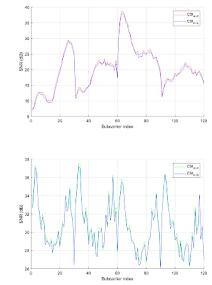
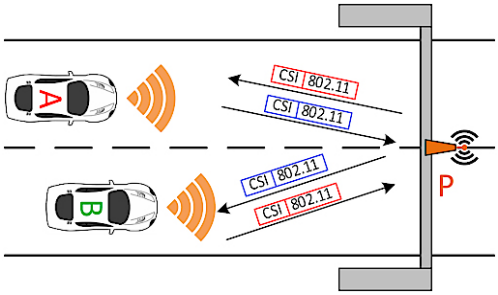
OTS0037 5 CI 0414 FSP0001 XI Fr, 22.Jun 2018
Forschung/Auto/IT/Sicherheit/Technologie

IT-Sicherheit beim autonomen Fahren



IT-Sicherheit beim autonomen Fahren

Credit: FH St. Pölten
Fotograf: Oliver Eigner



IT-Sicherheit beim autonomen Fahren

Credit: FH St. Pölten
Fotograf: Oliver Eigner

Projektleiter Ernst Piller, FH St. Pölten

Credit: privat
Fotograf: privat

Utl.: FH St. Pölten entwickelt neue Methode für sicheren Informationsaustausch zwischen Fahrzeugen mittels Funkdaten =

St. Pölten (OTS/FHSTP) - Neue technische Errungenschaften wie das Internet der Dinge oder die direkte drahtlose Kommunikation zwischen Objekten erhöhen den Bedarf an effizienter Verschlüsselung und Informationssicherheit. Ein Projekt der FH St. Pölten entwickelt derzeit ein neues Verfahren zur Verschlüsselung von Daten für den Bereich des autonomen Fahrens und das Internet der Dinge. Die Technik soll auch mit in Zukunft verfügbaren neuen Computer-Technologien noch sichere Kommunikation ermöglichen.

Beim autonomen Fahren müssen Fahrzeuge miteinander kommunizieren, also Informationen austauschen. Manipulierte Kommunikation ist hier nicht nur eine Frage der IT-Sicherheit, sie kann Menschenleben gefährden. Ein wesentlicher Punkt in der Kommunikation zwischen den Fahrzeugen ist die sichere Verschlüsselung der Information.

Bisher werden für das Verschlüsseln mathematische Verfahren eingesetzt. Doch digitale kabellose Kommunikation mit sensiblen Daten wie beim Internet der Dinge (IoT) oder dem autonomen Fahren erfordert neue Verfahren, die auch bei zukünftigen Technologien, wie z. B. Quantencomputern, noch sicher sind. Dafür entwickelt das von der FH St. Pölten durchgeführte Projekt „KIF - Kryptografie mit Integration von Funkmessdaten“ nun einen neuen Ansatz. Statt mathematischer Verfahren zum Genieren der Schlüssel werden Funkdaten genutzt.

Zwtl.: Verschlüsselungsmethode für die Zukunft

„Verkehrsinfrastruktur wird für mindestens 20 Jahre ausgelegt. In spätestens 15 Jahren werden Quantencomputer mit ausreichenden Geschwindigkeiten für die praktische Anwendung erwartet. Derzeitige Verfahren zur Objekt-/Daten-Authentifizierung und Datenintegritätsprüfung sind dann aus Sicherheitsgründen nicht mehr verwendbar. Daher suchen wir bereits jetzt nach einer quantencomputersicheren Methode auf Basis physikalischer Methoden, die auch dann noch sicher ist“, sagt Ernst Piller, Leiter des Projekts sowie des Instituts für IT-Sicherheitsforschung der FH St. Pölten.

Basis der neuen Methode ist das Erzeugen und Verteilen von kryptografischen Schlüsseln auf Basis der Messung von Funkkanaleigenschaften einer hochfrequenten Funkübertragung: Bei beiden Objekten (jeweils Sender und Empfänger), zum Beispiel Fahrzeugen, werden Funksignale sowie reflektierende Echos des Signals und deren Verzögerung gemessen. Daraus lassen sich Zufallsdaten erzeugen, die zum Generieren des Schlüssels verwendet werden und die von potentiellen Angreiferinnen und Angreifern nicht abgehört werden können.

Zwtl.: Projekt KIF - Hochsichere, langzeitige Kryptografie für kabellose Kommunikation mit Integration von Funkmessdaten

Das Forschungsprojekt wird vom Bundesministerium für Verkehr, Innovation und Technologie im Rahmen des österreichischen

Förderprogramms für die Sicherheitsforschung KIRAS finanziert. PartnerInnen im Projekt sind die Cryptas it-Security GmbH, das Bundesministerium für Europa, Integration und Äußeres (BMEIA), ASFINAG und Bundesministerium für Landesverteidigung und Sport (BMLVS).

[https://www.ots.at/redirect/fhstp27] (https://www.ots.at/redirect/fhstp27)

Bild(er) zu dieser Aussendung finden Sie im AOM / Originalbild-Service sowie im OTS-Bildarchiv unter http://bild.ots.at

~

Rückfragehinweis:
Fachhochschule St. Pölten
Mag. Mark Hammer
Marketing und Unternehmenskommunikation
+43/676/847228269
mark.hammer@fhstp.ac.at
www.fhstp.ac.at
0676/847 228 269
presse@fhstp.ac.at
https://www.fhstp.ac.at/de/presse

~

OTS0037 2018-06-22/10:00

221000 Jun 18

Link zur Aussendung:
https://www.ots.at/presseaussendung/OTS_20180622_OTS0037