CryptoOne-System : Sicherheit im Computernetze

Fabrice Dufils Siyapdje

Bachelor of Sciences Informationstechnick

Betreuer:

H. Pr. Dr Martin Damm

University College London, UK

January 2015

Chapter 1

Erklärung

"Hiermit erkläre ich, dass ich die vorliegende
Arbeit selbstständig verfasst und keine anderen als
die angegeben Quellen und Hilfsmittel benutzt habe."

Abstract

Table of Contents

Chapter 2

Einführung

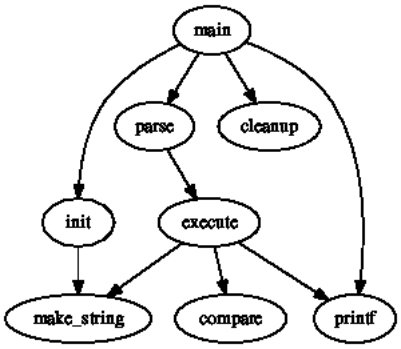
2.1 Gliederung

Diese Arbeit lässt sich in drei große Abschnitte aufteilen: Kapitel 2 behandelt die Anförderungen eines sicheren Dokumentaustausch die für das Verständnis der weiteren Kapitel wichtig sind. Im folgenden Kapitel 3 werden beispielhaft die aktuelle Stand der Technick vorgestellt und ihre technische Umsetzung aufgeführt. In Kapitel 4 wird anhand der Problemstellung ein Konzept für die Dokumentaustauschplattform erstellt, welches in den Kapiteln 5 und 6 konkretisiert und implementiert wird. Die letzten beiden Kapitel 7 und 8 fassen die Ergebnisse dieser Arbeit zusammen und machen Vorschläge für eine Verbesserung des Systems.

2.2 Motivationen

Der Austausch von vertraulichen Informationen im Netz ist grundsätzlich problematisch. Wie können Informationen zwischen Parteien augetauscht werden, ohne dass Unberechtigte diese mitlessen können.

Der Austausch von vertraulichen Informationen mittels schriftlicher Aufzeichnungen ist grundsätzlich problematisch. Wie sollten Informationen zwischen Parteien ausgetauscht werden, ohne dass Unberechtigte diese mitlesen können. Die Lösung des Problems besteht darin, die Nachricht verschlüsselt zu übertragen. D. h. die ur- sprüngliche Nachricht wird so verändert, dass es Unberechtigten deutlich erschwert wird, den Inhalt einer abgefangenen Nachricht zu erfassen. Bereits in der Antike wurden vertrauliche Informationen verschlüsselt übermittelt. Schon damals bestan- den schon folgende Probleme, die noch heute - trotz aufwendigerer Verschlüsselung – relevant sind. • (1) Wer kann Nachrichten ver- bzw. entschlüsseln und wie? • (2) Wie werden die Schlüssel zwischen Sender und Empfänger ausgetauscht? Die Notwendigkeit eines sicheren Dokumentenaustauschs hat sich in den letzten Jahren als immer drängender erwiesen, da zum einen ein Austausch via Internet sehr schnell und einfach möglich ist. Zum anderen ist spätestens durch die NSA-Affäre deutlich geworden, dass eine Datenübertragung via Internet nicht für vertrauliche Informationen ohne weitere Maßnahmen geeignet ist.



e

2.3 Stand der Technick

2.3.1 Email (SMTS)

2.3.2 FTP Server

2.3.3 Web EDI

2.3.3.1 AS2

Chapter 3

Anforderungen

3.1 Funktionale Anforderungen

Die folgenden funktionalen Anforderungen müssen durch das System erfüllt wer- den.

- Der Administrator muss in der Lage sein, neue Benutzer im System hinzuzu- fügen und zu entfernen.
- Der Benutzer kann eine Vertrauensbeziehung zu anderen Benutzern erstellen und sie wieder zerstören.
- Der Benutzer kann eine Gruppe erstellen und entfernen.
- Der Benutzer kann vertraute Benutzer in einer Gruppe hinzufügen und ent- fernen
- Der Benutzer kann den Zugriff auf seine Dateischlüssel an alle Mitglieder einer Gruppe freigeben und diese Freigabe auch wieder zurückziehen. Die funktionalen Anforderungen sind in der Abbildung

2.1 zusammengefasst.

3.2 Nicht funktionale Anforderungen

- Das System oder Konzept muss die Integrität eines Benutzers oder seines öffentlichen Schlüssels gewährleisten und den Mechanismus definieren, mit dem sie geprüft werden.
- Das System muss die Sicherheit sensible Daten (Benutzerpasswörter) ge- währleisten. Die Passwörter dürfen nicht in Klartext gespeichert werden.
- Der Dateienschlüsselaustausch zwischen den Mitgliedern einer Gruppe muss sicher sein, damit keine weiteren Akteure darauf zugreifen können.
- Das System muss über ein robustes Authentifizierungsverfahren verfügen.
- Das Authentifizierungsverfahren muss widerstandsfähig sein gegen gewöhn- liche Angriffe, wie Replay Attacks, Offline- und Online-Dictionary-Attacks, etc.
- Das Konzept sollte den Mechanismus so definieren, dass Dateien zurückzu- gewonnen werden, nachdem das System unsicher geworden ist.
- Das System muss es ermöglichen, dass zwei Benutzer mit unterschiedlichen IT-Infrastrukturen Dateien untereinander austauschen können.
- Eine SSL-Verbindung mit SSL-Zertifikat ist für die Erstellung dieses Kon- zepts nicht zugelassen.

- Das System muss portierbar sein. Es darf keine Installation auf dem lokalen Rechner des Benutzers benötigen. Auf diesem Rechner dürfen auch keine Daten(Dateien oder Schlüssel) gespeichert werden.

References