Prof. Dr. Stefan Katzenbeisser
Dekan des Fachbereichs Informatik,
Technische Universität Darmstadt

© E. Bosselmann | CYSEC

Autonome Fahrzeuge – aber sicher!

Blockierende Bremsen auf der Autobahn, bösartige Eingriffe in die Bordelektronik, Fernsteuerung von Fahrzeugen durch Hacker, falsche Anzeigen im Cockpit – ein Albtraum für Fahrer und Ingenieure. Trotzdem Szenarien, die nicht völlig unrealistisch sind. Sicherheitsforscher haben in der Vergangenheit mehrfach unter Laborbedingungen demonstriert, dass moderne Fahrzeuge – auch aus der Ferne – durch Hackerangriffe manipulierbar sind. Auch wenn bisher noch keine tatsächlichen Angriffe publik wurden, sollten Hersteller und Zulieferer das Problem ernst nehmen. Sobald Angriffswege und -werkzeuge bekannt sind, ist es nur eine Frage der Zeit, bis sie auch genutzt werden.

Hackerangriffe stellen insbesondere für autonome Fahrzeuge eine enorme Herausforderung dar: Sie sind vernetzt und immer erreichbar, enthalten umfangreiche Rechnersysteme, deren Komplexität die Wahrung der IT-Sicherheit zur echten Herausforderung macht, und nehmen ihr Umfeld über potenziell verwundbare Sensoren wahr. Autonome Fahrzeuge werden Teil der kritischen Infrastruktur „Transport und Verkehr“ und somit lohnende Ziele für verschiedene Typen von Angreifern sein, etwa für den einsamen Hacker, der die Welt mit seinen Fähigkeiten beeindrucken will, für kriminelle Gruppen, die analog zu den bekannten Ransomware-Angriffen Lösegeld erpressen wollen, oder für staatliche Akteure im Fall zwischenstaatlicher Konflikte.

Systeme, bei deren Entwurf nicht von Anfang an Aspekte der IT-Sicherheit berücksichtigt wurden, können nicht sicher sein. Die Nachrüstung von IT-Sicherheit ist teuer, aufwendig und komplex. Zudem existieren vielfältige Abhängigkeiten zwischen der funktionalen Sicherheit sowie der IT-Sicherheit: Intelligente Angreifer können in der Lage sein, die in einem Sicherheitsnachweis getroffenen probabilistischen Annahmen zu umgehen. IT-Sicherheit muss daher im Fahrzeug immer mitbedacht werden – frei nach dem Motto „If it is not secure, it is not safe“.

Bei der Entwicklung eines neuen Produkts sollte daher ein Security-Engineering-Prozess durchlaufen werden: Man betrachtet zuerst alle „Assets“ sowie die zu erwartenden Angreifer und bewertet diese entsprechend ihrer Kritikalität. Im Zuge eines Risikomanagements entscheidet man daraufhin, gegen welche Angreifer man sich schützen kann beziehungsweise will und gegen welche nicht. Letzteres muss dokumentiert werden. Hieraus leitet man technische Schutzverfahren ab, die Hand in Hand mit Managementprozessen die IT-Sicherheit gewährleisten. Im Gegensatz zur funktionalen Sicherheit sollte dieser Security-Engineering-Prozess während der Produktlebenszeit periodisch wiederholt werden, da Angriffsmethoden, -ziele und -werkzeuge einem steten Wandel unterliegen. Dies erfordert Ressourcen, sichert aber auch langfristig den Erfolg. Nehmen wir die Herausforderung an!