Crypto-debate: Strategies for responsible behavior of law enforcement and intelligence agencies on matters of cryptography, vulnerabilities and tools

Martin Schallbruch

Issue 3, 2017

In January 2017, the Digital Society Institute hosted a workshop on the "Crypto-debate: Strategies for responsible dealings with security agencies on matters of cryptography, vulnerabilities and tools." Dr. Stefan Grosse (Federal Ministry of the Interior), Ralf Koenzen (Lancom Systems), Linus Neumann (Chaos Computer Club) and Stefan Heumann (Stiftung Neue Verantwortung) contributed to the workshop.

I. The facts

Twenty years after the first so-called crypto-debate, questions about the government's need to restrict or weaken cryptography are still on the agenda. The focus remains on the tension and tradeoff between the government's interest in accessing encrypted information and the resulting damage to IT security as a whole.

The extent to which cryptography is used and the proportion of communication that is encrypted has grown. Encrypted communication is increasingly offered as standard by large service providers. More than half of traffic to web servers is now made via encrypted SSL connections. Cryptography has also been greatly simplified for individual users – e.g., through built-in VPN connections.

The government also calls for and promotes the use of cryptography in communication and data storage. Approximately 150 regulations under German federal law directly or indirectly demand the use of encryption procedures – e.g., for communication with the state (taxes, social data, and critical processes such as drug and cancer registries). Encryption is increasingly demanded in government approval digital devices (e.g., cash registers, tachographs, electricity meters, card readers in health care). Europe's harmonized IT security and data protection laws require extensive encryption of sensitive information, the protection of confidentiality, and the protection of the integrity and availability of systems.

These developments pose a growing challenge for police and intelligence services. These security agencies have been confronted with a sharp increase in the amount of encrypted evidence that they must handle and process. The importance of digital evidence is similarly growing, as digital systems are increasingly used or targeted in the commission of crimes. Spot tests show an uptick in the use of encryption by criminals; however, there is a lack of reliable empirical findings on the actual problems that security agencies face when it comes to cryptography. Publicly available cases show that encrypted communication makes investigations considerably more difficult but, only in the rarest of cases does it make them impossible.

While the German federal government has so far adhered to the principles of cryptography established by the Federal Cabinet in 1999, other countries have given authorities the right to interfere with cryptography (UK, CN, FR) or are debating laws that would do so (US). Instead of weakening cryptography or implementing backdoors, Germany wants to expand the know-how of security agencies by establishing a central office (ZITIS) and developing advanced technical procedures to deal with encrypted communication. In addition, broader obligations for telecommunication providers will also be examined.

II. Strategic options available to security agencies

When carefully implemented, strong encryption cannot be broken. As a matter of principle, security agencies have three options for dealing with cryptography:

Weaken the systems

Using covert influence during the technical development stage or through open statutory regulations, security agencies could weaken cryptographic implementations or install backdoors. Both factors would harm the IT security of affected fields and could lead to significant collateral damage, in the form of attacks on critical infrastructure or industrial espionage. Recent reports—such as that from the European IT security agency ENSIA, or that from the Encryption Working Group of the US House of Representatives—regard such weaknesses as threats to national security. Because of the high risk of detection, covert influence have to be restricted to very small numbers of application. Once such actions come to public light, the targets will very quickly switch to other methods available on the internet.

Exploit vulnerabilities and hack systems

The exploitation of vulnerabilities in hardware or software systems in a manner unwanted by the user is known as "hacking" (…even if the actions are deemed legal, insofar as they do not violate § 202a StGB). "Lawful hacking" isn't technically different from the approach of hackers with other motivations. The exploitation of vulnerabilities by security agencies interferes with individuals' legally-guaranteed rights to the protection of the integrity and confidentiality of IT systems. Such actions thus require appropriate and proportionate justification. The extent to which the state damages the IT security by exploiting such vulnerabilities depends on the quality/properties of said vulnerabilities. Fundamentally, there are a multitude of weaknesses in any IT system. While the exploitation of publicly known and already patched vulnerabilities does not affect IT security in general, withholding information about critical, publicly unknown vulnerabilities can have serious consequences. These include threats to the economy, critical infrastructures, and, in extreme cases, threats to human lives. Regulations for dealing with such weaknesses thus need to be high priority and must sit on a firm legal basis. These issues concerning system vulnerabilities always necessarily affect matters of national security (e.g., classified information). Further, a high demand by the State for such vulnerabilities could see the growth of a 'vulnerability market' – this needs to be carefully monitored.

Obligate service providers:

If service providers make cryptographic tools available to users, they could be required to assist law enforcement in accessing encrypted content. If this is generally the case for the entire industry, this will weaken the IT security of communication partners. If the service provider is only pursued in individual cases (and insofar as accessing encrypted information with their help is possible), there will be no major difference between this and other system-side assistance given to security agencies, such as the installation of interfaces for wiretapping. A likely consequence of this approach is that groups targeted by security agencies will switch to other services.

III. Recommendations

Recommendations for companies

Companies in general

In view of the European legal situation in the area of data protection and IT security, as well as the threat of industrial espionage, the use of cleanly-implemented, strong cryptography for both personal data, for key trade secrets (IP), and for the structural data of IT and OT networks, is strongly recommended.

IT security companies

Strong cryptographic methods have now become the standard and are required by lawmakers and large user companies both nationally and internationally. Insofar as national law requires the mitigation of procedures, the installation of backdoors, or other cooperation with security agencies, specific national versions of products should be drawn up to ensure that the overall security assessment is not impaired.

Recommendations for security agencies

No systematic weakening

In the interests of national security and German industry, authorities should refrain from any measure which would weaken confidence in cryptographic processes. This includes the secret influence or open regulation of crypto processes, as well as the restriction of service providers with regard to the nature of the cryptography made available to their users.

High effort for individual cases

On the basis of existing or possibly extended legal powers, security agencies should be able to access the digital communications of suspects on an individual basis, to the extent permitted by law. This includes the exploitation of errors in the implementation of cryptography, cryptomanagement, the exploitation of known vulnerabilities in products, or the use of other resources such as human sources or remote forensic methods.

Technological Capabilities

The security agencies' ability to access systems is given particularly for those systems whose security falls just short of carefully-implemented strong cryptographic algorithms. Security agencies must be able to build up and maintain the ability to access such a system. International examples (e.g., UK, FR) suggest that this is only possible through a central state authority accessible by all security agencies.

Recommendations for policy

Evidence-based policy

The ramifications of cryptography on the work of security agencies needs to be monitored according to the cornerstones established by the German Federal Cabinet in 1999, and this should be pursued through a broader (and public) scientific research program.

Policy stance

The abandonment of crypto-regulation is the most important measure to achieve Germany's encryption policy target. Without weakening cryptography, the internationally-comparable, positively developing market for cryptographic technology will persist and expand, something that German and European data protection laws strongly promote. At the same time, the state can promote the application and further development of cryptographic methods by setting high security standards for its procurement policy.

Vulnerabilities

Security agencies should have a legislative process whereby they can deal with hardware and software system vulnerabilities. The state's obligation to help address vulnerabilities should be taken for granted. Vulnerabilities that can be exploited by security agencies should be positively defined, in particular by defining a 'seriousness' threshold. When it comes to suppressing knowledge of vulnerabilities, a decision process needs to be defined which takes account of the associated costs and benefits, any related consequences, and users' fundamental rights. Existing examples of such processes (e.g., Vulnerability Equity Process in the USA) should be scientifically analyzed and tested for portability.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI Industrial & Policy Recommendations (IPR) Series

Kryptodebatte: Strategien zum verantwortungsvollen Umgang der Sicherheitsbehörden mit Kryptografie, Schwachstellen und Werkzeugen

Martin Schallbruch

Issue 3, 2017

Im Januar 2017 war das Digital Society Institute Gastgeber für einen Workshop zur „Kryptodebatte – Strategien zum verantwortungsvollen Umgang der Sicherheitsbehörden mit Kryptografie, Schwachstellen und Werkzeugen“. Impulse zu dem Workshop steuerten Dr. Stefan Grosse (Bundesministerium des Innern), Ralf Koenzen (Lancom Systems), Linus Neumann (Chaos Computer Club) und Stefan Heumann (Stiftung Neue Verantwortung) bei.

1. Sachstand

Zwanzig Jahre nach der ersten sogenannten Kryptodebatte wird die Frage der staatlichen Beschränkung, Schwächung oder Umgehung von Kryptografie weiterhin diskutiert. Im Mittelpunkt steht nach wie vor das Spannungsverhältnis zwischen einem staatlichen Interesse, in einzelnen Fällen auf verschlüsselte Informationen zuzugreifen, und dem dadurch möglicherweise verursachten Schaden für die IT-Sicherheit insgesamt.

Verändert hat sich das Ausmaß der Nutzung von Kryptografie und der Anteil verschlüsselter Kommunikation an der gesamten elektronischen Kommunikation. Verschlüsselung von Kommunikation wird von großen Dienstleistern zunehmend standardmäßig bereitgestellt. Mehr als die Hälfte der Zugriffe auf Webserver erfolgt mittlerweile über verschlüsselte SSL-Verbindungen. Die individuelle Nutzung kryptografischer Verfahren durch Nutzer hat sich stark vereinfacht, z.B. bei VPN-Verbindungen.

Auch der Staat fordert und fördert die Nutzung der Kryptografie für Kommunikation oder Datenspeicherung. Etwa 150 Regelungen des geltenden deutschen Bundesrechts fordern bereits heute direkt oder mittelbar den Einsatz von Verschlüsselungsverfahren, etwa für die Kommunikation mit dem Staat (Steuern, Sozialdaten, kritische Prozesse wie Arzneimittelzulassung oder Krebsregister). Zunehmend wird Verschlüsselung als Teil der staatlichen Zulassung digitaler Geräte eingefordert (Registrierkasse, Tachograph, Stromzähler, Kartenleser im Gesundheitswesen). Das europäisch harmonisierte IT-Sicherheits- und Datenschutzrecht verlangt durch den Verweis auf den Stand der Technik weitgehende Verschlüsselung von sensiblen Informationen, zum Schutz der Vertraulichkeit ebenso wie zum Schutz der Integrität und Verfügbarkeit von Systemen.

Für die Polizeien und Nachrichtendienste ergibt sich durch diese Entwicklung eine wachsende Herausforderung. Die Sicherheitsbehörden sind mit einer stark steigenden Zahl verschlüsselter Beweismittel konfrontiert. Die Bedeutung digitaler Beweismittel nimmt gleichzeitig zu, weil der Anstieg von Straftaten, bei denen digitale Systeme Ziel oder Tatmittel sind, die Auswertung digitaler Spuren wichtiger werden lässt. Einzelne Stichproben belegen die gestiegene Nutzung von Verschlüsselung durch Straftäter. Belastbare empirische Erkenntnisse über die tatsächlichen Probleme der Sicherheitsbehörden mit der Kryptografie liegen allerdings nicht vor. Die öffentlich verfügbaren Fallsammlungen zeigen, dass die Verschlüsselung von Kommunikation die Ermittlung zwar erheblich erschwert, jedoch in den seltensten Fällen unmöglich macht.

Während die deutsche Bundesregierung bislang an den 1999 vom Bundeskabinett beschlossenen Krypto-

Eckpunkten festhält und auf eine Regulierung von Kryptografie verzichtet, haben andere Staaten den Behörden die Möglichkeit der Beeinflussung von Kryptografie eingeräumt (UK, CN, FR) oder entsprechende Gesetzentwürfe in der Beratung (US). Deutschland will statt der Schwächung von Kryptografie oder Schlüsselhinterlegung durch die Gründung einer Zentralstelle (ZITIS) das Know How der Sicherheitsbehörden ausbauen sowie erweiterte technische Verfahren entwickeln, um mit kryptierter Kommunikation umzugehen. Zudem soll eine weitergehende Verpflichtung für Telemediendienstanbieter (analog TKG) geprüft werden.

II. Strategische Handlungsoptionen für Sicherheitsbehörden

Sauber implementierte starke Verschlüsselungsverfahren sind nicht zu brechen. Grundsätzlich stehen den Sicherheitsbehörden beim Umgang mit Kryptografie daher drei Optionen offen:

Systeme schwächen

Durch verdeckte Einflussnahme auf die technische Entwicklung oder durch offene gesetzliche Regelungen könnten Implementierungen kryptografischer Verfahren abgeschwächt oder Hintertüren eingebaut werden. Beides schwächt die IT-Sicherheit der jeweiligen Einsatzfelder und kann zu erheblichen Kollateralschäden führen, etwa Angriffe auf kritische Infrastrukturen oder die Ausnutzung zur Wirtschaftsspionage. Aktuelle Reports etwa der Europäischen IT-Sicherheitsagentur ENISA oder der Encryption Working Group des US-Repräsentantenhauses sehen in einer solchen Schwächung eine Gefahr für die nationale Sicherheit. Wegen des hohen Entdeckungsrisikos sind verdeckte Einflussnahmen durch Sicherheitsbehörden nur für sehr kleine Einsatzfelder möglich. Bei Bekanntwerden ebenso wie bei offener Kryptoregulierung werden wesentliche Zielgruppen der Sicherheitsbehörden sehr schnell auf andere im Internet verfügbare Verfahren ausweichen.

Schwachstellen ausnutzen und Systeme hacken

Die Nutzung von Schwachstellen in Hardware- oder Softwaresystemen zu einem vom Nutzer des Systems ungewollten Zweck ist als „Hacking“ anzusehen (... auch wenn bei Hacking durch Sicherheitsbehörden der Straftatbestand des § 202a StGB wegen der fehlenden Unrechtmäßigkeit nicht greift). „Lawful Hacking“ unterscheidet sich technisch grundsätzlich nicht vom Vorgehen anders motivierter Hacker. Die Ausnutzung von Schwachstellen durch die Sicherheitsbehörden greift in das grundrechtlich verbürgte Recht auf Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme ein, bedarf einer entsprechenden Rechtfertigung und muss verhältnismäßig ausgestaltet sein. Wie stark der Staat durch den Umgang mit Schwachstellen die IT-Sicherheit beeinträchtigt, hängt von der Qualität der genutzten Schwachstelle ab. Grundsätzlich gibt es in jedem IT-System eine Vielzahl von Schwachstellen. Während die Ausnutzung von öffentlich weithin bekannten und bereits gepatchten Schwachstellen zum Eindringen in ungepatchte Systeme keine Beeinträchtigung der allgemeinen IT-Sicherheit darstellt, kann das Zurückhalten von kritischen, öffentlich nicht bekannten Schwachstellen zum Zwecke sicherheitsbehördlicher Nutzung gravierende Auswirkungen haben. Hierzu zählt die Gefährdung von Wirtschaft, kritischen Infrastrukturen und im Extremfall auch von Leib und Leben. Regelungen zum Umgang mit Schwachstellen haben daher eine hohe Grundrechtsrelevanz und Sensibilität und bedürfen in Deutschland einer gesetzlichen Grundlage. Des Weiteren betrifft der Umgang mit Schwachstellen immer auch Aspekte der nationalen Sicherheit (z.B. des Geheimschutzes). Im Übrigen kann eine starke staatliche Nachfrage nach Schwachstellen zu einem Anheizen des Schwachstellenmarktes führen; dies muss sorgfältig beobachtet werden.

Dienstleister verpflichten

Sofern und soweit kryptografische Verfahren Nutzern durch Dienstleister zur Verfügung gestellt werden, können diese auf Grundlage gesetzlicher Ermächtigung angehalten werden, die Sicherheitsbehörden bei dem Zugriff auf die verschlüsselten Nachrichteninhalte zu unterstützen. Sofern das generell für den gesamten Dienst erfolgt, schwächt dies ebenfalls die IT-Sicherheit der Kommunikationspartner. Sofern der Dienstleister nur in Einzelfällen in Anspruch genommen wird und mit seiner Hilfe eine Erleichterung des Zugriffs auf verschlüsselte Informationen möglich ist, besteht kein großer Unterschied zu anderen systemseitigen Hilfestellung für Sicherheitsbehörden wie der Einbau von TKÜ-Schnittstellen. In der Konsequenz

dieses Vorgehens ist damit zu rechnen, dass Zielgruppen der Sicherheitsbehörden auf andere Dienste ausweichen.

III. Empfehlungen

Empfehlungen für Unternehmen

Anwenderunternehmen

Angesichts der europäischen Rechtslage im Datenschutz- und IT-Sicherheitsrecht sowie der Bedrohungslage durch Wirtschaftsspionage ist der Einsatz sauber implementierter starker Kryptografie sowohl für personenbezogene Daten, für wichtige Betriebsgeheimnisse (IP) als auch für Strukturdaten der IT- und OT-Netze dringend zu empfehlen.

IT-Sicherheitsunternehmen

Starke kryptografische Verfahren haben sich mittlerweile als Standard durchgesetzt und werden national und international von Gesetzgebern und großen Anwenderunternehmen gefordert. Sofern durch nationales Recht die Abschwächung von Verfahren, der Einbau von Hintertüren oder die sonstige Zusammenarbeit mit Sicherheitsbehörden verlangt werden, sollten hierfür spezielle nationale Versionen der Produkte erstellt werden, um die Sicherheitsbewertung insgesamt nicht zu beeinträchtigen.

Empfehlungen für die Sicherheitsbehörden

Keine systematische Schwächung

Im Interesse nationaler Sicherheit und auch aus industriepolitischem deutschen Interesse sollten die Behörden auf jegliche Maßnahme verzichten, die eine Schwächung des Vertrauens in kryptografische Verfahren zur Folge hätte. Dazu gehören die heimliche Beeinflussung oder offene Regulierung von Kryptoverfahren ebenso wie die Beschränkung von Diensteanbietern im Hinblick auf die der Art der ihren Nutzern zur Verfügung gestellten Kryptografie.

Hoher Aufwand im Einzelfall

Die Sicherheitsbehörden sollten Fähigkeiten bereithalten, auf Basis bestehender oder ggf. erweiterter gesetzlicher Befugnisse in Einzelfällen auf digitale Kommunikation Verdächtiger im rechtlich zulässigen Umfang zuzugreifen. Dazu gehören das Ausnutzen von Fehlern bei der Implementierung von Kryptografie, beim Kryptomanagement, das Ausnutzen bekannter Schwachstellen in Produkten oder auch der Einsatz von sonstigen Hilfsmitteln wie menschlichen Quellen, Quellen-TKÜ oder Online-Durchsuchung.

Technologische Fähigkeiten

Die Möglichkeiten der Sicherheitsbehörden bestehen vor allem im Zugriff auf die Systeme, deren Sicherheit knapp unterhalb einer sorgfältigen Implementierung starker Kryptografie liegt. Die Fähigkeit zu einem solchen Zugriff müssen die Sicherheitsbehörden auf Dauer aufbauen und erhalten. Internationale Beispiele (z.B. UK, FR) legen nahe, dass dies nur durch eine zentrale staatliche Instanz möglich ist, die für alle Sicherheitsbehörden technisch entwickelt.

Empfehlungen für die Politik

Empirische Grundlage verbessern

Die in den deutschen Kryptoeckpunkten angelegte Beobachtung der Auswirkungen der Kryptografie auf die Arbeit von Sicherheitsbehörden sollte durch eine breitere und öffentlich gemachte wissenschaftliche Begleitforschung fortgeführt werden.

Verschlüsselungsstandort

Der Verzicht auf eine Kryptoregulierung ist die wichtigste Maßnahme, um das von der Politik ausgegebene Ziel des Verschlüsselungsstandorts Deutschland zu erreichen. Ohne Schwächung von Kryptografie wird sich der auch im internationalen Vergleich positiv entwickelnde Markt für Kryptoverfahren verstetigen und auch die durch deutsches und europäisches Datenschutzrecht stark beförderte Anwendung von Kryptografie verbreitern. Gleichzeitig kann der Staat die Anwendung und Weiterentwicklung kryptografischer Verfahren befördern, indem er in seiner Beschaffungspolitik durchgängig auf hohe und nachgewiesene Sicherheit setzt.

Schwachstellen

Den Sicherheitsbehörden sollte vom Gesetzgeber ein Prozess vorgegeben werden, wie mit Schwachstellen in Hardware- und Softwaresystemen umzugehen ist. Dabei sollte von einer Verpflichtung des Staates zur Mitwirkung bei der zeitnahen Schließung von Schwachstellen ausgegangen werden. Die für Sicherheitsbehörden nutzbaren Schwachstellen sollten positiv definiert werden, insbesondere durch Definition einer „Erheblichkeitsschwelle“ für Schwachstellen. Für das Zurückhalten von Schwachstellen ist ein Abwägungsprozess zu definieren, der die damit verbundenen Folgewirkungen und ihre Grundrechtsrelevanz einbezieht. Vorhandene Beispiele für solche Prozesse (z.B. Vulnerability Equity Process in USA) sollten wissenschaftlich analysiert und im Hinblick auf die Übertragbarkeit geprüft werden.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.