Erweiterung der AUTOSAR Security Architektur um Erkennungs- und Gegenmaßnahmen hinsichtlich relevanter Angriffsszenarien im Bereich Automotive Ethernet

Tobias Finke*, Dominik Schoop, Harald Melcher

Fakultät Informationstechnik der Hochschule Esslingen – University of Applied Sciences

Wintersemester 2014/2015

Heutzutage befindet sich in einem modernen Fahrzeug eine Vielzahl an Steuergeräten, die miteinander Informationen austauschen müssen. Durch die stetig wachsende Komplexität steigen auch die spezifischen Anforderungen an die Netzinfrastruktur im Fahrzeug. Deshalb haben sich neben dem gängigen CAN-Bus weitere Bus-Systeme wie beispielsweise FlexRay, MOST und LIN im Fahrzeug etabliert. Immer mehr Verbreitung im Fahrzeug findet in letzter Zeit auch Ethernet.

Ethernet bietet durch hohe Datenraten und einfache Erweiterbarkeit für neue Protokolle einige Vorteile gegenüber bestehenden Bussystemen, weshalb es bei vielen aktuellen Neuentwicklungen in der Automobilbranche als Basistechnologie verwendet wird.

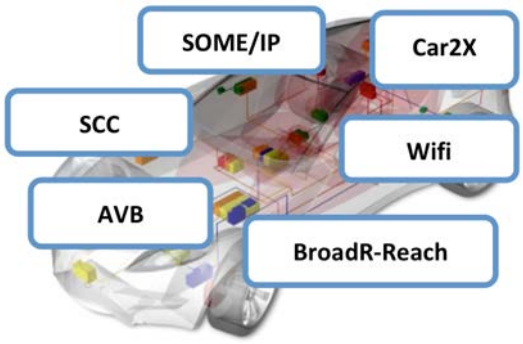

Abbildung 1: Verwendung von Ethernet im Automobilbereich

Die Verwendung von Ethernet stellt den Automobilhersteller und seine Zulieferer aber vor die große Herausforderung, ihre Systeme vor Hackerangriffen zu schützen, die im PC-Umfeld seit Jahren praktiziert werden.

Im Rahmen dieser Arbeit wird eine Analyse bestehender Bedrohungen durchgeführt. Anhand der Ergebnisse dieser Analyse kann eine Bewertung durchgeführt werden, die dann zu konkreten Designvorschlägen für die AUTOSAR- bzw. die MICROSAR-Architektur der Firma Vector Informatik GmbH führen soll.

Das Hauptaugenmerk liegt hier bei Angriffen auf Protokollebene. Umleitung von Netzwerkverkehr mittels ARP-Spoofing, Fälschen von Absenderadressen mittels IP-Spoofing oder auch DoS-Angriffe, die Steuergeräte lahmlegen können, sind einige Beispiele.

Einen Großteil der Betrachtungen nimmt das IPv6-Protokoll ein. Hier sind vor allem beim Neighbor Discovery Protocol (NDP) viele Angriffsvektoren zu finden [1], welche ohne größeren Aufwand ausnutzbar sind. Im Internet Control Message Protocol for IPv6 (ICMPv6) sind Funktionalitäten wie ARP direkt integriert. Informationen für das Zuweisen einer IPv6-Adresse oder über welchen Weg ein Steuergerät seine Daten schicken soll, werden ungeschützt auf dem Netzwerk übertragen. Einem Angreifer ist es theoretisch leicht möglich, sich als Router auszugeben und den Netzwerkverkehr über sich umzuleiten, mitzulesen und zu verändern. Firewalls und Intrusion-Detection-Systems (IDS) können, vor allem in Anbetracht der benötigten Rechenkapazitäten, nur bedingt vor solchen Angriffen schützen, weshalb sich hier Protokollerweiterungen wie Secure Neighbor Discovery (SEND) [2] in Kombination mit Cryptographically Generated Address (CGA) [3] als Lösung anbieten.

*Diese Arbeit wurde durchgeführt bei der Firma Vector Informatik GmbH, Weilimdorf

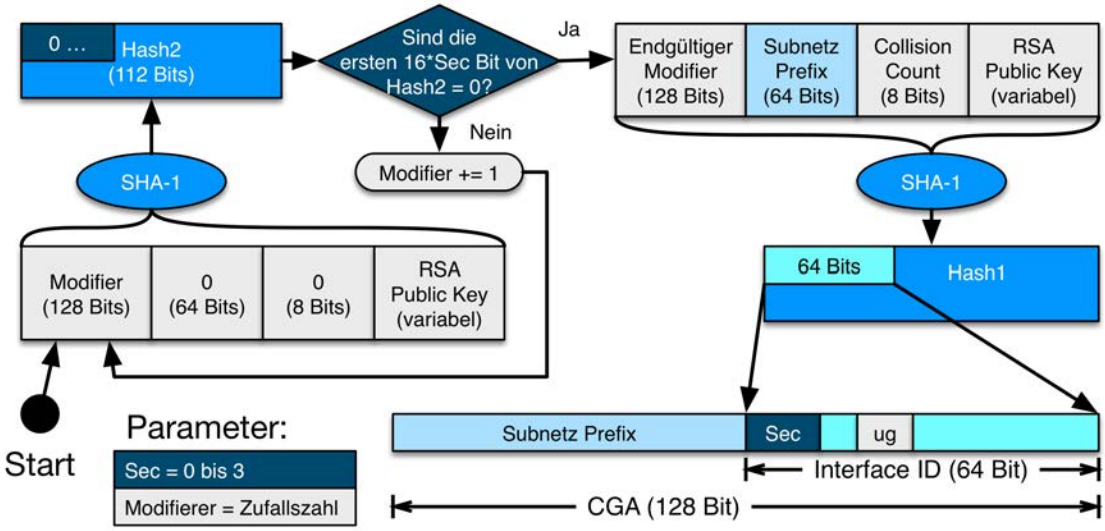

Abbildung 2: Generierung einer CGA (Kryptografisch generierte IPv6-Adresse)

Durch die Verwendung der Mechanismen von SEND und CGA kann sich ein Steuergerät, mit einem RSA-Schlüsselpaar und einem von einem Router erhaltenen Subnetz-Präfix, eine IPv6-Adresse über ein Kryptografisches Verfahren generieren (siehe Abbildung 2). Das CGA-Verfahren und die darin verwendeten Algorithmen werden in der Arbeit genauer betrachtet und auf die Tauglichkeit für Steuergeräte untersucht.

ICMPv6-Nachrichten, können mit dem privaten Schlüssel des Steuergerätes durch eine Signatur unterschrieben werden. Ein Kommunikationsteilnehmer auf der anderen Seite kann somit sein empfangenes Paket auf folgende Bedingungen überprüfen:

1. Passt die CGA (IP des Senders) zum mitgeschickten öffentlichen Schlüssel und den CGA-Parametern?
2. Gehört die Signatur zum mitgeschickten öffentlichen Schlüssel?
3. Ist der Inhalt der Nachricht unverändert?

Des Weiteren ist es mit SEND und eines erweiterten X.509v3-Zertifikats möglich, Router zu zertifizieren. Diese können dann ihre Identität gegenüber einem Steuergerät beweisen und nachweisen, dass sie für den entsprechenden Adressbereich zuständig sind und sich beim Steuergerät als Standard-Route für den Netzwerkverkehr eintragen dürfen. Das Prinzip der Public Key Infrastructure (PKI) findet man auch im Internet beim HTTPS-Protokoll. Hier bestätigt ein Server seine Identität einem Webseitenbesucher mittels eines Zertifikats, welches der Besucher überprüfen kann.

Für einen Angreifer ist es durch SEND nicht mehr möglich, eine Adresse zu übernehmen, sich für ein anderes Steuergerät oder einen anderen Router auszugeben und gefälschte Nachrichten zu verschicken. Beim Aufbau der Verbindungsstrukturen in lokalen Netzwerken kann somit Authentizität und Integrität durch ICMPv6 in Verbindung mit SEND und CGA sichergestellt werden.

[1] Minoli, Kouns 2008 Security in an IPv6 Environment
[2] Secure Neighbor Discovery (RFC3971)
[3] Cryptographically Generated Addresses (RFC3972)

Bildquellen:

- Abbildung 1: Vector Informatik
- Abbildung 2: Hasso Plattner Institut