idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Bergische Universität Wuppertal
Marylen Reschop

10/20/2021

http://idw-online.de/en/news777818

Research projects, Transfer of Science or Research
Information technology, Social studies
transregional, national

Datensicherheit: Informatiker der Bergischen Uni erforschen smarte Verschlüsselungsverfahren

Smarte Verschlüsselungsverfahren zur Speicherung vertraulicher Daten stehen im Mittelpunkt von zwei neuen Forschungsprojekten, die jetzt unter Leitung von Informatiker Prof. Dr.-Ing. Tibor Jager an der Bergischen Universität Wuppertal gestartet sind. Für die beiden Vorhaben erhält der Lehrstuhl für IT-Security and Cryptography eine Förderung der Deutschen Forschungsgemeinschaft (DFG) in Höhe von insgesamt rund 600.000 Euro.

Im Projekt „Foundations of Secure Storage for Encrypted Instant Messaging" nimmt das Forschungsteam Sicherheitslücken in Instant Messengern wie WhatsApp, Threema und Signal ins Visier: Während die Verschlüsselung von Daten auf dem Transportweg von Nachrichten – auch „data in transit" genannt – durch moderne Techniken als kryptografisch sehr stark gilt, bildet die Speicherung der gesendeten Nachrichten auf dem Telefon oder als Backup in der Cloud – das sogenannte „data at rest" – immer noch eine Schwachstelle und somit potenzielle Angriffspunkte. Angreifer*innen könnten darüber die starke Transportverschlüsselung umgehen und aushebeln und sich schließlich doch Zugriff auf die Daten verschaffen. Daher wollen die Forschenden untersuchen, wie die starken Sicherheitseigenschaften, die für „data in transit" bereits erreicht wurden, auch auf „data at rest" übertragen werden können. „Dies würde die Sicherheit von modernen Instant Messaging Verfahren signifikant stärken", so Dr. Gareth Davies, Wissenschaftlicher Mitarbeiter am Lehrstuhl und Experte für kryptografische Speicherung von Daten.

Im Projekt „Foundations of Smart Encryption" geht es um die Untersuchung von „Smart Encryption", einer neuartigen Klasse von Verschlüsselungsverfahren, die auf sogenannten „Smart Contracts" aufbaut. „Ein Smart Contract wiederum ist ein Programm, das auf der Blockchain-Technologie basiert. Alle relevanten Informationen und Bedingungen werden auf dieser Blockchain gespeichert und das Programm wird automatisch ausgeführt, wenn die Bedingungen erfüllt sind. Die Daten, die in Smart Contracts gespeichert werden, sind zunächst jedoch stets öffentlich sichtbar", so Prof. Jager. Mit Smart Encryption-Verfahren lassen sich Programme entwickeln, bei denen nicht alle Daten sichtbar sind, und entsprechend verschlüsselte Daten nur dann entschlüsselt werden können, wenn es das Programm durch bestimmte Kriterien vorgibt.

Für die Praxis ergeben sich daraus zahlreiche Anwendungsmöglichkeiten. Ein Beispiel ist die zeitbasierte Verschlüsselung, bei der Daten bis zu einem festgelegten Zeitpunkt sicher verschlüsselt sind und danach sofort für jeden frei zugänglich. Dies ermögliche es, so die Forschenden, vertrauliche Daten „in die Zukunft" zu senden, was zum Beispiel in digitalen Auktionen mit geheim abgegebenen Geboten eingesetzt werden könne. „Bei klassischen Auktionen könnte ein korrupter Auktionator die geheim abgegebenen Gebote vorab öffnen und diese Gebote Dritten mitteilen. Zeitbasierte Verschlüsselung ersetzt den Auktionator und garantiert, dass die Gebote bis zum Auktionsende sicher verschlüsselt bleiben und sich erst danach fast wie von selbst entschlüsseln", erklärt Tibor Jager.

Einen anderen konkreten Anwendungsfall nennt Dr. Saqib Kakvi, ebenfalls Wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Jager: „Wir sprechen von ‚Accountable Lawful Interception': Verschlüsselte Nachrichten können nur dann von einer Behörde entschlüsselt werden, wenn ein Richter einen Durchsuchungsbefehl dafür digital unterzeichnet." In

diesem Durchsuchungsbefehl ließen sich zudem Kriterien beschreiben, die dafür sorgen, dass die Behörde nur bestimmte Daten entschlüsseln kann. „Zum Beispiel: Alle Nachrichten von Alice an Bob, die im September 2021 gesendet wurden'. Es ist der Behörde jedoch nicht möglich, Daten zu entschlüsseln, die dem richterlichen Beschluss nicht entsprechen, also zum Beispiel Nachrichten von Dritten oder Nachrichten von Alice an Bob aus anderen Zeiträumen", erklärt der Wissenschaftler. Im Gegensatz zu anderen Ansätzen, um Verschlüsselung für Behörden zugänglich zu machen, so der Experte, stecke in Smart Encryption viel weniger Missbrauchspotenzial.

„Die Diskussion um entsprechende Verfahren führen IT-Sicherheitsexpert*innen und Bürgerrechtler*innen mit der Politik schon länger", so Prof. Jager. „Wir sehen solche kryptografischen Backdoors generell sehr, sehr kritisch, wegen des immensen Missbrauchspotenzials. Eine absolute Mindestanforderung ist, dass transparent und unfälschbar, also ‚accountable', nachvollziehbar ist, wann eine Behörde auf welche Daten zugegriffen hat. Ob und unter welchen Voraussetzungen dies überhaupt möglich ist, werden wir im Projekt untersuchen."

contact for scientific information:

Prof. Dr.-Ing. Tibor Jager
Lehrstuhl für IT-Security and Cryptography
E-Mail tibor.jager@uni-wuppertal.de

Prof. Dr.-Ing. Tibor Jager
Friederike von Heyden