Für Krypto-Deregulierung

Andreas Pfitzmann, TU Dresden, Fakultät Informatik, e-mail: pfitza@inf.tu-dresden.de

Herrn Dr. Sandls Darstellung der politischen Dimension der Kryptographie stimme ich zu und hoffe, daß die deutsche Delegation bei den laufenden OECD-Verhandlungen an der von ihm geschilderten Position festhält. Ich hoffe, sie erreicht auch etwas!

Aus technischen Gründen (siehe Box 1) halte ich eine Regulierung der Herstellung, des Einsatzes oder auch nur des Exports von kryptographischen Systemen für kontraproduktiv. Viele Organisationen teilen inzwischen diese Position (siehe Boxen 2-4). Wünschenswert wäre nicht nur ein Verzicht auf weitergehende Regulierung, sondern sogar eine Deregulierung: Der Export von kryptographischen Systemen aus der Bundesrepublik Deutschland ist zur Zeit genehmigungspflichtig – dieser Genehmigungsvorbehalt sollte aufgehoben werden, und die Bundesregierung sollte sich zusätzlich dafür einsetzen, daß auch andere Länder, insbesondere die USA und Frankreich, entsprechend handeln.

Zu den von Herrn Dr. Sandl erwähnten Überraschungen im Bereich Kryptographie nur wenige Sätze:

Ein kryptographisches System ist unsicher, wenn
(a) es unsicher implementiert ist,
(b) es eine zu kurze Schlüssellänge hat oder
(c) schlechte Kryptoalgorithmen verwendet werden.

Durch die Presse gingen in den letzten Monaten
(a) ein Implementierungsfehler der Firma Netscape, die für die Schlüsselerzeugung zu wenig Zufall verwendete, so daß erheblich weniger verschiedene Schlüssel möglich waren, als Netscape annahm.
(b) das Brechen eines Kryptosystems mit erheblich zu kurzer Schlüssellänge, nämlich nur 40 Bit, mittels Ausprobieren aller 2^{40} möglichen Schlüssel. Anzumerken ist, daß bisher Exportgenehmigungen aus den USA nur erteilt werden, wenn die Schlüssellänge maximal 40 Bit beträgt. Daß solch kurze Schlüssel unsicher sind, sollte niemanden überraschen.

Unsicherheiten von „Pretty Good Privacy“ (mit den Kryptoalgorithmen RSA und IDEA) im Sinne von (a), (b) oder (c) sind mir nicht bekannt. Allerdings auch hierzu eine Warnung: Kein kryptographisches System kann sicherer sein als der Rechner oder der Chip, auf dem die kryptographischen Algorithmen ausgeführt werden. Wer also auf einem im wesentlichen unsicheren PC-Betriebssystem wie MS DOS, Windows 95 oder MacOS arbeitet und Programme ausführt, die Trojanische Pferde enthalten können (das sind eigentlich alle, die man nicht im Detail kennt), sollte sich nicht wundern, wenn seine Kryptogramme geknackt werden. Gleiches gilt auch für Nutzer von Mehrbenutzersystemen (etwa unter UNIX), deren Systemverwalter unaufmerksam oder gar böswillig sind.

Box 1

M. Huhn, A. Pfitzmann: Technische Randbedingungen jeder Kryptoregulierung (Zusammenfassung)

Jede Sicherheitsinfrastruktur für digitale Signatursysteme ermöglicht den sicheren Austausch von Schlüsseln für Konzelationssysteme (Vertraulichkeitsschutz).

sichere digitale Signaturen → sichere Konzelation

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 für die Verbrechensbekämpfung.

Key-Escrow Konzelation ohne Dauerüberwachung → Konzelation ohne Key-Escrow

Mittels steganographischer Verfahren 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.

Multi-Media-Kommunikation → unbeobachtbare Kommunikation mittels Steganographie

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.

Konzelationsschlüssel für Kommunikation und geheime Signierschlüssel sind jederzeit ersetzbar
→ Key-Escrow als Schlüsselbackup ist unsinnig

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.

vollständige Fassung in
DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 20/1 (1996) 23-26 sowie unter
http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/lit/sirene.lit.html

Box 2

Pressemitteilung der Gesellschaft für Informatik e.V. (Bonn, den 28.2.1996)

Bedenken der Gesellschaft für Informatik gegen staatliche Einschränkung der Kryptographie

Zusammenfassung

Gesellschaft für Informatik e.V. hält staatliche Einschränkungen der Nutzung kryptographischer Verfahren für bedenklich und als Mittel zur Bekämpfung der organisierten Kriminalität für wirkungslos.

In der politischen Diskussion der jüngeren Vergangenheit ist wiederholt gefordert worden, den Gebrauch von Kryptographie, d.h. deren Einsatz, Herstellung, Einfuhr und Ausfuhr staatlich zu beschränken. Auch in Deutschland gibt es dazu detaillierte Überlegungen in Richtung auf gesetzgeberische Maßnahmen. Hierzu erklärt die Gesellschaft für Informatik:

Wer Nachrichten überträgt muß sich darauf verlassen können, daß diese Nachrichten unverfälscht erhalten bleiben (Integrität) und keinem Unbefugten bekannt werden (Vertraulichkeit).

Diese Forderungen zu erfüllen, ist seit jeher Aufgabe einer sicheren d.h. einer verläßlichen Kommunikation. In einer Informationsgesellschaft, in der Unternehmen, Behörden und Privatpersonen in weiter wachsendem Maße Nachrichten über offene Kommunikationsinfrastrukturen (Netze) übertragen, wird die Forderung der Nutzer nach angemessener Sicherung der Informationen vor unerwünschter Ausspähung oder Änderung zur zentralen Frage.

Diese Forderung ist erfüllbar. Bei digitaler Übertragung sind sichere kryptographische Verfahren bekannt und praktikabel, sogenannte "starke" Kryptographie. Über diese starken kryptographischen Verfahren hinaus können zusätzlich steganographische Techniken verwendet werden. Mit diesen können geheime Informationen in umfangreicheren, unverfänglichen Daten so versteckt werden, daß sie sich von Dritten nicht entdecken lassen. Das aber bedeutet auch: Nicht nachweisbare, vertrauliche Kommunikation kann gar nicht verhindert werden.

Eine Überwachung von Nachrichten in digitalen Netzen ist praktisch nicht möglich, insbesondere die organisierte Kriminalität wird u.a. steganographische Techniken anwenden. Als technische Möglichkeit zur effektiven Verbrechensbekämpfung bietet sich statt Einschränkung der Kryptographie eher eine gezielte Überwachung der Endgeräte an, auf denen die Nachrichten im Klartext erscheinen.

Um in bestimmten Fällen die Entschlüsselung von Nachrichten in digitalen Netzen zu ermöglichen, verlangen u.a. die Strafverfolgungsbehörden eine Hinterlegung der geheimen Schlüssel. Diese Maßnahme kann aber die Abhörbarkeit der Nachrichten von Verdächtigen nicht grundsätzlich garantieren (siehe oben). Dagegen ist die Schlüsselhinterlegung ein zusätzliches Risiko für die Geheimhaltung der Schlüssel und damit der Daten aller, gerade auch der unbelasteten Teilnehmer. Durch eine zentrale Hinterlegung und zusätzliche Sicherungskopien wird diese Gefahr noch wesentlich gesteigert.

Beschränkung der Kryptographie ist zur Bekämpfung der organisierten Kriminalität ungeeignet. Sie wird aber den dringend notwendigen Schutz von Betriebs-, Geschäfts-, Berufs- und Privatgeheimnissen gefährden.

http://www.iig.uni-freiburg.de/gi/dsits/Krypto_Regulierung.txt

Box 3

Telesec (Deutsche Telekom AG): Kryptokontroverse

Mit dem wachsenden Einsatz kryptographischer Verfahren im privaten und kommerziellen Umfeld werden auch die Forderungen nach einer staatlichen Kontrolle solcher Verfahren lauter. Die Diskussion bewegt sich dabei im Spannungsfeld zwischen staatlichen Sicherheits- und privaten Geheimhaltungsinteressen. Beide Interessen sind grundsätzlich im Normengefüge verankert und lassen sich auch prinzipiell mit vertretbaren Argumenten in ihrer praktischen Relevanz begründen. Dennoch: Eine gesetzliche Beschränkung oder gar ein Verbot des nationalen Einsatzes kryptographischer Verfahren im privaten oder kommerziellen Umfeld gibt es in der Bundesrepublik nicht und jeder Versuch, solche Restriktionen durchzusetzen, muß sich sowohl einer verfassungsrechtlichen als auch einer praktischen Überprüfung unterziehen.

+ **Verfassungsrechtlich** ist in der Hauptsache das durch Art. 10 Abs. 1 GG (Grundgesetz) umfassend geschütze Fernmeldegeheimnis relevant. Einschränkungen dieses Rechts sind nur durch Regelungen möglich, die auf Basis der strengen Voraussetzungen des Art. 10 Abs. 2 GG erlassen wurden.

  Die bisher existenten Regelungen dieser Art lassen im wesentlichen nur ein Abhören (Überwachen und Aufzeichnen) der Kommunikation durch die dazu berechtigten Stellen (die sogenannten Bedarfsträger) zu. Ein diesem Vorgang nachgeschaltetes Dechiffrieren individuell verschlüsselter Kommunikation ist gesetzlich nicht geregelt und darf folglich nicht zu einer weiteren Einschränkung des Fernmeldegeheimnisses führen. Anders gesagt: Wenn im Rahmen einer Abhörmaßnahme nur kryptographisches Wirrwarr aufgezeichnet werden konnte, muß es die abhörende Stelle aus eigener Kraft leisten, dem Wirrwarr Klartext zu entlocken. Ein Anspruch beispielsweise darauf, daß die Deutsche Telekom AG als Anbieter von Verschlüsselungsverfahren Schlüsselduplikate ohne Einverständnis des Schlüsselinhabers vorhalten und bei Bedarf zur Verfügung stellen muß, besteht nicht. Im Gegenteil, schon ein nicht mit dem Schlüsselinhaber abgestimmtes Vorhalten von Schlüsselduplikaten würde gegen geltendes Datenschutzrecht verstoßen. Im Telekom Trust Center werden daher auch keine geheimen Verschlüsselungsschlüssel aufbewahrt. Diese werden vielmehr unmittelbar nach der Personalisierung einer Chipkarte unwiderruflich gelöscht. Anders wird nur auf ausdrücklichen Wunsch eines Kunden verfahren.

  Auf der Suche nach Möglichkeiten, das Fernmeldegeheimnis über den Abhörvorgang hinaus weiter einzuschränken, werden aktuell zwei Optionen diskutiert. Das Verbot jeglicher privater oder kommerzieller Kryptographie und das Verbot nur der autonomen Kryptographie bei gleichzeitiger Zulassung von Diensteanbietern, die dann aber zur Aufbewahrung und Vorlage der Schlüsselduplikate verpflichtet sein sollen. Verfassungsrechtlich unbedenklich wären beide Optionen nur dann, wenn sie als verhältnismäßig gewertet werden könnten. Dies ist jedoch angesichts der nachfolgend aufgeführten praktischen Auswirkungen eines totalen oder eingeschränkten Kryptoverbots nicht der Fall, so daß beiden Optionen eine verfassungsrechtliche Unbedenklichkeit nicht bescheinigt werden kann.

+ **Praktisch** ist absehbar, daß Kryptoverbote leerlaufen und damit dem berechtigten Wunsch nach einem verbesserten Schutz der inneren Sicherheit nicht gerecht werden können, insgesamt also weder sinnvoll noch verhältnismäßig sind. Die Gründe für diese Prognose sind vielfältig. Der wohl wichtigste Grund ist, daß Kryptoverbote selbst von Laien und erst recht von kriminellen Organisationen, derer man mit einem Kryptoverbot eigentlich Herr werden will, ohne großen Aufwand unterlaufen werden können. Zu vielzählig sind die international verfügbaren, bereits

eingesetzten und damit nicht mehr kontrollierbaren Verschlüsselungsverfahren und zu verbreitet sind die Möglichkeiten, verschlüsselte Kommunikation zu verbergen (z.B. Steganographie). Kryptoverbote gehen damit in ihrer Durchsetzung auch und gerade deshalb ins Leere, weil die Bedarfsträger in aller Regel schon nicht merken werden, daß in der Masse der täglich möglichen Informationsübermittlung eine davon verschlüsselt stattgefunden hat. Merken sie es ausnahmsweise doch, werden die zu befürchtenden Sanktionen niedriger sein, als der Wert der verbotenermaßen verschlüsselt geführten Kommunikation. Dies jedenfalls dann, wenn es kriminelle Organisationen, die Zielgruppe eines Kryptoverbots also, trifft.

\+ **Das Fernmeldeanlagengesetz (FAG), ein heimliches Kryptogesetz?**

Als 1995 die auf Basis der Verordnungsermächtigung des § 10b FAG (Fernmeldeanlagengesetz) erlassene FÜV (Fernmeldeverkehr-Überwachungs-Verordnung) in Kraft trat, herrschte in Fachkreisen zunächst Verwirrung über eine zu Spekulationen Anlaß gebende Formulierung in § 8 Absatz 4 FÜV. Dort heißt es in Satz 2:

Falls der Betreiber dem Teilnehmer Verschlüsselungsmöglichkeiten für die Nachrichten bereitstellt, hat er [...] dem Bedarfsträger die für eine Entschlüsselung erforderlichen Informationen zeitgerecht zur Verfügung zu stellen.

Weil sich diese Formulierung so oder so ähnlich in einem Kryptogesetz wiederfinden könnte, herrschte anfänglich Streit darüber, ob § 8 Absatz 4 Satz 2 FÜV das "Kryptogesetz durch die Hintertür" sei. Der Streit war jedoch schnell beigelegt, da diese Verpflichtung als Kryptogesetz offensichtlich verfassungswidrig wäre. Die FÜV findet, wie erwähnt, ihre rechtliche Grundlage im FAG. Damit ist klar, daß sich sämtliche Verpflichtungen ausschließlich auf Fernmeldeanlagen und nicht auf davon unabhängige Dienstleistungen beziehen können. Jede weitergehende Verpflichtung würde den Rahmen der Verordnungsermächtigung des § 10b FAG sprengen und wäre bereits deswegen als verfassungswidrig einzustufen (Art. 80 GG). Darüber hinaus würde eine nur auf Betreiber von Fernmeldeanlagen beschränkte Verpflichtung, Schlüsselduplikate vorzuhalten und im Bedarfsfall zur Verfügung zu stellen, gegen den Gleichbehandlungsgrundsatz gemäß Art. 3 Absatz 1 GG verstoßen und müßte sich zudem allgemein an Art. 12 Absatz 1 GG messen lassen. Als eine weitere verfassungsrechtliche Schranke einer Auslegung des § 8 Absatz 4 Satz 2 FÜV im Sinne eines Kryptogesetzes wird in der juristischen Literatur die Verletzung des Fernmeldegeheimnisses der Teilnehmer genannt, da diese zwar eine Überwachung ihres Fernmeldeverkehrs, nicht aber die Preisgabe von auch zu anderen als zu Fernmeldezwecken nutzbaren Verschlüsselungsschlüsseln dulden müssen.

Literaturhinweise:

Bizer, Kryptokontroverse - Der Schutz der Vertraulichkeit in der Telekommunikation, DuD 1996, 1-14.

Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, DuD 1996, 23-26.

Grimm, Kryptoverfahren und Zertifizierungsinstanzen, DuD 1996, 27-36.

http://www.telesec.de/recht3.htm

Box 4

Fachverband Informationstechnik im VDMA und ZVEI (Frankfurt, den 25. September 1996)
(German Information Technology Manufacturers' Association)

Position zur Einführung des "Gesetzes zur digitalen Signatur" und zur Regulierung von Verschlüsselungsverfahren

Die Wirtschaft begrüßt die Initiative der Bundesregierung zu einem "Gesetz zur digitalen Signatur (Signaturgesetz - SigG)". Die Einführung der geplanten Regelung schafft die Voraussetzungen, um die moderne Informations- und Kommunikationstechnik auch für beweisverwertbare und formgerechte Rechtshandlungen (Willenserklärungen, Archivierung von Dokumenten etc.) einzusetzen. Dies erschließt ein erhebliches Rationalisierungspotential in Wirtschaft und Verwaltung, was dem Wirtschaftsstandort Deutschland zugute kommt. Darüber hinaus verbessert die digitale Signatur die Sicherheit bei der Nutzung von Informations- und Kommunikationstechniken entscheidend. Es liegt daher im Interesse der Wirtschaft, daß das geplante Signaturgesetz schnell in Kraft tritt.

Um die erforderliche Rechtssicherheit zu schaffen, ist es nach unserer Auffassung jedoch in einem zweiten Schritt erforderlich, dem "elektronischen Dokument" mit digitaler Signatur gesetzlich den gleichen Wert einzuräumen wie der herkömmlichen papiergebundenen Schriftform. Rechtsvorschriften, die bisher die Schriftform vorgeben, sollten künftig auch die digitale Form mit digitaler Signatur zulassen (z.B. Handelsdokumente und Steuerdaten).

Die Akzeptanz und die breite Nutzung der digitalen Signatur wird wesentlich vom Beweiswert eines "elektronischen Dokuments" und seiner Gleichstellung mit dem der papiergebundenen Form (z.B. digital signierte Verträge und Quittungen) abhängen. Deshalb schlagen wir vor, diese Thematik baldmöglichst zu klären.

In den Zusammenhang mit der digitalen Signatur wird auch immer wieder die Diskussion um eine Kryptoregulierung gestellt, da die zugrunde liegenden Verfahren auch für Verschlüsselung nutzbar sind. Hier sind die berechtigten Interessen von Wirtschaft, Privatpersonen und Sicherheitsbehörden angemessen zu berücksichtigen. Unternehmen und Privatpersonen müssen sicher und vertraulich kommunizieren können, für die Sicherheitsbehörden geht es letztendlich darum, die gesetzlichen Abhörmöglichkeiten zu erhalten. Dabei ist zu berücksichtigen, daß aufgrund der technischen Entwicklung gegenwärtig keine realistische und wirtschaftlich tragbare Möglichkeit zu sehen ist, diese Zielsetzung aufrecht zu erhalten. Die früher geheime Kryptologie wird heute weltweit an Universitäten gelehrt und nicht zu überwindende Verschlüsselungsverfahren können z.B. über das Internet bezogen werden. Dazu kommen noch weitere Umgehungsmöglichkeiten wie die Steganographie. Vor diesem Hintergrund wird jede Regulierung der Verschlüsselung zwecks Aufrechterhaltung der Abhörmöglichkeiten von Sicherheitsbehörden zwangsläufig ins Leere laufen.

Die Verwendung sicherer Verschlüsselungsverfahren ist im Hinblick auf die Bedeutung der Ressource Information und die gleichzeitige Bedrohung durch Wirtschaftsspionage für die deutsche Wirtschaft unerläßlich. Eine Regulierung schafft nur unnötigen Verwaltungs- und Kostenaufwand in beträchtlicher Höhe und mindert die Exportchancen deutscher Sicherheitsprodukte. Sie trifft im Ergebnis nur gesetzestreue Unternehmen und Bürger, deren Verfahren darüber hinaus auch unsicherer werden (jede legale Zugriffsmöglichkeit kann auch mißbraucht werden, z.B. durch ausländische Dienste).

Deshalb sollte von einer Regulierung von Verschlüsselung zwecks Aufrechterhaltung der Abhörmöglichkeiten von Sicherheitsbehörden Abstand genommen werden.

http://www.telesec.de/fvit.htm