Lauschen verboten

Wenn zwei Menschen oder Software-Anwendungen im Web miteinander kommunizieren, liest manchmal ein Dritter heimlich mit. Kryptographische Verfahren könnten dies verhindern, aber Software-Entwickler tun sich mit der Umsetzung schwer. Deshalb wollen TU-Forscher die Verschlüsselung automatisieren.

Von Boris Hänßler

Andrea möchte ihrem Freund Stefan eine Nachricht schicken. Damit niemand mitliest, vereinbart sie mit Stefan mittels Kommunikation über das Netz einen geheimen Code, den nur er und sie entschlüsseln können. Falls die Nachricht in falsche Hände gerät, besteht sie ohne den Schlüssel nur aus einer unsinnigen Zeichenfolge. Was Andrea und Stefan allerdings nicht ahnen: Ein Spion hat sich dazwischen geschaltet. Der Code, auf den sich Andrea und Stefan geeinigt hatten, stammt in Wirklichkeit von diesem Spion. Er hat ihn den beiden Gesprächspartnern geschickt, indem er ihnen vorgaukelte, der jeweils andere zu sein. So kann er alle Nachrichten mitlesen und Andrea zum Beispiel um ein wichtiges Passwort bitten. Die fühlt sich sicher, weil sie denkt, sie schickt es ihrem Freund.

So ungefähr kann man sich eine Man-in-the-Middle-Attacke vorstellen, bei der ein Angreifer die Kommunikation im Internet manipuliert. Der Schlüssel oder Code, um den es geht, ist in der Informationstechnik Teil eines sogenannten kryptographischen Verfahrens. Es soll Daten schützen, die innerhalb einer Anwendung oder zwischen verschiedenen Anwendungen hin und her geschickt werden. Meist laufen Verschlüsselungsverfahren im Hintergrund ab, ohne dass wir sie als Nutzer bemerken. Wenn wir zum Beispiel einen Online-Shop besuchen, handeln unser Browser und der Online-Shop automatisch einen einzigartigen Schlüssel aus, mit dem die Daten, etwa die Bestellung oder Bankverbindung, mathematisch verfremdet werden. Ein Dritter könnte ohne Schlüssel nichts mit ihnen anfangen.

„Wissenschaftler aus der Kryptographie und Softwaretechnologie arbeiten hier eng zusammen. Das passiert weltweit noch viel zu selten."

Kryptographie begegnet uns ständig: Bei der Nutzung von Apps, beim Versenden von E-Mails, bei der Kommunikation über Messenger-Dienste oder bei der internen Kommunikation in Unternehmen – immer dann, wenn sensible Daten im Spiel sind. Verschlüsselungsverfahren gewähren eine gewisse Sicherheit unter bestimmten Annahmen hinsichtlich der Fähigkeiten der potentiellen Angreifer, aber nur, falls die Entwickler der Verschlüsselungsverfahren diese korrekt implementiert und die Entwickler der Anwendungen diese korrekt in ihren Code integriert haben. Und da liegen einige nicht vernachlässigbare Probleme: Die Einrichtung der Verfahren ist umständlich, und App- und Software-Entwickler sind keine Kryptographie-Experten. Sie machen Fehler. Allein in den Jahren 2013 bis 2015 sind 1769 Sicherheitsschwachstellen, die in der „National Vulnerability Database" (http://nvd.nist.gov), der nationalen Schwachstellen-Datenbank der USA, registriert wurden, auf solche Fehler zurückzuführen – damit waren in diesem Zeitraum Probleme mit der Integration von Verschlüsselungsverfahren in Anwendungen die vierthäufigste Quelle von registrierten Schwachstellen.

Das ist nicht verwunderlich, wenn man Studien betrachtet, die in den letzten Jahren während der wichtigsten wissenschaftlichen Konferenzen im Bereich der Cybersicherheit veröffentlicht wurden. Diese zeigen nämlich, dass die Integration eine wichtige Schwachstelle ist, insbesondere auch, weil die Nutzung kryptographischer Bibliotheken Wissen über zu viele Details erfordert, das Anwendungsprogrammierer oft nicht besitzen. Die Entwickler müssen etwa dafür sorgen, dass einzelne Schritte eines Verschlüsselungsverfahrens in einer bestimmten Reihenfolge ausgeführt werden. Dafür gibt es, je nachdem, was geschützt werden soll, konkrete Empfehlungen. Entwickler haben aber oft nicht die Zeit, sich mit entsprechenden Handbüchern zu beschäftigen. Eine weitere Fehlerquelle sind die sogenannten digitalen Zertifikate, welche die Gültigkeit eines Schlüssels bestätigen. Manchmal schalten Entwickler das Validierungsverfahren für die Zertifikate ihrer Software aus, um sie schneller testen zu können und vergessen anschließend, es wieder einzuschalten. „Beide Fehler geschehen häufig, auch bei seriösen Anbietern, und das sind nur zwei Beispiele unter vielen", sagt Mira Mezini, Leiterin des Fachgebietes Softwaretechnik an der TU Darmstadt. Angreifer haben stets den Vorteil, dass sie nur eine Sicherheitslücke finden müssen, um Daten abzugreifen, während die Entwickler vor der gewaltigen Aufgabe stehen, alle denkbaren Lücken zu schließen.

Es sei weder möglich noch sinnvoll, dass alle Software-Entwickler zugleich Verschlüsselungsexperten seien, insbesondere, wenn man bedenke, dass laut einem Bericht von IDC vom Dezember 2013, zu finden unter http://bit.ly/2a86Mju, unter den weltweit 18.5 Millionen Software-Entwicklern 7.5 Millionen Hobby-Programmierer seien – Tendenz steigend, so Mira Mezini. „Deshalb sollten sich Kryptographie-Experten und Software-Entwickler besser gegenseitig ergänzen." Genau das ist der Ansatz in dem von der Deutschen Forschungsgemeinschaft geförderten Sonderforschungsbereich „CROSSING" an der TU Darmstadt. Ein interdisziplinäres Team der TU Darmstadt entwickelt darin nicht nur neuartige Verschlüsselungsverfahren, sondern auch neuartige Sicherheitslösungen, um die Integration von Verschlüsselungsverfahren in Anwendungsprogrammcodes zu vereinfachen und damit langfristig das Vertrauen in die Informationstechnik zu stärken.

In „CROSSING" gibt es drei Schwerpunkte: Zum einen entwickeln die Forscher neue kryptographische Primitive. Das sind die kleinsten Bausteine in kryptographischen Verfahren. Im zweiten Schwerpunkt

Informationen

Fachgebiet Softwaretechnik
Prof. Dr.-Ing. Mira Mezini
Telefon: 06151/16-21360
E-Mail:
mezini@st.informatik.tu-darmstadt.de
www.stg.tu-darmstadt.de

entstehen aus diesen Primitiven neue kryptographische Systeme. Im dritten Schwerpunkt, in dem Mira Mezini beteiligt ist, unterstützen die Forscher die Software-Entwickler dabei, kryptographische Primitive und Systeme in ihren Anwendungen fehlerfrei einzusetzen. Gerade dies kam in der Cybersicherheitsforschung bisher zu kurz. „Bislang hat sie sich, wenn überhaupt, auf Endnutzer von Software konzentriert, um ihnen Software-Werkzeuge zur Verfügung zu stellen, mit denen sie sich vor schadhafter Software schützen können“, sagt Mezini. In CROSSING stünden erstmalig Software-Entwickler im Mittelpunkt.

Doch wie können die Forscher den Entwicklern helfen? „Unsere Annahme ist, dass die Fehler, die sie bei der korrekten Nutzung der kryptographischen Verfahren machen, deutlich reduziert werden können, wenn wir mehr auf die Bedürfnisse der Entwickler eingehen und sie aktiv bei der Integration der Verschlüsselungsverfahren in die Anwendungsprogrammcodes mit intelligenten Werkzeugen unterstützen, sprich mit intelligenten Verschlüsselungsbibliotheken, deren Komponenten zu einem signifikanten Anteil sich selbst automatisiert in die Anwendungscodes einbauen.“ In einem ersten Schritt hat Mezinis Team die Kernfrage in einer empirischen Studie an die Entwickler selbst gerichtet. „Entwickler arbeiten aufgabenorientiert“, sagt sie. „Sie wünschen sich Verschlüsselungsbibliotheken, die ihnen sagen: Diese Verschlüsselungskomponenten gibt es für deine Aufgabe, und so muss man sie konfigurieren, kombinieren und nutzen, damit sie für diese Aufgabe Sicherheit gewährleisten. Am besten wäre es, wenn die Bibliothek diese Aufgaben für die Entwickler übernehmen – also automatisiert umsetzen – könnte.“ Ein Entwickler möchte zum Beispiel einen Kommunikationskanal verschlüsseln. Die Bibliothek schlägt ihm dann die Komponenten für die Verschlüsselung vor und wie sie konfiguriert und integriert werden, damit sie sich gegenseitig nicht negativ beeinflussen. Das Ziel ist, geeignete softwaretechnische Methoden und Verfahren zu entwickeln, welche in intelligente Verschlüsselungsbibliotheken eingebaut werden. In einem weiteren Schritt soll das Verfahren weiter automatisiert werden. Am Ende gibt es in der intelligenten Verschlüsselungsbibliothek zwei Schnittstellen: Die eine besteht zu den Herstellern neuer kryptographischer Verfahren und überprüft, ob die Verfahren korrekt implementiert sind, die zweite zu den Software-Entwicklern und stellt sicher, dass korrekt implementierte Verschlüsselungsverfahren auch korrekt in Anwendungssoftware integriert und benutzt werden. So werden Verfahren doppelt geprüft – beim Hochladen in die Verschlüsselungsbibliothek und während der Implementierung der Anwendungssoftware. Letzteres geschieht idealerweise direkt in einer Software-Entwicklungsumgebung.

Software wird heute in solchen Entwicklungsumgebungen programmiert. Es handelt sich um integrierte Werkzeuge, die das Programmieren, Überprüfen und Testen von Software vereinfachen. Die populärste Entwicklungsumgebung für die Programmiersprache JAVA ist „Eclipse“. Mezini sagt: „Wir möchten zunächst die Funktionalität von Eclipse durch die Anbindung zu unserer intelligenten Verschlüsselungsbibliothek so erweitern, dass bereits während der Programmierung im Hintergrund laufend geprüft wird, ob die kryptographischen Algorithmen an der richtigen Stelle sind und korrekt konfiguriert und eingesetzt werden. Weitere Entwicklungsumgebungen können ebenso erweitert werden.“ Dieses Vorgehen würde zudem gewährleisten, dass eine Anwendung auch dann noch sicher bleibt, wenn der Programmierer sie weiter entwickelt bzw. wenn Verschlüsselungsverfahren, die über die Bibliothek integriert wurden, als nicht mehr sicher gelten. Die Entwickler sparen somit Zeit und können sich darauf verlassen, stets das aktuell bestmöglichste Verfahren eingesetzt zu haben.

Abbildung: Katrin Binner

Informatik-Professorin Mira Mezini, Leiterin des Fachgebiets Softwaretechnik an der TU Darmstadt.

Neben Mezini und dem Kollegen Eric Bodden, der vor einigen Monaten an die Universität Paderborn gewechselt ist, arbeiten zwei Doktoranden und ein PostDoc an dem Projekt. „Wir hoffen, dass langfristig eine aktive Community entsteht, die unsere Verschlüsselungsbibliothek lebendig hält“, sagt Mezini. „Eine wichtige Basis haben wir geschaffen, indem wir Kryptographen und Software-Ingenieure zumindest an der TU Darmstadt enger zusammen gebracht haben. Das passiert weltweit noch viel zu selten.“

Der Autor ist Technikjournalist.