Klaus Schmeh

Kryptografie

Verfahren, Protokolle, Infrastrukturen

6., aktualisierte Auflage

dpunkt.verlag

Klaus Schmeh

klaus.schmeh@dpunkt.de

Lektorat: Dr. Michael Barabas
Copy-Editing: Annette Schwarz, Ditzingen
Satz: Klaus Schmeh
Herstellung: Susanne Bröckelmann
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: Druckerei C.H. Beck

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN:
Print 978-3-86490-356-4
PDF 978-3-86491-907-7
ePub 978-3-86491-908-4
mobi 978-3-86491-909-1

6., aktualisierte Auflage 2016

Wieblinger Weg 17
69123 Heidelberg

5 4 3 2 1 0

Vorwort von Prof. Bernhard Esslinger

»Cryptography is about communication in the presence of adversaries.«
Ron Rivest, 1990

»Transparenz. Das ist das Höchste, was man sich in einer technologisch hoch entwickelten Gesellschaft erhoffen kann. … sonst wird man einfach nur manipuliert ...«
Daniel Suarez in *Darknet*, 2011

»The best that can be expected is that the degree of security be great enough to delay solutions by the enemy for such a length of time that when the solution is finally reached, the information thus obtained has lost all its value.«
William Friedman in *Military Cryptanalysis*, 1936

»Immer wenn man etwas konkret formuliert, wird man angreifbar, aber wenn man nicht konkret wird, ist es nicht nachvollziehbar.«
Unbekannt

Buch und Vorwort

Als Herr Schmeh mich fragte, ob ich das Vorwort zu seinem Kryptografie-Buch schreibe, war meine erste Reaktion: »Warum ich und warum ein weiteres Buch über Kryptologie?«

Auf beide Fragen hatte Herr Schmeh eine einleuchtende Antwort:

- Ich sollte das Vorwort schreiben, da er jemand suchte, der intensive theoretische, praktische und berufliche Erfahrung auf diesem Gebiet habe und diese Erfahrungen pointiert in das Vorwort einfließen ließe (ich war bei SAP CISO und Entwicklungsleiter der Sicherheitskomponenten des Systems R/3, bei der Deutschen Bank Leiter IT-Sicherheit und Chef des »Cryptography Competence Center« und bin unabhängiger Consultant für Risikomanagement, also für eine angemessene und effiziente Allokation der Ressourcen. Außerdem habe ich einen Lehrauftrag zu IT-Sicherheit und Kryptologie und leite seit über 15 Jahren ein Open-Source-Projekt, das das bisher erfolgreichste Lernprogramm zu Kryptologie erstellt).
- Sein Buch hat aufgrund mehrerer Eigenschaften ein Alleinstellungsmerkmal: Aktualität, Umfang/Vollständigkeit, Betonung der Anwendungssicht, Behandlung auch der umliegenden Felder (Geschichte, Gesellschaft, Politik, Wirtschaftsspionage, …) und – aufgrund seiner journalistischen Erfahrung – die gewohnt leicht verständliche Beschreibung auch komplexer Zusammenhänge.

Kryptografie – eine spannende Angelegenheit

Kryptografie ist eine in mehrfacher Hinsicht spannende Angelegenheit:

- Für **Historiker**, weil sie schon immer Teil des strategischen und taktischen Arsenals der Mächtigen war.
- Für **Mathematiker und Informatiker**, weil sich in der Zahlentheorie und der mathematischen Kryptologie ständig neue Forschungsergebnisse ergeben (z. B. die Möglichkeiten für die Cloud durch homomorphe Verschlüsselung, generische Analysemethoden wie SAT-Solver, die Berechnung von Gröbner-Basen, sehr große Gitterreduktionen, erweiterte Grenzen bei neuen und alten Verschlüsselungsverfahren wie das Zerlegen eines gegebenen 232-stelligen Produktes in seine beiden Primzahl-Faktoren durch Kleinjung etc. im Jahre 2009 oder das Knacken eines Pairing-basierten 923-Bit-Verschlüsselungssys-

tem durch Fujitsu etc. in 2012). Und das zukünftige Quanten-Computing sorgt dafür, dass weiter intensiv an neuen Verfahren geforscht wird (z. B. haben Sicherheitsforscher um Bernstein/Lange im Zuge des europäischen Forschungsprojektes PQCRYPTO Mitte 2015 konkrete Ansätze empfohlen).

- Für **Praktiker und Sicherheitsverantwortliche**, weil es stets neue Entwicklungen gibt: Auf der Angreiferseite werden etablierte Protokolle, die man für sicher hielt, kreativ missbraucht oder mit Man-in-the-Middle-Attacken umgangen. Vor allem aber bieten normale Produkte den Angreifern jede Menge Einfallstüren: Es ist unglaublich, wie viele Fehler beim Schlüsselmanagement und in den Implementierungen gemacht werden – und das nicht nur bei »einfachen« Produkten wie Routern (die Sicherheitsfirma SEC Consult untersuchte die öffentlich zugängliche Firmware von mehr als 4000 Geräten und gab im Nov. 2015 die Schätzung ab, dass bei 9 Prozent aller SSL-Endpunkte im Netz die privaten Schlüssel bekannt sind), sondern auch bei sogenannten Marktführern wie Symantec und PeopleSoft, die beispielsweise Schlüssel fest in produktiven Executables ablegten (ist inzwischen behoben). Auch auf der Seite »der Guten« kommen neue Techniken zum Einsatz: Nutzen von virtualisierbarer Hardware oder auch Open-Source-Lösungen wie OpenXPKI, das weit über die Grundfunktionalität einer PKI hinausgeht und zusätzlich die Anpassung an eigene Geschäftsprozesse über eine Workflow-Engine ermöglicht, eine Abstraktionsebene für die praxisnahe Anbindung beliebiger Datenquellen bietet, Zertifikats-Renewal-Software (CertNanny) über Automatisierungs-APIs wie SCEP andockt, externe CAs wie SwissSign anbindet, Tracking-Systeme wie RT integriert und CA-Rollover nahezu automatisiert. OpenXPKI ist ein sehr »konservativ« (im positiven Sinne) geführtes Open-Source-Projekt, das erst nach zehnjähriger Projektlaufzeit und über fünf Jahren produktiven Einsatzes im Oktober 2015 die Version 1.0 releaste (www.openxpki.org).
- Für **IT-Manager**, weil sich hier ganz praktisch die Fragen nach dem richtigen Umgang mit dem Risiko stellen, nach den angemessenen Maßnahmen, nach der Balance zwischen technischen und organisatorischen Maßnahmen (Anweisungen, Schulungen, Kontrolle), nach der erlangten Sicherheit, die sich aus der Wahl der richtigen Algorithmen/Protokolle, korrekter Implementierung und der Benutzerfreundlichkeit ergibt.
- Für **jedermann**. Um sich zu schützen, insbesondere nachdem man dank Snowden genauer weiß, wie die NSA die ganze Prozesskette der Sicherheit schwächte. Um zu verstehen, wie man mit Kryptografie seine Privatsphäre einigermaßen schützen kann. Dass man dazu auch selbst beitragen muss und kann – beispielsweise mit kostenloser Open-Source-Software zum Verschlüsseln seiner E-Mail (Thunderbird), durch (Let's-encrypt-)Zertifikate für seine Webseiten, durch Nutzung von VeraCrypt zur Partitionsverschlüsselung, durch Unterbinden des massenhaften anlasslosen Abhörens und, und, und.

Kryptografie im Unternehmen

Unternehmen investieren nicht einfach in IT-Sicherheit. Stattdessen werden Risikobetrachtungen angestellt, und es wird versucht, das optimale Maßnahmenbündel zur Verringerung/Vermeidung (Mitigation) des Risikos zu finden. Dabei kann Kryptografie die richtige Maßnahme sein, sie ist es aber nicht immer. Sie ist es vor allem dann, wenn sie mit Sachverstand eingesetzt wird. Manchmal sind organisatorische Maßnahmen billiger, manchmal wirken Mitarbeiterschulungen nachhaltiger. Immer kommt es auf den richtigen Mix an. Unter den technischen Maßnahmen wirkt Kryptografie proaktiv – im Gegensatz zu reaktiven Maßnahmen wie Monitoring.

Investitionen erfolgen nicht nur aus langfristig geplanten Überlegungen, sondern vermehrt auch wenn Aufsichtsbehörden, Kreditgeber oder Börsen Auflagen erteilen (z. B. »Two-Factor Authentication« der FFIEC, Schlüsselaufbewahrung in HSMs als Forderung der MAS, Basel-2, Compliance-Forderungen, SOx).

Im Gegensatz zur Lehre an den Hochschulen und zur Arbeit der Forscher stellen sich den Anwendern primär die Fragen nach den Kosten der Umsetzung (einmalige Kosten für Entwicklung und Roll-out, laufende Kosten für Betrieb und Schlüssel-Management), zur Vermeidung von Outages und zur Akzeptanz bei den Benutzern.

Kryptografie – typische Erscheinungen

Dabei ergeben sich im Umfeld der Kryptografie die sonst auch in der IT und im Management manchmal typischen Erscheinungen:

- Gartner-Hype-Kurven, die z. B. von PKI zuerst die Lösung aller Sicherheitsprobleme erwarteten, dann PKI »verdammten«, und nun ist PKI doch fast überall im Einsatz (Online-Banking, Webauthentisierung, SOA, Flaschenpfandsystem)
- »Angesagte« Produkte bieten für ein bestimmtes Problem eine Lösung an, aber gleichzeitig schafft ihr Einsatz neue Probleme (z. B. mathematisch sehr spannende neue Verfahren mit schönen Namen, die von Firmen mit Venture Capital vermarktet werden. Dabei ist dann die Anzahl der Mitarbeiter in den Vertriebs-, Marketing- und Rechtsabteilungen um ein Vielfaches höher als die Anzahl der kryptografischen Kompetenzträger oder der eigentlichen Softwareentwickler). Ebenso zu hinterfragen sind angesagte Begriffe wie BYOD, bei denen noch ein ganzes Bündel an Fragen ungeklärt ist: Hierbei sollten Firmen ihren Mitarbeiter eher erstklassige Smartphones (auch zur Privatbenutzung in einem abgetrennten Bereich) ausgeben, als jeden Handytyp der Mitarbeiter zuzulassen. Interessen von Herstellern und Netzwerk-Providern zielen aber eher auf den privaten Besitz ab, da dort im Gegensatz zu den Firmen keine besonderen Firmenkonditionen zu gewähren sind.

- Manager müssen verstehen lernen, dass man bei Infrastrukturen nicht nur nach den Alternativen Make or Buy fragen sollte, sondern vor allem nach der nahtlosen Integration in die eigene IT-Landschaft und welchen Einfluss man hat, dass bedarfsgerechte Neuerungen umgesetzt werden, um Kostenvorteile zu heben.
- Top-Manager, die ihre speziellen Gadgets wollen und die sie sich auch genehmigen können, obwohl die Sicherheitsarchitektur und die Interoperabilität dafür nicht ausreichend gegeben sind (was z. B. dazu führt, dass gerade wichtige E-Mails im Klartext versandt werden).
- Eine Konzentration der Anbieterfirmen und ein Marktverhalten einzelner großer IT-Security-Anbieter, das darauf abzielt, die Kunden abhängig zu machen. Nicht offengelegte Schnittstellen werden als Sicherheitsmerkmal verkauft (Security by Obscurity oder verborgene Hintertüren?). Die nächste Hardwaregeneration gibt es umsonst, dafür sind die Updates umso teurer. Ein Hersteller, der schon mit einem Produkt zum Virenschutz im Unternehmen ist, verkauft sein Data-Loss-Prevention-Produkt zum Dumpingpreis. Alles aus einer Hand kann späteres Wechseln nahezu unmöglich machen und gerade im Sicherheitsbereich der Spionage Tür und Tor öffnen.
- Es zählen Kosten und kurzfristige Gewinne, sodass beispielsweise nicht hinterfragt wird, warum eine Backup-Lösung auf amerikanischem Boden viel billiger ist als in Europa und warum die Backup-Bänder unverschlüsselt ins Bergwerk gebracht werden. Hier helfen nur staatliche Auflagen und Haftung für den Verlust von Daten. Vorbildlich und Arbeitsplätze schaffend sind die Schweizer Regelungen, die beispielsweise die Verarbeitung der Kontendaten in ihrem gesamten Lebenszyklus nur auf Schweizer Boden erlauben.
- Unternehmen, die vorauseilenden Gehorsam und unterwürfige Scheinloyalität fördern, deren Top-Manager Kritik und offene Diskussion abwürgen, gelangen schneller an den Rand der Pleite (dies zeigen die Betrugsfälle in der Finanz- und Automobilindustrie der letzten Jahre). Modernes Risikomanagement schaut sich inzwischen auch an, wie Führungskräfte mit konstruktivem Widerspruch und selbstbewussten Warnungen umgehen und ob die proklamierten Werte auch wirklich gelebt werden.
- In Arbeitsgruppen über Layout, Strategie und Businessmodelle meint jeder mitreden und sich profilieren zu können – im Gegensatz zu sehr erfolgreichen technischen Arbeitsgruppen, wo nur mitreden kann, wer über die nötige Kompetenz verfügt. Karriere-affine Kollegen und Entscheider diskutieren oft gerne bei den ersten Arbeitsgruppen mit, denn sie führen zur unternehmensinternen »Visibilität« und ignorieren die Bedeutung der zweiten.
- Technisch überlegene Standards »vergessen« den Benutzer, dem beispielsweise zugemutet wird, ein Zertifikat in den Keystore seines E-Mail-Clients zu bringen, obwohl er doch nur sicher mailen will.

- Diskussionen um rechtliche Erfordernisse, die von sehr wenigen Dogmatikern beherrscht werden, die Einfluss auf die Politik und den Gesetzgeber nehmen (z. B. im deutschen SigG/SigV) und die selbst dann an ihren teuren Empfehlungen festhalten, wenn fast keiner diese nutzt und wenn sie unserer internationalen Wettbewerbsfähigkeit im Wege stehen. Man braucht sich nicht zu wundern, wenn die Standards in den verbreiteten Produkten dann von einzelnen, schnellen Herstellern geprägt und in internationale Normungsgremien (IETF, IEEE, PKCS) eingebracht werden, die kein Verständnis für inkompatible nationale Sonderwege haben. Ebensowenig braucht man sich dann zu wundern, dass innerhalb von pragmatisch agierenden Zusammenschlüssen (wie der European Bridge-CA oder den virtuellen Behörden-Poststellen) die Sicherheit real deutlich erhöht wird mithilfe von fortgeschrittenen Zertifikaten (die zigmillionenfach im Einsatz sind), während die akkreditiert-qualifizierten »Sonderlocken« noch nicht einmal die 100.000 erreichten. Mit solchen über die EU-Direktive hinausgehenden akkreditiert-qualifizierten Signaturen (die zudem bei der Validierung das inkompatible »Kettenmodell« verlangen) erschwert man die Verbreitung der digitalen Signatur beträchtlich. Hier zeigt sich, dass man sehr genau spezifizieren sollte, für welche Fälle man Anforderungen aufstellt: So wenig, wie man für die allermeisten der im Alltag geschlossenen Verträge einen Notar braucht, so selten muss man bei elektronischen Verträgen vom Spezialfall des Anscheinsbeweises im Prozessfall ausgehen. Es geht nicht um »richtige« oder maximale Sicherheit, sondern um eine bessere!
- Gefährlich für die kritischen Infrastrukturen sind nicht einzelne Hacker, sondern rational handelnde und oft mafiamäßig/militärisch organisierte Angreifer, die auf Gewinn aus sind und meist zuerst den leichtesten/kostengünstigsten Weg für ihre modernen Raubzüge wählen. Das »Spiel« zwischen Cyber-Kriminellen und »guten« Cyber-Nutzern und ihren Verbündeten wird nicht enden. Dabei wird die Benutzerinteraktion (ermöglicht vom Softwareentwickler, aber getragen vom Verständnis und Mitwirken des Nutzers) immer zentral und schwierig bleiben.
- Und natürlich hat alles mehrere Seiten, so dass sich sicher auch Kritiker (und berechtigte Einwände) an dieser bewusst überspitzt formulierten Kritik finden …

Kryptografie in der Realität

In der Realität hat Kryptografie inzwischen fast überall Einzug gehalten: von Pay-TV über Auto-Wegfahrsperre, Handy bis in jeden Webbrowser. Fast alle großen Unternehmen betreiben eigene PKIs, mit denen ihre Mitarbeiter sichere E-Mails versenden könnten, sich sicher in WLANs anmelden können oder sicher Dateien auf outgesourcten Servern verschlüsseln könn(t)en. Softwarehersteller

wie SAP statteten ihre Software mit generischen Schnittstellen wie der GSS-API aus, so dass die Kunden die Wahl haben, die Sicherheitsfunktionen wahlweise von PKI- oder Kerberos-basierten Systemen zu nutzen.

Kryptografie erwies sich dann als sicher und erfolgreich im Einsatz in Firmen und im Internet, wenn sie

- hohe Interoperabilität gewährleistete (keine Insellösungen),
- für die Benutzer (nahezu) transparent war (kein oder kaum Mehraufwand) und
- ausgereift war.

Eine weitere Voraussetzung war, dass Expertenwissen im Voraus genutzt wird, was Geld spart und Fehler vermeidet, die im Nachhinein aufwändig zu beheben sind: Das Management von Schlüsseln für Maschinen, Dienste, Personen und Infrastrukturen muss verstanden und geplant werden. Beispielsweise machen CAs mit Modullängen von 512 Bit keinen Sinn. Hier hat Microsoft im August 2012 mit seinem Security Advisory 2661254 gute Dienste geleistet (das entsprechende Windows-Update verhindert die Verwendung von Zertifikaten mit RSA-Schlüsseln von weniger als 1024 Bit Länge durch die MS-Krypto-API). Ein anderes Beispiel: Der Lebenszyklus von Schlüsseln muss Zertifikats-Renewal und Schlüsselverlust von vornherein berücksichtigen. Insbesondere kleineren Firmen, die kostenlose PKI-Software von Microsoft oder aus dem Open-Source-Bereich oder Managed PKIs von Trustcenter wie VeriSign nutzen (und damit die rein technische Seite abdecken), ist hier zu raten, Experten-Know-how kurzfristig in der Architektur-Phase einzukaufen.

Das erforderliche Expertenwissen ist inzwischen breiter vorhanden, da viele Lehrstühle IT-Sicherheitsexperten ausgebildet haben. Sowohl für diese neuen Kollegen als auch für alle, die Fragen zu diesem Thema haben, vermittelt das Buch von Klaus Schmeh einen hervorragenden Überblick. Insbesondere gefällt mir, dass es trotz seiner Breite auf einem ganz aktuellen Stand ist und dabei genau so weit in die Tiefe geht, dass man die Verfahren verstehen und einordnen kann und dass man Produkt- und Protokoll-Entscheidungen treffen kann. Imponiert hat mir insbesondere die klare und unaufgeregte Art der Darstellung im Kapitel zum Chiffren-Design. Hier lässt sich Experten-Know-how ohne Mathe und mit klarem Urteil prima nachvollziehen.

Im ausführlichen Literaturverzeichnis finden sich alle Originalpapiere, die auch die genaue Mathematik enthalten. Zusätzlich können Sie spielerisch einzelne Verfahren mit der im Buch erwähnten freien Lernsoftware CrypTool (in den Varianten CrypTool 1, CrypTool 2 und JavaCrypTool) ausprobieren.

Und zu Recht wird in diesem Buch unter den »wichtigsten weiterführenden Büchern« Ross Anderson mit *Security Engineering* aufgeführt, denn die praktischen Probleme sind oft verschieden von denen, über die theoretisch orientierte

Experten gerne diskutieren (z. B. das Ausnutzen von Paddingfehlern statt Angriffe mit differenzieller Kryptoanalyse, das Eindringen über Passwortraten und auf Anwendungsebene, das Nutzen der menschlichen Psychologie und immer stärker auch die Ökonomie der IT-Sicherheit und der Malware-Industrie). Beide Sichtweisen sind wichtig.

Aufgrund von Snowdens Whistleblowing ist zur Erkenntnis geworden, was vorher als Vermutung von Verschwörungstheoretikern abgetan wurde: Die NSA hört nahezu jede Kommunikation anlasslos ab und archiviert diese, die Kryptoverfahren werden sowohl bei der Standardisierung als auch bei der Implementierung geschwächt. Besondere Raffinesse zeigten NSA und GCHQ bei den Advanced-Persistent-Threat-Hacks mit der Spionage-Software Regin beispielsweise gegen Belgacom. Alle Betroffenen reagieren gleich: Sie untersuchen, finden nichts, aber haben als Ergebnis das Problem angeblich im Griff.

Eine weitere Erkenntnis, zu der uns Snowden verhalf: Die Schützer des Staates tendieren zu elektronischer Überwachung – und zeigen bei ihren eigentlichen Aufgaben erstaunlich geringen Erfolg und viel internes Kommunikations-Missmanagement. Die gute Nachricht: Die Mathematik der modernen Verfahren (wie AES, RSA mit richtiger Parametrisierung und Modulen von mindestens 2048 Bit Länge, SHA2) ist nicht geknackt; die NSA ist keine Macht mit Alien-Fähigkeiten, aber eine Macht, die wirklich groß und umfassend planen und handeln kann.

Wie alt das Thema Missbrauch von Überwachung schon ist, zeigt das folgende Zitaten-Duo:

> *Jeder neue Angriff auf die Privatsphäre wird mit einer allgegenwärtigen Kultur der Angst gerechtfertigt.*
>
> John Twelve Hawks (aus den Anmerkungen zum zweiten Band der Traveler-Trilogie von 2005–2009)

> *Ich behaupte, dass, wer immer in diesem Augenblick zittert, schuldig ist, denn die Unschuld hat von der öffentlichen Überwachung nichts zu befürchten.«*
>
> Maximilien de Robespierre, 1794 im französischen Nationalkonvent, als Kritik an seinen staatlich verordneten Verhaftungen und Morden laut wurde

Auch diese Themen im Umfeld der Kryptografie werden in diesem Buch aktuell behandelt. Für die Zielgruppe der Nichtmathematiker ist es daher weiterhin das Kryptografie-Standardwerk im deutschsprachigen Raum, das nicht nur bei meinen Studenten als Einstieg sehr geschätzt wird.

Ich wünsche auch der 6. Auflage alles Gute.

Bernhard Esslinger

Januar 2016