Spookfiles A58

Spookfiles A58

Häufig gestellte Fragen: (Daten-) Sicherheit und Datenschutz

Das Herausragende an dem Phantomstaudienst, der im Rahmen des Projekts Spookfiles A58 entwickelt wurde, ist, dass den Teilnehmern eine maßgeschneiderte Empfehlung direkt in ihr Fahrzeug gesendet wird. Um so einen personalisierten Dienst möglich machen zu können, werden jedoch eine Menge Daten benötigt. Dabei geht es unter anderem um sehr spezielle Angaben über die Fahrzeuge der Teilnehmer: Standort, Geschwindigkeit, Richtung usw. Welche Aspekte spielen im Bereich (Daten-) Sicherheit und Datenschutz hier eine Rolle? Und wie geht Spookfiles A58 damit um?

Über Spookfiles A58

Die Provinz Nordbrabant ist Auftraggeber des Projekts Spookfiles A58, das ein Teil des „Beter-Benutten-“ Programms des niederländischen Ministeriums für Infrastruktur und Umwelt ist. Bei diesem Projekt arbeiten Unternehmen, Behörden und Wissenseinrichtungen gemeinsam an der Einführung kooperativer Systeme und Dienste. Auf der A58 zwischen Tilburg und Eindhoven sind zu diesem Zweck mittlerweile 34 Baken am Fahrbahnrand (Roadside-Units, RSUs) aufgestellt, die mit WiFi-P ausgestattet sind. Diese können mit entsprechenden Geräten in vorbeifahrenden Autos kommunizieren. Der erste Dienst, der auf diesem System läuft, ist der Phantomstaudienst: Auf Basis genauer Informationen über Stockungen und Stauwellen auf der Teststrecke erhalten die Teilnehmer personalisierte Geschwindigkeitsempfehlungen *direkt in ihr Fahrzeug*. Dies sorgt dafür, dass sie noch nicht erkennbare Situationen besser antizipieren und sich dadurch leichter und reibungsloser durch den Verkehr bewegen können.

(DATEN-)SICHERHEIT

Welche Probleme spielen im Bereich (Daten-) Sicherheit eine Rolle?

Bei der Arbeit mit Daten – und natürlich beim Versand von Daten – spielen in Bezug auf die Sicherheit der Daten drei Arten von Bedrohungen eine Rolle. Zuallererst stellt sich die Frage, ob die ***Authentizität*** gewährleistet ist. Beispiel: Kann ich als Abnehmer eines personalisierten Dienstes für mein Fahrzeug darauf vertrauen, dass die Information auf dem Bildschirm meines

Geräts tatsächlich von meinem Serviceprovider stammt?[1] Zweitens geht es um die ***Integrität***. Ist die Empfehlung, die auf meinem Bildschirm erscheint, richtig? Wurde nichts bewusst oder unbewusst an den Daten verändert? Als Drittes steht die Sorge nach der ***Verfügbarkeit***. Funktioniert der Dienst, wenn ich ihn benutzen will? Oder tritt irgendwo in der Kette ein Problem mit dem Erfassen oder Teilen von Daten auf und führt dies zum „Ausfall" des Dienstes?[2]

Kann man diese Probleme verhindern?

So etwas wie eine 100 %-ige (Daten-) Sicherheit gibt es nicht. Das Ziel von Sicherheitsmaßnahmen ist es daher auch, Risiken auf ein *annehmbares Maß* zu reduzieren. Was ein annehmbares Maß ist, ist von Anwendung zu Anwendung verschieden. Es versteht sich von selbst, dass ein Dienst, der (zum Teil) das Führen eines Fahrzeugs übernimmt, größere Risiken birgt und daher viel strenger gesichert werden muss als ein Dienst, der nur Informationen oder Empfehlungen vorsieht.

Gibt es spezielle Sicherheitsrisiken beim Projekt Spookfiles A58?

Die Risiken sind gering, da es sich bei dem angebotenen Phantomstaudienst um einen Informationsdienst handelt. Das Schlimmste, was passieren kann, ist, dass eine falsche Empfehlung auf dem Bildschirm des Geräts im Auto angezeigt wird (z. B. eine Empfehlung, die Geschwindigkeit zu verringern, obwohl dies nicht notwendig ist) oder dass mal keine Empfehlung gegeben wird. In beiden Fällen ist ja auch noch der Fahrer da, der selbstverständlich jederzeit seine eigene Entscheidung treffen kann.

Natürlich sind solche Probleme unerwünscht und sei es auch nur, weil durch jedes Problem das Vertrauen in das kooperative System und den Phantomstaudienst (und damit dessen Erfolg) gestört wird.

Welcher (Daten-) Sicherheitsansatz wurde bei Spookfiles A58 gewählt?

Spookfiles A58 ist ein gemeinschaftliches ITS-Entwicklungs- und -Testprojekt. Daher wurde beschlossen, sich auf moderne (Daten-) Sicherheitsmaßnahmen zu verlassen. Diese eignen sich für den Phantomstaudienst, sind aber insbesondere für die Zukunft und noch zu entwickelnde Dienste gedacht.

Die wichtigste Maßnahme ist, dass alle von den Roadside-Units und kooperativen Geräten in den Autos versandten Nachrichten mit einer digitalen Signatur versehen sind. Dies gewährleistet die ***Integrität*** und ***Authentizität*** der Kommunikation, mit anderen Worten, ob Daten tatsächlich unverändert weitergeleitet wurden und aus einer zuverlässigen Quelle stammen. Den Prozess des Signierens und Kontrollierens nennt man *Public Key Infrastructure*, kurz PKI – eine Erläuterung hierzu siehe nachfolgenden Frage.

[1] Derartige Probleme spielen natürlich auch für die anderen Parteien, die an dem Dienst beteiligt sind, eine Rolle, wie z. B. für den Serviceprovider selbst (Stammen die Daten, die der Serviceprovider zurückbekommt, tatsächlich von seinen Kunden?), für die Straßenverkehrszentrale usw. Wir beschränken uns hier auf Beispiele des Endanwenders.
[2] Die Sicherheitsprobleme rund um die Speicherung von Daten (Können Unbefugte sich keinen Zugang dazu verschaffen?) werden in dem Abschnitt über den Datenschutz besprochen.

Um für eine optimale ***Verfügbarkeit*** zu sorgen, läuft das Spookfiles A58-System auf Qualitätsservern mit hoher „Uptime“.

Wie arbeitet das verwendete PKI-System?

Jedes System innerhalb von Spookfiles A58, das drahtlose Nachrichten versendet – das sind die Roadside-Units und die kooperativen Geräte in den Autos – bekommt zwei Arten von digitalen „Schlüsseln“: geheime Schlüssel für die Units und Geräte und ein öffentlicher Schlüssel, der über eine Datenbank für jedermann zugänglich ist. Die Ausgabe und Registrierung der Schlüssel wird streng überwacht.

Nehmen wir einmal folgenden Fall: Ein Serviceprovider will eine Geschwindigkeitsempfehlung versenden. Vor dem Versand „unterzeichnet“ der Serviceprovider diese Nachricht mit seinem ***geheimen Schlüssel***: auf Basis des Inhalts der Mitteilung ***generiert*** der Schlüssel eine ***digitale Signatur***. Sobald ein kooperatives Gerät in einem Auto diese Geschwindigkeitsempfehlung erfasst, sucht es den ***öffentlichen Schlüssel*** der sendenden Roadside-Unit. Mit diesem öffentlichen Schlüssel kann die ***Signatur*** unter der Nachricht ***kontrolliert*** werden: Wurde die Signatur mit dem richtigen geheimen Schlüssel generiert (= ist der Absender derjenige, der er vorgibt zu sein) und passt sie mit dem Inhalt der Nachricht zusammen? Wenn ein „OK“ zurückgesendet wird, dann weiß das kooperative Fahrzeuggerät, dass sowohl die Authentizität als auch die Integrität vorhanden ist. Wenn ein „false“ zurückgesendet wird, dann ist entweder der Absender nicht derjenige, der er vorgibt zu sein, oder die Nachricht wurde verändert.

Werden bei dem PKI-System von Spookfiles A58 Verschlüsselungstechniken angewendet, welche die Nachrichten unlesbar machen?

Nein. Aus einem ganz einfachen Grund: Das Wesentliche bei einem kooperativen System ist ja gerade die Zusammenarbeit und der freie Austausch von Daten zwischen den verschiedenen Komponenten innerhalb des Systems (also zwischen den Fahrzeuggeräten untereinander und zwischen den Geräten in den Autos und den Roadside-Units). Die Verschlüsselung von Daten steht im Widerspruch zu diesem Prinzip und sie ergibt für kollektive Anwendungen wie Geschwindigkeitsempfehlungen auch überhaupt keinen Sinn.

Das bedeutet, dass zum Beispiel die Geschwindigkeitsempfehlungen vom Serviceprovider oder die Standort- und Geschwindigkeitsdaten aus Fahrzeugen im Prinzip von jedermann „gelesen“ werden können. Für die *Sicherheit* ist das kein Problem – solange keine falschen oder unberechtigten Nachrichten versendet werden – aber es ergeben sich natürlich wohl einige Probleme bezüglich des Datenschutzes. Siehe hierzu Abschnitt „Datenschutz“ weiter unten.

Wie sieht es mit der (Daten-) Sicherheit aus, wenn mehr Dienste auf dem kooperativen System verfügbar sind?

Bei jedem neuen Dienst muss geschaut werden, ob die vorhandenen Maßnahmen für eventuelle (neue) Risiken noch ausreichend sind. Wenn nötig, müssen dann zusätzliche Schutzmaßnahmen vorgesehen werden.

DATENSCHUTZ

Welche Aspekte spielen im Bereich Datenschutz eine Rolle?

Es werden Daten gesammelt und gespeichert u. a. über einzelne Fahrzeuge, wie z. B. Standort und Zeitpunkt. Bestimmte Informationen werden auch mit Dritten geteilt. Das sind die ersten Risiken: Ist sichergestellt, dass keine Unbefugten an die Daten gelangen können und wird darauf geachtet, dass keine sensiblen privaten Daten geteilt werden?

Dann ist da auch noch der Umstand, dass der Austausch von Nachrichten aufgrund des offenen und kollektiven Charakters des kooperativen Systems nicht verschlüsselt wird. Theoretisch könnte dadurch auch jemand anderes die Nachrichten empfangen und mitlesen.

Wie werden die Datenschutzrisiken beim Speichern und Teilen der (Fahrzeug-) Daten auf ein Minimum begrenzt?

Alle Quelldaten, die für das Projekt Spookfiles A58 gesammelt werden, werden auf Servern in sogenannten Serverparks gespeichert, die sowohl physisch als auch digital streng gesichert sind.

Die gesammelten Daten sind aus verkehrstechnischer Sicht für „Dritte“ interessant, weil sie zum Beispiel ein genaues Bild über die Geschwindigkeit und Stabilität des Verkehrsflusses vermitteln. Um zu verhindern, dass Dritte sich auf einzelne Fahrzeuge fokussieren können, sollen die Daten nur *in aggregierter Form* angeboten werden. Daneben können Start- und Zielpunkte jeder einzelnen Fahrt entfernt werden. Die Start- und Zielpunkte lassen sich nämlich kaum aggregieren und um zu verhindern, dass doch Informationen über einzelne Fahrten geteilt werden, können die letzten paar Hundert Meter abgeschnitten werden.

Alle Nachrichten können abgefangen und mitgelesen werden. Zu welchen speziellen Datenschutzrisiken führt dies und wie werden diese ausgeschaltet?

Bei den Daten, die Serviceprovider über die Roadside-Units verbreiten, gibt es keine Datenschutzprobleme: Es geht um Geschwindigkeitsempfehlungen und Warnungen, vergleichbar mit Meldungen, die auch auf Matrixtafeln angezeigt werden können.

Bei der Datenspur, die von den On-Board-Units hinterlassen werden, sieht das anders aus. Obgleich jede einzelne „Nachricht“ keine Probleme bereitet – ein bestimmtes Fahrzeug A fuhr im Moment t zu einem Ort x – wird es zum Problem, wenn alle Nachrichten eines kooperativen Fahrzeugs abgefangen und auf eine Karte projiziert werden: Es zeichnet sich dann eine Route ab. Dies verschafft Einblicke in das Reiseverhalten einzelner Fahrzeuge (und damit: des Nutzers/Fahrers).

Das Risiko scheint nicht sehr hoch zu sein, aber das kooperative System von Spookfiles A58 ist bereits darauf vorbereitet, das Problem mit entschlossenen Maßnahmen anzugehen. So verfügen die On-Board-Units über verschiedene digitale Identitäten, mit denen die Nachrichten unterzeichnet werden können. Die Verwendung mehrerer Identitäten erschwert es Dritten, auf Basis von verschickten Nachrichten einen Absender zu erkennen.

Die On-Board-Units können alle fünf Minuten ihre Kennung („MAC-Adresse“) ändern zu lassen, sodass sie nie länger als einige Minuten dieselbe ID aussenden.[3] Auch das kooperative System selbst „weiß“ dann nicht, welche ID zu welchem Fahrzeug gehört. Das verhindert wiederum das Verfolgen der On-Board-Units an sich.

Wie sieht es mit dem Datenschutz aus, wenn mehr Dienste auf dem kooperativen System verfügbar sind?

Das muss bei jeder neuen Anwendung geprüft werden: Welche (neuen) Daten werden erfasst, gespeichert und geteilt und inwieweit stellt dies ein (neues) Datenschutzrisiko dar? Mit dem heutigen System der sicheren Speicherung von Daten und der Datenaggregation wurde bereits eine solide Basis für den Schutz privater Daten gelegt. Außerdem ist das kooperative System bereits darauf vorbereitet, Start- und Zielpunkte der Fahrten zu verändern und die MAC-Adressen zu ändern, was zu einer enormen Verbesserung des Datenschutzes beiträgt.

Sicherheits- und Datenschutzmaßnahmen nach europäischen Standards

Alle (Daten-) Sicherheits- und Datenschutzmaßnahmen, die beim Projekt Spookfiles A58 angewendet werden, entsprechen dem europäischen Rahmen, der vom ETSI, dem Europäischen Institut für Telekommunikationsnormen, aufgestellt wurde. In dem Projekt Spookfiles A58 hat man sich daher nicht so sehr neue Konzepte ausgedacht, sondern vorhandene Konzepte *in die Praxis umgesetzt*. Dabei wurden wichtige Kenntnisse und Erfahrungen gesammelt: Viele dieser Konzepte wurden zuvor noch nicht in so einer Größenordnung angewendet.

Die Anknüpfung an bestehende Konzepte und Vereinbarungen ist natürlich mit Blick auf die Zukunft wichtig. Wenn zusätzliche Maßnahmen im Bereich Sicherheit und Datenschutz notwendig sind, weil auch erweiterte Anwendungen eingesetzt werden, muss das Sicherheits- und Datenschutzsystem von Spookfiles A58 nicht vollständig angepasst werden. Das bestehende System kann einfach erweitert werden.

24 Mai 2016

Weitere Informationen: Trudy van de Westelaken, Kommunikationsbeauftragte des Projekts Spookfiles A58: info@spookfiles.nl.

[3] Viele Geräte haben eine feste MAC-Adresse, die On-Board-Units jedoch nicht. Das hängt alles mit der verwendeten Kommunikationstechnologie WiFi-P zusammen, die auf „verbindungsloser Kommunikation“ basiert. Es wird daher nicht wie bei GSM eine Verbindung hergestellt (das nimmt auch zuviel Zeit in Anspruch): Es werden nur Nachrichten versendet. Dann kann auch problemlos die ID geändert werden.