KIF

Hochsichere, langzeitige Kryptografie für kabellose Kommunikation mit Integration von Funkmessdaten

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2016	**Status**	abgeschlossen
Projektstart	01.09.2017	**Projektende**	30.06.2019
Zeitraum	2017 - 2019	**Projektlaufzeit**	22 Monate
Keywords			

Projektbeschreibung

Hochsichere Kryptografie wird im Zeitalter der Digitalisierung und Globalisierung immer wichtiger. Des Weiteren entsteht durch das Internet der Dinge und die direkte kabellose Kommunikation zwischen Objekten ein neuer gigantisch großer Markt für sichere Kommunikation. Dies gilt vor allem für das autonome Fahren, wo manipulierte Kommunikation Menschenleben kosten kann. Da straßengebundene Verkehrsinfrastruktur (inklusive Fahrzeuge) für lange Zeitabschnitte ausgelegt wird, müssen die dabei verwendeten Technologien auch dafür vorgesehen sein. Für eine Verkehrsinfrastruktur der Zukunft mit autonomen Fahren ist zur Garantie einer langandauernd ausreichend hohen Sicherheit der kabellosen Kommunikation, d.h. z.B. für den Schutz vor Cyber-Angriffen, die aktuell verwendete asymmetrische Kryptografie aber nicht mehr geeignet.
Das Problem liegt dabei vor allem in der langfristigen Sicherheitsbeurteilung bei den Verfahren zur Schlüsselverteilung, Datenintegrität und Objekt-Authentizität. Bei den aktuellen Verfahren, die auf der Zahlentheorie basieren, wie z.B. dem Diffie-Hellman Verfahren, hybriden Schlüsselverteilungsverfahren und Digitale Signaturverfahren (z.B. RSA, DSA, ECDSA) wird heute die Sicherheit durch nicht beweisbare Sicherheitsannahmen festgelegt. Vor allem aber sind in Zukunft mit den Quantencomputern diese Verfahren aus Sicherheitsgründen nicht mehr verwendbar. Daher wird versucht verstärkt auf physikalische Methoden und Post-Quanten-Systeme auszuweichen. Quantenkryptografie als möglicher hervorragender Teilersatz, die die gewünschte Sicherheit garantieren kann, ist jedoch teuer und im autonomen Fahren durch die Vielzahl an Objekten nicht anwendbar.
Seit einigen Jahren beschäftigt sich die Forschung mit einer neuen physikalischen Methode, der Erzeugung und Verteilung von kryptografischen Schlüsseln auf Basis der Messung von Funkkanaleigenschaften einer hochfrequenten Funkübertragung. Sie basiert auf der Reziprozität der Funkübertragung. Doch auch diese Technologie hat ihre Tücken, vor allem wenn es um Schlüsselentropie bei kurzer Kommunikationszeit, Messbarkeit in der Nähe („Abhörbarkeit“), Objekt-Authentizität und große Entfernungen geht.
Das Forschungsprojekt KIF beschäftigt sich mit diesen Herausforderungen. Vor allem sollen zwei spezielle Herausforderungen, die bisher in der Forschung wenig Beachtung gefunden haben, behandelt werden. Dabei geht es einerseits um die hochsichere Schlüsselerzeugung bei sehr kurzer Kommunikationszeit und einer großen Anzahl an verschiedenen Objekten, wie sie beim autonomen Fahren auftritt, und andererseits um die Telekommunikation über große Entfernungen, wo nicht mehr auf der Reziprozität aufgebaut werden kann.

Das Projekt KIF erforscht hochsichere Verfahren zur Erzeugung und Verteilung von kryptografischen Schlüsseln, die auf Funkkanaleigenschaften beruhen, und integriert dabei geeignet auch ein für ressourcenschwache Prozessoren effizientes Post-Quanten-Kryptoverfahren. Die Verfahren sollen die notwendige Entropie des Schlüssels, eine hochsichere Objekt-Authentizität, Datenintegrität und Vermeidung der „Abhörbarkeit“ garantieren und sowohl für kleine, als auch für große Entfernungen geeignet sein. Dabei sollen die speziellen Anforderungen des autonomen Fahrens erfüllt werden, wie mögliche hohe Objektgeschwindigkeit, schnell wechselnde Objekte, insgesamt hohe Anzahl an Objekten, rauhes Umfeld und später als Produkt klein und kostengünstig. Die GSK-Komponente enthält eine Sondierung der sozialwissenschaftlichen Erkenntnislage zu langlebigen kryptografischen Verfahren, insbesondere im Umfeld einer Verkehrsinfrastruktur (inklusive Fahrzeuge) für das autonome Fahren, mit einer Ableitung von Handlungsempfehlungen für Stakeholder.

Abstract

Highly secure cryptography is a topic of increasing concern, especially in the digital age with globalization in an unprecedented scale. Moreover, with internet of things growing very fast a completely new huge market has been opened for secure communication. This is a topic of great importance especially when it comes to autonomous driving where manipulated communication could result in fatalities. As transport infrastructure is built to long-term, there are also high demands for cryptography as well as all other utilized technology. However, in order to guarantee a long-term high level of security, current asymmetric cryptographic algorithms are not suitable. Furthermore, the long-term security evaluation of methods for key distribution, data integrity and authenticity poses the main problem. Current method are most namely Diffie-Hellman key exchange, hybrid key distribution techniques and digital signature (RSA, DSA, ECDSA). However, all of the before named method’s safety is derived from assumptions that cannot be proven for sure (complexity of prime factorization or dis¬crete logarithm). In addition, quantum computers are a serious threat towards those methods and thus should not be used in the distant future anymore. As a result, physical methods and post-quantum systems are topic of growing importance within cryptography. Although quantum cryptography is an excellent replacement ensuring the necessary security, it is very expensive and not suitable for autonomous driving due to the vast amount of objects.
For the last couple of years research has been concerned with new physical methods for generating and distributing cryptographic keys by utilizing high-frequency radio communication. It is relying on the reciprocity of the communication channel. This approach also comes with drawbacks, especially on the topics of a reasonably high key entropy, eavesdropping, object-authenticity and communications over a bigger distance.
Hence, the research project KIF is targeting based on the current state-of-the-art, these specific issues. Moreover, two challenges, which have not yet been discussed a lot, are to be handled. On the one hand there is the fast generation of highly secure cryptographic keys with a big amount of different objects as it occurs with autonomous driving. The other big challenge that is identified is the communication over bigger distances. For this second part methods need to be researched as reciprocity cannot be taken for granted anymore. Thus, the key generation would here be based on a good connection between the communication partners as well as pattern detection.
The project KIF researches highly secure methods to generate and distribute cryptographic keys utilizing channel data and in addition other data enabling even less powerful hardware to be more resilient to attacks by quantum computers. The methods should ensure sufficient entropy for the key, object authenticity, data integrity and eavesdropping protection while being applicable for short-range as well as long-range communications. Furthermore, this project aims to fulfill full functionality for autonomous driving with challenges such as high object velocities, fast changing objects, a large amount of different objects, rough environment and later on a small and cheap implementation.

Projektkoordinator

- Fachhochschule St. Pölten ForschungsGmbH

Projektpartner

- Bundesministerium für Europäische und Internationale Angelegenheiten
- Fachhochschule St. Pölten GmbH
- CRYPTAS it-Security GmbH