Technische Randbedingungen jeder Kryptoregulierung

Michaela Huhn, Andreas Pfitzmann

Zusammenfassung: *Politische Diskussionen über die Regulierung kryptographischer Techniken werfen häufig die verschiedensten Dinge durcheinander. Oft sind die in ihnen aufgestellten Forderungen an die technische Gestaltung unerfüllbar oder den angestrebten Zielen ganz und gar nicht dienlich. Hauptthema der politischen Diskussion sind Erzeugung und Verwaltung kryptographischer Schlüssel. Dabei wird davon ausgegangen, daß kryptographische Systeme eine fest vorgegebene Systemarchitektur und einen bestimmten Verwendungsmodus (Integritätssicherung oder Vertraulichkeitsschutz) besitzen. Beide Annahmen sind falsch:*

Jede Sicherheitsinfrastruktur für digitale Signatursysteme, die technisch zuverlässige Signierschlüssel bereitstellt, ermöglicht auch den sicheren Austausch von Schlüsseln für Konzelationssysteme (Vertraulichkeitsschutz).

Jedes Konzelationssystem kann zum zunächst nicht bemerkbaren Austausch von Schlüsseln für weitere aufgesetzte Konzelationssysteme verwendet werden. Dies relativiert insbesondere den Nutzen von Key-Escrow-Systemen, also von Kryptosystemen mit zwangsweiser Hinterlegung von „geheimen" Schlüsseln, die dann für die Verbrechensbekämpfung zugänglich sind.

Neben den bekannten asymmetrischen Konzelationssystemen kann jede datenintensive Anwendung mittels steganographischer Verfahren zum Konzelationssystem ausgebaut werden. Damit können Benutzer jede Einschränkung der Verwendung von kryptographischen Konzelationssystemen unterlaufen, sofern sie nur einen Bruchteil der vom Kommunikationssystem bereitgestellten Bandbreite benötigen. Auch steganographische Systeme können mit Schlüsseln parametrisiert und so in offenen Benutzergruppen sicher eingesetzt werden.

Außerdem sollte unterschieden werden zwischen Schlüsseln zum Schutz von Kommunikation und solchen zum Schutz langfristig zu speichernder Daten: Key-Escrow-Systeme zur Rekonstruktion verlorengegangener Schlüssel sind nur für die letztere Anwendung dem Nutzer dienlich, während sie für erstere vornehmlich den Sicherheitsbehörden die Überwachung der Kommunikation ermöglichen.

Resümee: Eine gesetzliche Regulierung von Konzelationssystemen mit dem Ziel der Verbrechensbekämpfung muß ihr Ziel verfehlen und sollte daher unterbleiben, da sie gravierende Nachteile für informationelle Selbstbestimmung und Sicherheit der Bürger wie auch für die Schutzinteressen der Wirtschaft hat.

Einleitung

Seitdem Rechner klein, billig und leistungsfähig geworden sind, ist der breite Einsatz kryptographischer Techniken problemlos möglich. Damit sind diese Techniken in das Zentrum politischer Diskussionen gerückt, ohne daß allen Beteiligten die technischen Randbedingungen bekannt sind. Deshalb gehen viele dieser Diskussionen – insbesondere solche über Kryptoregulierung zur Bekämpfung der sogenannten „Organisierten Kriminalität" – in die Irre. Dieser Beitrag nennt mathematisch-technische Grundzusammenhänge kryptographischer Systeme und zeigt Gestaltungs- und Regulierungsmöglichkeiten sowie Regulierungsgrenzen auf, die sich daraus ergeben. Anforderungen von politischer Seite, die dem nicht Rechnung tragen, sind *technisch* nicht realisierbar.

Benutzeranforderungen an Signaturschlüssel und Konzelationsschlüssel

Der Einsatz digitaler Signatursysteme wird zur Zeit für den elektronischen Rechtsverkehr und die elektronische Archivierung diskutiert. Für beide Anwendungsbereiche ergeben sich Zertifizierungsanforderungen an Signaturschlüssel, die neben den kryptographischen Eigenschaften des Signatursystems Voraussetzung für die Rechtsverbindlichkeit digital signierter Dokumente sind. So muß der Empfänger einer signierten Nachricht nicht nur prüfen können, daß Nachricht und Signatur zum öffentlichen Testschlüssel passen, sondern er muß den öffentlichen Testschlüssel auch nachweisbar einer Person zuordnen können[1].

Schlüsselpaare für Konzelation, also das Verschlüsseln von Daten zum Schutz vor unerwünschter Kenntnisnahme, brauchen nicht in einem rechtlich bindenden Sinne zertifiziert zu werden. Es mag sinnvoll sein, beim Aufbau einer Infrastruktur Schlüsselzertifizierungen einzusetzen, um die Authentizität der verwalteten Schlüssel zu sichern. Damit kann verhindert werden, daß in einer staatlich bereitgestellten Sicherheitsinfrastruktur Personen unter falschen Namen öffentliche Konzelationsschlüssel bereitstellen und auf diese Weise in den Besitz vertraulicher Nachrichten gelangen. Aber die Anforderung der Benutzer an Konzelationssyste-

me besteht darin, daß *sie* sich *gegenseitig* der Authentizität der öffentlichen Konzelationsschlüssel sicher sind, nicht daß sie diese vor Gericht nachweisen können. Daher können Kommunikationspartner, sobald es ihnen gelungen ist, einmal Schlüssel auszutauschen[2], deren Authentizität sie vertrauen, jedes beliebige Konzelationssystem zur weiteren vertraulichen Kommunikation verwenden. Die Erzeugung von Schlüsselpaaren in sogenannten TrustCentern kann also für Konzelation nicht erzwungen werden, denn niemand ist beim Gebrauch der Konzelationsschlüssel auf Zertifikate von TrustCentern angewiesen.

Dies ist bei Signaturschlüsseln anders. Eine Möglichkeit, die Zertifizierungsanforderungen der Signaturschlüssel für rechtsverbindliche elektronische Dokumente zu erfüllen, besteht darin, die Erzeugung dieser Schlüsselpaare ausschließlich in sogenannten TrustCentern vornehmen zu lassen – die TrustCenter zertifizieren nur von ihnen erzeugte Schlüssel[3].

Durch die so erzwungene Erzeugung der Signaturschlüsselpaare in TrustCentern besteht nun die Möglichkeit, alle geheimen Signierschlüssel dort zu speichern. Es wurde allerdings noch an keiner Stelle argumentiert, daß der Zugriff auf geheime Signierschlüssel hilfreich sei zum Zwecke der Strafverfolgung oder vorbeugenden Verbrechensverhinderung – denn solch ein Zugriff könnte nur zum Fälschen von Beweismitteln dienen.

Digitale Signaturen ermöglichen Austausch von Konzelationsschlüsseln

Jede Sicherheitsinfrastruktur für digitale Signaturen erlaubt den sicheren Austausch von Schlüsseln für Konzelation: Nach bekannten Algorithmen, die bereits in allgemein verfügbaren Programmen implementiert sind, kann jeder für Konzelation geeignete Schlüsselpaare generieren. Danach kann jeder seine öffentlichen Konzelationsschlüssel selbst zertifizieren[4], indem er eine Nachricht unterschreibt: „Der öffentliche Schlüssel ... gehört ...". Die Sicherheitsinfrastruktur für digitale Signaturen erlaubt nun jedem anderen Benutzer, die Unverfälschtheit dieser Nachricht zu prüfen und sich so Gewißheit zu verschaffen, daß alles, was mit diesem öffentlichen Schlüssel verschlüsselt wird, nur vom Inhaber des Schlüsselpaares wieder entschlüsselt werden kann.[5]

Konzelationsschlüssel, die mit Hilfe einer Sicherheitsinfrastruktur für digitale Signaturen verbreitet wurden, ermöglichen sowohl, Nachrichten vertraulich auszutauschen als auch Schlüssel für symmetrische Konzelationssysteme. Mit diesen kann dann hocheffizient konzeliert werden.

Sinnvolle Wahl der Sicherheitsparameter und Maßnahmen bei Schlüsselverlust berücksichtigen den gewünschten Schutzzeitraum

Es ist sowohl bei Signatursystemen als auch bei Konzelationssystemen danach zu unterscheiden, für welchen Zeitraum die Sicherheit der verwendeten Systeme gewährleistet sein muß. So müssen Sicherheitsparameter wie die Schlüssellänge danach eingestellt werden, ob es dem Benutzer wichtiger ist, in kurzer Zeit große Datenmengen zu verarbeiten, deren Vertraulichkeit oder Integrität nur über Wochen garantiert werden muß, oder ob die Daten über Jahrzehnte geschützt werden sollen, so daß auch Angriffe mit erheblich gesteigerter Rechenleistung berücksichtigt werden müssen.

Auch für Maßnahmen im Falle eines Schlüsselverlustes[6] ist die Zeitkomponente zu berücksichtigen. Der Verlust von Schlüsseln, die zum Schutz der Vertraulichkeit oder zur Integritätssicherung bei der *Übertragung* von Nachrichten verwendet werden, stellt für den Benutzer kein ernstliches Problem dar: Können etwa die mit Hilfe eines Konzelationssystems geschützten Daten nicht entschlüsselt werden, so generiert der Empfänger ein neues Schlüsselpaar und teilt dem Sender seinen neuen öffentlichen Konzelationsschlüssel authentisiert mit. Danach verschlüsselt der Sender die Daten unter Zuhilfenahme des neuen Schlüssels noch einmal und überträgt sie erneut. Diese Methode ist weit weniger aufwendig als jede sichere Form des Schlüsselbackups[7] und weitaus sicherer als Key-Escrow, d.h. die zwangsweise Hinterlegung von „geheimen" Schlüsseln bei sogenannten Escrow-Agencies. Gedacht ist dies dazu, daß sogenannte Bedarfsträger von den Key-Escrow-Agencies die „geheimen" Schlüssel erhalten, wenn eine Überwachung des Fernmeldeverkehrs durchgeführt werden soll.

Gleiches gilt hinsichtlich Schlüsseln für Signaturen. Verliert der Inhaber seinen geheimen Signierschlüssel, kann er nicht mehr passend zu seinem öffentlichen Schlüssel signieren. Er kann sich aber jederzeit ein neues Schlüsselpaar generieren und den neuen öffentlichen Schlüssel zertifizieren lassen. Dieser muß den Empfängern von zukünftig signierten Nachrichten samt Zertifikat mitgeteilt werden.

Der Verlust öffentlicher Schlüssel braucht nicht betrachtet zu werden, da ihre Öffentlichkeit ebenso wie die Öffentlichkeit ihrer Zertifikate beliebig weit verbreitete Speicherung für Benutzung und Backup erlauben.

Bei Schlüsseln für den Schutz der Vertraulichkeit oder der Integrität längerfristig gespeicherter Daten[8] führt ein Verlust des Entschlüsselungsschlüssels in der Regel zum Verlust der Daten. Hier muß der Schlüsselinhaber also ggf. Vorsorgemaßnahmen wie Schlüsselbackup oder Key-Escrow einplanen.

Schlüsselbackup und Key-Escrow sind nicht für Anwendungen sinnvoll, bei denen Daten auch ohne Schlüssel wiederbeschafft werden können, da die Sicherheit der geheimen Schlüssel in jedem Falle sinkt, wenn außer dem Schlüsseleigentümer noch weitere Personen oder Institutionen im Besitz (von Teilen) des geheimen Schlüssels sind.

Schlüsselbackup und Key-Escrow betreffen unterschiedliche Verwendungszwecke von Schlüsseln – ersteres betrifft die Archivierung von Daten, zweiteres wird von verschiedenen Seiten für Kommunikation vorgeschlagen. Da in der Kryptographie alles unabhängig sein sollte, was nicht abhängig sein *muß*[9], betreffen Schlüsselbackup und Key-Escrow also auch unabhängige Schlüssel. Außerdem sollten die Benutzer ihr Schlüsselbackup gemäß ihren Bedürfnissen gestalten können, während dies bei Key-Escrow nicht vorgesehen ist.

Benutzern von Verschlüsselung Key-Escrow-Systeme mit dem Argument nahe bringen zu wollen, damit sei auch ihr Schlüsselbackup-Problem gelöst, ist also unseriös: Zwei unabhängige Probleme, denen unterschiedliche Schutzinteressen zugrundeliegen, müssen auseinandergehalten und einzeln gelöst werden.

Key-Escrow-Systeme können zum zunächst unerkennbaren Schlüsselaustausch verwendet werden

Ähnlich wie sichere digitale Signaturen zum sicheren Austausch von Schlüsseln für Konzelation verwendet werden können, kann auch jedes Konzelationssystem, also insbesondere auch jedes Key-Escrow-System, benutzt werden, um Schlüssel für zusätzlich zu verwendende Konzelationssysteme zu vereinbaren. Statt einem Konzelationssystem direkt die vertraulich zu haltenden Nachrichten zu übergeben, wird zunächst ein öffentlicher Konzelationsschlüssel redundant codiert übertragen. Der Empfänger prüft die Redundanz (was dem Prüfen des Zertifikates bei Verwendung digitaler Signaturen entspricht). Sofern er keine Verfälschung des öffentlichen Schlüssels feststellt, verwendet er den öffentlichen Schlüssel entweder, um wirklich vertraulich zu haltende Nachrichten zu verschlüsseln oder aber zum Austausch eines weiteren Schlüssels für ein symmetrisches Konzelationssystem, mit dem dann effizienter verschlüsselt werden kann. Bei der weiteren Kommunikation werden dann die mit dem aufgesetzten Konzelationssystem bereits verschlüsselten Nachrichten mit dem zugrundeliegenden Key-Escrow-Konzelationssystem ein weiteres Mal verschlüsselt.

Die Verwendung zusätzlicher Verschlüsselungsmaßnahmen kann erst dann entdeckt werden, wenn der oder die Schlüssel des Key-Escrow-Systems von den Key-Escrow-Agencies herausgegeben und zum Entschlüsseln des Fernmeldeverkehrs benutzt wurden, was nach geltendem Recht eine Erlaubnis für einen Bedarfsträger[10] zur Überwachung des Fernmeldeverkehrs voraussetzt. Key-Escrow ist – wenn die Schlüsselherausgabe tatsächlich so restriktiv gehandhabt wird, wie in der öffentlichen Diskussion immer wieder betont wird – für die Ermittlungen der Bedarfsträger vermutlich kaum hilfreich, da gerade in den Fällen, wo Key-Escrow die Entschlüsselung von Nachrichten ermöglichen soll, höchstens die Verwendung zusätzlicher Verschlüsselungssysteme festgestellt werden kann. Daher wird neben der Einführung von Key-Escrow auch das Verbot anderer Verschlüsselungsverfahren diskutiert, was die Problematik allerdings in keiner Weise löst: Wird die Überwachung des Fernmeldeverkehrs restriktiv gehandhabt, so wird ein Übertreten des Kryptoverbots häufig „zu spät" bemerkt werden. Ein ernsthafter Durchsetzungsversuch des Kryptoverbots setzt also eine weitgehende Aushöhlung des Fernmeldegeheimnisses voraus. Doch selbst dann können sich Teilnehmer steganographischer Techniken bedienen (siehe unten), bei denen die Verwendung eines Verschlüsselungssystems praktisch nicht nachweisbar ist.

Daneben ist zu berücksichtigen, daß alle Stellen und Personen, die Kenntnis von dem geheimen Konzelationsschlüssel eines Benutzers erhalten haben, alle zu diesem Schlüssel gehörigen Nachrichten entschlüsseln können. Diese triviale Aussage macht Key-Escrow-Agencies und Bedarfsträger ggf. zu einem vielversprechenden Angriffspunkt für Wirtschaftsspionage und andere kriminelle Aktivitäten[11].

Kurzum: Key-Escrow zur Verbrechensbekämpfung wird weitestgehend wirkungslos sein – erfordert aber kaum realisierbaren technischen[12] und erheblichen organisatorischen[13] Aufwand, um die Aushöhlung der Rechte der Bürger und eine Steigerung der informationellen Verletzbarkeit von Wirtschaft und Gesellschaft in vertretbaren Grenzen zu halten.

Steganographie: Vertrauliche Nachrichten zu finden ist unmöglich

Nachrichten können nicht nur durch Konzelationssysteme vor unerwünschter Kenntnisnahme geschützt werden, sondern auch durch Steganographie: Die zu schützende Nachricht wird in einer anderen Nachricht, die notwendigerweise wesentlich länger ist, geeignet versteckt. Einige Möglichkeiten des Versteckens von Nachrichten sind in [MöPS_94] beschrieben. Selbst wenn Kryptographie – oder noch wesentlich allgemeiner: jede Form unüberwachbarer Kommunikation oder Speicherung – verboten würde, ist dem Anwender nichts zu beweisen, wenn die verwendete steganographische Technik gut ist. Natürlich ist es möglich und zur Erhöhung der Sicherheit empfehlenswert, die zu schützende Nachricht vor dem steganographischen Verstecken noch zu verschlüsseln.

In [MöPS_94 Kap. 3.3] ist beschrieben, wie ein steganographisches Verfahren mit einem zufällig gewählten Schlüssel parametrisiert werden kann[14]. Steganographische Algorithmen, die mit einem frei wählbaren Schlüssel parametrisiert sind, entsprechen in der Funktionalität Konzelationssystemen, bei denen die Algorithmen allgemein bekannt sind und die Sicherheit nur über geheimgehaltene Schlüssel gewährleistet wird. Sie sind wie solche Konzelationssysteme auch in *offenen* Benutzergruppen verwendbar, da das zugrundeliegende Verfahren nicht geheimgehalten werden muß. Damit sind alle beschriebenen Möglichkeiten zum Schlüsselaustausch nicht nur beim Einsatz von ausgewiesenen kryptographischen Verfahren, sondern auch beim Einsatz von Steganographie verwendbar.

Diese Überlegung basiert auf der Jahrtausende alten Erfahrung, daß die gleiche Nachricht für unterschiedliche Empfänger eine unterschiedliche Bedeutung haben kann. Steganographie ist nur ein hocheffizientes Verfahren, mit dem Benutzer, ohne sich persönlich zu treffen und ohne daß es von Dritten nachgewiesen werden kann, Nachrichten austauschen können oder vereinbaren, wie sie zukünftig auszutauschende Nachrichten interpretieren wollen. Die bereits verfügbaren und geplanten datenintensiven interaktiven Telekommunikationsanwendungen aus dem Multi-Media-Bereich bieten sich als Trägersysteme für steganographische Techniken geradezu an.

Schlußfolgerungen

Das oft gehörte Argument, die Schlüsselerzeugung gehöre aus Gründen der Verbrechensbekämpfung zusammen mit einer Aufbewahrung auch der geheimen Schlüssel zu den Aufgaben von TrustCentern, ist aus den dargelegten Gründen vollständig falsch. Das Argument, dies diene sogar den Interessen des Nutzers, entpuppt sich bei genauer Betrachtung als unzutreffend. Entsprechendes gilt auch für Key-Escrow.

Eine Regulierung kryptographischer Techniken zur Konzelation mit dem Ziel der Verbrechensbekämpfung ist nicht sinnvoll, da ein Kryptoverbot nicht wirksam durchsetzbar ist, aber die Sicherheitsinteressen von Bürgern, Wirtschaft und Gesellschaft empfindlich beeinträchtigt.

Eine andere, davon unabhängige Frage ist die rechtliche Anerkennung digitaler Signaturen: Sie ist technisch möglich und erscheint – in vorsichtigen Schritten unternommen – durchaus wünschenswert.

Ein Dankeschön

Hannes Federrath, Kai Rannenberg und Matthias Schunter danken wir für Hinweise zur (Un-)Verständlichkeit des Textes.

Anmerkungen

1 Daher werden der öffentliche Testschlüssel und die Identität der inhabenden Person digital signiert (beispielsweise von einem sogenannten TrustCenter), was allgemein als *Zertifizierung* des öffentlichen Schlüssels bezeichnet wird. Um derartige Zertifikate überprüfen zu können, muß der Empfänger einer signierten Nachricht den öffentlichen Schlüssel der zertifizierenden Stelle kennen. Ist dies nicht der Fall, so benötigt er wiederum ein Zertifikat für diesen Schlüssel. Es entsteht ein Zertifizierungsbaum, wie er beispielsweise in X.509 beschrieben ist.

2 z.B. mit Hilfe der staatlich bereitgestellten Sicherheitsinfrastruktur, aber auch durch persönlichen Austausch von Schlüsseln.

3 Dies ist allerdings nicht empfehlenswert, da zentrale Systemkomponenten, auf denen die Ausführung verschiedener voneinander unabhängiger Teilaufgaben konzentriert wird, immer auch Schwachpunkte einer Sicherheitsarchitektur bilden, vgl. [FJPP_95], und es vereinfacht die Zertifizierung auch nicht.

4 also die Authentizität des Konzelationsschlüssels für andere überprüfbar machen.

5 Soll diese Verwendung eines Signatursystems ausgeschlossen werden, so besteht die einzige Möglichkeit darin, daß die Sicherheit der Signaturen untergraben wird, indem digital signierte Nachrichten in Umlauf gebracht werden, bei denen der Unterzeichner eben nicht der Eigentümer des Signierschlüssels ist. Damit ist natürlich jede Rechtsverbindlichkeit von Dokumenten, die in diesem System signiert wurden, hinfällig.

6 Relevant für unsere Betrachtungen ist die Situation, daß Schlüssel vollständig verloren sind, d.h. sie existieren für niemand mehr. Andernfalls sind weitere geeignete Maßnahmen zu ergreifen, etwa das Führen von Sperrlisten durch die Stellen, die Schlüssel zertifiziert haben. Bevor Teilnehmer Schlüssel verwenden, müssen sie bei der Stelle, die sie zertifiziert hat, nachfragen, ob der Schlüssel nicht gesperrt ist.

7 Hierzu kann jeder seine eigenen geheimen Schlüssel mit einem Schwellwertschema in Teile zerlegen und einzelne Teile an ihm vertrauenswürdig scheinende Freunde, Organisationen etc. weitergeben. Zur Rekonstruktion ist dann eine vom Teilnehmer vor der Zerlegung gewählte Mindestzahl an Teilen nötig. Bei geschickter Wahl dieser Mindestzahl können einerseits wenige doch nicht vertrauenswürdige Teilverwahrer den geheimen Schlüssel nicht rekonstruieren, andererseits verhindert der Verlust einzelner Teile nicht die Rekonstruktion.

8 etwa für Archivierungszwecke, z.B. in Grundbuchämtern oder im Gesundheitswesen.

9 Viele Sicherheitslücken in kryptographischen Protokollen entstehen dadurch, daß dieselben Schlüssel für unterschiedliche Funktionen verwendet werden, etwa dasselbe RSA-Schlüsselpaar sowohl zur Konzelation als auch für digitale Signaturen.

10 Sicherheitsbehörden, sowie Verfassungsschutz, Bundesnachrichtendienst und MAD.

11 Gerade in Ländern, in denen die organisierte Kriminalität eine wichtigere Rolle spielt, zeigt sich immer wieder, daß der „Erfolg" der organisierten Kriminalität und Korruption der Sicherheitsbehörden zwei Seiten derselben Medaille sind.

12 Wie soll eine Zugriffskontrolle in den Datenbanken der Key-Escrow-Agencies fehlerfrei realisiert werden, und gleichzeitig ein kurzfristiger Zugriff auf die Schlüssel möglich bleiben? Die Erfahrung lehrt, daß bisher *jedes* größere technische System Fehler enthielt. Also müssen Risikozusammenballungen vermieden werden.

13 Es ist erstaunlich, daß gerade die Bedarfsträger Key-Escrow fordern, deren Erfolge und Skandale doch häufig auf der Erfahrung „Jeder Mensch hat seinen Preis" beruhen.

14 Der Schlüssel gibt beispielsweise die Abstände zwischen den Bitpositionen an, an denen die zu schützende Nachricht versteckt wird.

Literatur

MöPS_94: Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist; Datenschutz und Datensicherung DuD 18/6 (1994) 318–326.

FJPP_95: Hannes Federrath, Anja Jerichow, Andreas Pfitzmann, Birgit Pfitzmann: Mehrseitig sichere Schlüsselerzeugung, in: Patrick Horster (Hrsg.); TrustCenter; Proceedings der Arbeitskonferenz TrustCenter 95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 117–131.

Stichwörter: Kryptographie, Kryptoregulierung, Kryptographiegesetz, Verschlüsselung, digitale Signatur, Key-Escrow, TrustCenter, Konzelation, Vertraulichkeit, Steganographie.