UNIVERSITY OF APPLIED SCIENCES

Department of Computer Science

Seminar

IT Sicherheit

Remailer: Typ I bis III

Eingereicht am:

14. November 2015

Eingereicht von:

Mervyn McCreight

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Motivation

Bis zur Entwicklung der Typ-0 Remailer[1] lag der Fokus des allgemeinen Interesse darin, den Inhalt einer Nachricht, die über das Internet mit anderen Personen ausgetauscht wird, vor dem Einfluss dritter Personen zu schützen. Dies gelang durch Verschlüsselung des Nachrichteninhaltes mit Hilfe verschiedener gängiger Verschlüsselungsverfahren, die von Zeit zu Zeit immer effektiver wurden. Unter anderem ausgelöst durch die Einführung der Vorratsdatenspeicherung[2] entwickelte sich das Interesse auch den Absender und/oder Empfänger einer Nachricht vor Außenstehenden zu schützen, um einen Eingriff in die Privatsphäre zu verhindern. Zu diesem Zweck wurden sogenannte *Remailer* entwickelt. Das Ziel von Remailern ist es, Nachrichten und deren Austausch zu entpersonalisieren, sodass Anonymität für Absender und Empfänger erreicht wird.

Die folgenden Kapitel dieser Ausarbeitung werden einen Einblick in das Design der Remailertypen I bis III bieten. Außerdem wird beleuchtet, inwiefern diese verschiedenen Remailertypen nicht nur zeitlich, sondern auch designtechnisch aufeinander eingewirkt haben. Zusätzlich dessen, dass die Prinzipien, mit deren Hilfe die verschiedenen Remailerprotokolle Anonymität gewährleisten, erläutert werden, werden die unterschiedlichen Typen im Bezug auf der Sicherheit der Anonymisierung und ihrer Zuverlässigkeit analysiert.

1.2 Sitzungsmodell

Im Laufe dieser Ausarbeitung wird auf ein einheitliches Sitzungsmodell zurückgegriffen. Dieses Sitzungsmodell modelliert allgemein die Ziele und Eigenschaften, die für den Anwender eines Remailers und dessen Nachricht gelten. Weiterhin umfasst das Modell auch einen potentiellen Angreifer, für den definiert wird, über welches Wissen und Fähigkeiten er verfügt.

Das Sitzungsmodell besteht im wesentlichen aus drei verschiedenen Personen:

Alice möchte eine Nachricht versenden. Für außenstehende Personen soll nicht ersichtlich sein, an wen diese Nachricht gesendet wird.

Bob ist der Empfänger der Nachricht. Für außenstehende Personen soll nicht ersichtlich sein, von wem die Nachricht gesendet wurde.

Eve ist ein Angreifer. Sie möchte die Ziele von Bob und Alice gefährden, also die Anonymität von Alice und Bob aufheben.

[1] Nym-Remailer

[2] verpflichtet unter Anderem Internetprovider, den Datenverkehr ihrer Kunden zu protokollieren und über einen bestimmten Zeitraum zu speichern.

Eve stehen dabei eine Vielzahl von Fähigkeiten zur Verfügung. Genauer definiert kann Eve:

- das gesamte Netzwerk beobachten
- den vollständigen Traffic einsehen
- beliebige Pakete abfangen
- beliebige Pakete modifzieren
- beliebige Pakete versenden

Mit Hilfe dieser Fähigkeiten wird Eve versuchen die Anonymität von Bob und Alice zu kompromittieren. In diesem Fall gelingt es Eve einer Nachricht derer exakten Absender und Empfänger zuzuordnen. Der exakte Inhalt einer Nachricht ist für Eve in diesem Sitzungsmodell nicht zwingend interessant.

2

Typ-I Remailer

Ca. 1994 beschloss eine Interessensgruppe mit dem Namen "Cypherpunk[1]", das Prinzip eines Remailers aufzugreifen und zu verbessern und entwickelten das Cypherpunk-Remailer Protokoll. Dieses wird als Typ-I Remailer klassifiziert. Ziel der Entwicklung war es, die Unsicherheiten des Typ-0 Remailer zu beseitigen. Anders als bei dem Typ-0 Remailer, der ein pseudonymisierender Remailer ist, handelt es sich bei dem Typ-I Remailer um einen anonymisierenden Remailer. Das Ziel einer Anonymisierung ist das Verändern personenbezogener Daten in der Art, dass es unmöglich ist diese Daten einer Person zuzuordnen[2]. Die Anonymisierung bezieht sich in diesem Fall auf den Absender, sodass es das Ziel ist, jede Information über den Absender der Nachricht zu verstecken[3]. Folgerichtig bietet ein anonymisierender Remailer deutlich mehr Geheimnisschutz als ein pseudonymisierender Remailer.

2.1 Mix Netzwerke

Die technische Umsetzung des Cypherpunk-Remailers wurde sehr stark von der Idee der Mix Netzwerke von David Chaum beeinflusst. Ein Mix-Netzwerk ermöglicht anonyme Kommunikation innerhalb eines Netzwerkes. Ziel ist unter anderem, dass der Empfänger gegenüber dem Sender verborgen bleibt[4]. Ein Mix-Netzwerk besteht aus einer beliebig großen Menge an Mixen M. Ein Mix in einem Mix-Netzwerk ist üblicherweise ein Server, der von beliebigen Personen betrieben werden kann. Ein Mix fungiert in einem Mix-Netzwerk als Nachrichtenübermittler. Er versendet empfangene Nachrichten in der Form weiter, sodass sie nicht mehr auf angenommene Nachrichten zurückzuführen sind. Durch diese Eigenschaft wird Senderanonymität gewährleistet[5].

2.2 Nachrichtenaustausch

Einige Konzepte des Mix-Netzwerkes wurden aufgegriffen um den Typ-I Remailer zu entwickeln. Die wichtigsten Aspekte sind das Verschleiern des Nachrichtenweges durch das Senden über beliebige Knoten eines Netzwerks, sowie die schichtenweise Verschlüsselung einer Nachricht [6]. Zur Verschlüsselung der Nachrichten wird das PGP-Verfahren verwendet. Es handelt sich hierbei um ein asymmetrisches Verschlüsselungsverfahren, sodass ein Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel benötigt wird. Nachrichten, die über das Typ-I Remailer Protokoll versendet werden sollen, durchlaufen dementsprechend mehrere Remailer. Möchte Alice eine Nachricht N

[1] der Name entspringt dabei einem Wortspiel aus "Cipher"(engl. für Chiffre) und "Cyberpunk". Er verdeutlicht das Ziel der Gruppe, über Verschlüsselungstechniken Datenschutz in der elektronischen Datenverarbeitung zu erlangen.
[2] vgl. § 3 Abs. 6 BDSG
[3] vgl. S. 151 [HF13]
[4] In Mix Netzwerken bleibt zusätzlich noch der Empfänger dem Sender unbekannt. Diese Eigenschaft ist für die weitere Betrachtung dieser Ausarbeitung jedoch nicht wesentlich und wird dementsprechend nicht betrachtet.
[5] für vollständige Informationen über Mix-Netzwerke vgl. [Cha81]
[6] vgl. S. 84 [SS13]

an Bob übermitteln, sucht sie sich aus einer gegebenen Menge von Cypherpunk-Remailern eine endliche Teilmenge $C = (C_1, C_2, ..., C_n)$ an Remailern aus, über die die Nachricht Schritt für Schritt an Bob übertragen wird. Jeder Remailer verfügt für die PGP-Verschlüsselung über je einen öffentlichen Schlüssel E_C und einen privaten Schlüssel D_C. Im Folgenden wird eine Nachricht N, die mit einem öffentlichen Schlüssel E_x verschlüsselt wurde, als $E_x(N)$ bezeichnet. Für die selektierte Teilmenge an Remailern definiert Alice eine Routingreihenfolge $A = (A_1, A_2, ..., A_n, A_{Bob})$. Der letzte Eintrag A_{Bob} ist notwendig, da der letzte Remailer in der Kette die Nachricht letztendlich an Bob übermitteln muss. Alice verschlüsselt nun ihre Nachricht zusammen mit den entsprechenden Routing-Informationen nacheinander mit den öffentlichen Schlüsseln E_{C_x} der selektierten Remailer, in rückwärtiger Reihenfolge der Routingordnung, beginnend mit dem letzten Remailer C_n (schichtenweise Verschlüsselung):

$$N' = (A_1, E_{C_1}(A_2, E_{C_2}(...(A_n, E_{C_n}(A_{Bob}, E_{Bob}(N))) \tag{2.1}$$

Anschließend initialisiert sie das Versenden der Nachricht, indem sie N' an C_1 schickt.

Eine Nachricht, die einen Typ-I Remailer erreicht, enthält so, nach Entschlüsselung mit Hilfe des eigenen privaten Schlüssels D_C, folgende Informationen:

- eine Adresse A_i
- eine (verschlüsselte) Nachricht $E_j(...)$

Der Adressinformation A_i entnimmt der Remailer, an wen die Nachricht $E_j(...)$ weitergeleitet werden soll. Vor dem Weiterleiten der Nachricht modifiziert der Remailer den Header der Nachricht in der Art, dass unkenntlich gemacht wird von wem er diese Nachricht empfangen hat. Essentiell ist, dass ein Remailer durch die Adressinformation A nur den die Adresse des direkten Nachfolgers erhält. Außer Alice ist niemandem der vollständige Pfad des Nachrichtenverlaufs durch das Remailer-Netzwerk bekannt. Auf diese Weise wird verhindert, dass der Betreiber eines solchen Remailers in der Lage ist die Anonymisierung des Absenders zu kompromittieren. Dieses Verfahren wird fortgeführt, bis die Nachricht über den letzten Remailer C_n der Routingordnung den eigentlichen Empfänger Bob erreicht[7].

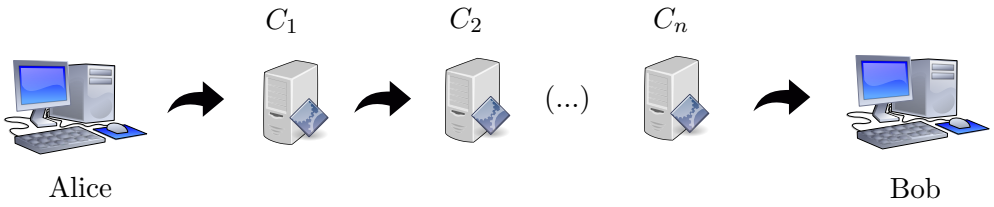

Abbildung 2.1: Exemplarische Nachrichtenübertragung mit Cypherpunk-Remailern

Als Absender ist Bob nun lediglich die Adresse des Remailers C_n bekannt. Der ursprüngliche Absender der Nachricht Alice bleibt verborgen. Auf diese Weise ist es Bob in diesem Protokoll allerdings nicht möglich, einem Absender einer Nachricht eine Antwort zu schicken.

[7] vgl. S. 72-77 [Kub07]

2.3 Analyse

2.3.1 Sicherheit

Auf den ersten Blick vielversprechend wirkend, sind die Cypherpunk-Remailer bei einer genaueren Betrachtung jedoch nicht sicher[8]. Geht man davon aus, dass es einem potentiellen Angreifer Eve möglich ist, den verursachten Traffic zu analysieren, ist es Eve möglich den Pfad einer Nachricht zu verfolgen (Traffic-Analyse). Dass dies möglich ist, hat im Wesentlichen zwei Gründe:

- Ein Remailer ändert die Größe einer Nachricht nur minimal.
- Ein Remailer leitet die Nachricht nach Empfang sofort weiter.

Das nur geringfügige Ändern der Nachrichtengröße (lediglich die Routing-Informationen entfallen), ermöglicht eine Zurordnung zwischen eingehenden und ausgehenden Nachrichten. Das sofortige Weiterleiten der Nachricht erleichtert diese Zuordnung ebenfalls. Diese Eigenschaften genügen Eve möglicherweise, den Verlauf einer Nachricht anhand des Sendezeitpunkts und der Größe zu verfolgen.

Ein weiterer Aspekt ist, dass ein Cypherpunk-Remailer nicht erkennt, ob eine Nachricht, die er empfängt, von ihm bereits empfangen und bearbeitet wurde. Das ermöglicht Replay-Angriffe, bei denen eine Eve eine Nachricht, die sie von Alice abgefangen hat, beliebig häufig in das Remailer-Netzwerk einspielt, um den Nachrichtenverlauf zu analysieren und so auf den Empfänger der Nachricht zu schließen.

2.3.2 Zuverlässigkeit

Der gewählte Aufbau des Cypherpunk-Remailer Protokolls führt außerdem dazu, dass eine ein Absender einer Nachricht nie weiß, ob der Empfänger die Nachricht tatsächlich empfangen hat. Ist einer der gewählten Remailer, über den die Nachricht weitergeleitet werden soll, defekt, oder nicht zu den anderen Remailern kompatibel, bricht die Übertragungskette an dieser Stelle und die Nachricht wird nicht zugestellt. Dadurch, dass zu dem Zeitpunkt der Kette weder Sender noch Empfänger bekannt sind, ist es nicht möglich das Fehlverhalten zu signalisieren.

[8] sicher insofern, dass die Anonymität eines Absenders gewährleistet wird.

3 Typ-II Remailer

3.1 Motivation

Das Mixmaster-Remailer Protokoll ist seit 1995 verfügbar. Die Motiviation und gleichzeitig das Ziel der Entwicklung der Typ-II Remailer war, die Schwächen der Typ-I-Remailer Generation zu beseitigen. Die wesentlichen Konzepte zur Umsetzung und Verbesserung wurden von Lance Cottrell in seiner Ausarbeitung "Mixmaster and remailer attacks" erarbeitet. In dieser legt er die Schwächen der Cypherpunk-Remailer offen und analysiert, wodurch diese entstehen, und stellt konkrete Vorschläge dar, wie die vorhandenen Sicherheitslücken möglicherweise zu umgehen sind. So erörtert er unter Anderem, dass und aus welchem Grund Cypherpunk-Remailer nicht zuverlässig verhindern, dass eine Verbindung zwischen eingehenden und ausgehenden Nachrichten an einem Knoten im Remailer-Netzwerk hergestellt werden kann[1]. Damit entwarf und implementierte Lance Cottrell das erste Design des Mixmaster Protokolls[2].

3.2 Funktionsweise

Das Mixmaster-Remailer Protokoll basiert, analog zum Cypherpunk-Remailer Protokoll, auf einem Netzwerk von Remailern, ähnlich einem Chaum'schen Mix-Netzwerk. Das Verfahren, nach dem eine Nachricht die verschiedenen Knoten des Netzwerks traversiert, bleibt größtenteils identisch. Auch hier wird ein asymmetrisches Verschlüsselungsverfahren verwendet, auf Basis dessen eine Nachricht entsprechend der öffentlichen Schlüssel der Remailer schichtenweise verschlüsselt wird. Hierbei muss der Pfad einer Nachricht im Netzwerk beim schichtenweisen Verschlüsseln der Nachricht bereits bekannt sein. Weiterhin manipuliert ein Remailer nach dem Empfangen und Entschlüsseln einer Nachricht den Nachrichtenheader, um den Absender der Nachricht unkenntlich zu machen. Auf diese Weise wird jede Art von absenderbezogenen Informationen entfernt und die Nachricht anonymisiert.

Bisher sind alle Schritte identisch dem Cypherpunk-Remailer Protokoll. Um die Schwächen der Typ-I Remailer zu entfernen, benötigte es der Einführung zusätzlicher Sicherheitsmaßnahmen, die im Folgenden erläutert werden.

Da die Aufbereitung einer Nachricht für das Mixmaster-Remailer Protokoll durch die zusätzlich eingeführten Sicherheitsmechanismen sehr komplex geworden ist, existiert Client-Software für das Mixmaster-Remailer Protokoll, die das Vorbereiten einer Nachricht für einen Anwender übernehmen. Da Mixmaster-Remailer nur noch Nachrichten akzeptieren, die genau dem spezifizierten Protokoll entsprechen, ist die Verwendung einer Client-Software notwendig. Möchte Alice nun eine Nachricht über Mixmaster-Remailer an Bob senden, muss sie anders als bei Cypherpunk-Remailern die Vorarbeit nicht manuell durchführen. Stattdessen verwendet sie die Client-Software.

[1] vgl. S. 276 [Ora01]
[2] vgl. [mix08] - zuletzt aufgerufen am 17.10.2015

3.2.1 Chunks

Im Mixmaster-Remailer Protokoll werden Nachrichten in gleichgroße Blöcke[3] aufgeteilt (beispielsweise 20 kB groß). Entstehen dabei ein oder mehrere Blöcke, die nicht die gewünschte Größe haben, werden diese mit zufällig generierten Daten aufgefüllt. Anstelle der vollständigen Nachricht werden nun die verschiedenen gleichgroßen Blöcke einer Nachricht über das Remailer-Netzwerk verteilt. Zusammengehörende Blöcke müssen hierbei nicht zwangsweise den selben Pfad durch das Netzwerk nehmen. Es ist sogar vorteilhaft, wenn die Blöcke möglichst über unterschiedliche Remailer in dem Netzwerk verteilt werden. Wichtig ist jedoch, dass der letzte Remailer, der die Nachricht schlussendlich an den ursprünglichen Empfänger überträgt, für alle Blöcke einer Nachricht identisch ist. Nur dieser letzte Remailer ist dazu in der Lage, die vollständige Nachricht wiederherzustellen, sofern er alle der Nachricht zugehörigen Blöcke empfangen hat. Anschließend leitet er die Nachricht an Empfänger weiter.

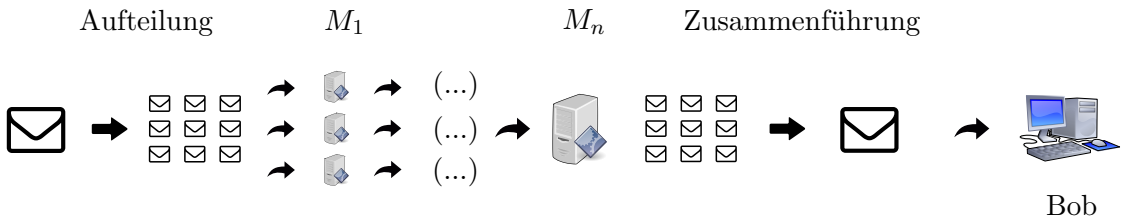

Abbildung 3.1: Exemplarische Nachrichtenübertragung mit Mixmaster-Remailern

Dieses gesamte Verfahren sorgt dafür, dass eine Nachricht nicht mehr anhand ihrer Größe durch das Remailer-Netzwerk verfolgt werden kann. Alle Nachrichten, die innerhalb des Remailer-Netzwerks übertragen werden, sind von gleicher Größe und für einen potentiellen Angreifer Eve identisch. Eine Zuordnung ist auf diese Art und Weise nicht mehr möglich.

3.2.2 Pool

Anders als bei den Cypherpunk-Remailern werden einkommende Nachrichten bei den Mixmaster-Remailern nicht sofort zum Zeitpunkt des Eintreffens weitergeleitet. Stattdessen speichert ein Mixmaster-Remailer seine einkommenden Nachrichten in einem Nachrichtenspeicher zwischen. Dieser Nachrichtenspeicher wird auch Nachrichtenpool genannt. In diesem werden einkommende Nachrichten gesammelt. Wichtig ist, dass die Reihenfolge der Nachrichtenspeicherung hierbei keinem festen Schema folgt. Einkommende Nachrichten werden in zufälliger Reihenfolge in dem Nachrichtenpool abgelegt. Für jeden Remailer ist ein Größenschwellwert für den Nachrichtenpool individuell konfigurierbar. Zu dem Zeitpunkt, an dem die Größe des Nachrichtenpools diesen Schwellwert übersteigt, werden in ihm befindlichen Nachrichten in zufälliger Reihenfolge an ihren entsprechenden Empfänger weitergeleitet.

(hier eventuell Grafik?)

Vorstellbar wäre nun, dass ein Remailer nie genügend Nachrichten empfängt um seinen Nachrichtenpool ausreichend zu füllen. Damit die bis dahin im Nachrichtenpool befindlichen Nachrichten nicht blockiert werden, wird nach Ablauf eines individuell festlegbaren Zeitintervalls, der Nachrichtenpool um zufällig generierte Pseudonachrichten erweitert, sodass der Größenschwellwert überschritten wird. Nun werden alle in ihm befindlichen Nachrichten, inklusive der Attrappen, weitergeleitet.

(hier eventuell Grafik?)

[3] auch "chunks"

Auf diese Weise ist es einem Angreifer Eve nicht mehr möglich eine Nachricht anhand der Zeit zu verfolgen. Eine Verbindung zwischen Empfangszeitpunkt und Absendezeitpunkt einer Nachricht an einem Remailer kann nicht hergestellt werden. Durch die gleichartigen Nachrichten[4] ist es einem Angreifer zusätzlich nicht möglich, überhaupt eine Verbindung zwischen einer einkommenden und einer ausgehenden Nachricht herzustellen.

3.2.3 Signatur

Weiterhin wurde bei dem Mixmaster-Remailer das Überprüfen der Integrität einer im Remailer-Netzwerk verschickten Nachricht als zusätzlicher Sicherheitsmechanismus eingeführt. Hierfür wird in einem verschlüsselten Header der Nachricht eine Signatur übertragen. Durch das Überprüfen der Signatur ist es einem empfangenen Remailer möglich zu überprüfen ob eine Nachricht entweder abgefangen und manipuliert, oder vollständig fremdeingeführt worden ist. Auf diese Weise ist es einem theoretischen Angreifer Eve nicht mehr möglich, manipulierte Nachrichten in das Remailernetzwerk einzuspielen um das Verhalten auf diese Nachrichten zu analysieren.

3.2.4 Identifikation

Zusätzlich zur Signatur enthält eine Nachricht in einem weiteren verschlüsselten Header noch eine eindeutige Identifikation, üblicherweise eine Nummer. Über diese ID ist es einem Remailer möglich eine Nachricht eindeutig zu erkennen. Dadurch ist er in der Lage zu erkennen, ob er die selbe Nachricht mehrfach empfängt. Hat ein Mixmaster-Remailer eine Nachricht bereits einmal empfangen und sie so weit behandelt, dass er sie in seinem Nachrichtenpool abgelegt, oder sogar weitergeleitet hat, wird er jede weitere Nachricht mit der selben Identifikation ignorieren. Durch das Einführen dieses Sicherheitsmechanismus hat Eve nicht mehr die Möglichkeit, die bei Cypherpunk-Remailern noch möglichen, Replay-Angriffe erfolgreich zu fahren. Fängt Eve eine Nachricht von Alice an einen Remailer ab, und versucht durch das mehrmalige Absenden der Nachricht an einen Remailer das Verhalten zu analysieren, schlägt dies fehl, da mehrfach gesendete Nachrichten ignoriert werden.

3.3 Sicherheitsanalyse

Das Mixmaster-Remailer Protokoll gilt bis zum heutigen Tage als praktisch sicher. Diese Sicherheit spiegelt sich auch in der aktuellen Benutzung von Remailern wieder. Mixmaster-Remailer sind das bis dato am meisten verwendetet Remailer-Protokoll.

Aus theoretischer Sicht sind aber auch Mixmaster-Remailer nicht in der Lage eine vollständige Anonymität zu garantieren. Eve ist es über eine Flooding-Attacke möglich, eine Nachricht vom Sender, durch das Remailer-Netzwerk bis zum Empfänger zu verfolgen. Dabei fängt Eve die Nachricht von Alice an den ersten Remailer-Netzwerkknoten ab und hält diese zurück. Anschließend überflutet[5] das Remailer-Netzwerk solange mit eigenen Nachrichten, bis die Nachrichtenspeicher der einzelnen Remailer aussschließlich mit Eves Nachrichten gefüllt sind. Nun ist jeder Nachrichtenverkehr im Remailer-Netzwerk auf Nachrichten von Eve zurückzuführen. Eve ist in der Lage jede dieser Nachrichten als ihre zu identifizieren, da sie den Empfänger ihrer eigenen Nachricht kennt. Ist dieser Status erreicht, versendet Eve die von Alice abgefangene und zurückgehaltene Nachricht. Da Eve alle anderen Nachrichten im Remailer-Netzwerk kennt, ist sie in der Lage die Nachricht von Alice über das gesamte Netzwerk bis zum Empfänger Bob zu verfolgen. Eve muss nur auf eine Nachricht

[4] gleichartig bezogen auf ihre Größe
[5] daher der Name "Flooding-Attacke"

warten, die nicht an den Empfänger ihrer Nachricht versendet wird. Der Empfänger dieser Nachricht muss der Empfänger der Nachricht von Alice, also Bob, sein.

Ein Angriff dieser Art ist in der Praxis nicht umsetzbar, da davon auszugehen ist, dass Mixmaster-Remailer zu jeder Zeit auch von fremden Personen verwendet werden. Zusätzlich müsste Eve die indivuellen Nachrichtenpuffergrößen aller Remailer kennen. Des weiteren müsste Eve mindestens alle Remailer des Nachrichtenpfades kennen. All diese Fakten zu erlangen ist für Eve in der Praxis kaum realisierbar. Dadurch ist es Eve zu keinem Zeitpunkt möglich den Status herzustellen, dass nur ihre Nachrichten in dem für Alice' Nachricht relevanten Teil des Remailer-Netwerks vorhanden sind.

4 Nym Server

4.1 Motivation

In den beiden vorherigen Kapiteln wurden die Typ-I und Typ-II Remailer vorgestellt. Bei beiden handelt es sich um anonymisierende Remailer. Die Konsequenz davon ist, dass die Identität des Senders zwar verborgen bleibt, es auf diesem Weg jedoch auch unmöglich ist einem Absender einer Nachricht zu antworten. Um diese Funktionalität anbieten zu können wurden Nym-Server entwickelt.

Ein Nym-Server ist ein Pseudonym-Server, der es seinen Benutzern erlaubt für sich auf ihm ein Pseudonym zu hinterlegen. Nun sind die Benutzer mit Pseudonym über den Nym-Server von anderen Personen über deren Pseudonym erreichbar, ohne dass andere Personen die reale Identität, die sich hinter dem Pseudonym verbirgt, erfahren.

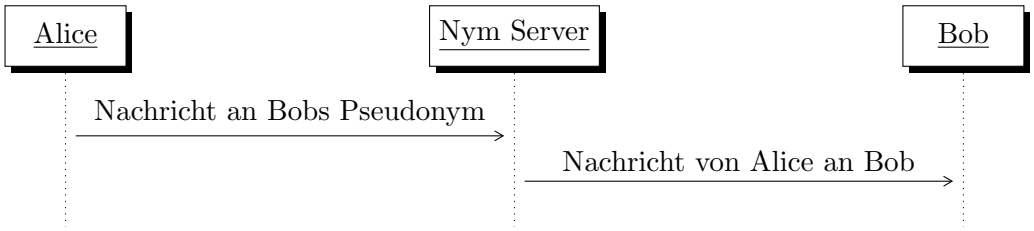

Abbildung 4.1: Senden einer Nachricht über einen Nym-Server (stark vereinfacht und prinzipiell)

Bei dem Typ-0-Remailer war es bereits möglich einem Absender einer Nachricht auf diese zu antworten. Grund dafür ist, dass der Typ-0-Remailer auch nur pseudonymisierend war. Er ersetzte die Absenderadresse durch ein Pseudonym und besaß eine Zuordnungstabelle zwischen Pseudonymen und tatsächlichen Identitäten. Dadurch war es einem Typ-0-Remailer möglich, Nachrichten die an ein Pseudonym gesendet wurden, an die tatsächliche Adresse weiterzuleiten. Der große Nachteil dieser Technik ist jedoch, dass einem Betreiber eines Typ-0-Remailers auf diese Weise eine Zuordnung zwischen verwendeten Pseudonymen und Identität vorliegt. Einerseits stellt diese Zuordnung eine starke Schwachstelle dar, da ein Angreifer möglicherweise dazu in der Lage ist diese Zuordnung ebenfalls zu erhalten, andererseits macht sich der Betreiber selbst angreifbar. So kann es dazu kommen, dass er z.B. durch den Staat dazu gezwungen wird die Identität eines Pseudonyms preis zu geben. Per Definition handelt es sich daher bei den Typ-0-Remailern nicht um Nym-Server[1].

4.2 Umsetzung mit Hilfe von Typ-I Remailern

Das Ziel von Nym-Servern ist es also, Pseudonymisierung zu gewährleisten. Dabei soll der Betreiber des Nym-Servers jedoch nicht über die tatsächlichen Identitäten, die hinter den Pseudonymen stehen, erfahren. Die Grundidee ist, dieses mit Hilfe des Typ-I-Remailer Protokolls zu erreichen.

[1] vgl. [nym]

Statt, wie bei den Typ-0-Remailern, eine tatsächliche Zuordnung zwischen Pseudonymen und Identitäten zu speichern, speichert ein Nym-Server Nyms. Ein Nym besteht hierbei aus folgenden Informationen[2]:

- einem öffentlichen Schlüssel
- einem Reply-Block
- einem Pseudonym

Der Reply-Block beinhaltet hierbei im Wesentlichen einen Pfad durch ein Typ-I Remailer-Netzwerk zum eigentlichen Empfänger, der sich hinter dem Nym verbirgt.

Möchte Bob ein Pseudonym bei einem solchen Nym-Server erstellen, muss er nun zuerst einen Reply-Block erzeugen. Anschließend schickt er diesen Reply-Block zusammen mit einem gewünschtem Pseudonym und einem öffentlichen Schlüssel gemeinsam an den Nym-Server. Der Nym-Server legt nun beim Empfang dieser Nachricht ein Nym mit den empfangenen Daten an[3]. Wichtig hierbei ist, dass Bob die Nachricht anonymisiert an den Nym-Server sendet, damit dem Nym-Server selbst zu keinem Zeitpunkt die wahre Identität von Bob bekannt ist. Nun ist Bob für Alice über den angegebenen Pseudonym für Alice erreichbar.

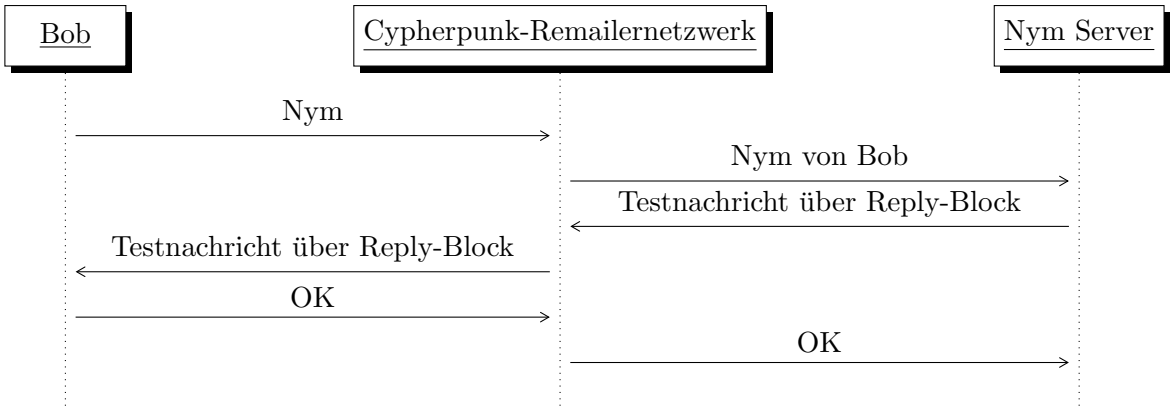

Abbildung 4.2: Registrierung eines Nyms

Zur Vereinfachung des Diagramms befindet sich der erste Remailer von Bobs Reply-Block in der obigen Abbildung im selben Remailernetzwerk, über das Bob seine Nymregistrierungsdaten anonymisiert an den Nym Server überträgt.

Möchte Alice Bob nun eine Nachricht zukommen lassen, schickt sie die Nachricht an Bobs Pseudonym auf dem entsprechenden Nym-Server. Empfängt der Nym-Server eine Nachricht, die an ein ihm bekanntes Pseudonym gerichtet ist, verschlüsselt er die Nachricht mit dem im Nym angegebenen öffentlichen Schlüssel und reicht sie zusammen mit dem hinterlegten Reply-Block an den ersten Remailer der im Reply-Block angegebenen Kette von Remailern weiter. Für die eigentliche Zustellung der Nachricht ist nun das Remailer-Netzwerk, in dem sich die Remailer im angegebenen Pfad befinden, zuständig. Die Nachricht wird nun entsprechend des Typ-I-Remailer Protokolls durch das Netzwerk und letztendlich an Bob übertragen[4]. Erhält Bob die Nachricht, ist er im letzten Schritt dazu in der Lage sie mit seinem privaten Schlüssel zu entschlüsseln und verfügt nun über die Nachricht.

[2] vgl. S. 25 [Loe09]
[3] vgl. S. 25 [Loe09]
[4] vgl. S. 26 [Loe09]

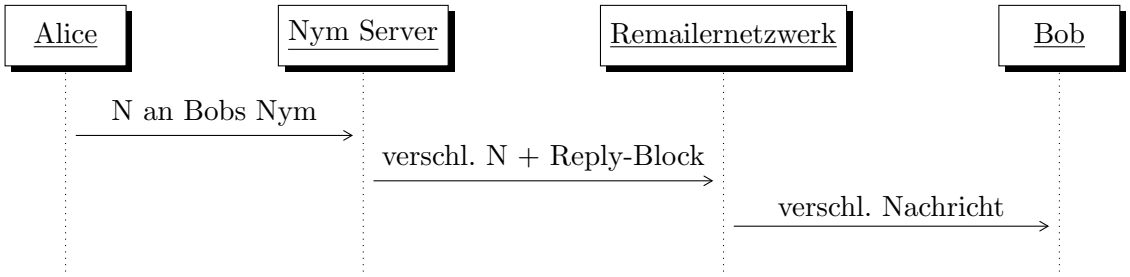

Abbildung 4.3: Weiterleitung einer Nachricht an ein Pseudonym

Da nur dem letzten Remailer der im Reply-Block angegebenen Kette die echte Adresse von Bob bekannt ist, und der schichtartig verschlüsselte Reply-Block nur im Verlauf der Übertragung im Typ-I-Remailer Protokoll entschlüsselt werden kann, nicht jedoch vom Nym-Server, hat der Nym-Server zu keinem Zeitpunkt die Möglichkeit die wahre Identität von Bob zu erfahren.

Die Schwächen dieses Verfahrens sind, da die Anonymität von Bob gegenüber dem Nym-Server betreiber, oder jedem Angreifer, der den Nym-Server beobachtet, nur vom Typ-I-Remailer Protokoll, mit Hilfe dessen die Nachricht tatsächlich an Bob übermittelt wird, abhängt, sind die sicherheitstechnischen Schwächen dieses Verfahrens identisch mit den Schwächen des Typ-I-Remailer Protokolls.

Eine Lösung über das Typ-II-Remailer Protokoll ist auf diese Art und Weise nicht möglich. Grund hierfür ist der im Mixmaster-Remailer verankerte Integritätscheck der zu übertragenden Nachrichten. Das Design des Mixmaster-Protokolls erfordert, zum Zeitpunkt der schichtenweisen Verschlüsselung, für die Angabe der Signatur, die Kenntnis der zu versendenden Nachricht. Im genannten Nym-Server Verfahren ist die Nachricht jedoch erst nach Erstellung des Reply-Blocks bekannt.

5 Typ-III Remailer

Die als Typ-II klassifizierten Mixmaster-Remailer gelten allgemein in der Praxis als sicher. Trotzdem wurde das Mixminion-Remailer Protokoll entworfen. Mixminion-Remailer stellen den Typ-III der Remailerklassifizierung dar. Die signifikanten Neuerungen, die mit dem Mixminion-Remailer Protokoll eingeführt wurden, waren:

- das Antworten auf anonyme Nachrichten
- verschlüsselte Kommunikation zwischen den Remailern (TLS statt SMTP)
- Einführung einer Verzeichnisserverstruktur

Das Möglichkeit auf eine empfangene anonyme Nachricht zu antworten ist der entscheidende Vorteil der Mixminion-Remailer. Kein anderes anonymisierendes Remailer Protokoll (Typ-I und Typ-II) unterstützt dieses Feature nativ.

Die Mixminion-Remailer sind, äquivalent zu den vorherigen Remailer Protokollen, eine Weiterentwicklung des vorherigen Protokolls. So bilden die Mixmaster-Remailer die technische Grundlage für die Entwicklung des Mixminion Protokolls. - Weiterentwicklung dient nicht primär der Sicherheit (Mixmaster gilt schon als sehr sicher), sondern der generell der Funktionalität

5.1 Funktionsweise

5.1.1 SURBs

Die Single-Use-Reply-Blocks[1] wurden eingeführt, um dem Empfänger das Antworten auf eine empfangene anonyme Nachricht zu ermöglichen. Dabei soll die Anonymität des Senders einer anonymen Nachricht jedoch erhalten bleiben.

Betrachtet man die Lage basierend auf den vorherigen Remailer-Protokollen, kann Bob eigentlich nicht auf eine über ein Remailer-Netzwerk versandte Nachricht von Alice antworten. Das liegt daran, dass ihm lediglich die Identität des letzten Remailers bekannt ist, er die Identität von Alice jedoch nicht kennt.

Um Bob ein Antworten zu ermöglichen, erstellt Alice einen Single-Use-Reply-Block und hängt diese an die Nachricht an. Der SURB befindet sich dabei in verschlüsselter Form im Header der Nachricht. Ein SURB enthält zwei wichtige Informationen:

- die E-Mail Adresse von Alice in verschlüsselter Form
- einen Pfad durch das Remailer-Netzwerk zu Alice

[1] kurz: SURBs

Wichtig ist, dass der SURB selbst für den Empfänger nicht entschlüsselbar ist. Bob ist weiterhin nicht in der Lage die Identität von Alice zu entschlüsseln. Dazu ist lediglich ein Mixminion-Remailer in der Lage. Bob kann jedoch den SURB dazu verwenden um Alice auf ihre anonyme Nachricht zu antworten. Hierfür hängt Bob seine Antwortnachricht an den SURB an und verschickt dieses Konstrukt an den ersten Remailer des im SURB vorhandenen Remailerpfades. Der letzte Remailer dieses Pfades ist nun dazu in der Lage die Adresse von Alice zu entschlüsseln um die Antwort letztendlich an Alice weiterzuleiten.

Bob kann dabei pro empfangenen SURB nur eine Nachricht an Alice schicken. Das liegt daran, dass ein SURB nur einfach verwendbar ist[2]. Möchte Bob Alice eine weitere Nachricht schicken, muss er auf eine weitere Nachricht von Alice, die einen SURB enthält, warten, um diesen SURB für eine erneute Antwort zu verwenden. Nach der einmaligen Verwendung eines SURBs werden alle weiteren Nachrichten, die mit Hilfe dieses SURBs versendet werden, wie Duplikate betrachtet und verworfen.

5.1.2 Nachrichten

Typisierung

Bisher existierten in den Remailer-Protkollen nur eine Art von Nachricht – eine anonyme Nachricht von Alice an Bob. Die Hinzunahme von Antwortnachrichten, die gesondert behandelt werden müssen, ist die Einführung einer Typisierung von Nachrichten für das Mixminion-Remailer Protokoll unerlässlich. Hierbei werden zwischen drei Arten von Nachrichten unterschieden[3]:

1. normale Nachrichten
2. direkte Antworten über SURBs
3. anonyme Antworten

Eine normale Nachricht entspricht hierbei einer anonymisierten Nachricht von Alice zu Bob, wie sie aus den bisherigen Protokollen bekannt ist. Bei einer direkten Antwort über einen SURB gibt Bob bei der Antwort seine Identität preis. Da er nicht weiß, ob er wirklich Alice antwortet, denkbar wäre auch, dass Alice die Adresse eines Dritten in dem SURB angegeben hat, ist es wünschenswert, dass Bob ebenfalls die Möglichkeit hat bei einer Antwort anonym zu bleiben[4]. Hierfür existiert die dritte Art einer Nachricht. Hierbei bleibt die Identität von Bob auch dem Empfänger der Antwort verborgen.

Ununterscheidbarkeit

Bereits in den vorherigen Kapiteln wurde darauf hingewiesen, dass es für die Gewährleistung der Sicherheit unerlässlich ist, dass der Datenverkehr innerhalb des Remailer-Netzwerks für einen potentiellen Angreifer Eve transparent sein muss. Eve darf nicht dazu in der Lage sein durch die Analyse des Datenverkehrs eine Verbindung zwischen einkommenden und ausgehenden Nachrichtenvekehr herstellen zu können.

Dieser Zustand muss auch nach der Einführung verschiedener Nachrichtentypen erhalten bleiben. Die Nachrichtentypen müssen daher nach außen hin ununterscheidbar bleiben. Das ist wichtig, damit es Eve nicht möglich ist, über die Unterscheidung der Nachrichtentypen Rückschlüsse bezüglich

[2] daher SINGLE-USE-Reply-Block
[3] vgl. S. 4 [DDM]
[4] das ist nur ein beispielhafter Grund. Logischerweise könnte Bob auch aus anderen Gründen anonym bleiben wollen

des Nachrichtenverkehrs zu ziehen. Diese Transparenz wird dadurch gewährleistet, dass alle drei Nachrichtenarten strukturell identisch aufgebaut sind. Sie verfügen über gleichgroße Header- und Bodygrößen[5].

Strukturen der unterschiedlichen Typen

Die Nachrichten die in einem Mixminion-Remailer Netzwerk verschickt werden, sind grundsätzlich ingesamt 32kB groß. Durch diese Gleichförmigkeit der Größe liefert eine Analyse des Traffic keinen Aufschluss darüber, welche Arten von Nachrichten gerade in dem Remailer-Netzwerk ausgetauscht werden.

Jede Nachricht im Mixminion-Protokoll besteht dabei grundlegend aus den Komponenten

- Header
  - primärer Header
  - sekundärer Header
- Body (Payload)

Signifikant ist, dass der Header sich in zwei Teile aufteilt – dem primären und dem sekundären Header. Dabei haben sowohl der primäre als auch der sekundäre Header jeweils eine Größe von 2kB und der Body eine Größe von 28kB. Der Body einer Nachricht enthält, unabhängig vom Typ der Nachricht, in jedem Fall die eigentlich zu übertragende Information; im letzten Schritt also die Nachricht des Senders an den Empfänger. Die Typisierung einer Nachricht wird durch den Inhalt des primären und sekundären Headers unterschieden.

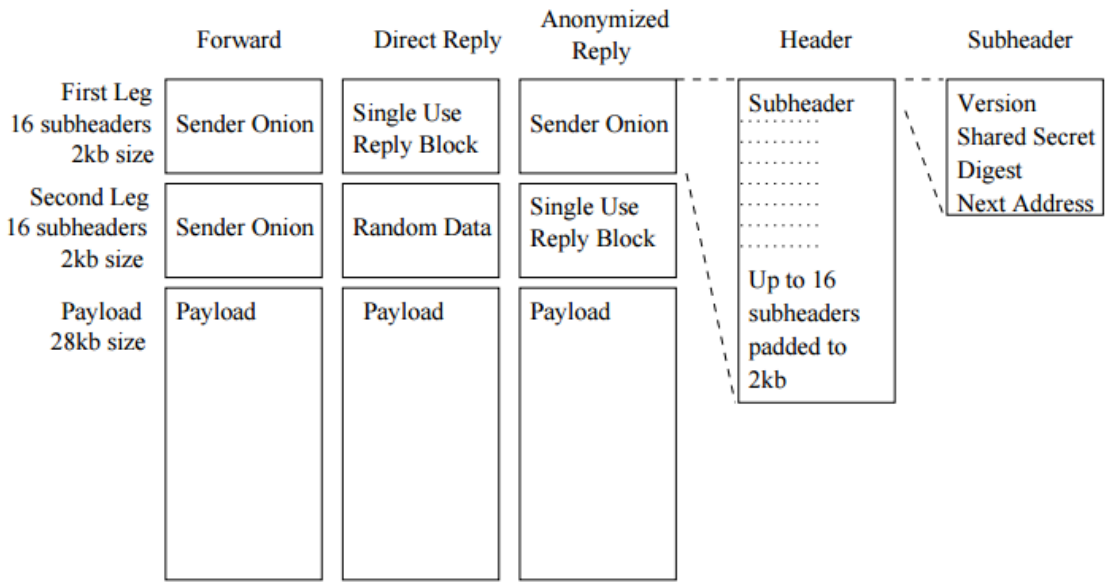

Abbildung 5.1: Die Struktur von Nachrichten im Mixminion-Protokol

Source: S. 4 [DDM]

Die obige Abbildung beschreibt den Inhalt des primären und des sekundären Header in den verschiedenen Nachrichtenfällen. Man sieht, dass sowohl der primäre als auch der sekundäre Header

[5] Body wird häufig auch Payload genannt.

im Falle einer normalen Nachricht, als auch der primäre Header im Falle einer anonymen Antwort, Pfadinformationen durch das Netzwerk beinhalten. Ein solcher Pfad ist selbst wieder in Subheader aufgeteilt. Jeder Subheader entspricht hierbei einem Datum für einen Remailer des Pfades. Ein solcher Subheader beinhaltet im wesentlichen drei Daten

- ein Master-Secret für die Erstellung eines symmetrischen Schlüssels für den Aufbau einer verschlüsselten Verbindung zum nächsten Remailer im Pfad
- eine Adresse des nächsten Remailers im Pfad
- eine Prüfsumme zum Überprüfen der Integrität des Rests des Headers

Der Pfad des primären und der Pfad des sekundären Headers ergeben, im Falle einer normalen Nachricht, zusammen den Gesamtpfad der Nachricht durch das Remailer-Netzwerk zum Empfänger. Dabei entspricht der Pfad im primären Header dem ersten Teil, der Teil im sekundären Header dem zweiten Teil des Pfades. Sowohl der primäre als auch der sekundäre Header können sich maximal aus 16 dieser Subheader zusammensetzen. Demzufolge ist die maximale Länge der Route einer normalen Nachricht im Mixminion-Protokoll 32.

Bei einer direkten Antwort von Bob ist der SURB im primären Header der, der von Alice zum Antworten übermittelt wurde. Da in diesem alle Informationen enthalten sind, die benötigt werden um die Nachricht bis Alice durchzustellen, befinden sich im sekundären Header in diesem Fall keine signifikanten Informationen. Um den gleichartigen Schein zu wahren, wird der sekundäre Header mit Platzhalterdaten gefüllt.

Bei einer anonymen Antwort befindet sich der SURB von Alice im sekundären Header. Im primären Header befindet sich ein von Bob spezifizierter Pfad durch das Netzwerk, der vor dem Pfad des SURBs durchlaufen wird. Dadurch bleibt die Identität von dem Antworter Bob dem Empfänger der Antwort verborgen[6].

5.1.3 Verzeichnisserver

Eine weitere Neuerung im Mixminion-Protkoll ist die Einführung von Verzeichnisservern. Ein Verzeichnisserver trägt für jeden Mixminion-Remailer im Netzwerk drei unmittelbar relevante Informationen[7]:

- Die Existenz eines Remailers
- Den aktuellen Schlüssel des Remailers
- Den aktuellen Status des Remailers

Alle drei Eigenschaften werden den Verzeichnisservern von den Remailern selbst mitgeteilt. Wichtig ist, dass es nicht nur einen Verzeichnisserver pro Netzwerk gibt. Pro Netzwerk gibt es mehrere Verzeichnisserver. Diese verschiedenen Verzeichnisserver müssen dauerhaft synchronisiert sein, sodass sichergestellt ist, dass sie die gleichen Daten bezüglich des Remailernetzwerks verteilen (Redundanz). Dadurch wird auch verhindert, dass nicht funktionstüchtige Remailer weiter von einem Benutzer in deren Nachrichtenpfad eingebaut werden. Dies würde dazu führen, dass eine Nachricht nie ihren Empfänger erreichen würde. Des weiteren haben die Verzeichnisserver die Aufgabe, sich dauerhaft gegenseitig zu verifizieren. Dadurch wird verhindert, dass ein Angreifer einen manipulierten Verzeichnisserver einspielt, um beispielsweise alle Daten nur über bestimmte Remailer laufen zu lassen[8]. Bei dieser Vorgehensweise wird davon ausgegangen, dass nicht alle

[6] vgl. S. 4 [DDM]
[7] vgl. S. 8 [DDM]
[8] vgl. S. 9 [DDM]

Verzeichnisserver manipuliert sind, da ansonsten die gegenseitige Verifikation und Synchronization hinfällig wäre.

5.2 Ablauf

Möchte Alice eine Nachricht an Bob senden, benötigt sie zunächst alle nötigen Informationen vom Verzeichnisserver. Von diesem erhält sie zu jedem Remailer im Netzwerk dessen Status und aktuellen Schlüssel. Die schichtweise Verschlüsselung der Nachricht geschieht äquivalent zum Mixmaster Protokoll. Zusätzlich wird der sekundäre Header mit der Prüfsumme des Nachrichtenbodies verschlüsselt. Anschließend sendet sie die Nachricht an den ersten Remailer im Pfad.

Empfängt nun ein Remailer eine Nachricht, wird zunächst die Integrität der Daten über die im Subheader angegebene Prüfsumme überprüft. Anschließend baut er mit Hilfe des ebenfalls im Subheader angegebenen Master-Secrets eine gesicherte Verbindung (TLS) zum nächsten Remailer im Pfad auf und überträgt die Nachricht an diesen, nachdem er sie entsprechend der schichtweisen Verschlüsselung für seinen Teil entschlüsselt hat. Danach wird die gesicherte Verbindung wieder aufgelöst.

Die Stelle, an der der gesamte Pfad des primären Headers durchlaufen ist, wird "CrossoverPunkt genannt. An diesem Punkt wird der sekundäre Header mit Hilfe der Prüfsumme des Nachrichtenbodies entschlüsselt und der primäre mit dem sekundären Header vertauscht[9]. Wurde eine Nachricht in der Zwischenzeit in irgendeiner Form manipuliert, ändert sich die Prüfsumme des Nachrichtenbodies und der sekundäre Header ist nicht wiederherstellbar. In diesem Fall wird die Nachricht an diesem Punkt verworfen[10]. Dadurch werden Attacken, die ein manipulieren der Nachricht benötigen, verhindert. Nachdem der sekundäre Header erfolgreich entschlüsselt und entsprechend vertauscht wurde, wird wie im vorherigen Ablauf weiter verfahren, bis die Nachricht letztendlich zu Bob weitergeleitet wird.

5.3 Sicherheitsanalyse

In der Theorie handelt es sich bei dem Mixminion-Protokoll um das sicherste der drei hier betrachteten Remailer-Protokolle. Beim Design wurden neuste Forschungsergebnisse und durch die älteren Remailer-Protokolle gesammelten Erfahrungen genutzt, um sich gegen bekannte typische Angriffe gegen Remailer zu schützen[11]. Ebenso wurden viele Mängel der früheren Remailer-Protkolle herausgearbeitet und beseitigt.

Das Mixminion Protokoll ist jedoch nie in einem vollständigen Zustand implementiert worden. Es ist seit je her nie über die Beta-Phase der Implementierung hinaus gekommen. So existieren unter Umständen noch Fehler in der Implementierung, die die Sicherheit des Systems gefährden. Außerdem laufen viele Mixminion-Remailer aufgrund ihrer unfertigen Implementierung noch mit Debug-Einstellungen, sodass Aktivitäten geloggt werden. Dieser Zustand gewährleistet keine Sicherheit, insofern wird das Protokoll in der Praxis nicht aktiv genutzt. Dadurch konnten bisher auch keine praktischen Erfahrungen bzgl. der Sicherheit dieses Remailer-Protokolls gesammelt werden.

[9] dieser Vorgang wird als swap operation bezeichnet. Vgl. S. 4-5 [DDM]
[10] vgl. S. 5 [DDM]
[11] vgl. S. 5ff [DDM]

6

Zusammenfassung

6.1 aktueller Stellenwert der einzelnen Typen

Literaturverzeichnis

[Cha81] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24:84–88, 1981. http://www.freehaven.net/anonbib/cache/chaum-mix.pdf.

[DDM] G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: Design of a type iii anonymous remailer protocol. http://www.mixminion.net/minion-design.pdf.

[HF13] P. Horster and D. Fox. *Datenschutz und Datensicherheit: Konzepte, Realisierungen, Rechtliche Aspekte, Anwendungen.* DuD-Fachbeiträge. Vieweg+Teubner Verlag, 2013.

[Kub07] J. Kubieziel. *Anonym im Netz: Techniken der digitalen Bewegungsfreiheit.* Open Source Press, 2007.

[Loe09] K. Loesing. *Privacy-enhancing Technologies for Private Services.* Schriften aus der Fakultät Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg. University of Bamberg Press, 2009.

[mix08] Mixmaster protocol manpage. http://mixmaster.sourceforge.net/manpage.html, 2008.

[nym] Nym-server definition. https://www.techopedia.com/definition/1696/nym-server.

[Ora01] A. Oram. *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* O'Reilly Media, 2001.

[SS13] J. Sambleben and S. Schumacher. *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* Books on Demand, 2013.