ANGRIFFSSZENARIEN AUF V2G-SYSTEME

Netzsicherheit für intelligente **Ladesysteme**

Die V2G-Kommunikation umfasst die wechselseitige Kommunikation zwischen dem Elektrofahrzeug, der Versorgungseinrichtung bzw. Ladestation und dem Netz. Daher gibt es eine wachsende Sorge über die Sicherheit des Ladevorgangs bei Elektrofahrzeugen. In diesem Artikel werden zwei Hauptarten von Angriffen vorgestellt – der Denial-of-Service (DoS)-Angriff und der Man-in-the-Middle (MITM)-Sniffing-Angriff auf eine V2G-Installation.

In Vehicle-to-Grid-Systemen (V2G) ist der Datenaustausch zwischen Elektrofahrzeug und Versorgungseinrichtung essentiell, um die Anforderungen an das Laden des Fahrzeugs zu erfüllen. Diese Kommunikation muss vor Cyber-Angriffen geschützt werden. Die Vertraulichkeit der Datenübertragung zwischen Elektrofahrzeug und Versorgungseinrichtung muss gewahrt bleiben und die Identität von Fahrzeug und Einrichtung während der Kommunikation sichergestellt sein. Wenn die Versorgungseinrichtung das Elektrofahrzeug falsch identifiziert oder Ladeinformationen aus einer Malware-Quelle erhält, werden die Ladeanforderungen des Fahrzeugs möglicherweise nicht erfüllt. Die Aufrechterhaltung der Datenintegrität zwischen Elektrofahrzeug und Versorgungseinrichtung ist mit größtmöglicher Sorgfalt sicherzustellen. Datenkommunikation ist ein wesentlicher Bestandteil des V2G-Systems. Ihre Verfügbarkeit muss daher gewährleistet sein.

Die oben erwähnten Sicherheitsanforderungen wurden in verschiedenen Normen für V2G-Kommunikation berücksichtigt. Es gibt jedoch kein vollständig sicheres System, und jedes System muss ständig auf Schwachstellen überprüft werden. Die Durchführung von Sicherheitskontrollen während des Entwicklungszyklus reduziert das Risiko von Cyber-Angriffen.

© Glenn Price 2013

Integration von Netzsicherheitsprozessen in die V2G-Entwicklung

Es ist sehr wichtig, Netzsicherheitskontrollen und -prozesse in jede Phase des Entwicklungszyklus einzubeziehen. Die obige Abbildung zeigt das entsprechende V-Modell. Der Entwicklungsprozess beginnt immer mit der Analyse von Anforderungen und Architekturen, gefolgt von der Entwurfsphase. Während dieser Phase ist der Prozess der Sicherheitsanalyse durchzuführen. Der Vorteil der Durchführung einer Sicherheitsbewertung in diesen Phasen besteht darin, dass alle Sicherheitsanforderungen in Bezug auf Hardware, Software und Ressourcen zu Beginn des Prozesses bekannt sind und somit künftige Nacharbeitskosten minimiert werden. Während der Implementierungs- und Integrationsphase sind alle in der Sicherheitsbewertungsphase vorgeschlagenen Sicherheitsanforderungen umzusetzen. Unbekannte Schwachpunkte sind per Fuzzing zu ermitteln. Penetrationstests können nach der Implementierungs- und Integrationsphase durchgeführt werden, um die Ergebnisse der Sicherheitsbewertung zu überprüfen.

Gestaltung des Angriffsvektors

In diesem Artikel werden zwei Hauptarten von Angriffen vorgestellt – der Deni-

© Carl Hanser Verlag, München

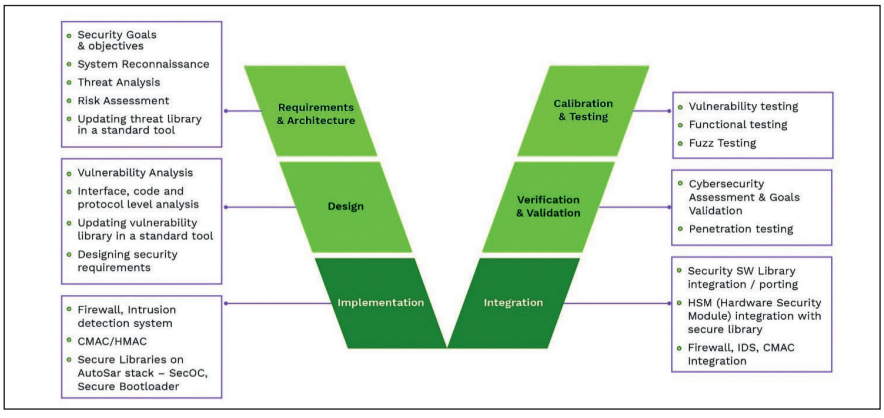


Bild 1: V-Modell der automobilen Netzsicherheit. © KPIT Technologies

al-of-Service (DoS)-Angriff und der Man-in-the-Middle (MITM)-Sniffing-Angriff auf eine V2G-Installation. Dazu werden folgende Voraussetzungen definiert:

- Der angreifende Knoten, das Elektrofahrzeug und die Ladestation befinden sich im gleichen Netzwerk.
- Der angreifende Knoten hat ein Linux-basiertes Betriebssystem.
- Der angreifende Knoten hat Privilegien zum Einholen von IP- und MAC-Adressen des Elektrofahrzeugs und der Ladestation.
- Das Laden erfolgt im externen Identifikationsmodus.

Für dieses Experiment wurde ein Open Source-V2G-Stack bereitgestellt, und es wurden 2 Mikrocontroller ausgewählt, der eine zur Simulation eines Elektrofahrzeugs und der andere zur Simulation einer Versorgungseinrichtung.

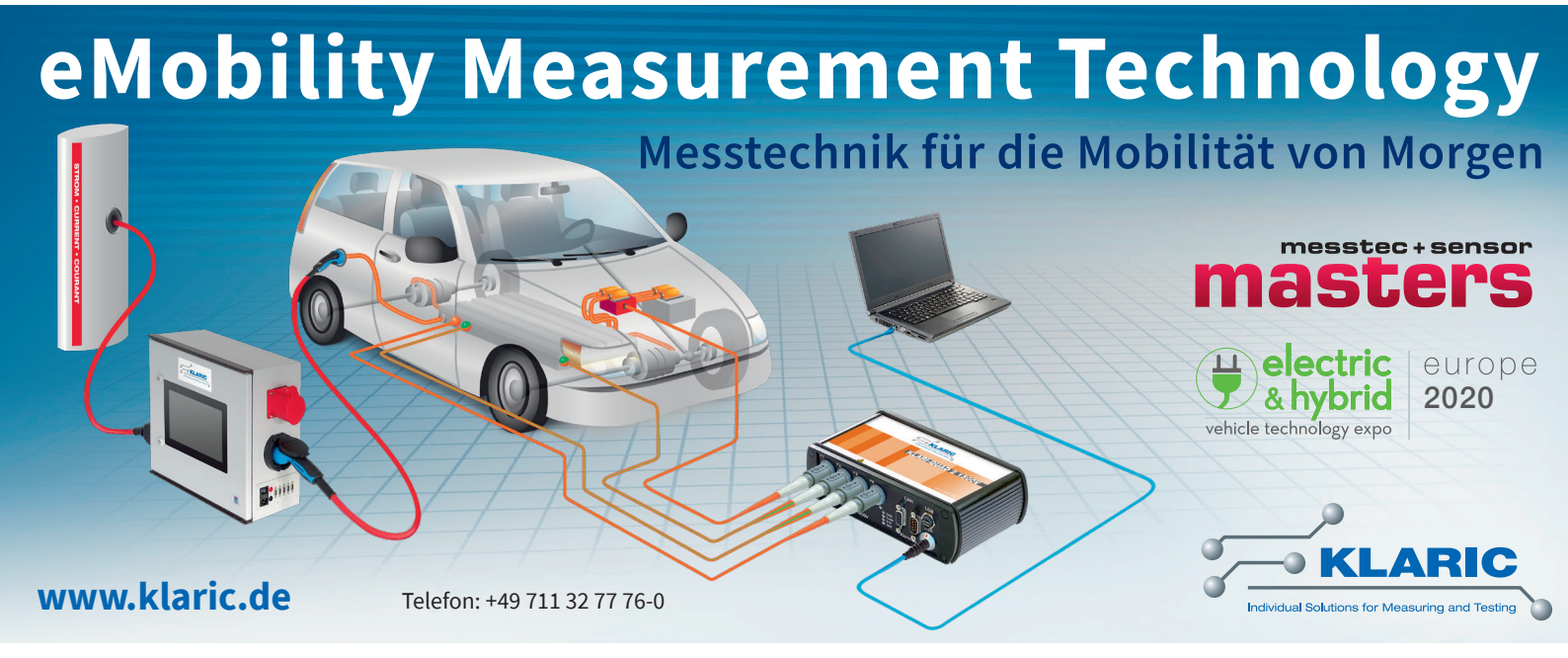
Die beiden Mikrocontroller wurden über Ethernet-Kabel mit einem Router verbunden. Als nächstes wurde ein geeignetes Tool zur Überwachung des Netzwerkverkehrs und ein Python-basiertes Tool ausgewählt, das den Netzwerkverkehr manipulieren kann. Desweiteren wurden entsprechende Konfigurationen am angreifenden Knoten zur Durchführung der Angriffe vorgenommen. Anschließend wurde der angreifende Knoten in das gleiche Netzwerk wie das Elektrofahrzeug und die Versorgungseinrichtung eingebracht.

Die V2G-Kommunikation in dieser Installation ist Ethernet-gestützt und die Kommunikation zwischen Elektrofahrzeug und Versorgungseinrichtung IP-basiert. Die Experten von KPIT Technologies haben sich daher auf die IPv6– und ICMP-Protokolle konzentriert, um Schwachstellen auf der Protokollebene festzustellen und den MITM-Sniffing-Angriff und den DOS-Angriff aufzubauen

Man–in-the-Middle-Sniffing-Angriff

Ein Man-in-the-Middle-Angriff ist eine Art Lauschangriff, bei dem die Kommunikation zwischen zwei Benutzern von einer unberechtigten Partei überwacht und/oder modifiziert wird. Dabei scheinen die berechtigten Parteien normal zu kommunizieren. Der Sender erkennt nicht, dass der Empfänger ein Angreifer oder eine unbefugte Partei ist, die versucht, auf die Nachricht zuzugreifen oder sie zu verändern, bevor sie an den vorgesehenen Empfänger weitergesendet wird. Durchgeführt wurde ein Man-in-the-Middle-Sniffing-Angriff, bei dem der Datenverkehr zwischen dem Elektrofahrzeug und der Ladestation abgefangen wurde. Der MITM-Sniffing-Angriff erfolgte über einen Nachbar-Cache unter Anwendung von Neighbor Solicitation und Neighbor Advertisement.

- Der angreifende Knoten sendet ein Neighbor Solicitation-Paket an das Elektrofahrzeug und gibt sich dabei als Ladestation aus, indem er die IP-Adresse der Ladestation nutzt, wie in Bild 2 gezeigt,
- Das Elektrofahrzeug sieht die Solicitation-Nachricht von der Ladestation kommen (die tatsächlich aber vom angreifenden Knoten stammt). Der Angreifer sendet seine eigene MAC-Adresse in der Quellverknüpfungsschicht in einer Neighbor Solicitation-Nachricht an das Elektrofahrzeug. Dies macht das Elektrofahrzeug glauben, dass es sich um die MAC-Adresse der Ladestation handelt, weshalb das Fahrzeug seinen Cache mit dieser MAC aktualisiert.
- Daher läuft der Datenverkehr vom Elektrofahrzeug zur Ladestation über den angreifenden Knoten, wie in Bild



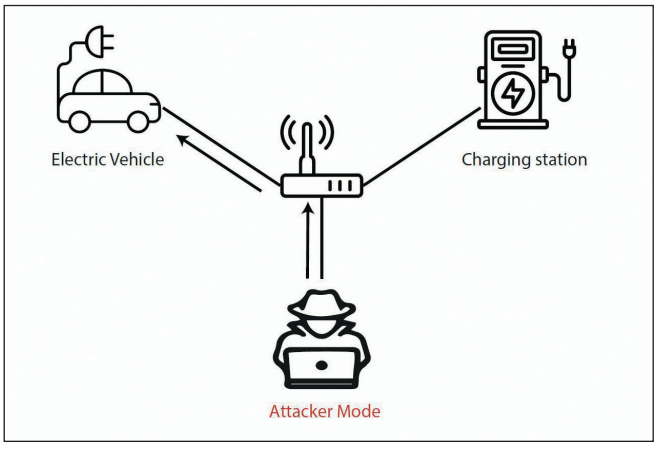


Bild 2: Angreifer sendet eine Unicast-Neighbor Advertisement an den EVCC. © KPIT Technologies

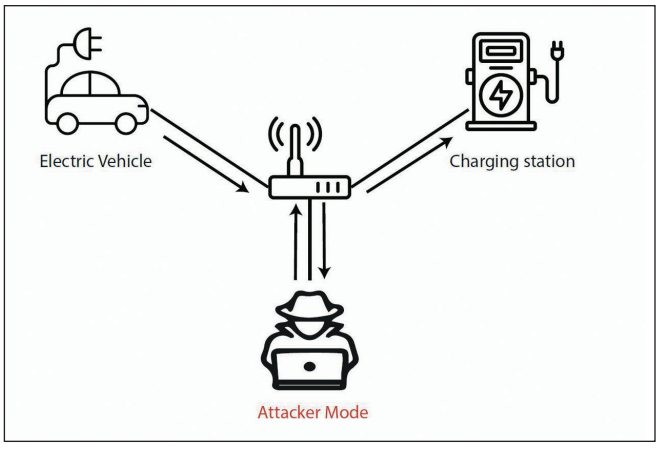


Bild 3: IPv6 Verkehrsfluss-Man-in-the-Middle-Sniffing. © KPIT Technologies

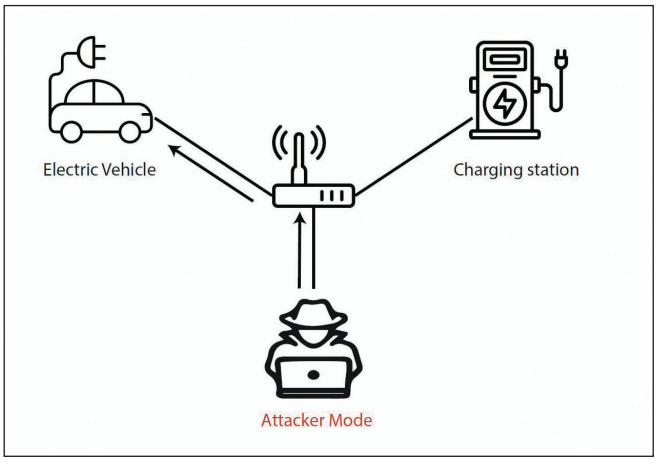


Bild 4: Angreifer sendet eine Unicast-Neighbor-Advertisement an den EVCC. © KPIT Technologies

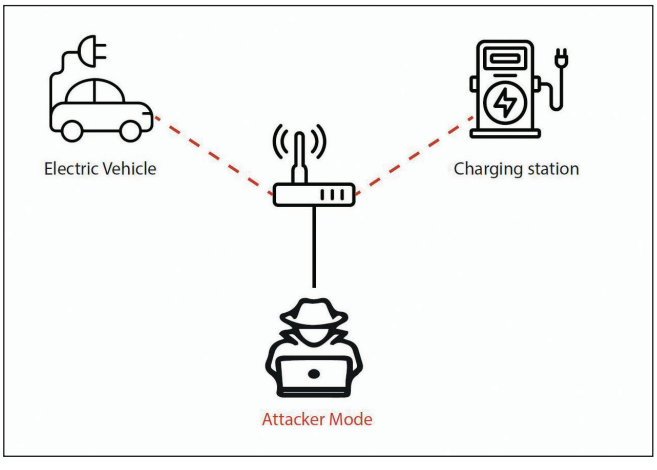


Bild 5: IPv6 Verkehrsfluss-Man-in-the-Middle-Sniffing. © KPIT Technologies

3 gezeigt. Am angreifenden Knoten wurde der Traffic mit einem Netzwerküberwachungs-Tool beobachtet. Diese Nachrichten wurden überwacht, um eine geeignete Nachricht/Phase in der Kommunikation zu finden, die sich für einen weiteren Angriff nutzen lässt.

Denial-of-Service-Angriff

Ein Denial-of-Service-Angriff ist ein Sicherheitsereignis, bei dem ein Angreifer einen legitimen Anwender davon abhält, Dienste zu nutzen. Der hier durchgeführte DoS-Angriff hat verhindert, dass der Kunde das Elektrofahrzeug auflädt. Auf der Grundlage von ausführlichen Analyse während der MITM-Paketüberwachung wurden die folgenden Änderungen am MITM-Sniffing-Angriffsskript vorgenommen.

- Zur Durchführung der DoS-Attacke wurde eine ungültige MAC-Adresse (im Netzwerk nicht verwendet) in der Neighbor Solicitation-Nachricht gesendet, wie in Bild 4 gezeigt.
- Daher hat die Nachricht ein ungültiges Ziel oder kein Ziel im Netzwerk, sodass Nachrichten vom Elektrofahrzeug die Ladestation nicht erreichen können. Bild 5 zeigt die Auswirkungen eines DoS-Angriffs auf den Kommunikationsfluss während des Ladevorgangs.

Fazit

Wenn alle Sicherheitskontrollen am beschriebenen Versuchsaufbau durchgeführt wurden, lässt sich die Anfälligkeit durch eine Sicherheitsbewertung in der Entwurfsphase (in diesem Fall am Versuchsaufbau) feststellen und in der Penetrationstestphase validieren. Bei KPIT wurde ein kompletter Prozess eingerichtet, um verschiedene Sicherheitskontrollen in unterschiedlichen Stadien der Systementwicklung einzubeziehen. Diese Sicherheitsmaßnahmen schließen Sicherheitsbewertung, Penetrationstests, Fuzzing und HSM-basierte Sicherheitsdienste in den Entwicklungszyklus der Automobilsysteme und der Fahrzeugkommunikation einschließlich V2V, V2I und V2G ein. ■ (oe)

www.kpit.com

Nalanda Joshi ist Softwareingenieurin für automobile Netzsicherheit bei KPIT Technologies.

Ajey Gotkhindikar ist Fachexperte für automobile Netzsicherheit bei
KPIT Technologies.

© Carl Hanser Verlag, München