Technische Bedingungen wirksamer Verschlüsselung

Sebastian Pape[*]

Literaturübersicht:

Abelson/*Anderson*/*Bellovin*/*Benaloh*/*Blaze*/*Diffie*/*Gilmore*/*Neumann*/*Rivest*/*Schiller*/*Schneier*, The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, Technischer Bericht, 1998, https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf; *Brown*/*Gjøsteen*, A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator, Cryptology ePrint Archive, Report 2007/048; *Buchmann*, Einführung in die Kryptographie, 1. Aufl. 1999; *Genkin*/*Pachmanov*/*Pipman*/*Tromer*/*Yarom*, ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels, ACM Conference on Computer and Communications Security (CCS) 2016; *Genkin*/*Shamir*/*Tromer*, Acoustic cryptanalysis, Journal of Cryptology, Volume 30 Issue 2, April 2017, 392; *Katzenbeisser*/*Petitcolas*, Information hiding techniques for steganography and digital watermarking, 1. Aufl. 2000; *Kerckhoffs*, La cryptographie militaire. Journal des sciences militaires. Bd. 9, 5–38, 1883, 161; *Kocher*, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of CRYPTO, Volume 1109 of Lecture Notes in Computer Science, 1996, 104; *Kocher*/*Jaffe*/*Jun*/*Rohatgi*, Introduction to differential power analysis. Journal of Cryptographic Engineering 1(1), 2011, 5; *Kurz*/*Neumann*/*Rieger*/*Engling*, Stellungnahme zur „Quellen-TKÜ“, 2016,

https://ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf; National Institute of Standards and Technology, Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators. 2012, http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf; *Randell*, Brief Encounters in Herbert/Jones, Computer Systems, Theory, Technology and Applications, 1. Aufl. 2004; *Schneier*, Did NSA Put a Secret Backdoor in New Encryption Standard?, 2007, https://www.wired.com/2007/11/securitymatters-1115/; *Schneier*, More Crypto Wars II, 2014, https://www.schneier.com/blog/archives/2014/10/more_crypto_war.html; *Wilson*/*Kehl*/*Bankston*, Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s, New America, Cybersecurity Initiative, 40 Seiten, 2015, https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/. Alle Webseiten wurden zuletzt am 27.6.2017 abgerufen.

I. Grundlagen

1

Kryptographie ist die Wissenschaft der Verschlüsselung von Daten. Diese kann für die Speicherung von Daten oder eine Kommunikation zwischen zwei Teilnehmern verwendet werden. In der Kryptographie ist es üblich, die Teilnehmer mit *Alice* und *Bob* zu bezeichnen. Man unterscheidet dann zwischen symmetrischen Verfahren, bei denen zur Ver- und Entschlüsselung derselbe Schlüssel verwendet wird (s. Abbildung 1), und asymmetrischen Verfahren, bei denen zur Ver- und Entschlüsselung verschiedene Schlüssel verwendet werden (s. Abbildung 2).

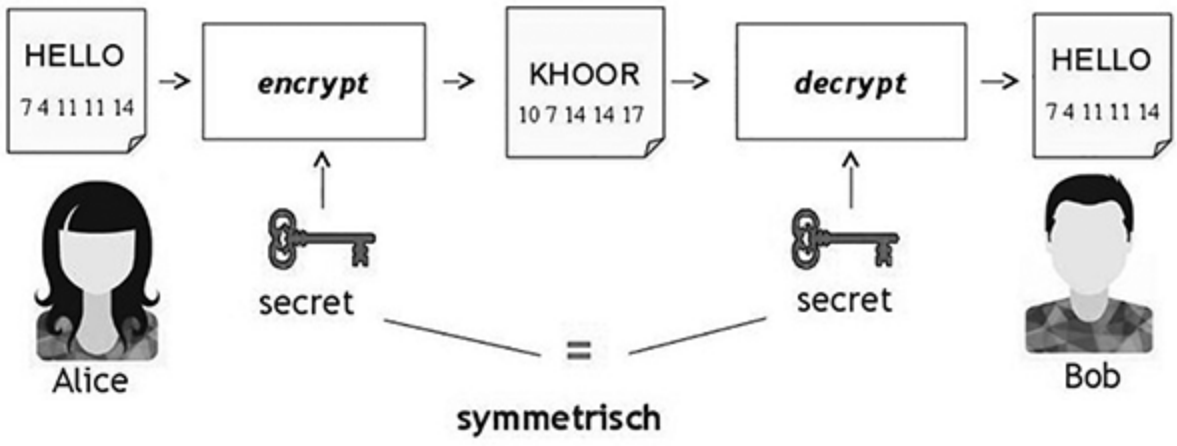

Abbildung 1: Schematische Darstellung symmetrischer Verschlüsselung

2

Vorteil der asymmetrischen Verschlüsselung ist, dass die Verschlüsselungs-Schlüssel (auch öffentliche Schlüssel genannt) in einem Verzeichnis hinterlegt werden können und die Kommunikationsteilnehmer nicht paarweise Schlüssel tauschen müssen.[1]

3

Das ***Kerckhoffs'*sche Prinzip**[2] besagt, dass die Sicherheit eines Verfahrens nur auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verfahrens beruhen sollte. Es gilt als Grundlage der modernen Kryptographie. Gründe dafür sind, dass es einerseits sehr schwer ist, einen Algorithmus auf Dauer geheim zu halten, da z. B. Mitarbeiter die Firma verlassen oder er durch Reverse Engineering erforscht werden kann. Andererseits ist es schwer, das gesamte Verfahren auszutauschen, falls es bekannt werden sollte.

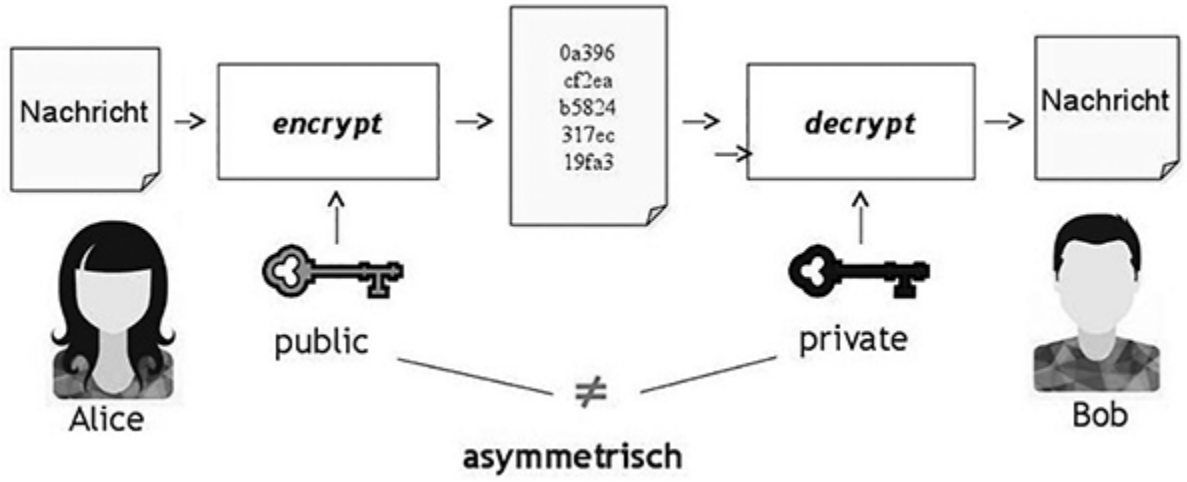

Abbildung 2: Schematische Darstellung asymmetrischer Verschlüsselung

4

Generell gilt aber, dass Verschlüsselung nur ein **Teil einer Sicherheitsmaßnahme** sein und nur im Zusammenspiel mit anderen Komponenten ein sicheres System schaffen kann. So sollten die Eigenschaften, was wann wie verschlüsselt wird bzw. wie und wo die Schlüssel aufbewahrt werden, nicht losgelöst vom Verschlüsselungsalgorithmus betrachtet werden.[3]

5

Besteht eine durchgängige Verschlüsselung vom Sender (*Alice*) zum Empfänger (*Bob*), so spricht man auch von einer **Ende-zu-Ende-Verschlüsselung**. Bei E-Mails ist dies in der Regel nur gegeben, wenn die Benutzer ein Verschlüsselungsprogramm wie Pretty Good Privacy (PGP) verwenden, da E-Mails zwar verschlüsselt zum Mail-Server übertragen werden, dort aber entschlüsselt und nicht verschlüsselt gespeichert werden.

II. Überwachungsmaßnahmen

6

Betrachtet man Kryptographie als Werkzeug, so gibt es – wie bei jedem anderen Werkzeug auch – gesellschaftlich akzeptierte und nicht akzeptierte **Verwendungszwecke**. Der Großteil der Kommunikation, wie beispielsweise E-Commerce (Einkaufen über das Internet) oder die private Nutzung von Instant-Messaging-Diensten dürfte weithin als gesellschaftlich akzeptiert gelten. Gerade aber auch die mögliche Nutzung

durch Kriminelle oder Terroristen sorgt zunehmend dafür, dass staatliche Stellen mit verschiedenen Mitteln die Verschlüsselung von Kommunikation oder Speicherung von Daten umgehen wollen. Historisch erklangen Forderungen nach Verboten oder dem Einbau von Umgehungsmaßnahmen in (starke) Verschlüsselung in den 90ern insbesondere in den Vereinigten Staaten als sog. **Crypto-War** (Verschlüsselungskrieg). Die Forderung ist dabei allerdings nicht auf die Vereinigten Staaten beschränkt, sondern findet sich auch in zahlreichen anderen Ländern. In der Regel wird die Forderung von Strafverfolgern und Geheimdiensten vorgebracht und verfolgt das Ziel, Zugriff auf verschlüsselte Kommunikation zu erhalten. Auf der anderen Seite des Konflikts stehen Bürgerrechtler, Datenschutzaktivisten und Technologie-Firmen, die sich dafür stark machen, den Zugang zu (starker) Kryptografie für jeden zu erhalten.[4]

7

Im Folgenden werden daher verschiedene technische Maßnahmen vorgestellt, die dazu dienen sollen, die Verschlüsselung zu umgehen. Dabei wird lediglich die Maßnahme technisch beschrieben und bewertet. Es erfolgt keine Diskussion, ob und unter welchen Umständen die Maßnahme rechtlich legitimiert ist oder ob sie einen zulässigen oder unzulässigen Eingriff in die (Grund-)Rechte des Betroffenen darstellt.

1. Verschlüsselungsverbote

8

Verschlüsselungsverbote sind der Versuch des Staates, die Benutzung von (starker) Kryptographie gesetzlich zu untersagen.

9

Dem steht entgegen, dass es zweifelhaft ist, ob gerade diejenigen, die eigentlich ausgespäht werden sollen, da sie kriminelle oder terroristische Aktivitäten planen, sich an das Verbot halten. Technisch sind Kontrollen nur mit sehr hohem Aufwand oder gar nicht möglich, da die Benutzer die verschlüsselten Daten auch in anderen Daten wie beispielsweise Bild-, Audio- oder Video-Dateien verstecken können (Steganographie[5]).

2. Schlüsselhinterlegung

10

Bei der **Schlüsselhinterlegung** wird der Einsatz von Kryptografie prinzipiell erlaubt, allerdings werden die Benutzer verpflichtet, ihren privaten Schlüssel bei einer entsprechenden Stelle zu hinterlegen, so dass bei Bedarf eine Entschlüsselung der Kommunikation oder des Speichers möglich ist (s. Abbildung 3).[6]

11

Problematisch dabei ist, dass nun die Schlüssel aller Benutzer in einer zentralen Datenbank liegen. Diese wird dadurch für Angreifer höchst attraktiv, so dass weitreichende Schutzmaßnahmen gegen externe und interne Angreifer getroffen werden müssen, um Missbrauch zu vermeiden. Ein weiteres Problem stellt auch hier die effektive Kontrolle der hinterlegten Schlüssel dar. Um sicher zu gehen, dass auch der richtige Schlüssel hinterlegt wurde, müssten eigentlich alle Verbindungen und Speicherungen permanent darauf geprüft werden, ob auch der hinterlegte Schlüssel verwendet wird (überwachte Schlüsselhinterlegung). Auch dies ist aber nur unzureichend, da eine Mehrfachverschlüsselung oder die bereits beschriebene Steganographie dies einfach aushebeln können.

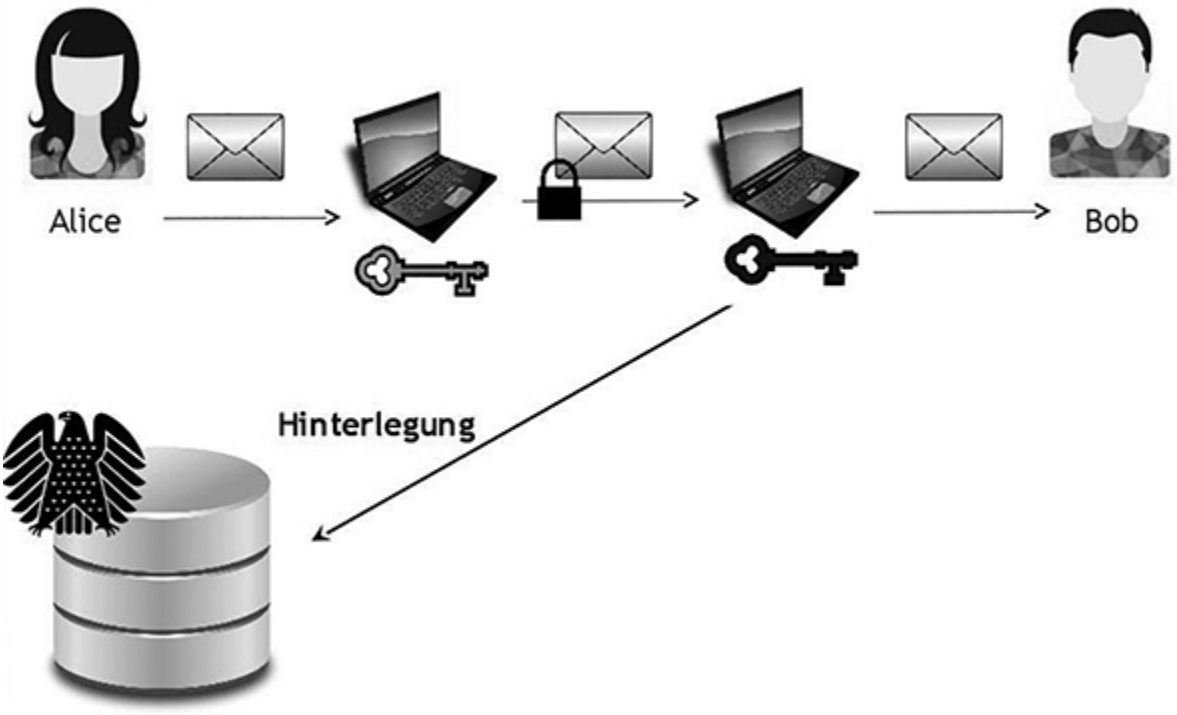

Abbildung 3: Schematische Darstellung Schlüsselhinterlegung

3. Hintertüren

12

Hintertüren in Verschlüsselungsalgorithmen beschreiben den Versuch, die grundlegenden Algorithmen derart zu gestalten, dass eine staatliche Stelle die Verschlüsselung bei Bedarf brechen kann (s. Abbildung 4).[7] Dies kann einerseits durch Schwächen im Algorithmus oder auch durch entsprechende Parameterwahl erfolgen.

13

Als Beispiel dafür gilt ein von der National Security Agency (NSA) in den NIST-Standard 800-90A[8] eingebrachter Zufallsgenerator, von dem später gezeigt wurde, dass er eine Hintertür enthält.[9] [10]

14

Das Hauptproblem bei dieser Methode ist, dass Benutzer auch hier nicht gezwungen werden können, die entsprechenden mit Hintertüren versehenen Algorithmen oder Programme zu benutzen. Open Source oder Eigenimplementierungen bereits bekannter starker Verschlüsselungsalgorithmen wären dann ohne entsprechende Hintertür verwendbar. Auf der anderen Seite könnten dann bei denjenigen, die die entsprechend geänderten Versionen mit Hintertüren verwenden, auch andere als die ursprünglichen Parteien in der Lage sein, die Hintertür zu finden und auszunutzen. Im Gegensatz zu den hinterlegten Schlüsseln entzieht sich dies der Kontrolle der staatlichen Stelle, da sie nicht notwendigerweise mitbekommt, dass sich Angreifer das notwendige kryptografische Wissen aneignen.

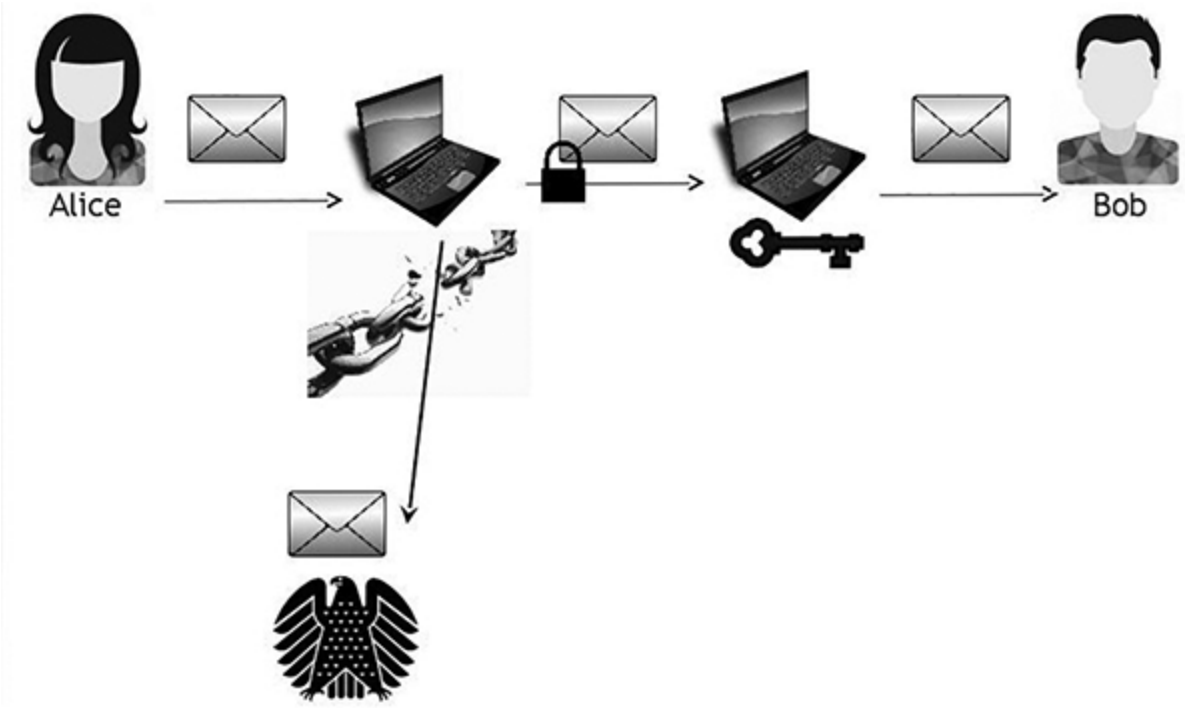

Abbildung 4: Schematische Darstellung Hintertür

4. Quellen-Telekommunikationsüberwachung

15

Bei der **Quellen-Telekommunikationsüberwachung** (Quellen-TKÜ) wird auf dem Gerät des Betroffenen ein Programm installiert, mit dem sich die Kommunikation vor der Verschlüsselung abhören lässt (s. Abbildung 5). Dazu muss entweder das Gerät (unbemerkt) entwendet werden, um das Programm zu installieren, oder es muss ein Fehler im Betriebssystem oder in einem installierten Programm ausgenutzt werden, um das Überwachungsprogramm unbemerkt auf dem Gerät des Betroffenen zu installieren.

16

Hauptproblem bei der Quellen-TKÜ ist, dass das eingesetzte Programm die Integrität des überwachten Gerätes verletzt. Durch die Installation – insbesondere in Verbindung mit dem Ausnutzen einer Sicherheitslücke- wird das System des Betroffenen verändert. In der Regel verfügt das installierte Programm zudem über die Funktion des Nachladens, um sich an Aktualisierungen des Gerätes anpassen zu können und weiterhin vor dem Betroffenen verborgen zu bleiben. Dadurch wird einerseits das

System des Betroffenen weiteren Risiken ausgesetzt, da z. B. Dritte eigene Module nachladen könnten. Andererseits erschwert dies eine mögliche Beweisführung, da der Nachweis, dass eine bestimmte Aktion wirklich vom Betroffenen ausgeführt wurde, nicht erbracht werden kann, wenn dazu das überwachte Gerät gleichzeitig ferngesteuert werden kann. Da sich das installierte Programm technisch nicht von Schadsoftware unterscheidet, besteht zudem das Risiko, dass der Betroffene das Programm entdeckt, beispielsweise durch einen Anti-Viren-Scanner. Diese arbeiten oft mit Heuristiken, so dass sie auch Schadprogramme erkennen können, von denen dem Anti-Viren-Hersteller kein Muster vorlag.[11]

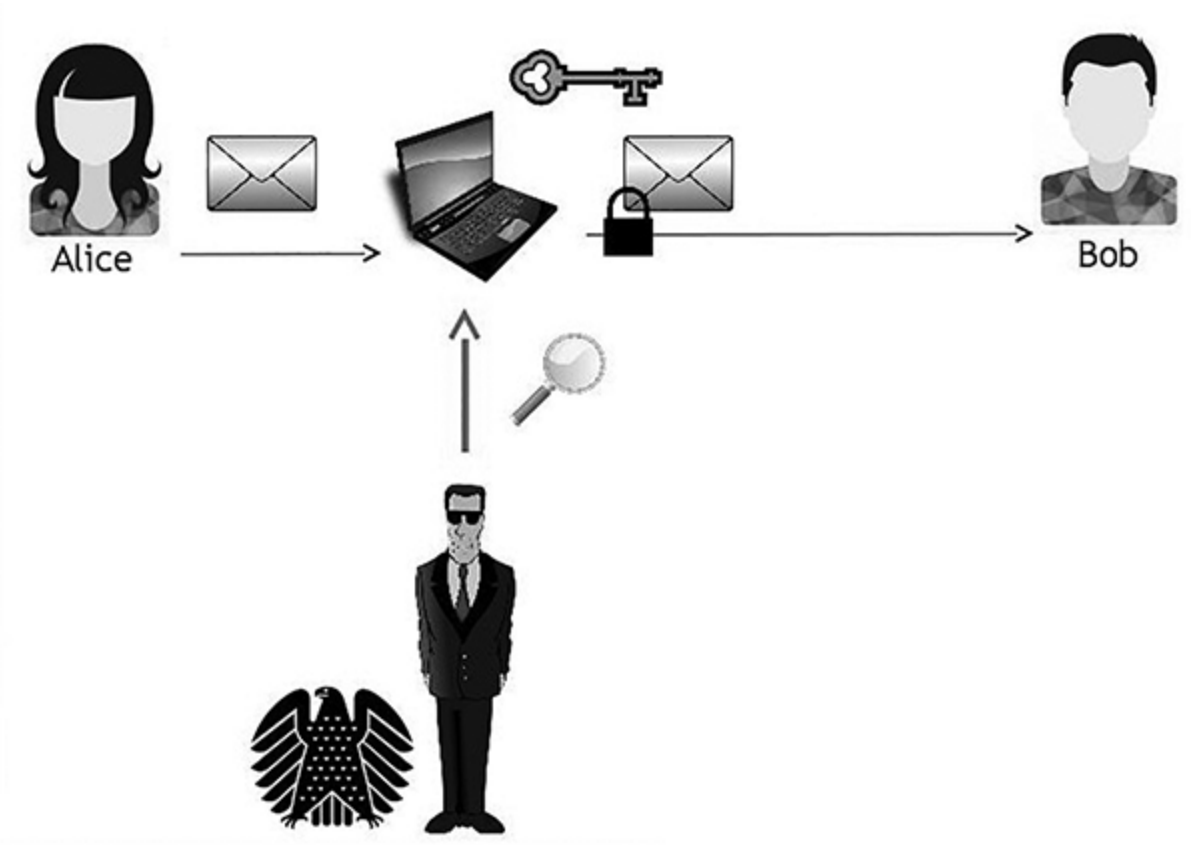

Abbildung 5: Schematische Darstellung Quellen-TKÜ

5. Onlinedurchsuchung

17
Technisch funktioniert die **Onlinedurchsuchung** sehr ähnlich wie die Quellen-TKÜ, nur dass dabei nicht auf Kommunikation, sondern auf gespeicherte Inhalte des Geräts zugegriffen wird (s. Abbildung 6). Dies

kann z. B. dann für die Überwacher hilfreich sein, wenn Inhalte verschlüsselt gespeichert werden. Im Gegensatz zu einer Beschlagnahmung des Geräts, bei der die verschlüsselten Inhalte nicht zugänglich sind, kann es sein, dass die entsprechenden Daten vom Benutzer entschlüsselt wurden und damit vom installierten Programm ausgespäht werden können.

18
Durch ihre technische Ähnlichkeit bestehen bei der Onlinedurchsuchung dieselben Probleme wie bei der Quellen-TKÜ. Durch das Nachladen von entsprechenden Modulen könnte außerdem ein als Quellen-TKÜ begonnenes Abhören leicht in eine Onlinedurchsuchung gewandelt werden.[12]

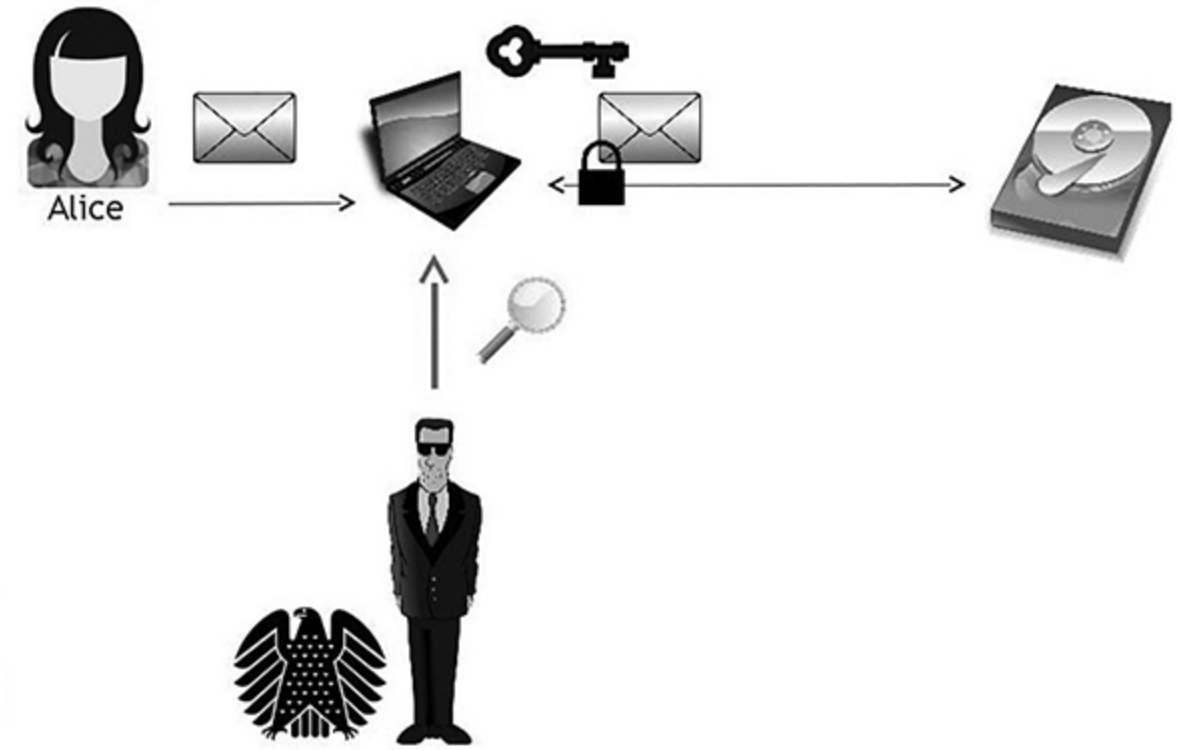

Abbildung 6: Schematische Darstellung Onlinedurchsuchung

III. Seitenkanalattacken

19
Wenn ein kryptografischer Algorithmus in der Theorie sicher ist, so heißt dies noch lange nicht, dass seine Implementierung auch sicher ist. Bei **Seitenkanalattacken** wird nicht das kryptografische Verfahren

gebrochen, sondern für eine bestimmte Implementierung des Verfahrens aus zusätzlichen Quellen (den Seitenkanälen) Information gewonnen, mit der ein Angriff dann möglich ist. Da die meisten Geräte in Abhängigkeit von den gerade für eine Operation verwendeten Werten unterschiedlich lange brauchen[13] oder unterschiedlich viel Strom verbrauchen[14], Strahlung abgeben[15] oder Geräusche emittieren[16], lässt sich ein dort gemessener Wert mit den gerade verarbeiteten Werten korrelieren. Enthalten die verarbeiteten Werte den Schlüssel oder Teile davon, lassen sich die beobachteten Daten mit dem Schlüssel korrelieren. Die so gewonnene Zusatzinformation kann ausreichend sein, um damit den Ciphertext zu entschlüsseln oder den verwendeten Schlüssel zu errechnen.

20
Problem dieser Methode ist allerdings ein in der Regel recht großer Aufwand, da einerseits vor Ort Informationen gewonnen werden müssen und andererseits die Auswertung und Korrelation der Informationen mit den kryptografischen Schlüsseln nicht trivial ist.

IV. Zusammenfassung und Schluss

21
Zusammenfassend lässt sich festhalten, dass keine der in Abschnitt II vorgestellten Überwachungsmaßnahmen bedenkenlos eingesetzt werden kann. Entweder sind die vorgestellten Maßnahmen von Hause aus nicht geeignet, starke Verschlüsselung effektiv zu verhindern oder sie greifen sehr massiv in die Integrität des Gerätes (z. B. Computer oder Mobilfunkgerät) ein.

22
Geht man weiterhin davon aus, dass das Ziel staatlicher Überwachungsmaßnahmen nur Schwerkriminelle und Terroristen sind, so erscheint es trotz des erhöhten Aufwands sinnvoll, sich auf Seitenkanalattacken zu beschränken. Das hätte die beiden Vorteile, dass diese einerseits zurzeit sehr schwer zu verhindern sind, aber andererseits aufgrund des nicht unbeträchtlichen Aufwands nicht gut genug skalieren, um eine Totalüberwachung der Bürger zu ermöglichen.

---

* Dr. *Sebastian Pape* ist Senior Researcher an der Stiftungsprofessur der Deutschen Telekom für Mobile Business & Multilateral Security in der

Abteilung für Wirtschaftsinformatik der Goethe-Universität Frankfurt.

[1] Vgl. *Buchmann* 1999.

[2] Vgl. *Kerckhoffs* 1883.

[3] Vgl. *Randel* 2004, S. 235, der *Needham* und *Lampson* die Äusserung zuschreibt: „Jeder der annimmt, dass ein Problem einfach durch Verschlüsselung gelöst ist, versteht weder Verschlüsselung noch das Problem." („Anybody who asserts that a problem is readily solved by encryption, understands neither encryption nor the problem.").

[4] Vgl. *Wilson/Kehl/Bankston* 2015.

[5] Vgl. *Katzenbeisser/Petitcolas* 2000.

[6] Vgl. *Abelson/Anderson/Bellovin/Benaloh/Blaze/Diffie/Gilmore/Neumann/Rivest/Schiller/Schneier* 1998.

[7] Vgl. *Schneier* 2014.

[8] Vgl. National Institute of Standards and Technology 2012.

[9] Vgl. *Brown/Gjøsteen* 2007.

[10] Vgl. *Schneier* 2007.

[11] Vgl. *Kurz/Neumann/Rieger/Engling* 2016.

[12] Vgl. *Kurz/Neumann/Rieger/Engling* 2016.

[13] Vgl. *Kocher* 1996.

[14] Vgl. *Kocher/Jaffe/Jun/Rohatgi* 2011.

[15] Vgl. *Genkin/Pachmanov/Pipman/Tromer/Yarom* 2016.

[16] Vgl. *Genkin/Shamir/Tromer* 2017.