CTMS Dokumentation

Haixin Cai, Jannik Vieten, Pascal Weisenburger
Wintersemester 2013 / 2014

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Theoretische Informatik
Kryptographie und Computeralgebra

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Zusammenfassung

Dieses Dokument stellt die Dokumentation zum *CA Trust Management System (CTMS)* dar und gibt Hinweise zur Benutzung sowie zur Architektur der entwickelten Komponenten. Dabei handelt es sich um eine Java-Anwendung die das Trust-Management übernimmt und eine Firefox-Extension, die die CTMS-Funktionalität im Browser benutzbar macht. Die hier vorgestellte Implementierung entstand im Rahmen eines Praktikums bei der CDC-Gruppe des Fachbereichs Informatik an der TU Darmstadt. Programmiert wurde das System von Haixin Cai, Jannik Vieten und Pascal Weisenburger, die Betreuung fand statt durch Johannes Braun und Moritz Horsch.

Inhaltsverzeichnis

1 Einleitung

Die heute im Internet eingesetzte *Public-Key-Infrastruktur (Web-PKI)*, die auf der Integrität von *Certificate Authorities (CAs)* basiert, gerät zunehmend in die Kritik, nicht ausreichend sicher und vertrauenswürdig zu sein. So kann jede CA ein Zertifikat für jede beliebige Domain ausstellen, was Angesichts der Einflussnahme von staatlichen Behörden auf einzelne CAs die Gefahr für Man-in-the-Middle-Angriffe real werden lässt.
In [1] stellen Braun et al. ein alternatives Trust-Modell vor, welches dieses Problem adressiert und der Vertrauensentscheidung einen benutzerspezifischen, individuellen *Trust View* zu Grunde legt, der sich den Bedürfnissen des Benutzers anpasst.
Dieses *CA Trust Management System (CTMS)* wurde nun implementiert und besteht im Wesentlichen aus zwei Komponenten. Die erste ist eine Java-Anwendung, die das Trust-Management übernimmt, die nötige Funktionalität für das Bewerten von Zertifikaten bereitstellt und sich vom Benutzer konfigurieren lässt. Die andere Komponente wird von einer Firefox-Extension gebildet, die auf die Trust-Berechnung der Java-Anwendung zurückgreifen kann, um während dem Surfen im Internet die Nutzung des CTMS möglich zu machen.

2 CTMS-Anwendung

TODO: Hier Inhalt einfügen!

3 Firefox-Extension

3.1 Überblick

Standardmäßig akzeptiert Firefox alle gültigen Zertifikate, die von beliebigen, im Browser registrierten CAs ausgestellt wurden. Das sind inzwischen sehr viele und diese Tatsache liegt dem Vertrauens-Problem der derzeitigen Web-PKI zu Grunde. Um das alternative Vertrauenskonzept der Trust Views zu benutzen, integriert sich die Firefox-Extension in den Browser und delegiert die Trust-Berechnung an die CTMS-Anwendung, um anschließend angemessen auf das Ergebnis zu reagieren und den Benutzer ggf. zu warnen.

3.2 Benutzung

Bei der Installation der Extension wird ein zusätzlicher Button in die Toolbar des Browsers integriert. Über diesen Button wird ein Menü bereitgestellt, in dem Einstellungen vorgenommen werden können. Dort lässt sich das Sicherheitslevel auf eine der drei Stufen „hoch“, „mittel“ oder „niedrig“ einstellen, was das Sicherheitsbedürfnis des Benutzers für die Webseiten widerspiegeln soll, die als nächstes besucht werden. Für Online-Banking oder e-Commerce dürfte beispielsweise ein höheres Level erforderlich sein, als für das Lesen einer Nachrichtenseite. Das ausgewählte Sicherheitslevel geht dann als Parameter in die Vertrauensberechnung der CTMS-Anwendung ein. Außerdem lässt sich über das Menü das Konfigurationsfenster der Extension aufrufen, in dem die Verbindungsinformationen (Host und Port) zur CTMS-Anwendung geändert werden können, mit der die Extension über HTTP kommuniziert.
Wird eine mit TLS geschützte Seite aufgerufen, nimmt die Extension Kontakt mit der CTMS-Anwendung auf und erwartet von ihr das Urteil, ob die Seite bzw. das ausgelieferte Zertifikat vertrauenswürdig ist. Ist das nicht der Fall, wird der Benutzer auf eine Warnseite umgeleitet, die den Sachverhalt erklärt, dem Benutzer aber gleichzeitig die Möglichkeit gibt es mit geändertem Sicherheitslevel erneut zu versuchen, oder die Website in jedem Fall zu besuchen. Bei letzterer Möglichkeit wird die betroffene Website für die Dauer der Browsersitzung von weiteren Trust-Überprüfungen ausgenommen.
Ist die CTMS-Anwendung nicht erreichbar, wird ebenfalls eine Warnseite angezeigt, die den Benutzer dazu auffordert die CTMS-Anwendung zu starten oder die Extension zu deaktivieren.

3.3 Architektur

TODO: schreiben

Literatur

[1] Johannes Braun, Florian Volk, Johannes Buchmann, and Max Mühlhäuser. Trust views for the web pki. 2013.