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

List of Listings

1 Grundlagen

1.1 Motivation

1.2 Zeitstrahl der Entwicklung

2 Typ-I Remailer

Ca. 1994 beschloss eine Interessensgruppe mit dem Namen "Cypherpunk", 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. [1] Die Anonymisierung bezieht sich in diesem Fall auf den Absender, sodass es das Ziel ist, jede Information über den Absender der Nachricht zu verstecken [2]. Folgerichtig bietet ein anonymisierender Remailer deutlich mehr Geheimnisschutz als ein pseudonymisierender Remailer.

2.1 Cypherpunk

2.2 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 [3]. 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.

2.3 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 [4]. Zur Verschlüsselung der Nachrichten wird das PGP-Verfahren verwendet. Es handelt sich hierbei um ein Public-Key Verfahren, sodass ein Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel benötigt wird. Nachrichten, die über das Typ-1 Remailer Protokoll versendet werden sollen, durchlaufen dementsprechend mehrere Remailer. Möchte Alice eine Nachricht N an Bob übermitteln, sucht sie sich aus

[1] vgl. § 3 Abs. 6 BDSG
[2] vgl. S. 151 [HF13]
[3] 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.
[4] vgl. S. 84 [SS13]

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-1 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 [5].

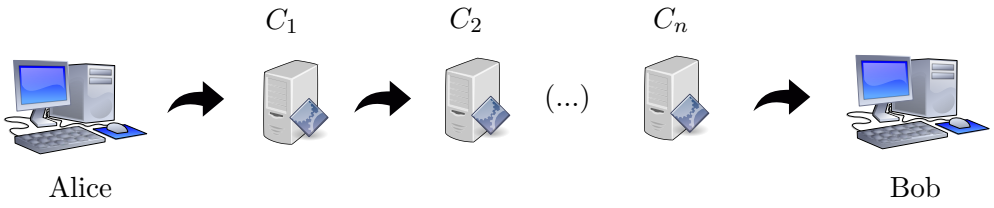

Abbildung 2.1: Exemplarische Nachrichtenübertragung mit Cypherpunk-Remailern

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.

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

2.4 Analyse

2.4.1 Sicherheit

Auf den ersten Blick vielversprechend wirkend, sind die Cypherpunk-Remailer bei einer genaueren Betrachtung jedoch nicht sicher[6]. 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.

2.4.2 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.

[6] 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

- benötigt anders als Cypherpunk-Protokoll einen Client.

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.

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,

[1] vgl. S. 276 [Ora01]
[2] vgl. [mix08] - zuletzt aufgerufen am 17.10.2015
[3] auch "chunks"

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.

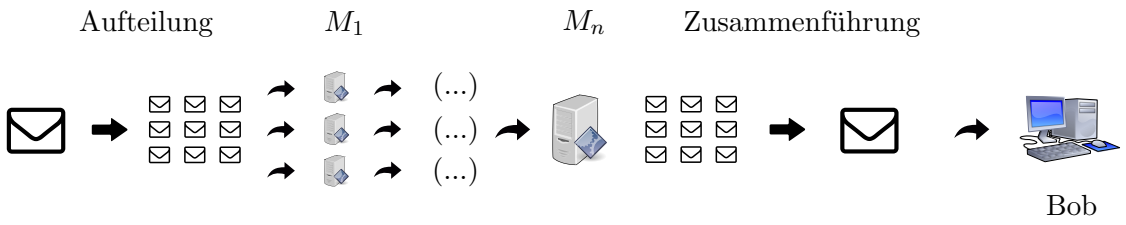

Abbildung 3.1: Exemplarische Nachrichtenübertragung mit Mixmaster-Remailern

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?)

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

[4] gleichartig bezogen auf ihre Größe

Angreifer zusätzlich nicht möglich, überhaupt eine Verbindung zwischen einer einkommenden und einer ausgehenden Nachricht herzustellen.

3.2.3 Signatur

- Integritätscheck von Nachrichten über Signatur. <- Verhindert das Einführen manipulierter Nachrichten. - Signatur enthält auch SSeriennummer"für Nachricht <- Verhindert mehrfach behandeln derselben Nachricht. Nachricht wird dann empfangen, aber ignoriert, also nicht in Pool gespeichert und weggeworfen.

3.3 Sicherheitsanalyse

- gilt als sicher - nur theoretischer Angriff denkbar Ein Angreifer hält die Nachricht, deren Empfänger er herausfinden möchte, zurück. Danach sendet er eigene Nachrichten an den Mixmaster. Dies macht er solange bis der Nachrichtenpool des Mixmasters mit seinen Nachrichten gefüllt ist. Danach schickt er die zurückgehaltene Nachricht los. Alle Nachrichten, die durch den Mixmaster gehen, werden entweder an den Angreifer oder aber an eine dritte Adresse gesendet. Die dritte Adresse ist die des Empfängers der zurückgehaltenen Nachricht.

4

Nym Server

4.1 Motivation

4.2 Umsetzung mit Hilfe von Typ-I Remailern

5 Typ-III Remailer

5.1 Motivation

5.2 SURBs

5.3 Nachrichten

5.3.1 Typisierung

5.3.2 Ununterscheidbarkeit

5.4 Verzeichnisserver

5.5 evtl. Nachrichtenaustausch

5.6 Sicherheitsanalyse

6

Zusammenfassung

6.1 aktueller Stellenwert der einzelnen Typen

Literaturverzeichnis

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

[Knu98] Donald E. Knuth. *The Art of Computer Programming, Volume 3: (2Nd Ed.) Sorting and Searching.* Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1998.

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

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

[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.