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

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros,

malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

1.1 Motivation

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui

cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

[Knu98]

1.2 Zeitstrahl der Entwicklung

2 Typ-I Remailer

Ca. 1994 beschloss eine Interessensgruppe mit dem Namen "Cypherpunk", die Entwicklung der Remailer voranzutreiben und entwickelten den Cypherpunk-Remailer. Dieser 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 es, dass der Empfänger gegenüber dem Sender verborgen bleibt. 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 Verschlüselung einer Nachricht. So werden Nachrichten über mehrere Typ-I Remailer verschickt. Möchte Alice eine Nachricht N an Bob übermitteln, sucht sie sich aus einer gegebenen Menge von Cypherpunk-Remailern eine endliche Teilmenge C = (C1, C2, ..., Cn) an Remailern aus, über die die Nachricht Schritt für Schritt an Bob übertragen wird. Für diese Teilmenge definiert Alice eine Routingreihenfolge. Jeder Remailer verfügt über je einen öffentlichen Schlüssel Ec und einen privaten Schlüssel Dc. Alice verschlüsselt nun ihre Nachricht zusammen mit den entsprechenden Routing-Informationen nacheinander mit den öffentlichen

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

Schlüsseln Ec der selektierten Remailer, in rückwärtiger Reihenfolge der Routingordnung, beginnend mit dem letzten Remailer Cn (schichtenweise Verschlüsselung).

(hier formelhafte oder bildhafte Erklärung der verzwiebelten Verschlüsselungsschichten. Lieber Formel als Bild).

Anschließen initialisiert sie das Versenden der Nachricht, indem sie N' an C1 schickt.

Eine Nachricht, die einen Typ-1 Remailer erreicht, enthält, nach Entschlüsselung mit Hilfe des eigenen privaten Schlüssels Dc, folgende Informationen:

- eine Routing-Information R
- eine Nachricht M

Der Routing-Information R entnimmt der Remailer, an wen die Nachricht M weitergeleitet werden soll. Dieses Verfahren wird fortgeführt, bis die Nachricht über den letzten Remailer Cn der Routingordnung Bob erreicht.

(hier eine Grafik einfügen, die den Senderverlauf der Nachrichten illustriert).

Als Absender ist Bob nun lediglich die Adresse des Remailers Cn bekannt. Der echte Absender Alice bleibt verborgen.

2.4 Sicherheitsanalyse

3

Typ-II Remailer

3.1 Motivation

3.2 Funktionsweise

3.3 Sicherheitsanalyse

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.