Kurz vorgestellt

Aktuelle Literatur zu Kryptographie und Kryptologie*

von Robert A. Gehring

Januar 1998

In den letzten vier Ausgaben wurde eine Einführung in die Kryptographie gegeben. Es bietet sich an, einige aktuelle Bücher, die sich dem Thema aus unterschiedlicher Perspektive nähern, ergänzend vorzustellen.

CRISIS

Das vielleicht interessanteste Buch, das seit Bruce Schneiers Standardwerk "Applied Cryptography" erschienen ist, trägt den Titel " Cryptography's Role In Securing The Information Society". Auf dem Einband sind die Anfangsbuchstaben der untereinanderstehenden Titelworte —mit Ausnahme des 'The'— in roter Schrift hervorgehoben, so daß man CRISIS liest. Das Fazit steht somit bereits am Anfang des Buches und hat als solches Symbolfunktion.

CRISIS ist das Resultat einer Arbeitsgruppe, des "Committee to Study National Cryptography Policy", die vom "Computer Science And Telecommunications Board" (CSTB) des US–amerikanischen "National Research Council" beauftragt war. Im "National Research Council" finden sich unter anderem Vertreter der US–amerikanischen Akademie der Wissenschaften. Unter diesen Umständen scheint es gerechtfertigt, das Buch als halboffizielles Werk zu betrachten. Wer die Debatte in den USA zum Thema Kryptographie verfolgt, wird um die Schwierigkeiten wissen, die Regierung und Geheimdienste mit deren unbeschränktem Einsatz haben. In Deutschland stellt sich die Situation ja ähnlich dar. Unter solchen Umständen hat ein Werk wissenschaftlicher Qualität eine besondere Bedeutung. Zu den Verfassern gehören Persönlichkeiten, wie Sam Fuller von der Digital Equipment Corporation und Ronald Graham von AT&T. Damit erhält der Bericht auch die Weihen der Praktiker und zusätzliche Reputation. Die US-Regierung wird daran kaum vorbeikommen, wenn sie sich daran macht, Gesetzesvorschläge, Kryptographie betreffend, zu unterbreiten.

*Erschienen im Linux-Magazin 02/1998, S. <65–67>. Online: http://www.linux-magazin.de/Artikel/ausgabe/1998/02/Review/review.html.

Wollte man sich kurz fassen, könnte man sagen, daß in dem Buch alle Aspekte von Kryptographie untersucht werden, die bei Bruce Schneier entweder nicht vorkommen oder knapp gehalten sind. Mit 688 Seiten steht es hinter dem genannten Werk Schneiers an Umfang kaum zurück und seine Bedeutung —auch für Deutschland und Europa— kann nicht unterschätzt werden. Es geht detailliert auf ziemlich alle Fragen des Einsatzes von Kryptographie in der Praxis ein. Die Abhängigkeit individueller Privatsphäre von kryptographischer Technologie spielt ebenso eine Rolle, wie die Interessen der Wirtschaft an Geheimhaltung ihrer Geschäftsdaten. Dabei verlieren die Autoren nie den Blick für die Wirklichkeit, wodurch sich das Werk wohltuend von vielen überflüssigen, weil bloß theoretischen Erörterungen deutscher Fachleute unterscheidet. Aber so ist es ja mit vielen amerikanischen Büchern.

Beispielhaft für die an den Tag gelegte Gründlichkeit sei hier die Erörterung des Begriffes ‘key escrow’ genannt, der ursprünglich zum Jargon der Immobilienhändler gehörte. Wer schon einmal auf eigene Faust versucht hat, die Bedeutung und den Ursprung dieses Begriffes zu recherchieren, wird um die Schwierigkeiten wissen. Die Wahl dieses Begriffes durch regierungsamtliche Stellen, scheint nicht zufällig erfolgt zu sein. So macht das Buch an vielen Stellen deutlich, wie Politik funktioniert.

Zweck des Werkes ist es dabei nicht, Partei für eine Seite —Pro oder Contra Kryptographie— zu ergreifen. Vielmehr geht es darum, anhand der realen Gegebenheiten die ungeheure Komplexität der Problematik zu verdeutlichen. Daß dabei Widersprüche und unbeantwortbare Fragen zuhauf auftauchen müssen, wird jedem klar sein, der sich etwas näher mit dem Thema beschäftigt. So steht am Ende eben jenes CRISIS, das bereits am Anfang in die Augen springt.

Zu empfehlen ist das Buch allen, die wissen wollen, warum auf der Originalausgabe von Bruce Schneiers Buch steht: “The book, the NSA never wanted to be published”. Und allen anderen, denen Kryptographie als Politikum gilt.

Cryptography’s Role in Securing The Information Society. National Academy Press, 1996. 87,00 DM.

Mehrseitige Sicherheit in der Kommunikationstechnik

Wie schon der Titel erahnen läßt, handelt es sich um ein deutsches Werk. Die darin enthaltenen Aufsätze sind das Ergebnis eines Kollegs “Sicherheit in der Kommunikationstechnik”, das von einer industrienahen Stiftung finanziert wurde. Dem Untertitel “Verfahren, Komponenten, Integration” kann man entnehmen, daß es sich eher um ein Werk für technisch Interessierte handelt. Der Gehalt der einzelnen Artikel fällt durchaus unterschiedlich aus, teilweise anschaulicher, als der Titel vermuten läßt.

Kryptographie wird in diesem Zusammenhang unter dem Blickwinkel, sichere Kommunikationssysteme installieren zu wollen, gesehen. Somit steht sie nicht im Mittelpunkt der meisten Aufsätze, sondern wird als integraler Bestandteil eines Systems betrachtet. Stichpunkte dazu sind: IT–Sicherheit, offene Kommunikationsnetze, Datenschutz und Digitale Signaturen. Teil eines solchen Systems sind nicht nur Geräte und Protokolle, sondern auch Akteure. Ihr Verhalten dominiert oft das Verhalten des

Systems. Einen Ausdruck findet diese Betrachtungsweise in Begriffen wie “persönliches Erreichbarkeitsmanagement” und “mehrseitige Sicherheit”. Nicht eben intuitiv, solche Phrasen.

Digitale Signaturen bilden in gewisser Hinsicht einen Schwerpunkt. Der Text des Signaturgesetzes (SigG), der zugehörigen Verordnung und der amtlichen Begründung sind im Buch enthalten. So kann sich jeder selbst überzeugen, daß im Signaturgesetz das Wort “Verschlüsselung” bzw. “Kryptographie” nicht vorkommt. Kunststück des Gesetzgebers! In der amtlichen Begründung kann man wenigstens lesen, warum dem so ist. Lehrreich!

Viele der Autoren stammen aus dem universitären Bereich und das schlägt sich in den Aufsätzen nieder: Sie sind nicht eben spannend, geschweige denn leicht zu lesen. An anderer Stelle wurde dafür der Begriff ‘Seminarstil’ geprägt.

Wer sich mit dem Buch beschäftigen will, braucht einen guten Grund. Leser mit eher allgemeinem Interesse werden nicht auf ihre Kosten kommen. Insgesamt hat man den Eindruck, es handelt sich um ein Werk für Insider. Das ist bedauerlich, hat die Problematik doch mehr öffentliches Interesse nötig. Fachleute werden mit Sicherheit das eine oder andere finden, das ihnen nützlich ist.

Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley Verlag, 1997. 89,90 DM

Abenteuer Kryptologie

Der Autor Reinhard Wobst ist einigen sicherlich bekannt. Er schreibt regelmäßig in der Zeitschrift UNIXopen zu den Themen Kryptographie und Kryptologie. Im vorliegenden Buch geht er erfreulich entspannt mit diesen um. Schneiers Werk hat der Innovation auf dem Gebiet sicherlich enge Grenzen gesetzt. R. Wobst gelingt es an einigen Stellen, diese Grenzen zu überschreiten. So beschreibt er sehr anschaulich, wie die ‘Verschlüsselung’ von Dateien, wie sie WordPerfect vornimmt, geknackt werden kann. Solche Beispiele wünschte man, häufiger in Fachliteratur zu finden.

Ansonsten macht das Buch mit allen wichtigen Begriffen der Kryptographie und Kryptologie mehr oder weniger bekannt, ohne dabei große mathematische Kenntnisse vorauszusetzen. Symmetrische und asymmetrische Verschlüsselung sind nach der Lektüre keine Fremdworte mehr, auch von Quantenkryptographie hat man einmal gehört.

Eine interessante Quelle weiterführender Informationen ist die beiliegende CD, auf der sich Programme und Texte aus dem Internet finden. PGP ist auch dabei. Der Zugriff auf die einzelnen Informationen erfordert allerdings viel Eigeninitiative, da die zusammengestellten Informationen kein einheitliches Format aufweisen. Die Aufbereitung läßt sehr zu wünschen übrig.

‘Anfängern’ kann das Werk als erste technische Lektüre empfohlen werden, nicht zuletzt wegen des relativ günstigen Preises. Wer später dann doch zum Schneier greift (ca. 120,00 DM), wird vieles wiedererkennen und kann seine Kenntnisse kontinuierlich vertiefen.

Reinhard Wobst: Abenteuer Kryptologie. Addison-Wesley Verlag, 1997. 69,90 DM

Verschlüsselte Botschaften

Es gibt auch Literatur über Kryptographie/Kryptologie, die für Laien interessant ist. Neben Geschichten von Edgar Allen Poe und Conan Doyle, die mit dem Thema eher phantasievoll umgehen, findet sich auch eine kleine Menge populärwissenschaftlicher Literatur im Buchladen, die durchaus seriös ist. Das Buch von Rudolf Kippenhahn, seines Zeichens Mathematiker und Astronom, gehört dazu.

Ausgangspunkte für die meisten Erläuterungen sind historische Miniaturen und Anekdoten. Die Geschichte der Kryptologie bietet dafür reichlich Stoff und R. Kippenhahn weiß unterhaltsam damit umzugehen. Boris Hagelin, Alan Turing, Julius Caesar und Galileo Galilei — sie alle hatten irgendwas mit Kryptologie zu tun. Kippenhahn zeigt, was, und führt so in Begriffe wie Caesar–Chiffrierung, Enigma, Umkehrwalze und elektronisches Geld ein. Viele Illustrationen veranschaulichen das Gelesene im wahrsten Sinn des Wortes.

Wer nicht tief in die Kryptologie einsteigen will, aber trotzdem eine Idee davon gewinnen will, ist mit diesem Buch gut bedient. Es gibt eine spannende Lektüre für längere Bahnfahrten oder Flugreisen ab. Das handliche Format und das eingebundene Lesezeichen (!) sind dabei sehr entgegenkommend.

Rudolf Kippenhahn: Verschlüsselte Botschaften. Rowohlt Verlag, 1997. 36,00 DM