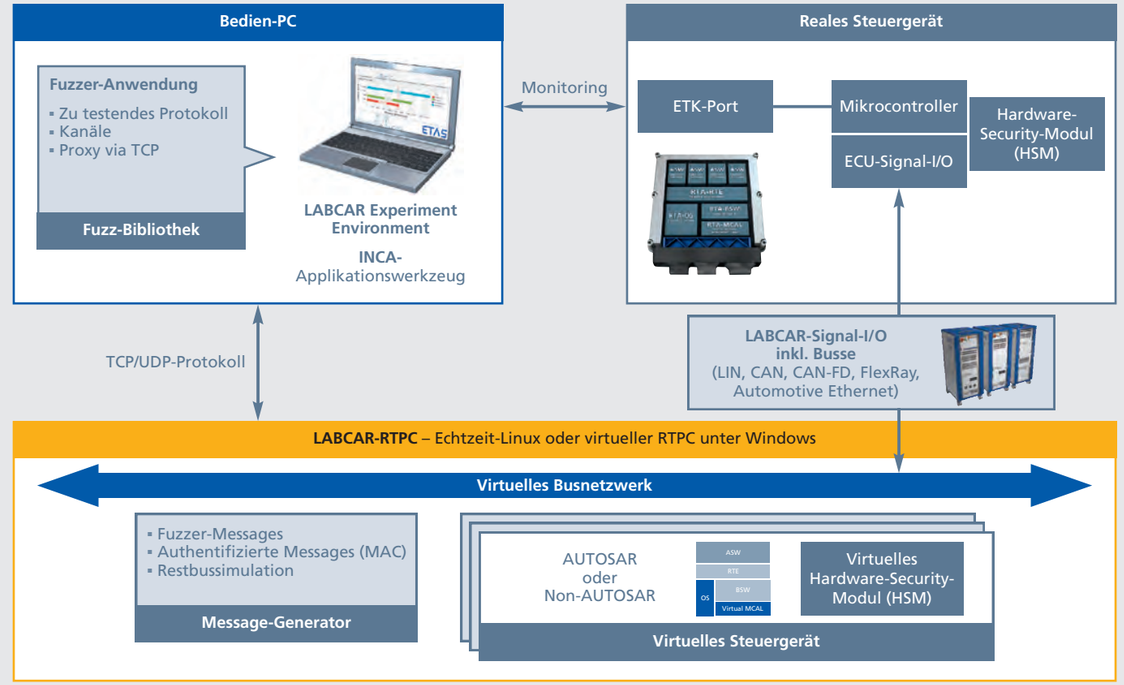
Für Security-Tests ist die True-Positive-Methode, also das Abprüfen eines erwarteten Verhaltens, wenig effektiv, da die Angriffsszenarien zum Zeitpunkt der Entwicklung in der Regel unbekannt sind bzw. bekannte Sicherheitslücken direkt geschlossen werden. Stattdessen gilt es, die Suche nach Schwachstellen zu systematisieren. Auch dafür eignen sich Software-in-the-Loop-(SiL-) oder HiL-Testumgebungen.

Die Herausforderung hierbei besteht darin, Kompetenzen aus unterschiedlichen Domänen zu vereinen: Security-Experten müssen sich mit der XiL-Test-Methodik und XiL-Testingenieure mit Methoden aus dem traditionellen IT-Umfeld vertraut machen, die nun zur Identifikation potenzieller Schwachstellen im eingebetteten System genutzt werden. Da hierbei vor allem sicherheitsrelevante Fahrzeugfunktionen im Fokus stehen, müssen derartige Security-Tests von Anfang an konsequent geplant und effizient ausgeführt werden.

ETAS und ESCRYPT haben diese Herausforderung früh erkannt und ihr Know-how aus den Bereichen Safety, XiL-Verfahren sowie Automotive Security zusammengeführt. Das Ergebnis ist eine Lösung, die das Beste beider Welten verbindet (siehe Grafik). Ein virtuelles Testfeld auf Basis der LABCAR-Hardware, dem Linux-basierten Simulationstarget LABCAR-RTPC (Real-Time-PC) und der virtuellen Steuergeräte-Lösung ISOLAR-EVE ermöglicht es, Angriffe auf einzelne Steuergeräteschnittstellen sowie Manipulationsversuche an Steuergerätefunktionen im Kontext des Gesamtfahrzeugs zu simulieren.

LABCAR für Security-Tests

Während ETAS für das Testsystem verantwortlich ist, bringt ESCRYPT die Security-Expertise bei der Auswahl sinnvoller Testverfahren ein – beispielsweise:



Prinzipieller Aufbau eines Security-Testsystems.

▪ **Penetration-(PEN-)Testing**, bei dem der Tester versuchen, das Verhalten von Steuergeräten von außen (zum Teil auch durch mechanischen Eingriff) zu verändern, unbefugt Daten auszulesen oder das eingebettete System zu beschädigen. Das teilautomatisierte „PEN-Testing-in-the-Loop" von ETAS und ESCRYPT nutzt für optimale Testabdeckung eine Angriffsbibliothek, die durch Erfahrungen aus ESCRYPT Consulting-Projekten kontinuierlich erweitert wird.

▪ **Fuzz-Testing**, bei dem eine Testsoftware – der „Fuzzer" – automatisiert zufällige Inhalte („Dumb Fuzzing") oder gezielt manipulierte Befehle und Signale generiert, mit denen er Steuergeräte-Ports flutet. Um Einbruchsversuche oder Manipulationen durch Hacker zu simulieren, fließt in der Regel für effizienteres Testen Wissen über das Protokoll, das Softwaresystem und die Krypto-Absicherung getesteter Steuergeräte in die Signalgenerierung mit ein.

▪ **Message-Authentification-(MAC-)Testing**, mit dem geprüft wird, ob wirklich nur unveränderte Botschaften von befugten Absendern Eingang in die Systeme finden. Dafür bietet das Testsystem die Möglichkeit zur Generierung kryptografischer Schlüssel und Zähler sowie Mechanismen für deren Interpretation im Rahmen der Decodierung. Anhand der Reaktionen einzelner und mehrerer Steuergeräte im Verbund lassen sich mit den Tests Schwachstellen in der Fahrzeug-IT systematisch aufdecken. Theoretisch gibt es eine nahezu unendliche Zahl an Testvektoren. Darum gilt es, Testfälle sinnvoll einzugrenzen. ETAS und ESCRYPT belassen es genau deshalb nicht bei der Bereitstellung von Simulations- und Testwerkzeugen – sondern bieten kompetente Beratung beim Erstellen der Testpläne und Konfigurieren der LABCAR-Testumgebung.

Die XiL-Technologie und Werkzeuge für Steuergerätezugriff (zum Beispiel ETK) von ETAS sind die Voraussetzung für umfassende Security-Tests: Tester haben vollen, zeitsynchronen Zugriff auf Speicher und interne Datenverarbeitung getesteter Steuergeräte und können deren Funktionen und Prozesse im Zuge der PEN-, Fuzz- und MAC-Tests exakt nachvollziehen. Erst diese Echtzeitmechanismen und erweiterten Monitoring-Funktionen ermöglichen Analysen in der nötigen Breite und Tiefe.

Fazit

ETAS und ESCRYPT haben über viele Jahre hinweg Kompetenzen in den Bereichen Automotive Security und XiL-basiertes Testen aufgebaut. Diese Kompetenzen wachsen nun zusammen, um Steuergeräte-Netzwerke rundum abzusichern. Bei Verwendung sinnvoller Testverfahren sind XiL-Systeme bestens geeignet, um Security-Mechanismen zu verifizieren und Sicherheitslücken aufzudecken. Damit ist ein weiterer wichtiger Schritt auf dem Weg zum sicher vernetzten Fahrzeug der Zukunft getan.

Welche Möglichkeiten das Testing-Labor von ESCRYPT bietet, erfahren Sie auf der nächsten Seite.

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