Interview mit Bruce Schneier

Bruce Schneier, Counterpane, schneier@counterpane.com
Marc Ruef, scip AG, maru@scip.ch

Bruce Schneier ist ein US-amerikanischer Experte für Kryptographie und Computersicherheit, Entwickler populärer Krypto-Algorithmen, Autor verschiedener Bücher über Computersicherheit und Mitgründer der Firma Counterpane Internet Security.

scip AG: Hallo Bruce. Danke, dass Du Dir die Zeit nimmst. Wie geht es Dir? Dein Assistent hat mich darüber informiert, dass Du unterwegs gewesen seist. Arbeitest Du Deine Vortragsreihe (Speaking Schedule, http://www.schneier.com/schedule.html) ab?

Bruce Schneier: Ja, die meisten Reisen, die ich unternehme, beinhalten Vorträge und dergleichen. Soeben bin ich von einem Seminar der Tufts Universität zurückgekommen, das den Titel "The Politics of Fear" trug. Nächste Woche trage ich dem Kongress meine Ansichten zum Thema Data-Mining vor und halte eine Präsentation an der Software Development West Konferenz. Danach werde ich nach Europa reisen, um dort einige Vorlesungen und Vorträge zu halten. So sieht der Grossteil meines gegenwärtigen Arbeitslebens aus.

Wann war denn das erste Mal, dass Du ernsthaft mit dem Thema Kryptographie in Kontakt gekommen bist? War Mathematik schon immer eines Deiner Hobbies?

Kryptographie war in der Tat immer ein Hobby. Ich kann mich noch sehr gut an die Bücher zum Thema erinnern, die ich in meiner Kindheit besessen habe. Danach habe ich einige Arbeiten für die US-Regierung gemacht, kam aber mit Kryptographie erst in den frühen 90er Jahren wirklich in Berührung, als ich das Buch "Applied Cryptography" (John Wiley & Sons, 1995) geschrieben habe.

Nun, viele Künstler und Programmierer haben ihre "Babies": Eine Entwicklung, die sie besonders schätzen und lieben. In Bezug auf Deine Arbeiten im Bereich der Kryptographie, welches sind da Deine Babies, auf die Du besonders stolz bist?

Wie jeder Ingenieur bin ich natürlich stolz auf jeden Algorithmus, der seine breite Anwendung findet. In der Hinsicht würde ich somit Twofish (1998) und Blowfish (1993) nennen. Doch in der Kryptographie gibt es eine interessante Zwiespältigkeit: Die wahren Erfolge eines Kryptologen sind seine erfolgreichen Angriffe. Blicke ich auf meine Arbeit zurück, dann erfreue ich mich am meisten an jenen zum Thema Kryptoanalyse, bei der ich die Algorithmen anderer Leute auseinander genommen habe.

Arbeitest Du denn zurzeit an etwas besonders interessantem?

Heutzutage konzentriere ich mich darauf, wie Sicherheit in ihrem Kontext funktioniert. Es reicht nicht aus, lediglich eine gute Sicherheitslösung zu haben, denn das meiste im Bereich der Sicherheit hat nichts mit Sicherheit ansich zu tun. Es ist wichtig das Umfeld der Sicherheit zu verstehen, die Psychologie der Entscheidungsfällung und den juristischen Rahmen der Sicherheitsbestrebungen.

Wie Du mir vor ein paar Jahren in einem privaten Schriftwechsel geschrieben hast, wird es von Deinem Buch "Applied Cryptography" keine dritte Auflage geben. Es habe sich zu viel geändert und der Bereich sei zu schnell vorangeschritten. Verneinst Du den Wunsch der Wissbegierigen Leser nach einer Neuauflage noch immer?

Unter dem Titel "Practical Cryptography" (John Wiley & Sons, 2003) habe ich eine konzeptionelle Weiterführung des besagten Buches publiziert. Es handelt sich dabei aber nicht um eine erweiterte Auflage des ersten. "Applied Cryptography" war sehr breitflächig abgestützt und versuchte sämtliche Bereiche des Themas abzudecken. "Practical Cryptography" hingegen ist fokussierter. Es diskutiert das grundlegende Problem der Kryptographie - der Aufbau eines sicheren Kanals zwischen zwei Parteien - und geht dabei detailliert auf die jeweiligen Aspekte ein. Ich denke, dass es ein viel besseres Buch ist für jemanden, der sich das Verständnis für die Funktionsweise kryptographischer Methoden aneignen will. Ebenso deckt es die Bedürfnisse von Entwicklern, die ihre eigenen Lösungen umsetzen wollen, besser ab.

„Blicke ich auf meine Arbeiten zurück, erfreue ich mich am meisten an jenen der Kryptoanalyse."

Was denkst Du, hätte der Zweite Weltkrieg

ein anderes Ende genommen, wären da nicht die "Codebreakers" auf der Seite der Alliierten gewesen? Einige Leute sagen, dass der Erste Weltkrieg durch Chemiker und der Zweite Weltkrieg durch Physiker gewonnen wurde. Der Dritte Weltkrieg hingegen würde durch Kryptologen entschieden werden. Denkst Du, dass das wahr ist? Handelt es sich beim globalen Terrorismus um den laufenden Dritten Weltkrieg?

In der Tat spielte die Kryptoanalysie eine wichtige Rolle im Zweiten Weltkrieg. Moderne Historiker meinen, dass der Krieg deswegen um etwa zwei Jahre kürzer ausfiel. Der Grund dafür ist einmalig in der Geschichte: Die Verschlüsselungsgeräte wurden in der maschinellen Ära durch elektronische Teile erweitert und die Code-Breaking Machines die ersten digitalen Computer der damaligen Zeit. Heute ist das nicht mehr so. Während Computer- und Netzwerksicherheit eine entscheidende Rolle bei zukünftigen "Weltkriegen" spielen werden - sowohl offensiv als auch defensiv -, wird das bei der Kryptoanalyse eher weniger der Fall sein.

In Bezug auf den "Krieg gegen den Terror" denke ich, dass es sich hier um einen Krieg im rhetorischen und keinen im klassischen Sinn handelt. Es macht keinen Sinn, den Krieg einem abstrakten Gebilde zu erklären. Es macht keinen Sinn, einer Taktik den Krieg zu erklären. Es macht ebenso keinen Sinn, den Krieg einer Strategie zu erklären, die schon tausende von Jahren seit Beginn der Zivilisationen angewendet wird. Krieg wird grundsätzlich einem Land erklärt. Danach wird eine der Parteien besiegt oder Waffenstillstand ausgehandelt. Wir alle wissen, wie wir hingegen die Taktik nennen wollen, die seit Anbeginn der Zeitrechnung und bis zum Ende der Zivilisation bestehen wird: Verbrechen. Terrorismus ist ein abscheuliches und schreckliches Verbrechen. Es als Krieg zu bezeichnen vernebelt lediglich die Sicht, mit der dem Terrorismus entgegengetreten werden muss.

Die Limitierung der (privaten) Nutzung kryptographischer Methoden durch Regierungen ist ein Mittel der Kontrolle und der Limitierung des Informationsaustauschs des Volkes. In den meisten Diktaturen halten genau diese Massnahmen das System am Leben. Denkst Du, dass in einem demokratischen System eine derartige Restriktion in irgendeiner Weise legitim sein kann? Oder darf das Recht auf Privatsphäre nie gegen Sicherheit (z.B. gegen Terrorismus und Verbrechen) eingetauscht werden?

Jede Technologie kann sowohl für gutartige als auch für bösartige Zwecke eingesetzt werden. In diesem Belang unterscheidet sich Kryptographie in keinster Weise. Wir alle benutzen Autos und fahren damit herum - Die bösen Jungs brauchen Autos hingegen, um nach einem Überfall zu flüchten. Wir alle benutzen Telefone zwecks Kommunikation - Und die bösen Jungs planen damit ihre Verbrechen. Das ist soweit okay, denn die Gesellschaft besteht glücklicherweise vorwiegend aus guten und ehrlichen Menschen, weshalb die positiven Auswirkungen einer Technologie meistens überwiegen. Restriktion in Bezug auf Kryptographie ist, wie Du das richtig angemerkt hast, ein Werkzeug der Diktatur. Es ist ein Mittel des Polizeistaats. Jegliche Aussage, dass derlei Einschränkungen dem Kampf gegen den Terror nützen würden, sind Lügen - Es ist lediglich ein Mittel, um die Bevölkerung zu kontrollieren.

In vielen Fällen wollen Kunden ein Black-box Testing ihrer Lösungen (z.B. Netzwerk-Umgebungen oder während des Software-Developements). Wie Du in Bezug auf Kryptographie immerwieder betont hast, gewährt "Security by Obscurity" niemals ein umfassendes Mass an Sicherheit. Denkst Du aber trotzdem, dass ein solches "Closed-Source Testing" in einigen Fällen und bestimmten Phasen eines Projekts sinnvoll sein kann?

„Jegliche Aussage, dass Einschränkungen der Kryptogtaphie dem Volk helfen würden, sind Lügen."

Klar. Überprüfungen geschlossener Systeme können durch solche Massnahmen in Bezug auf ihre Sicherheit hin verbessert werden. Obschon es sehr zeitintensiv und kostenaufwendig sein kann, kann es jenachdem sehr effektiv sein. In einem solchen geschlossen Testing bezahlt das Software-Unternehmen einem Experten-Team sehr viel Geld, um den Stand und die Schwächen der Sicherheit zu determinieren.

Bei Open-Source hingegen wird Software gerne einfach mal eben offen gelegt in der Hoffnung, dass einige Experten sich aus Interesse und Leidenschaft der Sache annehmen. Beide

Modelle können zu einer umfassend geprüften Software oder zu einer miserablen Lösung führen. Es geht nämlich nicht darum ob offen oder geschlossen, es geht primär darum, wer die Überprüfungen durchführt.

Die Lösung PGP (Pretty Good Privacy) von Phil Zimmermann war ein wichtiger Durchbruch und steht seit jeher jedermann, der sich um sicheren Datenaustausch bemüht, zur Verfügung. Doch erstaunlicherweise benutzen verhältnismässig nur wenige Firmen oder Einzelpersonen das besagte Produkt. Was denkst Du, sind die Gründe für das Ausbleiben eines umfassenden Einsatzes von PGP? Vielleicht, weil sich die jeweiligen Implementierungen zu komplex und zu unhandlich erweisen? Oder vielleicht deswegen, weil das Public-Key Prinzip für viele Leute einfach abschreckend wirkt? Nutzt Du PGP im alltäglichen Gebrauch?

PGP ist keineswegs ein Flop. Die PGP Corporation ist eine gesunde Firma und PGP verkauft sich besser dennje. Es gab eine Reihe von Gründen, warum PGP so lange gebraucht hat, um sich zu etablieren. Einer davon ist mit Sicherheit die Schwierigkeit der Nutzung. Die PGP Corporation hat sehr viel Aufwand betrieben, um das Interface zu verbessern und viele Dinge für den Benutzer transparent zu machen.

Ebenso ist es aber wichtig zu bemerken, dass Mail-Verschlüsselung nicht jedes Sicherheitsproblem der Informationsgesellschaft lösen kann. Die meisten Daten werden nämlich nicht während der Übertragung mitgeschnitten. Viel eher passiert das, wenn man sich selbst vor dem Rechner befindet und zwischenzeitlich einige böse Jungs in das Netzwerk eingebrochen sind. PGP löst dieses Problem nicht. Jedoch wird mit PGP Disk ein Produkt angeboten, das Verzeichnisse und Laufwerke zu verschlüsseln in der Lage ist. Das hat aber mit dem eigentlichen PGP nur mehr wenig zu tun.

Denkst Du, dass dafür IPv6 mit all seinen Sicherheits-Features die meisten Probleme heutiger Netzwerke lösen wird? Was ist Deine mittelfristige Voraussage für den Bereich der Computersicherheit? Werden Firmen auch in Zukunft "magische Zauberkistchen" verkaufen oder wird der Beratungsbereich zunehmends an Wichtigkeit gewinnen? Wie wird Information Security in zehn Jahren aussehen?

Sicherheit ist ein Prozess und kein Produkt. Die Industrie macht natürlich keine Anstalten, von der Bildfläche zu verschwinden. Doch die Lösungen zielen immer mehr auf Dienste denn auf Produkte ab. Das macht Sinn, denn Lösungen müssen heutzutage sehr flexibel und anpassbar sein. Flexible Dienste lassen sich eben einfacher den Bedürfnissen anpassen weder statische Produkte. Ich beobachte ein Anhalten dieses Trends.

Ein anderer, parallel auftretender Trend ist im Outsourcing gegeben. Unternehmen haben oftmals nicht das Wissen und die Kapazitäten, um mit Sicherheitsproblemen richtig umgehen zu können. Da bietet sich dann Outsourcing an. Diese beiden Trends haben dazu geführt, dass sich Managed Security Services (MSS) immer mehr etablieren und zunehmends einen Teil der Sicherheitsbestrebungen für sich in Anspruch nehmen.

Kennst Du die TV-Serie "Numb3rs" (2005)? Was hälst Du von der Idee, dass man jedes erdenkliche Problem mit Mathematik und Algorithmen lösen kann? Ist es naiv anzunehmen, dass unsere Welt eigentlich nur aus Zahlen besteht (z.B. wie die Pythagoräer)?

Jedes Werkzeug hat seinen Nutzen und ist in einer bestimmten Situation vorzuziehen. Es gibt Probleme, die mittels Mathematik adressiert werden können und halt eben auch andere, bei denen das nicht der Fall ist. Sicherheit ist eines der Gebiete, bei dem dies eher weniger der Fall ist, so nebenbei gesagt. Wir können zwar Mathematik nutzen, um eine bestimmte Klasse an Problemen zu lösen, wie zum Beispiel in der Kryptographie. Doch die wirklich komplexen Probleme der Informationssicherheit lassen sich damit nicht bewältigen.

„Es ist wichtig zu bemerken, dass Verschlüsselung nicht jedes Problem der Informationsgesellschaft lösen kann."

Und nun meine letzte und nicht immer ganz ernstgemeinte Frage. John Forbes Nash (US-amerikanischer Mathematiker und 1994 Nobelpreis-Träger in Economic Sciences) sagte einmal, dass er ein miserabler Schachspieler wäre. Wie sieht Dein Schachspiel aus? Oder magst Du lieber

Scrabble?

(*lacht*) Leider bin ich kein guter Schachspieler. Obschon ich eigentlich nicht genau sagen kann, ob das an meiner Denkweise oder der fehlenden Erfahrung liegt. Und ich hatte noch nie ein gutes Erinnerungsvermögen, was mich wiederum in die nicht-professionellen Scrabble-Spieler einreiht.

Vielen Dank für das interessante Interview. Ich wünsche Dir viel Spass bei Deinen Reisen und viel Glück beim nächsten Schachspiel.

Herausgeber

)SCIP(scip ag
scip AG
Technoparkstrasse 1
CH-8005 Zürich
+41 44 445 1818
mailto:info@scip.ch
http://www.scip.ch

Zuständige Person:
Marc Ruef
Security Consultant
+41 44 445 1812
mailto:maru@scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.