idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

CISPA Helmholtz Center for Information Security
Annabelle Theobald

23.10.2023
http://idw-online.de/de/news822685

Forschungsergebnisse, Wettbewerbe / Auszeichnungen
Informationstechnik
überregional

CISPA-Forscher will automatisierte Analyse von Protokollen verbessern

Gleich zwei Distinguished Paper Awards gab es in diesem Jahr auf der renommierten Cybersicherheitskonferenz USENIX für Forschungspaper, an denen Alexander Dax mitgearbeitet hat. Eine der beiden in der Forschungsgemeinschaft begehrten Auszeichnungen hat er für sein Paper „Hash gone bad: Automated discovery of protocol attacks that exploit hash function weaknesses“ erhalten. Darin zeigt er auf, dass automatisierte Sicherheitsanalysen von Internetprotokollen oft ungenau sind, weil sie von falschen Voraussetzungen – in diesem Falle perfekten Hashfunktionen – ausgehen.

Damit im Internet Daten sicher hin und her geschickt werden können, kommen verschiedene Protokolle zum Einsatz. Sie regeln, wer wann wem was und in welcher Form schicken darf. Eines der bekanntesten Internet-Protokolle im Dauereinsatz ist das sogenannte TLS, kurz für Transport Layer Security. Mit TLS wird vor allem geregelt, wie die Kommunikation zwischen Webanwendungen verschlüsselt wird. So kommunizieren zum Beispiel Browser wie Google Chrome und Mozilla bei jedem Aufruf einer Website mit einem Webserver. Damit diese Kommunikation nicht von Angreifer:innen unterwandert werden kann, muss im ersten Schritt vor der eigentlichen Kommunikation eine sichere Verbindung aufgebaut werden. So wird erstmal sichergestellt, dass die Kommunikationspartner:innen sind, wer sie vorgeben und nicht irgendein:e Dritte:r sich dazwischenschalten kann. Ist das geklärt, können sicher kryptografische Schlüssel ausgetauscht werden und so eine vertrauliche Kommunikation ermöglichen. Soweit so gut, aber wie kann das jetzt sicher passieren?

Hashfunktionen als Sicherheitsgarant

„Nahezu jedes Sicherheitsprotokoll nutzt Hashfunktionen“, erklärt Dax. Damit lässt sich ein Prüfwert und damit eine Art digitaler Fingerabdruck erstellen. Mit diesem lässt sich prüfen, ob Daten auf dem Weg von A nach B manipuliert wurden. „Diese Funktionen nehmen irgendeinen Wert, egal welcher Größe, und machen daraus einen kleineren Wert mit fixer Größe“, erklärt Dax. Damit alleine lässt sich noch nicht viel anfangen, die Funktionen müssen zusätzlich bestimmte Eigenschaften aufweisen. „Dazu gehört, dass ein bestimmter Dateninhalt, etwa ein Passwort, mit derselben Hashfunktion berechnet immer denselben Wert ergeben muss. Umgekehrt darf es aber nicht möglich sein, aus dem Hashwert auf den Dateninhalt zurückzuschließen.“ Eine weitere wichtige Eigenschaft von Hashfunktionen ist, dass verschiedene Ursprungsdaten nicht zum selben Hashwert umgerechnet werden dürfen. „Man spricht von Kollisionen, wenn das passiert“, sagt Dax. Und genau hier kommen sich Theorie und Praxis in die Quere. „In der Realität gibt es keine perfekten Hashfunktionen. Es ist immer nur eine Frage der Zeit, bis es Kollisionen gibt. Zudem hat sich der Stand der Technik geändert. Bei alten Hashfunktionen ist es mittlerweile möglich, mit genug Rechenpower solange verschiedene Werte durchzuprobieren, bis der Ursprungswert für einen Hashwert herausgefunden ist. Das nennt man Brute-Force-Angriff“, sagt Dax.

Netze müssen zukunftssicher sein

Solche Angriffe sind für moderne Hashfunktionen laut Dax sehr aufwendig und daher bislang kein alltägliches Problem. „Allerdings entwickelt sich die Technik sehr schnell weiter und wir müssen dafür sorgen, dass unsere Netze auch

zukunftssicher sind.“ Und damit kommt Dax‘ Forschung rund um Tools für die automatisierte Sicherheitsanalyse von Protokollen ins Spiel. „Es reicht nicht zu behaupten, dass ein Protokoll sicher ist. Wir müssen es auch formal beweisen können. Das heißt, wir brauchen präzise mathematische Definitionen davon, wie sich das Protokoll verhält und dann lässt sich berechnen, wie sicher es ist.“ Diese Prüfverfahren sind enorm aufwendig, weshalb sie mittlerweile automatisiert wurden. „Es gibt dazu Tools wie zum Beispiel den Tamarin Prover oder Proverif, die die Arbeit für uns übernehmen können. Das Problem ist: Diese Tools arbeiten bislang häufig nur mit modellhaften Abbildungen von Hashfunktionen, die in dieser Form perfekt sind. Wir wissen aber, dass sie es in der Praxis oft eben nicht sind.“

Zu perfekt ist auch nicht gut

Das anzuerkennen, ist der erste Schritt zur Verbesserung der Tools. Und es hat noch einen weiteren Vorteil: „Wir haben verschiedene Varianten von schwachen Hashfunktionen modelliert und in den Tamarin Prover und das Tool Proverif eingebaut. Wir wollen so auch herausfinden, wie groß der Einfluss von verschiedenen Schwächen in den Hashfunktionen auf die Gesamtsicherheit des Protokolls ist.“ Formale Sicherheitsbeweise von Protokollen sind dabei kein nerdiger Forschenden-Kram, sondern längst auch in den großen Tech-Unternehmen der Welt angekommen. „Viele große Unternehmen wie zum Beispiel Google beschäftigen Kryptografen, um zu prüfen, wie sicher die eingesetzten Protokolle sind. Das ist manuell sehr aufwendig und selbst die Kontrolle von automatisierten Sicherheitsanalysen erfordert derzeit noch viel Aufwand. Wir wollen die Tools so gut machen, dass dafür künftig deutlich weniger Personal und Aufwand erforderlich ist und die automatisierte Prüfung echte Protokoll-Sicherheit garantieren kann.“

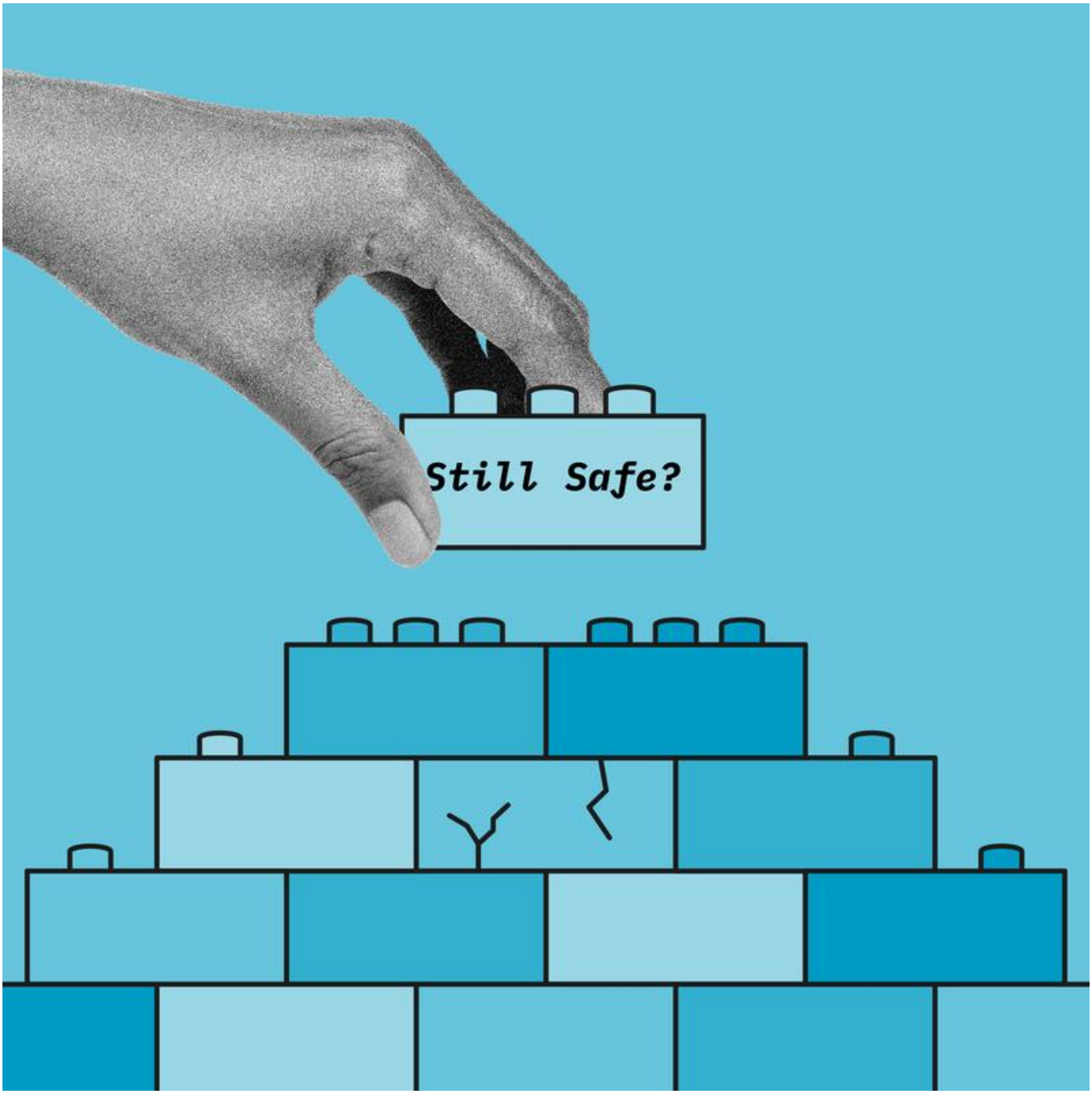
An der Quelle

Dax arbeitet in der Gruppe von CISPA-Faculty Prof. Dr. Cas Cremers und sitzt somit an der Quelle für Forschungsfragen rund um die automatisierte Prüfung von Protokollen. Cremers und Kolleg:innen haben vor einigen Jahren den bereits erwähnten Tamarin Prover entwickelt, der von Unternehmen wie Mozilla und Amazon genutzt wird. „Meine Forschung ist Teil eines größeren Projektes zur Verbesserung der automatisierten Sicherheitsanalyse. Ich arbeite schon seit Jahren daran mit. Dass meine Forschung zu Hashfunktionen jetzt in ein ausgezeichnetes Paper gemündet ist, ist toll“, sagt Dax. Er ist mittlerweile eine Art CISPA-Urgestein. „Ich bin schon seit 2016 mit dabei, war zunächst Hiwi bei Michael Backes, dann in der Gruppe von Robert Künnemann und jetzt bin ich als Doktorand bei Cas. Irgendwie bin ich mit dem CISPA mitgewachsen.“

Das Paper entstand in Zusammenarbeit mit CISPA-Faculty Cas Cremers, Vincent Cheval und Charlie Jacomme von INRIA Paris, Lucca Hirschi von LORIA und Inria sowie Steve Kremer von der Université de Lorraine (LORIA und Inria Nancy Grand-Est).

Originalpublikation:

https://publications.cispa.saarland/3862/



Graphic of the paper by CISPA researcher Alexander Dax.
Lea Mosbach
CISPA