Security of Symmetric Encryption against Mass Surveillance

Mihir Bellare, Kenneth G. Paterson, und Phillip Rogaway

vorgelegt von:
Kevin Haack

Matrikelnummer: 7094226
Studiengang: Informatik (M.Sc.)

Thema betreut von:
Prof. Dr.-Ing. Tibor Jager

Paderborn, 3. März 2017

Kurzzusammenfassung

Security of Symmetric Encryption against Mass Surveillance

Zusammenfassung

Spätestens seit den Snowden Leaks ist öffentlich bekannt, dass Massenüberwachung im Internet stattfindet. Codenamen wie PRISM werden in Zeitschriften veröffentlicht ([GG13]). Wir sehen, dass verschlüsselte Übertragungen unsere Daten nicht vor unbefugtem Zugriff schützen. Pseudozufallsgeneratoren die möglicherweise nicht ganz zufällig sind, wie zum Beispiel der NIST Dual EC DRBG, sorgen für potenziell unsichere VPN Verbindungen und Backdoors in eigentlich sicheren Übertragungen ([Sch07]) könnten in nahezu jeder Anwendung vorkommen. Das original Paper von Mihir Bellare, Kenneth G. Paterson und Phillip Rogaway soll die erste Salve im Kampf gegen Massenüberwachung abgeben ([MB14b]) und fokussiert sich auf symmetrische Verschlüsselungsschemen und einen speziellen Angriffsvektor, den sogenannte Algorithm Substitution Attacks. Es soll eine Grundlage mit der Definition und Formalisierung schaffen für die Abwehr dieses Angriffs. Denn symmetrische Verschlüsselungen bilden das Rückkrad vieler alltäglicher Übertragungstechniken wie zum Beispiel IPsec oder TLS. Diese Arbeit soll zunächst einen Überblick über das Originalwerk geben, Inhalte zusammenfassen und verdeutlichen. Es wird dargestellt, wie Algorithm Substitution Attacks funktionieren könnten und welchen symmetrische Schemen dagegen gefeit sind.

Stichworte

Algorithm Substitution Attacks, symmetrische Verschlüsselung, unique ciphertext scheme, key recovery

Inhaltsverzeichnis

1 Einleitung

1.1 Hintergrund

Seit den Snowden Veröffentlichungen ist öffentlich bekannt, dass Massenüberwachung im Internet Heute möglich ist und auch stattfindet. Durch zum Beispiel maniupulierte Pseudozufallsgeneratoren wie der NIST Dual EC DRBG entstehen Backdoors in eigentlich sicheren Übertragungen ([Sch07]). Diese Ausarbeitung des original Papers Security of Symmetric Encryption against Mass Surveillance von Mihir Bellare, Kenneth G. Paterson und Phillip Rogaway handelt von Algorithm Substitution Attacks, kurz ASAs, als eine spezielle Angriffstechnik gegen symmetrische Verschlüsselungsverfahren. Grundidee hinter einem ASA ist das korrumpieren eines eigentlich sicheren symmetrischen Schemas Π, durch den Austausch der Verschlüsselugsfunktion $\mathcal{E}$ durch eine Subversion $\widetilde{\mathcal{E}}$. Also findet der Angriff nicht von Außen, sondern von Innen statt. Eine solche Subversion soll das Geheimnis in der regulären Übertragung verstecken.

1.2 Big Brother

Big Brother ($\mathscr{B}$) steht in diesem Paper als Synonym für Regierungen oder Geheimdienste. Wir nehmen an, dass $\mathscr{B}$ durch seine politische und/oder finanzielle Macht in der Lage ist $\mathcal{E}$ gegen eine korrumpiere Subversion $\widetilde{\mathcal{E}}$ auf beliebigen Maschinen auszutauschen. In diesem Angriffsmodell ist $\mathscr{B}$ ein passiver Angreifer, der einen Masterschlüssel $\widetilde{\mathcal{K}}$ hält. Sein Ziel ist es dabei den Ciphertext $\mathcal{C}$ zu entschlüsseln oder mit Hilfe von $\widetilde{\mathcal{K}}$ den symmetrischen Schlüssel $\mathcal{K}$ zu ermitteln und letztendlich auch den Ciphertext $\mathcal{C}$ zu entschlüsseln. Dabei möchte Big Brother immer unentdeckt bleiben.

1.3 Good Guys

Als Gegenspieler treten in diesen Fall Alice und Bob als Nutzer an. Die Nutzer verwenden ein symmetrisches Verschlüsselungsschema Π mit dem symmetrischen Schlüssel $\mathcal{K}$. Dabei möchten sie mögliche korrumpierte Subversionen $\widetilde{\mathcal{E}}$ oder manipulierte $\mathcal{C}$s entdecken. Ziel des Nutzers ist es gegen ASAs resistente Schemen zu finden. So könnten effektiv Angriffe dieser Art verhindern werden.

1.4 Angriffs Ziele

Algorithm Substitution Attacks setzen auf symmetrische Verschlüsselungsschemen mit Zufallskomponenten ohne und mit öffentlichen nonce auf. Sie nutzen black-box Verhalten und die nicht Verifizierbarkeit dieser Zufälle. Selbst open source Bibliotheken kann man in der realen Welt ein gewisses black-box Verhalten zuschreiben, denn außer wenigen Entwicklern setzt sich kaum jemand mit den konkreten Implementierungen auseinander. In dem Originalwerk wird gezeigt, dass fast alle symmetrischen Verschlüsselungsverfahren angreifbar sind.

2 Grundlagen

Dieses Kapitel soll eine Grundlage für jeden Leser schaffen. Es werden die grundlegenden Rahmenbedingungen beschrieben, erste Begriffe und Notationen eingeführt um das spätere Verständnis des Originalwerks zu erläutern. So wird auf den folgenden Seiten ein symmetrisches Verschlüsselungsschema Π und dessen Subversion $\widetilde{\Pi}$ behandelt. Subversionen sind von $\mathscr{B}$ in das Schema eingeschleuste Komponenten, die ein Key Recovery ermöglichen sollen.

2.1 Die ideale Welt

Als Basis für alle Erläuterungen dient ein Model der idealen Welt (siehe Abbildung 2.1). In einer idealen Welt möchte Alice eine verschlüsselte Nachricht M an Bob schicken. Alice und Bob sind normale Nutzer, die im Besitz eines symmetrischen Schlüssels $\mathcal{K}$ sind. Für diese Übertragung wird ein symmetrisches Verschlüsselungsschema $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{K})$ verwendet. Das Schema Π besteht aus einer Funktion $\mathcal{E} = (\mathcal{K}, M)$, die mit dem symmetrischen Schlüssel $\mathcal{K}$ die Nachricht M verschlüsseln und eine Funktion $\mathcal{D} = (\mathcal{K}, \mathcal{C})$, die mit dem symmetrischen Schlüssel $\mathcal{K}$ einen Chiffretext $\mathcal{C}$ entschlüsselt. So ergibt sich eine erste allgemeine Definition eines symmetrischen Verschlüsselungsschemas. Big Brother $\mathscr{B}$ versucht in diesem Fall passiv die Nachricht zu entschlüsseln oder den Schlüssel $\mathcal{K}$ zu reproduzieren. Diese Art von Darstellung von Abbildung 2.1 werde ich noch mehrfach in der Arbeit verwenden. Im oberen Teil ist immer die ideale Welt und unten sind Bestandteile des Schemas durch Subversionen ausgetauscht. In diesem Fall ist die Verschlüsselungsfunktion $\mathcal{E}$ durch die Subversion $\widetilde{\mathcal{E}}$ ausgetauscht worden. Big Brother ist in der Lage, die Nachricht mit dem Masterschlüssel $\widetilde{\mathcal{K}}$ zu reproduzieren, wobei Bob die Nachricht weiterhin entschlüsseln kann.

2.2 Korrektheit

Letzteres ist essenzieller Bestandteil von Big Brothers Subversion. Jede Nachricht M die von Alice verschlüsselt versendet wird muss mithilfe von $\mathcal{K}$ von Bob wieder zu M entschlüsselt werden. Eben auch wenn Alice eine Subversion von Π verwendet. Wir können sagen, dass ein Schema $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ korrekt ist, wenn der Empfänger den Chiffretext immer zu der gleichen ursprünglichen Nachricht M entschlüsselt, die der Sender gesendet hat. Also wenn für alle Nachrichten gilt: $\mathcal{E}(\mathcal{K}, M_1) = \mathcal{C}_1$ und $\mathcal{D}(\mathcal{K}, \mathcal{C}_2) = M_2$, mit $\mathcal{C}_1 = \mathcal{C}_2$ und $M_1 = M_2$.

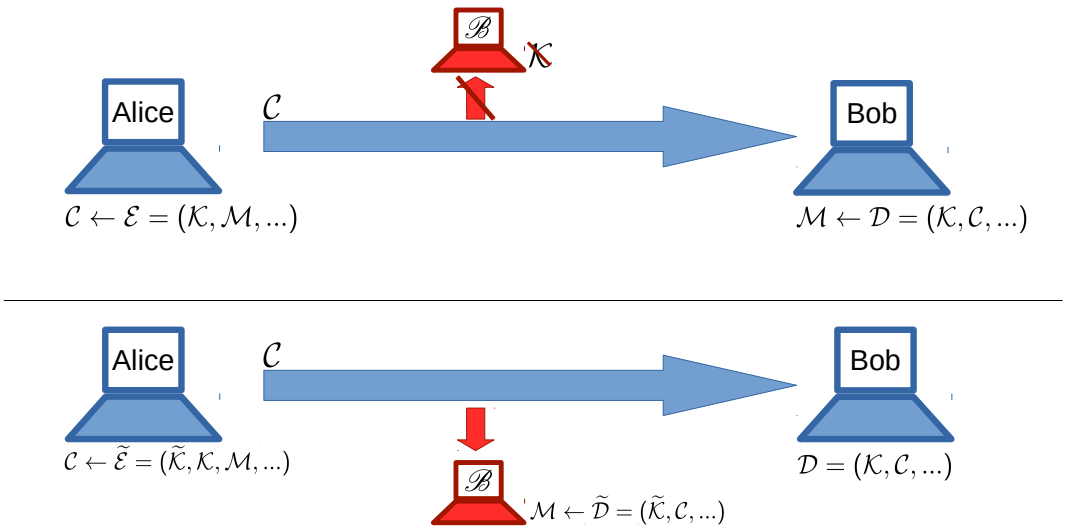

Abbildung 2.1: Symmetrische Verschlüsselung in einer idealen Welt.

2.3 Decryptability

Eine weitere wichtige Eigenschaft beschreibt die Entschlüsselbarkeit einer Subversion $\widetilde{\Pi}$ relativ zu Π. Wenn $\widetilde{\Pi}$ ein korrektes Verschlüsselungsschema ist und die Funktion $\tilde{\mathcal{E}}$ den Schlüssel K und den Masterschlüssel $\tilde{\mathcal{K}}$ verwendet, mit $K \neq \tilde{\mathcal{K}}$, dann erfüllt $\widetilde{\Pi}$ die Eigenschaft Entschlüsselbarkeit. Allerdings nur jemand, der $\mathcal{K}$ hält, darf mit der Funktion $\mathcal{D}$ die Nachricht korrekt entschlüsseln. Wir gehen davon aus, dass $\mathscr{B}$ immer versucht diese Eigenschaft zu erreichen um nicht entdeckt zu werden.

2.4 Detection Advantage

Die Erfolgschancen von ASAs können an der Entdeckbarkeit gemessen werden. Eine Subversion ist von Alice oder Bob entdeckbar, wenn nicht gesagt werden kann, ob der Chiffretext C von einer Subversion oder vom eigentlichen Schema Π erzeugt wurde. Die Eigenschaft Entschlüsselbarkeit bildet hierfür die Basis. Wenn eine Entschlüsselung fehlschlägt, führt dies wahrscheinlich auch zum Entdecken der Subversion. Allerdings ist anzumerken, dass selbst wenn die Wahrscheinlichkeit Entdeckt zu werden hoch ist, beutet es nicht, dass ein Nutzer in der Lage ist eine Subversion zu entdecken.

3 Angriffe

In diesem Kapitel stelle ich die drei Grundkonzepte von Algorithm Substitution Attacks vor. Dabei sind alle drei Konzepte in die Abschnitte Grundidee, Durchführung und Entdeckbarkeit unterteilt und erklärt.

3.1 IV-replacement (stateful) attack

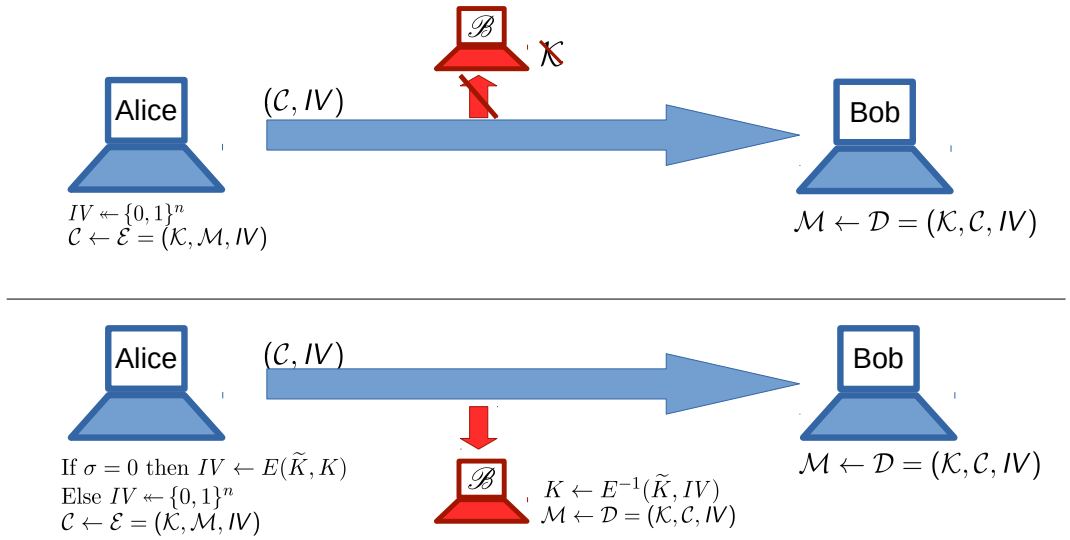

Abbildung 3.1: IV replacement (stateful) attack.

3.1.1 Grundidee

Der erste und simpelste Ansatz für eine ASA ist die IV replacement attack. Dieser Angriff zielt auf ein symmetrisches stateful Schema mit einem öffentlichen nonce ab. Ein solcher nonce könnte zum Beispiel ein Initialisierungsvektor sein. Grundidee ist es hierbei, dass der Schlüssel $\mathcal{K}$ im IV versteckt wird.

3.1.2 Durchführung

Zusammen mit dem Chiffretext $\mathcal{C}$ wird ein nonce übertragen, in diesem Beispiel der Initialisierungsvektor IV. Dieser ist Bestandteil der Verschlüsselung mit $\mathcal{E} = (\mathcal{K}, M, IV)$ und der Entschlüsselung mit $\mathcal{D} = (\mathcal{K}, C, IV)$. Im einfachsten Fall nehmen wir an, dass die $|IV|$ und die $|\mathcal{K}|$ identisch sind. Ausgenutzt

wird hierbei der Pseudozufallsgenerator, der einen nicht verifizierbaren Zufall geniert. Der IV wird also als Geheimnisträger missbraucht. Der Status σ dient hierbei auch als Status zur Erzeugung des IVs. Nur zu Beginn einer Verschlüsselung soll das Geheimnis $\mathcal{K}$ über den nonce verraten werden. Dieser Angriff kann eben so erweitert werden für $|\mathcal{K}| > |IV|$, indem immer nur Teile von $\mathcal{K}$ über den Status σ hinweg verraten werden. Big Brother reproduziert sich den geheimen Schlüssel $\mathcal{K}$ mit der Umkehrfunktion E^{-1} und seinem Masterschlüssel $\widetilde{\mathcal{K}}$.

3.1.3 Entdeckbarkeit

Eine solche Subversion ist unentdeckbar, wenn der vom Pseudozufallszahlengenerator (PRNG) erzeugte IV ununterscheidbar ist von einem zufällig gewähltem. Selbst für einen Beobachter der den Schlüssel $\mathcal{K}$ kennt ist so eine Subversion unentdeckbar. Allerdings steigt die Wahrscheinlich einer Entdeckung, wenn sich ein IV wiederholt. Dies wäre vorstellbar wenn das System resettet wird.

3.2 IV-replacement (stateless) attack

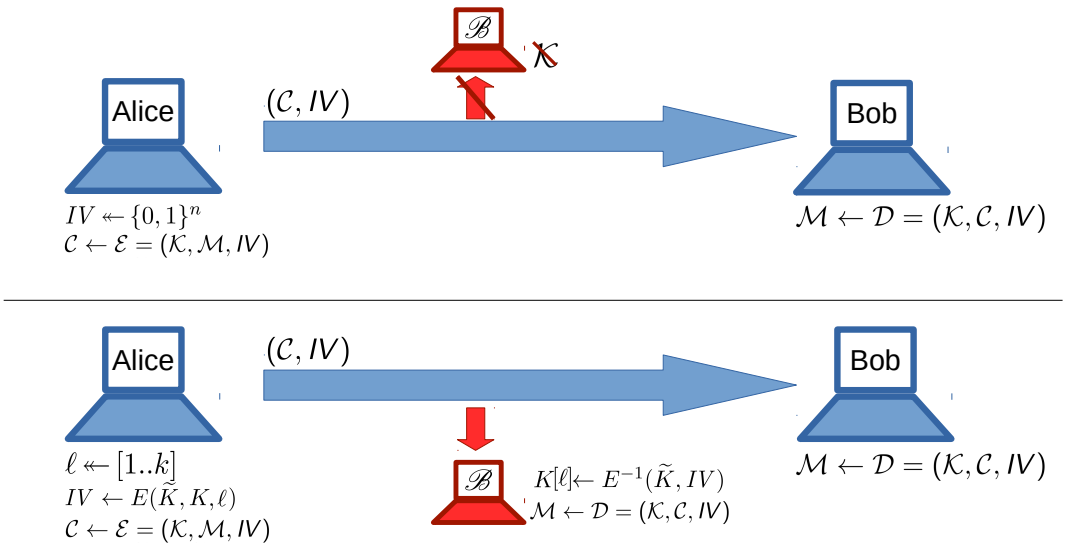

Abbildung 3.2: IV replacement (stateless) attack.

3.2.1 Grundidee

Der zweite Ansatz für eine ASA ist ebenfalls die IV replacement attack, diesmal für ein symmetrisches stateless Schema $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{K})$. Ansatzpunkt bei diesem Angriff ist wieder die Generierung des nonce. Grundgedanke ist es, bitweise und

mit einer gewissen zufälligen Verteilung Teile von $\mathcal{K}$ im IV zu versteckt. Bei jeder Generierung des IV wird ein zufälliges Bit von $\mathcal{K}$ im IV versteckt. Der Schlüssel $\mathcal{K}$ kann so nach endlicher Zeit von $\mathscr{B}$ bitweise und über mehrere Übertragungen hinweg rekonstruiert werden.

3.2.2 Durchführung

Alice geniert sich mit einer Subversion der Funktion E, in der der Masterschlüssel $\widetilde{\mathcal{K}}$ verwendet wird, einen IV. Dieser ist allerdings nicht ganz zufällig. Er ist so geschickt gewählt, dass er ein zufälliges Bit ℓ des geheimen Schlüssels $\mathcal{K}$ enthält. Dieser IV geht wie beim regulären Π in die Verschlüsselungsfunktion $\mathcal{E}$ ein. Big Brother ist nun in der Lage mit dem Masterschlüssel $\widetilde{\mathcal{K}}$ und der Umkehrfunktion E^{-1} von E ein Bit ℓ von $\mathcal{K}$ zu berechnen.

3.2.3 Entdeckbarkeit

Eine solche Subversion ist noch schwerer entdeckbar als die vorherige Angriffstechnik. Selbst ein Reset des Systems kann nicht zum Entdecken der Subversion führen. Je mehr Bits von $\mathcal{K}$ in einer Übertragung verraten werden, desto höher ist die Wahrscheinlichkeit, dass die Subversion entdeckt wird.

3.3 biased-ciphertext attack

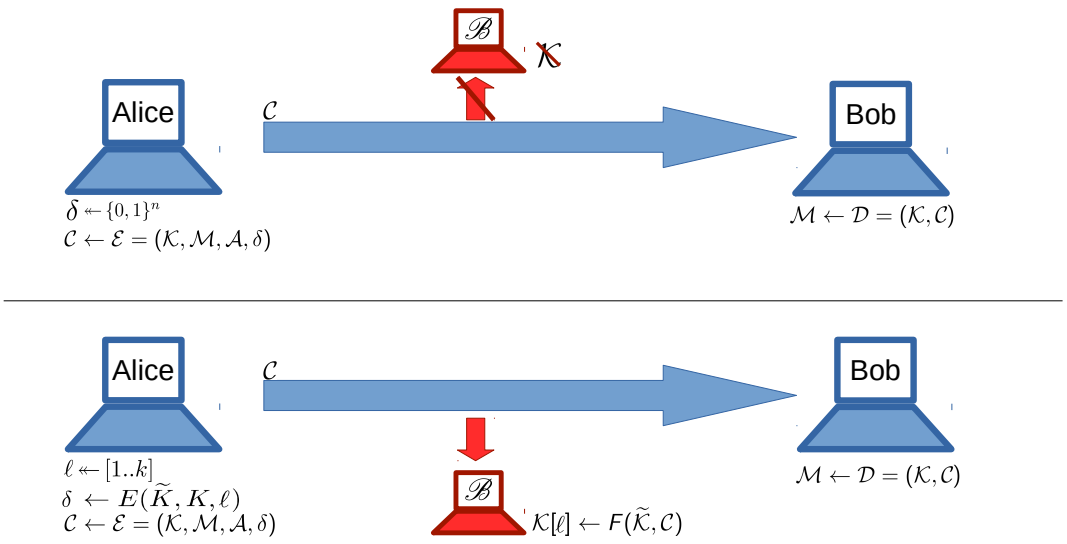

Abbildung 3.3: biased-ciphertext attack.

3.3.1 Grundidee

Die vorherigen Angriffe sind nur anwendbar auf spezielle Klassen von symmetrischen Verschlüsselungen. Ein universeller Ansatz für eine ASA ist die biased-ciphertext attack. In diesem Fall kann ein symmetrisches Schema ohne öffentlicher nonce angegriffen werden. Ziel sind symmetrische stateless Schemen mit kleiner Zufallskomponente. Bitweise werden Teile von $\mathcal{K}$ über den Chiffretext $\mathcal{C}$ selbst hinweg verraten.

3.3.2 Durchführung

Entscheidend bei diesem Angriff ist, dass kein öffentlicher nonce nötig ist. Wie auf Abbildung 3.3 zu sehen, wurde zum Verschlüsseln auf Alices Seite ein Zufall δ verwendet. Wie der IV in den vorherigen Angriffen, beinhaltet δ nicht verifizierbaren Zufall und der eigentliche Zufallszahlengenerator kann gegen die Funktion E ausgetauscht werden. Diese verwendet den Masterschlüssel $\widetilde{\mathcal{K}}$ um ein zufälliges Bit ℓ des geheimen Schlüssels $\mathcal{K}$ in dem jetzt nicht mehr ganz zufällig gewählten δ zu verstecken. Die Funktion $\mathcal{E}$ verwendet δ anschließend um den Chiffretext zu erzeugen. Big Brother ist nun in der Lage, mit Hilfe von $\widetilde{\mathcal{K}}$ und einer Funktion F bitweise den geheimen Schlüssel $\mathcal{K}$ zu reproduzieren. Wenn so nur ein einziges Bit ℓ von $\mathscr{B}$ errechnet werden kann, werden nur $|\mathcal{K}|$ Verschlüsselungen benötigt, um den vollständigen Schlüssel $\mathcal{K}$ zu bestimmen. Die Autoren legen Wert darauf, dass dies keine chosen-message attack ist. Big Brother kann den geheimen Schlüssel zurückrechnen, unabhängig von der Nachricht M oder der assoziierten Daten A. Es benötigt lediglich $|K|$ Verschlüsselungen für ein key recovery. Essentiell wichtig hierbei ist, dass das Tupel $(\mathcal{K}, \mathcal{M}, \mathcal{A}, \delta)$ injektiv zum Chiffretext $\mathcal{C}$ ist. Diese Bedingung schränkt die angreifbaren Schemen allerdings nicht sehr ein, denn auch auf Schemen mit öffentlich übertragenen IV trifft diese Bedingung zu.

3.3.3 Entdeckbarkeit

So lange die Subversion genügend Zufall verwendet, zum Beispiel mehr als sieben Bit, ist die Subversion unentdeckbar. Aber auch hier gilt: Ein Reset des Systems erhöht die Wahrscheinlichkeit sie zu entdecken.

4 Gegenmassnahmen

An dieser Stelle ist es wichtig Schemen zu finden, die resistent gegen ASAs sind. Aus den Angriffen, die ich zuvor vorgestellt habe können wir lernen, dass wir Schemen nutzen sollten, die deterministisch und stateful sind. Vor allem stateless Schemen haben sich als gefährdet erwiesen, da Angriffe bei diesen besonders schwer zu entdecken sind. Wichtig hierbei ist, dass eigentliche Sicherheitseigenschaften wie Vertraulichkeit und Authentizität keinen Einfluss auf die Resistenz gegen ASAs bieten. Diese Resistenz wird nur in einer Klasse von symmetrischen Schemen sichergestellt, einer Klasse die von den Autoren unique ciphertext schemes genannt wird.

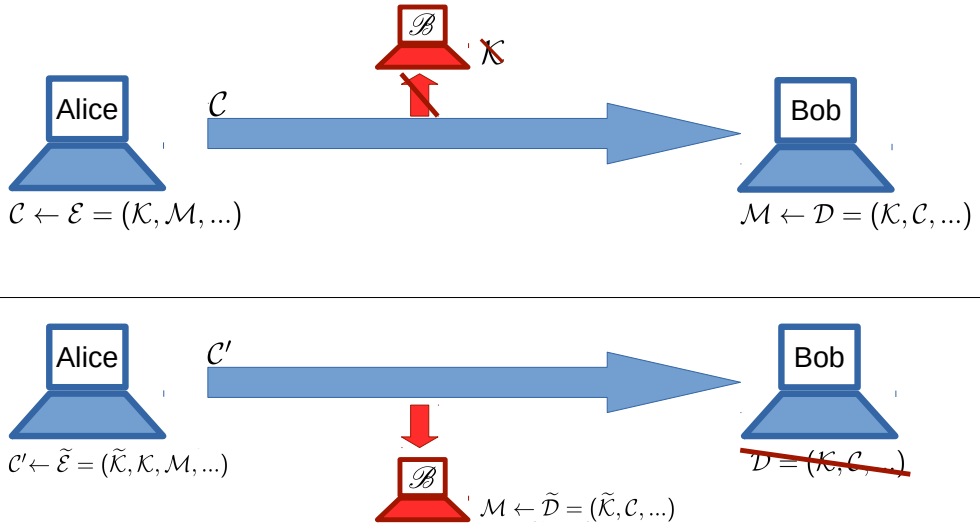

Abbildung 4.1: unique chiphertext scheme.

Um ein unique ciphertext Schema zu definieren, nehmen wir an, in dem symmetrischen Verschlüsselungsschema $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ soll folgendes gelten: Für jedes Tupel $(\mathcal{K}, \mathcal{M}, \mathcal{A}, \sigma)$ gibt es höchstens ein $\mathcal{C}$, das entschlüsselt die Nachricht $\mathcal{M}$ unter $\mathcal{K}$ ergibt. Also wenn diese Abbildung injektiv ist (siehe 4.2), dann ist Π ein unique ciphertext scheme.
Diese Eigenschaft trifft keineswegs auf alle Schemen zu. Für zwei verschiedene Chiffretexte $\mathcal{C} \neq \mathcal{C}'$ muss also immer $\mathcal{D}(\mathcal{C}) \neq \mathcal{D}(\mathcal{C}')$ gelten. Aus dieser Eigenschaft können wir Theorem 1 erstellen. Wie in Abbildung 4.1 zu sehen, sorgt eine Subversion von Π dafür, dass ein Chiffretext $\mathcal{C}' \neq \mathcal{C}$ beim Entschlüsseln bei Bob zu einer nicht korrekten Nachricht führt, also das Schema die Korrektheit aus Abschnitt 2.2 nicht erfüllt. In diesem Fall würde die Subversion

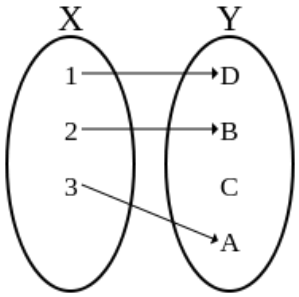

Abbildung 4.2: Injektivität.

entdeckt werden.

Theorem 1. *Sei* $\Pi = (K, E, D)$ *ein unique ciphertext scheme, dann gibt es kein Subversion* $\widetilde{\Pi} = (\widetilde{K}, \widetilde{E}, \widetilde{D})$ *von* Π*, mit der korrekt mit* $\mathcal{D}$ *entschlüsselt werden kann und* $\mathscr{B}$ *hat keine Erfolgschancen gegen* Π*.*

5 Zusammenfassung

ASAs sind nur ein Angriffsvektor gegen symmetrische Verschlüsselungen, doch liegen durchaus im Bereich des Möglichen. Wie in Kapitel 1 erwähnt, finden wahrscheinlich derartige Angriffe statt. Jederzeit könnten symmetrische Verschlüsselungen im Internet abgehört werden, ohne dass jemand etwas bemerkt. Schemen mit öffentlich übertragenen nonce sind generell gefährdet von ASAs, aber auch Schemen mit Zufallskomponenten, bei denen kein öffentlicher nonce übertragen wird sind durch die allgemeinere biased-ciphertext attack verwundbar. In dem Paper konnte gezeigt werden, dass die Klasse der unique ciphertext schemes eine sinnvolle Gegenmaßnahme gegen ASAs bilden. Einzig und allein das Scheitern beim Entschlüsseln enthüllt bei diesen Schemen Subversionen.
Wer Interesse an einen praktischen Ansatz hat, kann sich mit einem weiteren Paper der Stanford University beschäftigen ([EJG03]). The Design and Implementation of Protocol-Based Hidden Key Recovery behandelt unter anderem key recovery in SSL/TLS. Es wird gezeigt, wie key recovery in bestehende Protokolle wie SSL/TLS und SSH integriert wird ohne die Protokolle selbst zu verändern. Eine andere Arbeit von Mihir Bellare, Joseph Jaeger und Daniel Kane, Mass-surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks ([MB15]), beschäftigt sich weiterführend mit der biased ciphertext attack. Sie soll zeigen, dass ASAs noch viel mächtiger sein können als sie ohnehin schon sind. Als Einstieg in das Thema und einen kurzen Überblick bietet Kenneth G. Paterson in einer Präsentation auf der Crypto 2014 ([MB14b]). In knapp 20 Minuten gibt er eine Zusammenfassung des Originalwerks.

6 Literaturverzeichnis

[EJG03] Benny Pinkas und Philippe Golle Eu-Jin Goh, Dan Boneh. The design and implementation of protocol-based hidden key recovery. 2003.

[GG13] Ewen MacAskill Glenn Greenwald. Nsa prism program taps in to user data of apple, google and others. *The Guardian*, 06 2013.

[MB14a] Kenneth G. Paterson und Phillip Rogaway Mihir Bellare. Security of symmetric encryption against mass surveillance. 8616:1–19, 2014.

[MB14b] Phillip Rogaway Mihir Bellare, Kenneth G. Paterson. Security of symmetric encryption against mass surveillance. `https://www.youtube.com/watch?v=rg-Trmi17T8` und Crypto 2014, 10 2014.

[MB15] Daniel Kane Mihir Bellare, Joseph Jaeger. Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. 08 2015.

[Sch07] Bruce Schneier. Did nsa put a secret backdoor in new encryption standard? *WIRED Business*, 11 2007.

7 Abbildungsverzeichnis