Universität Hamburg
Fachbereich Informatik

Ausarbeitung

C-Mix Verfahren in der IT-Sicherheit

vorgelegt von

Maik-Chiron Graaf & Merlin Koglin
Matrikelnummer 6807902 & ???????
Studiengang Informatik

eingereicht am 15. Juni 2016

Betreuer: Prof. Dr.-Ing. Hannes Federrath
Erstgutachter: Prof. Dr.-Ing. Hannes Federrath
Zweitgutachter: N.N.

Inhaltsverzeichnis

Zusammenfassung

Für den eiligen Leser sollen auf etwa einer halben, maximal einer Seite die wichtigsten Inhalte, Erkenntnisse, Neuerungen bzw. Ergebnisse der Arbeit beschrieben werden. Durch eine solche Zusammenfassung (im engl. auch Abstract genannt) am Anfang der Arbeit wird die Arbeit deutlich aufgewertet. Hier sollte vermittelt werden, warum der Leser die Arbeit lesen sollte.

Einleitung

In der heutigen Zeit sind Nachrichten, die über das Internet versendet werden nicht mehr weg zu denken. Zunehmend fragen sich die Benutzer ob ihre Anonymität bei Benutzung von Mails und Messengern gewährleistet wird. Deshalb gibt es in der IT-Sicherheit verfahren, die Mithilfe von Kryptographischen-Techniken versendete Nachrichten verschlüsseln. Das C-Mix Verfahren mit welchem wir uns in der vorliegenden Ausarbeitung auseinandersetzen werden ist ein solches Verfahren. Es wurde von David Chaum einem Pionier in der IT-Sicherheit konzipiert und ist eine Weiterentwicklung der von ihm ebenso konzipierten Chaumsche Mixe aus dem Jahr 1981. Da die Chaumsche Mixe bei heutiger Technik nicht mehr so effizient sind wurde das C-Mix Verfahren entwickelt.[2][3] Wir wollen uns in dieser Ausarbeitung näher damit beschäftigen ob das Problem mit dem C-Mix verfahren gelöst wurden ist und ob das Verfahren neue Probleme bereit hält.

Dafür benutzen wir die von uns ausgewählten Paper, die im Literaturverzeichnis gelistet sind als Quellen.

1 Übersicht Chaumsche Mixe

1.1 Funktionsprinzip

Die Chaumsche Mixe gewährleisten wie bereits erwähnt die Anonymität der Kommunikation in dem sie Sender und Empfänger voreinander anonym halten. Dies gelingt indem die zu verschickenden Nachrichten mehrere Stationen sogenannte Mixe durchlaufen. Sie sorgen dafür, dass die Nachrichten, sowohl Empfänger als auch Sender nicht zueinander in Beziehung gesetzt werden können. Damit dies gelingt haben die Mixe verschiedene Aufgaben. Zum einen muss ein Mix die Nachrichten mithilfe eines Verschlüsselungssystems verschlüsseln und ein anderer später wieder entschlüsseln. Durch diese Methode des Umkodieren ist es nicht mehr möglich eine Beziehung zwischen Eingangs und Ausgangsnachrichten zu finden. Ein anderer Mix muss die Nachrichten Sammeln und ein weiterer Umsortieren damit man nicht ausgehend von der Reihenfolge des Eintreffens und Weiterleitens der Nachrichten am Mix eine Beziehung zwischen Sender und Empfänger vorfinden kann. Mithilfe einer Rückadresse, die als Teil einer Nachricht gesendet wird und einem Mix, der diese Rückadresse zwischen speichert und umkodiert können sich zwei Nutzer nun gegenseitig Nachrichten senden und dabei anonym bleiben.[3][4]

1.2 Probleme

Die Chaumsche Mixe haben durchaus ihre Grenzen, innerhalb eines Echtzeitsystems ist das Sammeln der Nachrichten sehr ineffizient, da man durchaus lange warten muss um mehrere Nachrichten zusammen zu bekommen. Deshalb wird in solchen Echtzeitsystemen das Sammeln der Nachrichten weggelassen oder kurz gehalten. Das Umsortieren der Nachrichten kann deshalb nicht oder nur mit wenig Nachrichten erfolgen. Daraus resultiert, dass die Sicherheit sinkt und das ganze Verfahren in Echtzeitsystemen somit angreifbarer wird.[2][3][4]

2 Das cMix Verfahren

2.1 Idee

Die grundsätzliche Idee des cMix Verfahrens ist es, Schlüsselberechnungen in Echzeit zu vermeiden. Hierdurch entsteht auf der einen Seite eine Steigerung der Effizienz von Mix-Netzen, d.h. bessere Performance, also weniger Verzörerte Kommunikation. Auf der anderen Seite wird hierdurch der Energiebedarf verringert, was z.B. zu längerer Akkulaufzeit eines Smartphones führen kann. Um dies zu erreichen werden vor der Kommunikation Schüssel berechechnet (precomputation) und zwischen dem Sender und den Mix-Nodes ausgetauscht. Diese werden dann als Seed für einen Pseudozufallsgenerator verwendet, um weitere (gleiche) Schlüssel zu erzeugen.

2.2 Funktionsprinzip

2.3 Sicherheitsanalyse

Der Schluss

fasst die Ergebnisse noch einmal zusammen, bewertet die eigenen Ergebnisse kritisch und benennt die offenen Fragen. Es ist völlig normal, dass im Verlauf der Bearbeitung neue Problemstellungen und Forschungsfragen entstehen, die dann wieder der Ausgangspunkt für weitere Arbeiten sein können.

Thema: Das cMix-Verfahren von 2008

Bearbeiter: Maik Graaf, Merlin Koglin, Anne Litjens

Datum: 15. Juni 2016

Literaturliste

[1] Vinayak Kandiah, Dijiang Huang, Harsh Kapoor: C-Mix: A Lightweight Anonymous Routing Approach. Information Hiding (2008) 294–308.

[2] David Chaum, Farid Javani, Aniket Kate, Anna Krasnova, Joeri de Ruiter, Alan T. Sherman, Debajyoti Das: cMix: Anonymization by High-Performance Scalable Mixing. IACR Cryptology ePrint Archive Report 2016/008.

[3] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 4/2 (1981) 84–88.

[4] Krishna Sampigethaya, Radha Poovendran: A Survey on Mix Networks and Their Secure Applications. Proceedings of the IEEE 94/12 (2006) 2142–2181.

[5] Anja Jerichow, Jan Mueller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol. IEEE Journal on Selected Areas in Communications 16/4 (1998) 495–509.

[6] Michael G. Reed, Paul F. Syverson, David M. Goldschlag: Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications 16/4 (1998) 482–494.

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen – benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht. Ich versichere weiterhin, dass ich die Arbeit vorher nicht in einem anderen Prüfungsverfahren eingereicht habe und die eingereichte schriftliche Fassung der auf dem elektronischen Speichermedium entspricht.

Ggf. streichen: Ich bin damit einverstanden, dass meine Abschlussarbeit in den Bestand der Fachbereichsbibliothek eingestellt wird.

Hamburg, den 15. Juni 2016

_____