Geheimschriften in der Praxis

Die Kryptografie hat eine sehr lange Geschichte – seit Entwicklung der Schrift haben Menschen nach Techniken gesucht, das geschriebene Wort vor den Augen unbefugter Dritter zu verbergen. Und ebenso intensiv wurde nach Methoden geforscht, Verschlüsseltes wieder lesbar zu machen. Es gibt zahlreiche belegte Fälle, in denen die unerwartete Entschlüsselung geheimer Nachrichten Weltgeschichte geschrieben hat – viele davon sind in dem Buch „Geheime Botschaften" von Simon Singh nachzulesen – wie das Babington-Komplott, das zum Todesurteil von Maria Stuart führte, das Zimmermann-Telegramm, das den Eintritt der USA in den ersten Weltkrieg zur Folge hatte, oder das Brechen der deutschen Chiffriermaschine Enigma durch die Polen und Engländer, das den U-Boot-Krieg entschied und das Ende des 2. Weltkriegs einleitete.

Die wirksame Verschlüsselung von Nachrichten hat mit dem Computerzeitalter noch an Bedeutung gewonnen. Heute stehen uns dank Computern weit komplexere Verschlüsselungsalgorithmen zur Verfügung als vor 70 Jahren – aber auch die Kryptoanalytiker profitieren von der schnellen Rechentechnik. Wie schon in der Geschichte der Kryptoanalyse sind auch heute viele Angriffe gar nicht auf dem „direkten" Weg – der Analyse des Verschlüsselungsverfahrens selbst – erfolgreich, sondern erreichen das Ziel, indem sie Seiteneffekte des Verfahrens untersuchen (Zeit, Stromverbrauch, Abstrahlung etc.), um daraus Rückschlüsse auf das verwendete Schlüsselmaterial zu ziehen. Beispiele für solche Seitenkanalanalysen finden sich in diesem Heft.

Manchmal machen es die Entwickler von kryptografischen Verfahren und sicherheitsrelevanten Produkten den Kryptoanalytikern allerdings auch besonders leicht, wie zuletzt die Analyse des in Bayern eingesetzten „Bundestrojaners" durch den Chaos Computer Club gezeigt hat: Zur Verschlüsselung der an die Strafverfolgungsbehörden übermittelten Daten wurde zwar das Standard-Verfahren AES verwendet, allerdings im ECB-Mode (unverknüpfte 128-bit-Blöcke) und mit einem in der Software fest programmierten und immer gleichen Schlüssel.[1]

Die Verwendung moderner Kryptoverfahren – z. B. zur Erzeugung und Prüfung digitaler Signaturen – erfordert jedoch nicht nur eine korrekte Implementierung, sondern auch Verfahren und Prozesse, die die Vertrauenswürdigkeit des Schlüsselmaterials sicherstellen. Dass das in der Praxis nicht so einfach ist, zeigen nicht nur aktuelle Vorfälle bei Zertifizierungsinstanzen, bei denen geheimes Schlüsselmaterial abhanden kam oder erfolgreich Schlüssel unter einer falschen Identität zertifiziert wurden. Auch bei der grenzüberschreitenden Vertrauenswürdigkeit und Akzeptanz digitaler Signaturen in Europa zeigen sich die Tücken im Detail, wie die Beiträge in diesem Heft zeigen.

Aus den Erfahrungen der vergangenen zehn Jahre müssen wir lernen, dass sich der sichere Einsatz kryptografischer Produkte in der Praxis ohne Systemsicherheit, korrekte Implementierungen, bewährte operative Prozesse, vertrauenswürdige Instanzen und für den Umgang mit Schlüsseln und kryptografischen Verfahren sensibilisierte Benutzer nicht erreichen lässt.

Mit der wachsenden Bedeutung der Kryptografie und der steigenden Komplexität heutiger IT-Systeme ist zu erwarten, dass dies auch in Zukunft keine geringe Herausforderung sein wird.

Dirk Fox und Peter Schartner

1 Chaos Computer Club: *Analyse einer Regierungs-Malware*, Oktober 2011. URL: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf