© 123RF.com/lightwise

Sicheres Update von Automotive-Software

Automatische Updates der On-Board-Software unserer Autos stellen die Forderung nach höchster Datensicherheit, genauer gesagt nach der Security. Die Bandbreite nicht erwünschter Manipulationen des Steuergerätenetzwerks eines Fahrzeugs reicht vom Einspielen gefälschter Updates über die Nutzung der Update-Schnittstelle als Einfallstor bis hin zu Hardware-Angriffen. Es gibt unterschiedliche Ansätze, um diesen Risiken entgegenzuwirken. In dem von dem BMBF geförderten Forschungsprojekt SIBASE (Sicherheitsbaukasten für sichere eingebettete Systeme) wurde ein Sicherheitsbaukasten für die Absicherung von eingebetteten Systemen geschaffen. Der SIBASE Automotive Demonstrator wendet diesen Sicherheitsbaukasten im Bereich Automotive an und demonstriert einen Gesamtprozess für ein sicheres Update.

Die Notwendigkeit von Software-Updates ist auch im Bereich Automotive durch zwei Tatsachen gegeben: Zum einen befinden sich die in Software gefassten Funktionalitäten in steter Weiterentwicklung. Zum anderen aber ist Software erfahrungsgemäß selbst nach intensivem Test immer mit einer gewissen Restfehlerrate behaftet. Diese Restfehler können unter im Test nicht verwirklichten Umständen zutage treten und ein Softwareupdate erforderlich machen. Um überflüssige Werkstattfahrten zu vermeiden, sollen solche Updates per Fernwartung durchgeführt werden. Daraus ergibt sich die Notwendigkeit für höchstmögliche Security, um möglichst unerwünschte Manipulationen ausschließen zu können und mit dem Software-Update kein neues Einfallstor für Angreifer zu schaffen. Ein mehrstufiger Update-Prozess sorgt für die geforderte Sicherheit.

Wenn im Folgenden das Adjektiv „sicher" verwendet wird, ist stets „sicher im Sinne von Security" gemeint, falls nichts anderes angegeben.

Zur Realisierung dieses Prozesses sind methodisch zwei Schritte notwendig. Zunächst müssen die aus der IT bekannten sicheren, aber auch umfangreichen Sicherheitsverfahren korrekt auf das Anwendungsfeld Automotive übertragen werden. Dabei muss die im Vergleich zu IT-Systemen geringere Leistung von eingebetteten Systemen berücksichtigt werden. Da es ohne Beeinträchtigung des Sicherheitsniveaus nicht ohne weiteres möglich ist, die Verfahren zu vereinfachen, wird dieses Problem stattdessen z. B. über eine geschickte Systempartitionierung gelöst. Im zweiten Schritt ist es notwendig, die einzelnen Stufen des Update-Vorgangs zu betrachten und sie in Hinsicht auf die spätere Umsetzbarkeit des Prozesses auf ein Massen-Update von Millionen von Fahrzeugen zu prüfen und entsprechend zu entwerfen.

i Public-Key-Infrastruktur (PKI)

Eine Public-Key-Infrastruktur ist ein Verfahren, um die Gültigkeit von x509-Zertifikaten festzustellen. Diese Zertifikate enthalten neben Gültigkeitszeitraum, Aussteller und Verwendungszweck vor allem einen öffentlichen Schlüssel, dessen Authentizität durch das Zertifikat bestätigt wird und dann kryptographisch verwendet werden darf. Damit das Zertifikat gültig ist, muss es von einer vertrauenswürdigen Entität unterschrieben werden. Wird diese Vertrauenswürdigkeit wiederum über ein Zertifikat gewährleistet, entsteht rekursiv eine Kette von Zertifikaten, die bis zu einem bekannten Stammzertifikat komplett nachvollzogen werden muss, um die Gültigkeit eines einzelnen Zertifikats zu ermitteln.

Der Prozess wurde an dem von Infineon und Mixed Mode gemeinschaftlich mit der Unterstützung eines Automotive-Beirats entwickelten SIBASE Automotive Demonstrator implementiert und getestet. In dem Demonstrator wird gezeigt, wie ein Steuergerät sicher aktualisiert werden kann, ohne dass das Steuergerät selbst den gesamten Prozess abbilden muss. Stattdessen erfolgt das Update im Verbund mit einem Bordcomputer, der vergleichsweise viel Leistung und Speicher bietet. Damit ist er in der Lage, die aufwendigen Security-Verfahren zu realisieren, die nötig sind, um das Auto nach außen hin zu schützen. Gleichzeitig bietet er für die Steuergeräte im Auto eine einfachere, aber dennoch sichere Update-Schnittstelle an. Die Sicherheitsfrage wird also innerhalb und außerhalb des Autos getrennt betrachtet.

Weiterhin wurde dem Prozess zugrundegelegt, dass alle Software-Komponenten, also auch die direkt am Update-Prozess beteiligten, Programmierfehler enthalten können und daher austauschbar sein müssen. Da das Update robust sein muss und ein unvollständiges Update nicht zu einen Ausfall führen darf, wurde das System so entworfen, dass der Update-Vorgang jederzeit neustartfähig ist, ohne dabei mehr Programmspeicher für SW-Redundanzen auf dem Steuergerät zu investieren, als unbedingt notwendig.

In dem Aufbau (Bild 1) wird für beide Geräte ein Infineon AURIX Mikrocontroller TC2xx verwendet, der sich aufgrund seines Einsatzgebiets Powertrain im Falle des Demonstrators für beide Anwendungsfälle eignet. Der Mikrocontroller verfügt über ein Hardware-Sicherheitsmodul (HSM), das eine Manipulation mit physikalischem Zugriff verhindert. Ein HSM ist ein zusätzliches Subsystem auf einem Chip, das mit einer eigenen Firmware aktiv agiert, vor Zugriffe des Hauptsystems geschützt ist und kryptographische Hardware zur Verfügung hat.

Datenvorbereitung

Ein sicheres Update beginnt bereits bei der Vorbereitung der Daten. Die neue Firmware soll zumindest kryptographisch signiert werden, bei höherer Sicherheitsanforderung auch verschlüsselt. Es kann notwendig sein, dass Firmware-Updates nicht nur einfach, sondern mehrfach verschlüsselt und signiert werden müssen, damit alle beteiligten Hersteller ihre IP-Rechte wahren können. Für die Signatur sollte eine Public-Key-Infrastruktur (PKI) eingesetzt werden, weil diese am besten mit vielen Update-Abnehmern (Fahrzeugen) skaliert. Die spätere Prüfung dieser PKI im Auto stellt das ressourcenaufwendigste Security-Verfahren dar. Gründe hierfür sind zum einen, dass umfangreiche x509-Zertifikate geprüft werden müssen, und zum anderen, dass Zwischenzertifikate einer Zertifikatskette womöglich erst aus dem Internet nachgeladen werden müssen (siehe Kastentext).

Auslösung des Updates

Zunächst wird der Bordcomputer des Fahrzeugs über das anstehende Update informiert. Beim SIBASE Automotive Demonstrator dient ein WLAN-Tablet als Update-Provider. Damit der Bordcomputer gefunden werden kann, muss er sich bei dem Update-Provider registrieren. Das Tablet sendet dem Bordcomputer eine Update-Liste, die die neue Software-Zusammensetzung des Steuergeräts inklusive der zugehörigen Daten zur Prüfung der Integrität beschreibt. Die Prüfdaten werden später beim sicheren Booten verwendet. Die Integrität und Authentizität der Liste ist über die PKI aus Schritt 1 abgesichert. Im Falle des Demonstrators handelt es sich bei diesem Schritt also um ein Zwangs-Update, da der Update-Provider direkt in das Auto eingreift. Da diese Stufe jedoch nicht zwangsläufig das sofortige Auslösen der Folgestufen mit sich zieht, ist es für den Fahrer keine Einschränkung, wenn er in diesem Schritt übergangen wird. Das zentrale Auslösen des Updates durch den Hersteller soll zu einer zügigen Verbreitung und somit zum schnellen Schließen von Sicherheitslücken beitragen.

Sicheres Herunterladen des Updates

Anschließend müssen die in der Update-Liste aufgeführten Updates heruntergeladen werden, was der Bordcomputer selbstständig erledigt. Anders als im vorhergehenden Schritt, wird nun also das Auto aktiv und der Update-Provider verhält sich passiv. Hintergrund ist »

die Berücksichtigung wechselnder Konnektivität und gegebenenfalls auch der Verbindungskosten. Hier ist es möglich, die Präferenzen des Fahrzeughalters mit einzubeziehen. Da die Downloads kryptographisch abgesichert sind, muss die Übertragung selbst nicht gesichert werden und die Software könnte auch von Drittanbietern (z. B. von Content Distribution Networks) geladen werden, was die IT-Kosten für den Hersteller reduzieren kann. Das Auto findet eine gültige Bezugsquelle wiederum über eine Anfrage bei zentralen Servern.

Die heruntergeladenen Updates werden auf dem Bordcomputer zunächst zwischengespeichert und weiterverarbeitet. Der Vorteil einer internen Zwischenspeicherung beruht auf der höheren Zuverlässigkeit des internen Kommunikationsnetzes: Während das Herunterladen aus dem Internet durch Funklöcher und Tiefgaragen verlangsamt oder aufgehalten werden kann, kann das eigentliche, zeitkritische Update der Steuergeräte zügig ausgeführt werden. Sollte der Bordcomputer bestimmte Updates nicht laden können, kann er dies dem Hersteller melden und im Extremfall auch dem Fahrer bekannt geben.

Ausführung des Updates

Nach vollständigem und erfolgreichem Download muss ein sicheres (im Sinne von Safety) Zeitfenster für das eigentliche Update gefunden werden. Dies könnte automatisch geschehen oder unter Einbezug des Fahrzeughalters. Im Demonstrator wird das Update vereinfacht sofort ausgelöst.

Über das interne Kommunikationsnetz versetzt der Bordcomputer alle Steuergeräte in einen Update-Modus. Hierbei speichert jedes Steuergerät den Update-Request sicher über sein HSM, das das Steuergerät im Update-Modus hält, bis das Update erfolgreich war, selbst wenn das Steuergerät zwischendurch wegen eines Fehlers neu gestartet wird.

Die eigentlichen Flash-Routinen des Steuergeräts sind nicht auf diesem selbst gespeichert, sondern werden stattdessen dynamisch zu Beginn des Updates vom Bordcomputer heruntergeladen, der wiederum als zentraler Speicher dient. Ziel dieser Umstrukturierung ist es, den benötigten zusätzlichen Flash jedes einzelnen Steuergeräts zu minimieren. Da ein Update-Fehlschlag über Update selbst repariert werden soll, muss das Gerät notwendige Update-Routinen in Redundanz speichern. Das Auslagern der Flash-Routinen erlaubt es, einen Großteil dieses Overheads zu vermeiden.

Bild 1: Auf dem SIBASE Automotive Demonstrator ist links das Steuergerät und rechts der Updatecomputer verbaut. In der Mitte hängt eine Visualisierungseinheit, die die On-Board-Kommunikation aufzeigt. Der Update-Computer ist über eine WLAN-Erweiterung an ein Windows-Tablet angebunden. (© Mixed Mode)

Die sichere Weiterleitung der Update-Daten wird durch die Security des Kommunikationsprozesses des HSM von jedem Kommunikationspartner gewährleistet. Dabei werden auf sichere Weise Schlüssel ausgetauscht, sodass von außen in diesen Vorgang nicht manipulativ eingegriffen werden kann. Zusätzlich wird die Authentifizierung durch die Zugangsdaten abgewickelt, die durch im Fahrzeug eingebauten Zertifikaten abgesichert sind. Weitere Sicherheitsverfahren, wie zum Beispiel die Entschlüsselung der Daten mit einem herstellerspezifischen Schlüssel, bleibt den Steuergeräten selbst überlassen.

Abschluss des Updates

Sobald die Installation der neuen Applikationen vollständig ist, informiert das Steuergerät das HSM, das die neuen Prüfdaten im seinem sicheren Speicherbereich ablegt, wodurch diese dem sicheren Boot zur Verfügung stehen. Sollte das Update unvollständig sein (z. B. durch eine kurzzeitige Unterbrechung der Versorgungsspannung), wird dies spätestens beim nächsten Booten festgestellt. In diesem Fall wird der Updatevorgang von dem HSM automatisch erneut eingeleitet. Der Update-Vorgang gilt als beendet, wenn von allen Steuergeräten eine Erfolgsmeldung beim Bordcomputer eingetroffen ist und dieser das Update für beendet erklärt.

Bewertung

Der im SIBASE Automotive Demonstrator vertretene Ansatz über den Einsatz eines zentralen Bordcomputer bietet eine Reihe entscheidender Vorteile.

So ist zum einen die zentrale Abwicklung der externen Security-Schnittstelle über ein leistungsstarkes System eine Möglichkeit, eine PKI zu realisieren, deren Aufwand für die Absicherung dezentral gestaltet ist. Während bei einer zentralen Lösung eine enorm hohe IT-Last entsteht, führt bei einer PKI der Bordcomputer jedes Fahrzeugs die kryptographischen Rechenoperationen der Absicherung für sich durch. Wenngleich dies für einzelne Steuer-

geräte eine untragbare Last bedeutet, ist es für Systeme mit der Rechenleistung einer Haupteinheit gut realisierbar.

Zum zweiten müssen alle Steuergeräte in einem Auto mit dem Update-Prozess kompatibel sein. Gäbe es keinen zentralen Zwischenspeicher, müsste jedes einzelne Steuergerät volle Redundanzen bieten, um die Robustheit des Updates zu gewährleisten. Die Investition in einige Gigabyte zentralen Speichers erscheint daher als eine vergleichsweise kostengünstige Alternative. Die Anforderungen an die Steuergeräte wird von Hardware- auf Software-Kompatibilität reduziert.

Drittens ermöglicht der Bordcomputer die flexible Gestaltung des internen Sicherheitsmanagements. So löst sich wie nebenbei die Frage, wie die Steuergeräte auch untereinander zur Kommunikation (also nicht nur für Updates) ein Vertrauensverhältnis aufbauen können. Hier bietet sich der Bordcomputer als zentrale Instanz des Vertrauens an. Wenn die Unterschrift des Bordcomputers werksseitig in den sicheren Speicherbereich des HSM der Steuergeräte eingebracht wird, dann können Steuergeräte anderen Steuergeräten, die ebenfalls signiert worden sind, einander vertrauen, ohne eine umfangreiche Prüfung durchführen zu müssen. Im Falle eines Hardware-Austauschs wird dem Bordcomputer durch eine zertifizierte Anfrage das neue Steuergerät vorgestellt, wodurch das Gerät in das interne Vertrauenszone des Autos aufgenommen wird.

Das Forschungsprojekt SIBASE wurde vom Bundesministerium für Bildung und Forschung unter FKZ 01IS13020 gefördert. ■ (oe)

» **www.mixed-mode.de**

» **www.hanser-automotive.de/2820158**

Hier finden Sie die Download-Version des Beitrags.

Hans-Christian Wild ist Embedded Software Engineer bei der Firma Mixed Mode GmbH in Gräfelfing wo er sich vorwiegend mit vernetzten Systemen und deren Security beschäftigt. Er war am Forschungsprojekt SIBASE für 1,5 Jahre beteiligt.

Phillip Gesien ist Embedded Software Engineer bei der Firma Mixed Mode GmbH in Gräfelfing. Er arbeitete im Forschungsprojekt BMBF SIBASE mit und ist zurzeit im Forschungsprojekten BMBF MiBZ tätig.