VerSchlüsselerlebnisse

CrypTool unterstützt Verständnis für die Grundlagen der Internetsicherheit

Ein wesentlicher Aspekt der Maßnahmen zur Informations-Sicherheit ist die Sensibilisierung von Mitarbeitern. Um ein Grundverständnis, eigene Einsicht, im Idealfall sogar Interesse für das Thema Kryptographie zu vermitteln, hilft das Freeware-Paket CrypTool, indem es die Grundlagen von Verschlüsselung und digitaler Signatur veranschaulicht und die Folgen falscher Anwendung erfahrbar macht.

Von Bernhard Esslinger, Frankfurt

In einer idealen Welt hat jede Institution oder Firma eine Security Policy, die die Wichtigkeit der gespeicherten Informationen herausstellt. Alle Mitarbeiter sind ausreichend sensibilisiert, die IT hat die entsprechenden Maßnahmen und Prozesse implementiert und jeder weiß konkret, was das bedeutet und wie er sich zu verhalten hat. Leider leben wir nicht in einer idealen Welt... Daher muss man sowohl an Technik und Organisation als auch an der Sensibilisierung der Mitarbeiter (Awareness) immer wieder arbeiten.

Wird der Stellenwert von Technik und Organisation nur selten in Frage gestellt, so wird die Mitarbeiter-Awareness oft etwas stiefmütterlich behandelt. Obwohl diese dritte Säule der IT-Sicherheit ebenfalls eine conditio-sine-qua-non ist, begegnet man hier häufig einer großen Zögerlichkeit. Dabei geht es um das Wichtigste im Unternehmen: den Menschen. Und hier ist sehr viel Fingerspitzengefühl erforderlich, denn Menschen sind verschieden, kommen aus unterschiedlichen Kulturen und man muss die richtige Balance innerhalb der normalen Arbeitsabläufe finden.

Inzwischen haben viele Firmen Maßnahmen ergriffen, wie beispielsweise:

_____ Belehrung durch die Personalabteilung gleich bei der Einstellung,

_____ Einbau von Sicherheitsthemen in die allgemeine Mitarbeiter-Schulung,

_____ Intranet-Webseiten zur IT-Sicherheit (inkl. CERT),

_____ gedruckte Broschüren mit allen wichtigen Maßnahmen und Informationen,

_____ Fortbildungen, welche die recht anspruchsvolle Thematik der Internetsicherheit erfahrbar machen und ihre Grundlagen vermitteln.

Den letzten Punkt unterstützt das Freeware-Paket CrypTool, und zwar sowohl für den interessierten Endanwender als auch für Entwickler und Designer. CrypTool liegt komplett mit umfangreicher Online-Dokumentation auf Deutsch und Englisch vor.

Verständnis vermitteln

CrypTool vermittelt das notwendige Grundverständnis für die Kryptographie, die inzwischen fast unsichtbar nicht nur bei der Internetnutzung, sondern auch im Alltag Eingang gefunden hat. In der Deutschen Bank wird das Tool zum Beispiel bereits in der Ausbildung der Azubis verwendet.

Mit CrypTool kann man verschiedene Verschlüsselungsverfahren ausprobieren und auch analysieren. Es zeigt sich, dass und wie selbsterfundene oder klassische Verfahren automatisiert zu knacken sind. So zum Beispiel das bis ins 19. Jahrhundert als absolut sicher geltende Vige-

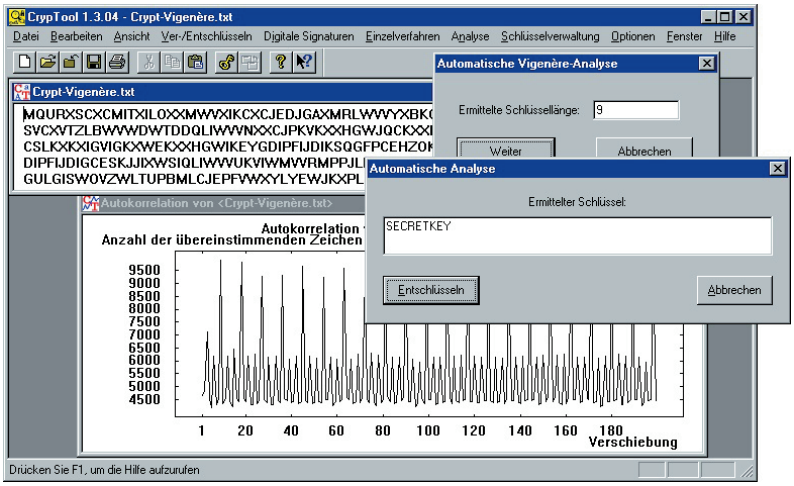

Bild 1: Analyse des klassischen Verfahrens von Vigenére. Mithilfe der Autokorrelation lässt sich bei der polyalphabetischen Substitution die Schlüssellänge bestimmen. Die anschließende Cäsar-Analyse liefert den geheimen Schlüssel.

nére-Verfahren: eine polyalphabetische Erweiterung der Cäsar-Verschlüsselung, die ohne großen Aufwand mithilfe von Autokorrelation und einfacher Frequenzanalyse automatisch zu brechen ist (vgl. Bild 1). Ebenso erhält man ein Gefühl dafür, dass auch moderne Verfahren bei zu kurzer Schlüssellänge per Brute-Force knackbar sind (Bild 2).

Der in CrypTool gesetzte Schwerpunkt der Gegenüberstellung von Kryptoverfahren und Kryptoanalyse hilft zu verstehen, dass es für jedes Verschlüsselungsverfahren mehr oder weniger erfolgreiche Analysemethoden gibt. Einige sind voll automatisiert, während man sich bei anderen Methoden als echter Code-Brecher versuchen kann, um sich, ausgehend von einem vermuteten Text(fragment), Schritt für Schritt mit den jeweils gewonnenen Informationen dem geknackten Klartext anzunähern.

Digitale Signaturen

Die symmetrische Ver- und Entschlüsselung ist der leichter zu beherrschende Teil der heutigen Kryptographie. Die für viele Laien neuen Methoden der asymmetrischen Kryptographie sind dagegen der Schlüssel für die Realisierung von Authentizität, Integrität und digitaler Signatur im Internet. In CrypTool wurde daher besonders viel Wert auf das bekannte RSA-Kryptosystem gelegt. Wer Grundkenntnisse in Mathematik besitzt, kann sich mithilfe der RSA-Demonstration sein eigenes Schlüsselpaar erzeugen und die einzelnen Schritte der Ver- und Entschlüsselung nachvollziehen: Man kann Nachrichten verschlüsseln und eine Signatur verifizieren und auch einen Faktorisierungsangriff auf den öffentlichen RSA-Schlüssel starten. Der Angriff ist mit CrypTool bis zu Schlüssellängen von 250 Bit erfolgreich (Quadratische-Sieb-Methode).

Die Demonstration des RSA-Kryptosystems ermöglicht zu verste-

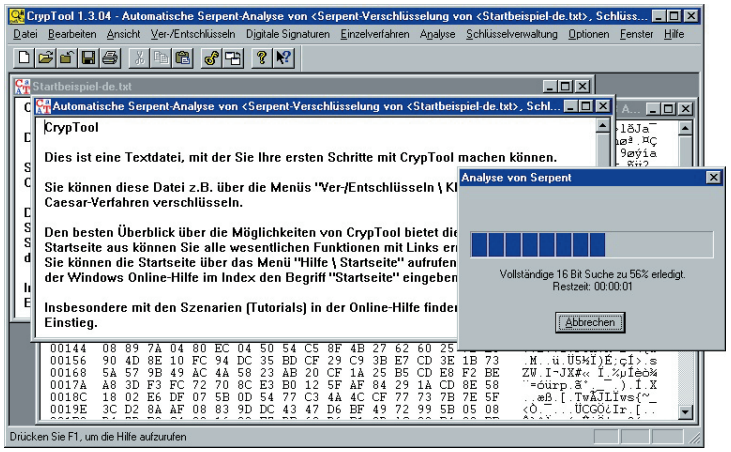

Bild 2: Brute-Force-Analyse eines modernen symmetrischen Verfahrens. Mithilfe der Entropie können der wahrscheinlichste Ausgangstext und der Schlüssel identifiziert werden. Mit CrypTool lassen sich mit einem durchschnittlichen PC bis zu 20 unbekannte Bit eines Schlüssels innerhalb weniger Minuten finden.

Historie von CrypTool

Gerade Awareness und Sensibilität der Menschen für das Thema Kryptographie erreicht man am besten durch eigene Erfahrung und didaktisch gut aufbereitete Information. Diesem Zweck dient das Programm CrypTool. Seine Entwicklung unter der Leitung von Bernhard Esslinger wurde vor rund fünf Jahren bei der Deutschen Bank im Zuge des End-User-Awareness-Programms begonnen. Inzwischen arbeiten mehrere Firmen und Hochschulen damit und entwickeln es gemeinsam weiter. Seit fast drei Jahren steht es als Freeware zur Verfügung und fand beispielsweise auch Eingang auf der Bürger-CD des BSI (s. a. www.bsi-fuer-buerger.de).

Die monatliche Downloadrate von CrypTool liegt bei über 1000. Eingesetzt wird es sowohl in Firmen zur Steigerung der Sensibilität für IT-Sicherheit als auch in der Lehre an mehreren Hochschulen und in der Ausbildung an Schulen und bei Azubis.

CrypTool bietet einen spielerischen Einstieg in die Kryptographie. Es steht komplett auf Deutsch und Englisch zur Verfügung. Neben vielen Funktionen aus der klassischen und modernen Kryptographie und Kryptoanalyse umfasst es eine umfangreiche Online-Dokumentation.

Das bisher vor allem von der Deutschen Bank, der Secude GmbH und dem Forschungszentrum Informatik Karlsruhe entwickelte und betreute Programm wurde im September 2002 an den von Frau Prof. Dr. Claudia Eckert geleiteten Lehrstuhl *Sicherheit in der Informationstechnik* (Fachbereich Informatik) der TU Darmstadt übergeben, wo es als Open-Source-Projekt weiterentwickelt und der Internet-Gemeinde zur Verfügung gestellt wird.

Nutzen und Einsatzgebiete:

_____ Mitarbeiter: Awareness für IT-Sicherheit, allgemeine Mitarbeiter-Schulung,
_____ schnelleres und besseres Verständnis,
_____ Entwickler: bessere Konzepte, korrekter Einsatz der Kryptographie.

CrypTool liegt auf www.cryptool.de zum kostenlosen Download und Einsatz bereit. Den besten Einstieg finden Sie ausgehend von der Startseite der Online-Hilfe, indem Sie die Links ausprobieren und die Szenarien durchspielen.

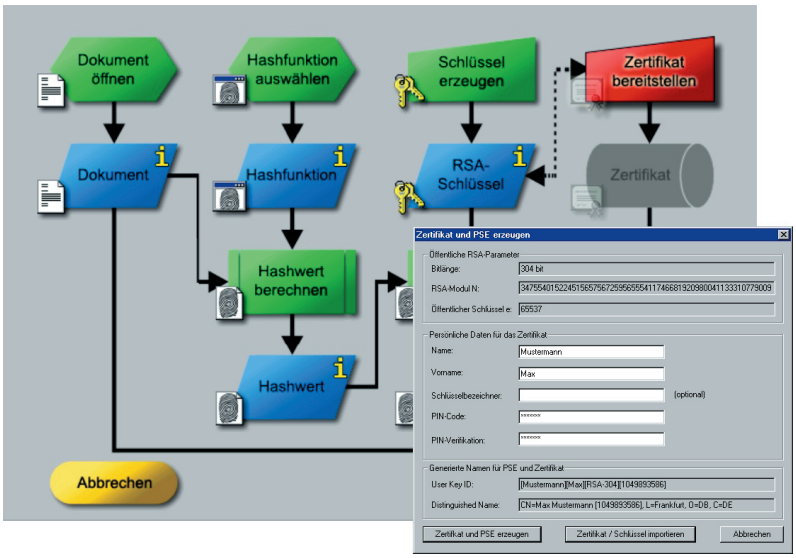

Bild 3: Erzeugen eines eigenen RSA-Zertifikats im Rahmen der Signatur-Demonstration

hen, wie RSA funktioniert und ab welcher Schlüssellänge das System sicher ist. Weitere Details und aktuelle Forschungsergebnisse sind einem mit CrypTool ausgelieferten Skript zu entnehmen.

Passwörter

Mit dem Verständnis der Arbeitsweise kryptographischer Algorithmen schafft Cryptool gleichzeitig ein Bewusstsein für das, was starke Kryptographie *nicht* leisten kann, zum Beispiel ein gutes Passwort zu wählen. Die Wahl schlechter Passwörter ist der noch immer häufigste Fehler von Anwendern. Hier kann man mit Demonstrationen anhand echter Passwortdateien und ihrer Analyse mit Tools wie John-the-Ripper (www.openwall.com/john/) echte Aha-Erlebnisse schaffen.

Darüber hinaus müssen aber auch die Entwickler und Administratoren wissen, wie sie mit den Passwörtern umgehen sollten. Selbst wenn eine kryptographische Anwendung sicher ist, so ist letztendlich die Benutzersicherheit von einem geheimen Text – dem „Passwort" – abhängig.

Das Passwort selbst ist aber in der Regel für Kryptosysteme nicht direkt anwendbar, sondern man berechnet aus dem Passwort erst den eigentlichen Schlüssel. Dabei kommt es auf die richtige Anwendung der entsprechenden Algorithmen an.

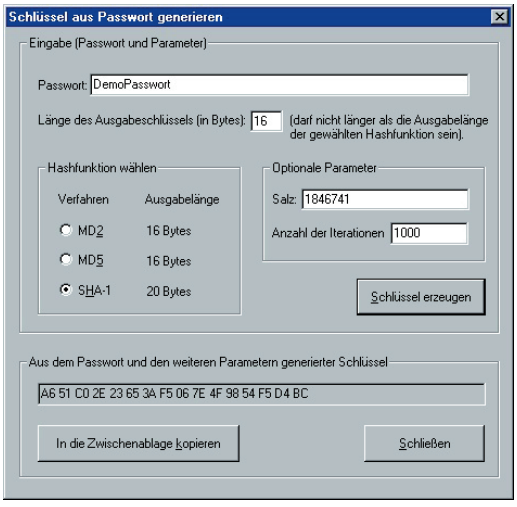

Bild 4: Schlüsselgenerierung aus einem Passwort nach PKCS#5

CrypTool zeigt beispielsweise, wie per PKCS#5-Verfahren [5] ein Hashwert berechnet wird (vgl. Bild 4), aus dem auf das ursprüngliche Passwort nicht direkt zurückzurechnen ist. Der hergeleitete Schlüssel ist neben dem Passwort auch von anderen Parametern abhängig: Der zusätzliche Initialisierungswert, das „Salz", ermöglicht es aus ein und demselben Passwort unterschiedliche Schlüssel zu generieren. Die Anzahl der Hash-Iterationen erhöht indessen den Aufwand für Wörterbuchangriffe.

Wenn Angreifer die Datei der gehashten Passwörter erlangen und womöglich sogar die Parameter wie Hashverfahren, Anzahl der Hash-Iterationen sowie den für jedes Passwort individuellen Salzwert kennen, dann führen Brute-Force- oder Wörterbuch-Attacken bei schlecht gewählten Passwörtern sehr schnell zum Erfolg. Wenn die Entwickler des Systems die Parameter der PKCS#5-Aufruffunktionen nicht angemessen ausgenutzt haben, geht es umso leichter. Bei einem Angriff auf eine Passwortdatei, die keinen Salzwert nutzt, lassen sich beispiels-weise alle Passwörter gleichzeitig analysieren. Eine Attacke auf eine produktive Passwortdatei ohne Salz mit 3 000 Passwörtern hat etwa gezeigt, dass 50 % davon mit einem normalen PC innerhalb eines Tages zu bestimmen waren.

Es sollte jedem bewusst sein, dass gegen einen Angreifer, der die Passwortdatei in die Hand bekommen hat, letztendlich nur gute Passwörter helfen. Und Administratoren sollten sich immer wieder vergewissern, dass es keine Möglichkeit gibt, diese Passwortdateien zur Analyse herunterzuladen.

Entwicklerhilfe

Wenn Entwickler unter Zeitdruck eine über das Internet zugängliche Ressource schützen müssen, kommt es vor, dass sie sich „abenteu-

Kryptographie	Kryptoanalyse
Verschlüsselungsklassiker ■ Cäsar ■ Vigenére ■ Hill ■ Monoalphabetische Substitution ■ Homophone Substitution ■ Playfair ■ Permutation ■ Addition ■ XOR ■ Vernam	Angriffe auf klassische Verfahren ■ ciphertext only: Cäsar, Vigenére, Addition, XOR ■ known plaintext: Hill, Playfair ■ manuell: Monoalphabetische Substitution
Zum besseren Nachvollziehen von Literaturbeispielen ist ■ Alphabet wählbar ■ Behandlung von Leerzeichen etc. einstellbar	Unterstützende Analyseverfahren ■ Entropie, gleitende Häufigkeit ■ Histogramm, N-Gramm-Analyse ■ Autokorrelation ■ ZI P-Kompressionstest
Moderne symmetrische Verschlüsselung ■ IDEA, RC2, RC4, DES, 3DES ■ AES-Kandidaten der letzten Auswahlrunden ■ AES (=Rijndael)	Brute-Force-Angriff auf symmetrische Algorithmen ■ für alle Algorithmen ■ Annahme: Entropie des Plaintext klein ■ 20 Bit innerhalb von Minuten abgesucht
Asymmetrische Verschlüsselung ■ RSA mit X.509-Zertifikaten ■ RSA-Demonstration (zum Nachvollziehen von Literaturbeispielen, Alphabet und Blocklänge einstellbar)	Angriff auf RSA-Verschlüsselung ■ Faktorisierung des RSA-Moduls ■ praktikabel bis ca. 250 Bit bzw. 75 Dezimalstellen
Hybridverschlüsselung (RSA + AES) ■ visualisiert als interaktives Datenflussdiagramm	Angriff auf Hybridverschlüsselung ■ Angriff auf RSA oder ■ Angriff auf AES
Digitale Signatur ■ RSA mit X.509-Zertifikaten (Signatur zusätzlich visualisiert als interaktives Datenflussdiagramm) ■ DSA mit X. 509-Zertifikaten ■ Elliptic Curve DSA, Nyberg-Rueppel	Angriff auf RSA-Signatur ■ Faktorisierung des RSA-Moduls ■ praktikabel bis ca. 250 Bit bzw. 75 Dezimalstellen
Hashfunktionen ■ MD2, MD4, MD5 ■ SHA, SHA-1, RIPEMD-160	kein Angriff implementiert
Zufallsgeneratoren ■ Secude ■ X##2 modulo N ■ Lineare Kongruenz Generator (LCG) ■ Inverse Kongruenz Generator (ICG)	Analyse von Zufallsdaten ■ FIPS-PUB-140-1 Test-Batterie ■ Periode, Vitany, Entropie ■ Gleitende Häufigkeit, Histogramm ■ N-Gramm-Analyse, Autokorrelation ■ ZIP-Kompressionstest

Tabelle 1: Gegenüberstellung der in CrypTool implementierten Verfahren und ihrer Analysemethoden

Literatur

[1] CrypTool Homepage, www.cryptool.de

[2] Bernhard Esslinger, CrypTool – spielerischer Einstieg in klassische und moderne Kryptographie, DuD 10/2002

[3] Henrik Koy, Jörg Schneider, Selbst geknackt, c't 14/2001, S. 204

[4] Claudia Eckert, IT-Sicherheit, Konzepte – Verfahren – Protokolle, Oldenbourg, 2. Aufl. 2003, ISBN 3-486-27205-5

[5] RSA Laboratories, PKCS #5 v2.0 Password-Based Cryptography Standard, 1999, www.rsasecurity.com/rsalabs/pkcs/pkcs-5/

[6] Jan Blumenstein, Methoden und Werkzeuge für Angriffe auf die digitale Signatur, Bachelor-Arbeit des Kooperativen Studiengangs Informatik an der Fachhochschule Darmstadt, 2003

[7] Donald E. Knuth, The Art of Computer Programming, Vol.2: Seminumerical Algorithms, Addison-Wesley, ISBN 0-2018-9684-2

erliche", selbst entwickelte Kryptosysteme ausdenken (vgl. www. counterpane.com/crypto-gram-9902. html#snakeoil). Beliebt sind Varianten der polyalphabetischen Substitution. CrypTool führt Entwicklern vor Augen, dass solche Systeme sich oft allein mit statistischen Verfahren analysieren und knacken lassen (vgl. Bild 1).

Aber auch wenn Entwickler bewährte Kryptographie-Bibliotheken nutzen, fehlt ihnen oft das Verständnis, wie diese Funktionen sicher einzusetzen sind. Häufige Fehler sind beispielsweise erratbare Session-IDs, öffentlich lesbare Passwortdateien gekoppelt mit unzureichenden Methoden für die Berechnung von Passwort-Hashes oder die Nutzung symmetrischer Verschlüsselung mit zu kleinen Schlüssellängen (wie RC4 mit 40 Bit). Auch hier liefert CrypTool erfahrbare Hintergrundinformationen zu den wichtigsten kryptographischen Methoden wie Zufallsgeneratoren, symmetrischen/asymmetrischen Verschlüsselungs- sowie Hashverfahren.

CrypTool selbst verwendet zum Beispiel die Industrie-bewährte SECUDE-Bibliothek (www.secude.de) zur symmetrischen Verschlüsselung sowie für digitale Signaturen. Entwickler können diese Funktionen als Referenz-Implementierung nutzen.

Visualisierungen

Nachdem die Basisverfahren (oder kryptographischen Primitive, wie die Zahlentheoretiker sagen) in CrypTool implementiert waren, wurde seit Version 1.3 besonderer Wert auf die didaktische Darstellung der modernen Verfahren gelegt:

_____ Ein interaktives Flussdiagramm zum Erzeugen digitaler Signaturen zeigt mit konkreten Zahlen alle Einzelschritte beim Signieren eines frei wählbaren Dokuments (s. Bild 3).

_____ Ein interaktives Flussdiagramm für die Hybridverschlüsselung unterstützt den Anwender, die Mechanismen hinter SSH-Verbindungen und S/MIME-E-Mail-Verschlüsselung zu verstehen.

_____ Änderungen in einem Textdokument können sofort als Hashwert-Änderung sichtbar gemacht werden (Hashwert-Demonstrator).

_____ Auch das für den Schlüsselaustausch wichtige Diffie-Hellman-Verfahren ist ab Version 1.3.04 (öffentlich verfügbar seit Mai 2003) als interaktives Flussdiagramm implementiert.

Für jeden mit mathematischem Abiturwissen gibt es die bereits erwähnte RSA-Demonstration, um tiefer in die Thematik der digitalen Signatur und der Hybridverschlüsselung einzusteigen. Beim Erstellen elektronischer Signaturen spielen neben den Signaturalgorithmen auch

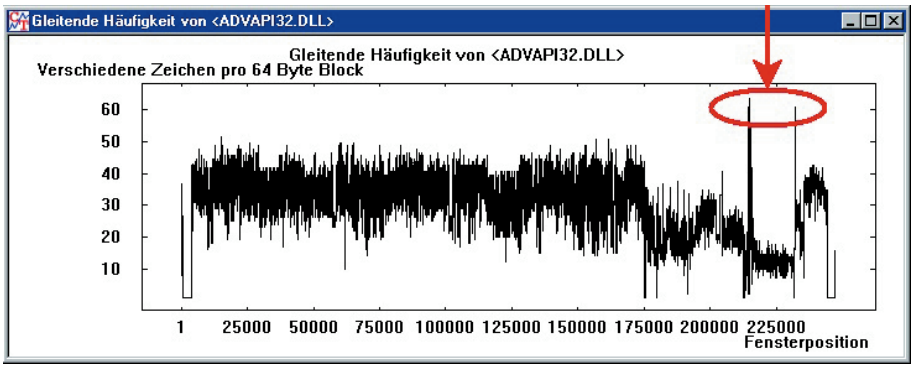

Bild 5: Die CrypTool-Funktion „Gleitende Häufigkeit" zeigt, dass in der Windows-Bibliothek advapi32.dll an zwei Stellen wahrscheinlich verschlüsselte Daten abgelegt sind. Im Beispiel zeigt sich der so genannte NSA-Key (vgl. www.cnn.com/TECH/computing/9909/03/windows.nsa.02/)

CrypTool als Rahmen für effiziente Diplomarbeiten

Das Potenzial, das CrypTool für die wissenschaftliche Entwicklung bietet, möge das Beispiel einer Bachelor-Abschlussarbeit in der Deutschen Bank verdeutlichen [6]. Dabei wurde das Thema der Hashfunktionen in CrypTool weiter vertieft: Die Implementierung des Floyd-Algorithmus hat gezeigt, wie wertvoll CrypTool als „Rahmen" sein kann. Studenten, die an Themen im Umfeld der Kryptographie arbeiten, können ihre Erkenntnisse damit schneller implementieren und sie auch für andere experimentell erfahrbar machen. Damit entsteht neben ihrer schriftlichen Ausarbeitung noch etwas Dauerhaftes und allgemein Nützliches.

Aufgabe der genannten Bachelor-Arbeit war es, digitale Signaturen durch Hashkollisionen mithilfe des Geburtstagsparadoxons praktisch anzugreifen und daraus eine Aussage zur Sicherheit heutiger Hashverfahren herzuleiten. Veranschaulichungen sind deshalb sehr wertvoll, da akademische Angriffe für „normale" Menschen nur schwer einzuschätzen sind.

Als Geburtstagsparadoxon wird das „paradoxe" Ergebnis bezeichnet, dass zwar 253 Gäste notwendig sind, damit wenigstens ein Gast mit 50 % Wahrscheinlichkeit am gleichen Tag wie der Gastgeber Geburtstag hat, hingegen aber schon bei 23 Gästen diese Wahrscheinlichkeit erreicht wird, wenn man nur fordert, dass wenigstens zwei Gäste am gleichen Tag Geburtstag haben.

Beim so genannten Geburtstagsangriff werden – ausgehend von zwei Nachrichten M1 und M2 mit unterschiedlichen Hashwerten – zwei veränderte Nachrichten M1' und M2' mit identischem Hashwert bestimmt. Diese unterscheiden sich nur durch unsichtbare Zeichen von den Ausgangsnachrichten (z. B. zusätzliche Leerzeichen am Zeilenende). Später wird die unverfängliche Nachricht M1' dem Opfer zum Signieren vorgelegt. Der Angriff ist erfolgreich, wenn die Nachricht M1' signiert wurde. Durch den Austausch von M1' mit M2' erhält der Angreifer eine gültige Signatur für M2' (perfekte Fälschung). Mithilfe des Geburtstagsparadoxons zeigt man, dass für Hashfunktionen der Bitlänge x im Mittel nach Erzeugung von etwa $2^{(x/2)}$ Nachrichten M1' und M2' eine Hashkollision gefunden wird. Die Suche der Hashkollision wird mit dem Floyd-Algorithmus implementiert (s. Exercise 3.1-6 in [7]).

So wie man mit dem Brute-Force-Verfahren beliebige Verschlüsselungsalgorithmen angreifen kann, so generisch kann man mit dem Floyd-Algorithmus jedes beliebige Hashverfahren angreifen, ohne dass man Kenntnis von eventuellen Strukturschwächen haben müsste.

Die Implementierung in CrypTool im Rahmen der Bachelor-Arbeit von Jan Blumenstein führte zu einer didaktisch-anschaulichen Beschreibung des Angriffs und einer klaren Aussage zur minimal notwendigen Länge von Hashwerten. Damit kann jeder die praktischen Ergebnisse der Arbeit nachvollziehen:

_____ Im Zeitraum von wenigen Tagen findet man mit einem einzigen PC in der MD5-Hashfunktion Teilkollisionen für bis zu 72 Bit. Diese Kollision in einem so kurzen Zeitraum zu finden, war selbst für die Fachleute der Deutschen Bank überraschend. Dazu fanden sich nach bestem Wissen des Autors in der Literatur bislang keine konkreten Angaben. Praktische Ergebnisse bleiben außerdem in der Regel besser haften als „abstrakte" Voraussagen.

_____ Aufgrund der praktischen Ergebnisse ist leicht einzusehen, dass digitale Signaturen mit Hashverfahren bis zu 128 Bit Länge gegenüber massiv parallelen Verfahren konkret angreifbar sind. Dies bestätigt das vorsichtige Vorgehen des BSI, für Hashverfahren wie RIPEMD einen genügend großen Sicherheitspuffer gegenüber den „aktuellen" Erkenntnissen zu fordern. Die Anforderungen des BSI an fortgeschrittene und qualifizierte Signaturen berücksichtigen bereits Hashverfahren mit diesen längeren Werten.

Hashwerte eine wichtige Rolle. Der Hashwert-Demonstrator liefert einen Eindruck für eine wesentliche Eigenschaft von kryptographischen Hash-Funktionen: selbst eine nur kleine Änderung der Eingabe verändert den Hashwert grundlegend. Damit kann jeder von Hand versuchen, eine Hashwert-Kollision zu bestimmen.

Ohne ein derart vermitteltes Grundverständnis dürften Mitarbeiter und Bürger nur schwer den richtigen Umgang mit elektronischen Ausweisen und Signatur-Zertifikaten pflegen. Die Hintergrundinformationen helfen darüber hinaus einzuschätzen und zu verstehen, welche Methoden das Internet wirklich sicher machen.

Das CrypTool-Paket steht unter www.cryptool.de (auf Deutsch) und www.cryptool.com/org (auf Englisch) zum Download zur Verfügung. Es wird unter der Federführung der TU-Darmstadt durch die Mitwirkung von interessierten „Laien" (z. B. Mitarbeiter von Firmen), Studenten und akademischen Mitarbeitern fortlaufend weiterentwickelt. ■

Bernhard Esslinger (bernhard.esslinger@db.com) ist Leiter IT-Sicherheit bei der Deutsche Bank AG und Lehrbeauftragter für IT-Security an der Uni Siegen.

Verantwortlich für die IT-Sicherheit…

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

<kes>

- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

ABONNEMENT-BESTELLUNG

☐ **Ich abonniere die Zeitschrift <kes> ab Heft Nr.....**
Als Dankeschön erhalte ich das erste Heft gratis.

Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem <kes>-Archiv.
Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars formlos widerrufen.

Nach Ablauf der Widerrufsfrist wird das Abonnement zu den regulären Bedingungen gültig:

Jahresbezugspreis (6 Ausgaben) € 122,00 inkl. MwSt. und Versandkosten (Schweiz SFr 238,00 / restl. Ausland € 137,00).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

Ich bin einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weitergibt.

PROBEHEFT-ANFORDERUNG

☐ Bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim