Für jedes Problem das richtige Werkzeug: Stochastik bei Seitenkanalangriffen

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

Die Evaluierung kryptographischer Algorithmen und Protokolle erfordert den Einsatz zum Teil tiefliegender Techniken aus unterschiedlichen mathematischen Gebieten. Besondere Bedeutung besitzen u.a. die Zahlentheorie wie auch algebraische und komplexitätstheoretische Ansätze. Stochastik und Statistik spielen dagegen eine eher untergeordnete Rolle.

Starke kryptographische Algorithmen und Protokolle sind jedoch nur eine notwendige, aber keineswegs eine hinreichende Voraussetzung für sichere IT-Systeme. Ebenso wichtig ist ihre sichere Implementierung und dabei insbesondere das Zusammenspiel mit den kryptographischen Mechanismen und ihrer algorithmischen Umsetzung. Die Chipkartenindustrie und universitären Forschungsgruppen verfolgen daher vor allem Seitenkanalangriffe mit großer Aufmerksamkeit und entwickeln sie weiter. Seitenkanalangriffe richten sich meist gegen Chipkarten, aber in den letzten Jahren sind auch Softwareimplementierungen verstärkt in den Fokus geraten.

Vereinfacht gesagt, versuchen Seitenkanalangriffe, aus physikalischen Messwerte (z.B. Laufzeiten, Stromaufnahme oder elektromagnetische Abstrahlung) teilschlüsselabhängige Informationen zu extrahieren, um den gesuchten Schlüssel in kleinen Portionen (z.B. bit- oder byteweise) zu bestimmen. Diese teilschlüsselabhängigen Nutzinformationen werden jedoch in aller Regel durch weitere arithmetische Operationen und / oder gezielte algorithmische oder Hardware-Gegenmaßnahmen überdeckt und damit verschleiert. Ein gemeinsames Ziel von Angreifern und Designern von Kryptosystemen besteht darin, einen Angriff bzw. einen Klasse von Angriffen zu optimieren, wenngleich aus völlig unterschiedlichen Gründen. Während ein Angreifer schlicht seine Erfolgsaussichten optimieren möchte, ermöglicht dies dem Designer, das wahre Risikopotential auszuloten und zuverlässige und vertrauenswürdige Gegenmaßnahmen zu entwickeln.

Fortgeschrittene stochastische und statistische Ansätze haben sich bei vielen unterschiedlichen Problemstellungen als die geeigneten Werkzeuge erwiesen, dieses Ziel zu erreichen. Gerade bei hardwarenahen Kryptographietagungen besitzen konkrete experimentelle Resultate, etwa das Brechen einer Testimplementierung samt einer ad-hoc Gegenmaßnahme, häufig einen höheren Stellenwert als die verwendeten mathematischen Methoden und eine tiefer gehende Analyse der Situation, um die eigentliche Ursache für den Angriff herauszuarbeiten und in einem zweiten Schritt zuverlässige Gegenmaßnahmen auch für modifizierte Angriffsvarianten zu entwickeln. Zudem erreichen Erkenntisse von hardwareorientierten Fachtagungen Softwareentwickler oft nur mit großer zeitlicher Verzögerung, obwohl ähnliche stochastische Ansätze teilweise auch Seitenkanalangriffe gegen Softwareimplementierungen ermöglichen (auch wenn die Angriffe im Detail sehr verschieden sein können). Diese beiden Effekte haben in der Vergangenheit verschiedentlich (z.B. bei OpenSSL) dazu geführt, dass Schutzmaßnahmen schrittweise nachgebessert werden mussten, nämlich als Antwort auf neue Angriffe.

Im Vortrag werden verschiedene Angriffe gegen Chipkarten und Softwareimplementierungen besprochen. Gemeinsamkeiten und Unterschiede werden herausgearbeitet, die angewandten stochastischen Methoden dargestellt und Implikationen aufgezeigt.