Knowledge-Based Data Access In Facebook

Präsentation der Bachelorarbeit

Agenda

- Motivation
- Theoretische Grundlagen
- Entwicklung
- Demo
- Evaluation
- Weiterentwicklung

Motivation

- Nutzer werden zu gläserne Menschen gegenüber ihren Facebook Freunden
- Facebook nutzt manuell angelegte Listen für die Privatsphäre
- Zwei neue Szenarien sollen ermöglicht werden:
  - Zugriff auf Informationen für Personen die den User gut kennen
  - Gute Freunde erhalten Zugriff auf Informationen ohne das eine Facebook Freundschaft besteht
- Aufgabe: Erstellen einer Firefox Erweiterung, welches beide Szenarien erfüllt

- Was sind „gute“ Freunde?

- Mozilla Firefox Erweiterungen folgen dem MVC Ansatz
  - XUL (XML User Interface Language)
  - JavaScript
  - SQLite

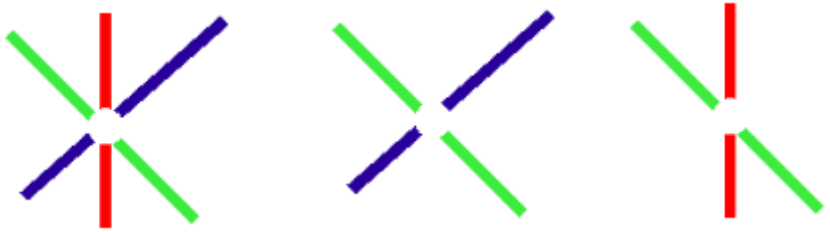
```
<?xml version="1.0"?>
<?xml-stylesheet href="chrome://KDAF/skin/skin.css" type="text/css"?>
<!DOCTYPE overlay SYSTEM "chrome://KDAF/locale/translations.dtd">
<overlay
        id="KDAF"
        xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">

         <stringbundleset id="stringbundleset">
             <stringbundle id="string-bundle" src="chrome://KDAF/locale/string.properties"/>
        </stringbundleset>

        <script src="chrome://KDAF/content/sjcl.js"/>
        <script src="chrome://KDAF/content/NoteHandler.js" />

        <statusbar id="status-bar">

        <statusbarpanel id="facebook-extension-bar-icon"
                        context="facebook-menu"
                        class="statusbarpanel-iconic"
                        src="chrome://KDAF/skin/status-bar.png"
                        tooltiptext="Starte KDAF"  />

            <menupopup id="facebook-menu" type="menu" position="before_end">

                <menuitem id="decryptMenu" label="&KDAF.statusbar.DecryptTitle;" oncommand="NoteHandler.startDecryptionDialog()" disabled="true" />

                <menuitem id="encryptMenu" label="&KDAF.statusbar.EncryptTitle;" oncommand="NoteHandler.startNewNoteDialog()"/>

                <menuitem id="keyManMenu" label="&KDAF.statusbar.keyManTitle;" oncommand="NoteHandler.startKeyManagerDialog()" />

                <menuseparator/>

                <menuitem label="&KDAF.statusbar.OptionTitle;"  oncommand="NoteHandler.startPreferencesDialog()"/>
                <menuseparator/>
            </menupopup>
        </statusbar>
</overlay>

```

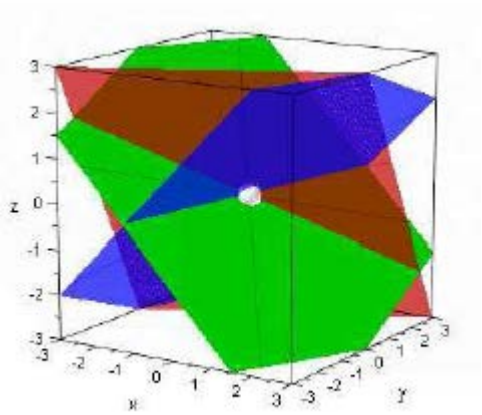
Theoretische Grundlagen – Facebook

- Facebook stellt für Entwickler den s.g. „social graph“ bereit
- Unterschiedliche HTTP Schnittstellen ermöglichen den Zugriff auf diesen Graph
- Bestimmte Abfragen benötigen die Erlaubnis der User
- SDKs vereinfachen den Zugriff auf den social graph
  - Sicherheitsprobleme innerhalb von Firefox Erweiterungen
  - SDK unabhängige Authentifizierung musste implementiert werden

Theoretische Grundlagen – Secret Sharing

- Secret Sharing löst das Problem, Schlüssel in einer Gruppe zu verteilen
  - (*n*,*n*) vs. (*n*,*k*)-Verfahren
- Nutzung der Geometrie, wobei der Schnittpunkt das Geheimnis ist
- Shamir‘s Secret Sharing veröffentlichte ein Verfahren, welches ein Polynom vom Grad (*k-1*) und die Lagrange-Interpolation nutzt





Theoretische Grundlagen – Secret Sharing

- Gegeben sind das Geheimnis *D*, die Obergrenze *n* und die Untergrenze *k*, eine Primzahl *p* mit $p > k$ und $p > n$
- Das Polynom $f(x)$ wird erstellt:

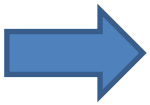
$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \in Z_p$$

  - $a_0 = D$
  - $a_1, \cdots, a_{k-1}$ sind zufällig gewählt Koeffizienten
- Jeder Beteiligter erhält ein Tupel $(x_i, s_i = f(x_i))$
- Zur Berechnung von *D* wird die Lagrange-Interpolation genutzt:

$$D = f(0) = \sum s_i \cdot \prod_{\substack{j=1, \\ j \neq i}} \frac{-x_j}{x_i - x_j}$$

Entwicklung - Konzept

- User sollen durch existierendes Wissen, neue Informationen erhalten
  - Wissen im Bereich von sozialen Netzwerken meint, Wissen über eine bestimmte Person
- Unterscheidung von Freunden und guten Freunden
  - besitzen mehr Informationen und auch spezielleres Wissen



Nutzer müssen eine gewisse Anzahl von Informationen über die Person kennen, um an neue Informationen zu gelangen.

Entwicklung - Design

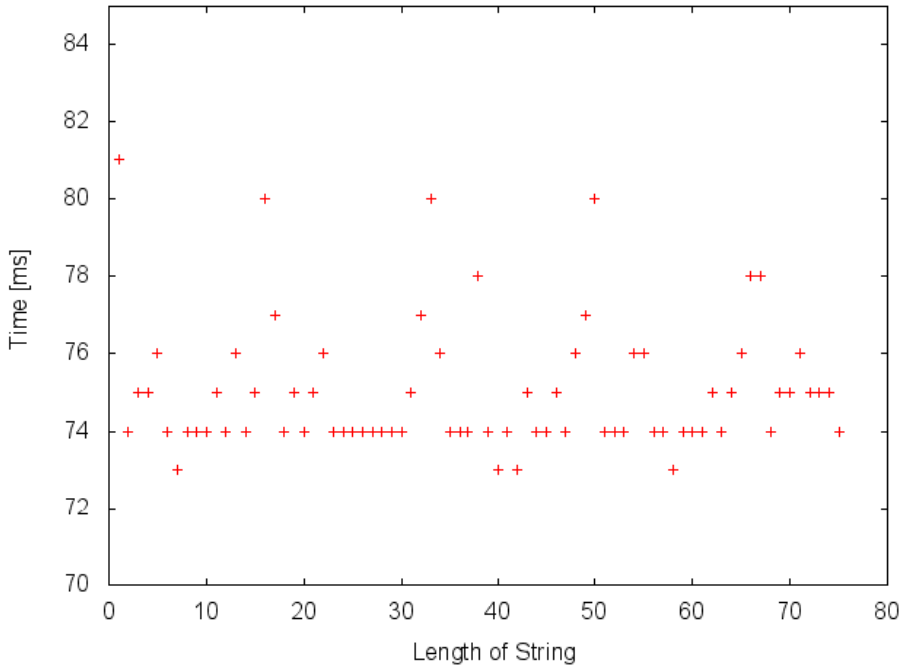
- Kryptographie
  - Symmetrischer Algorithmus: AES-256
  - Hashfunktion: SHA-2
- Datenaustausch
  - Daten werden im JavaScript Object Notation (JSON) übertragen
  - Wohldefiniertes Format

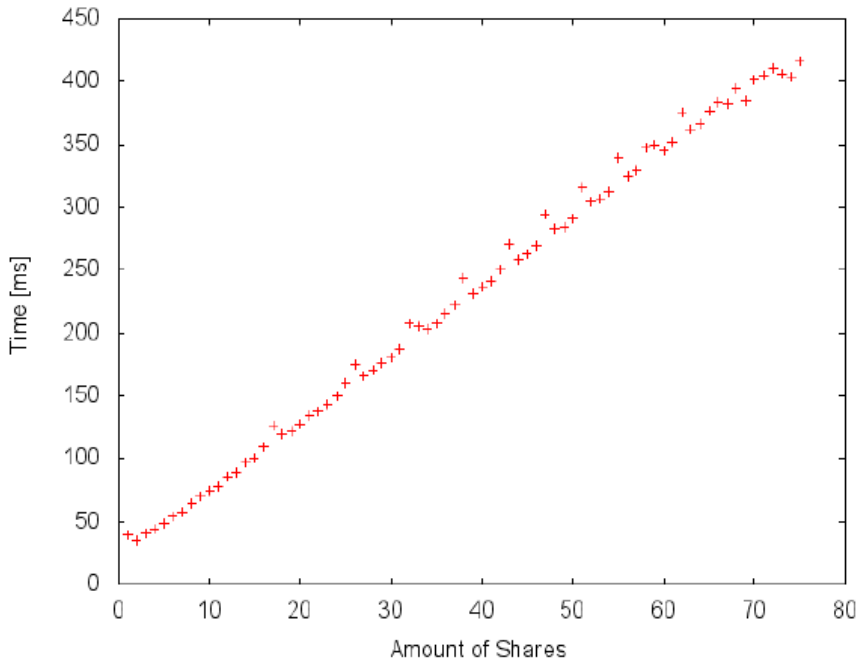
```
{
  "Description 1":"Encrypted Share 1",
  "Description 2":"Encrypted Share 2",
  "Description 3":"Encrypted Share 3",
  "Profile":"Encrypted Message",
  "Options":"Options"
}
```

Demo

Evaluation

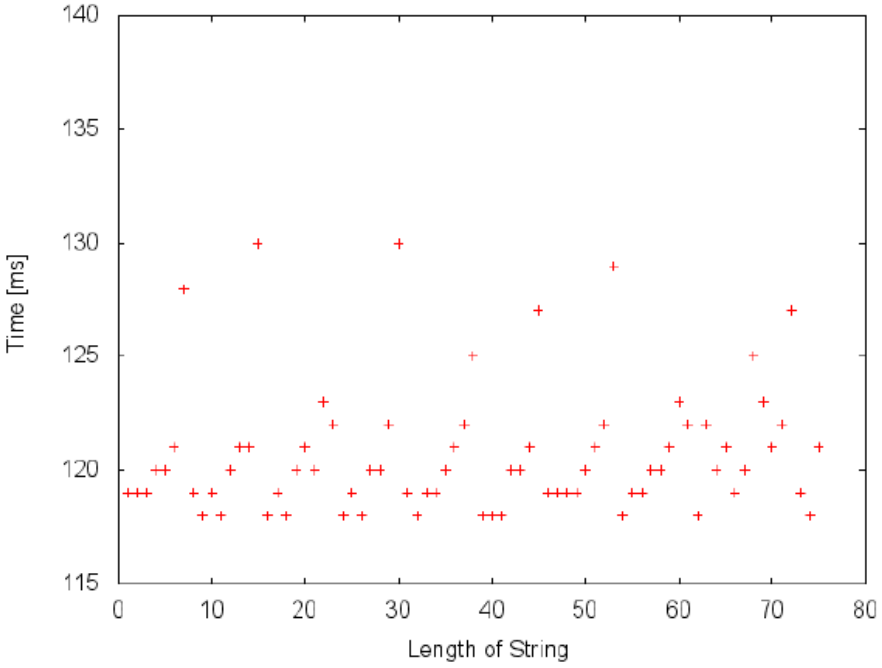
- Überprüfung der Skalierbarkeit und der Performance
  - Zeitmessung bei der Verschlüsselung mit variabler Länge der Informationen
  - Zeitmessung bei der Verschlüsselung mit variabler Menge von geheimen Informationen

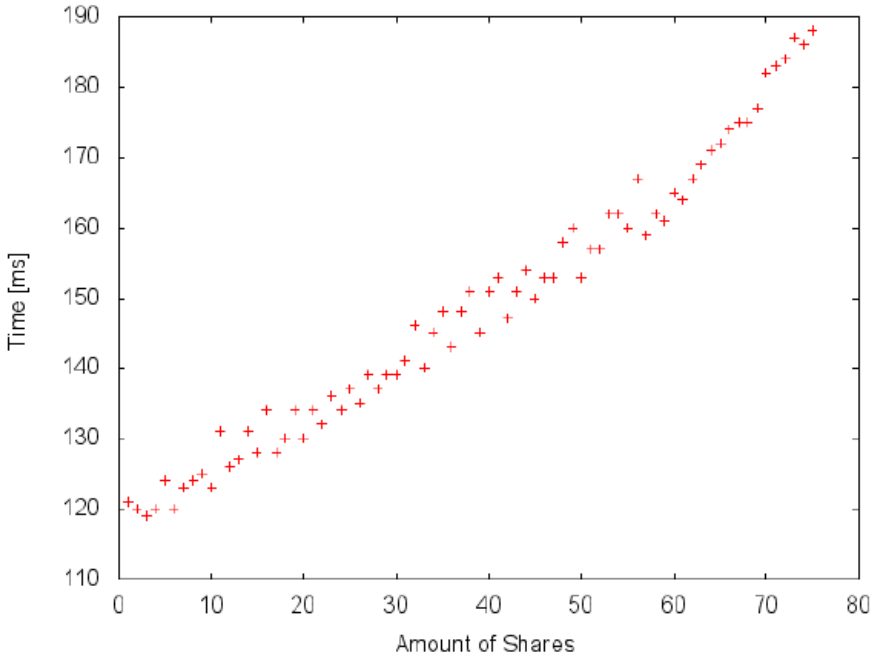




Evaluation

- Überprüfung der Skalierbarkeit und der Performance
  - Zeitmessung bei der Entschlüsselung mit variabler Länge der Informationen
  - Zeitmessung bei der Entschlüsselung mit variabler Menge von geheimen Informationen





Weiterentwicklung und Literatur

- Entschlüsselung von Bildern ermöglichen
- Löschen oder das Ändern von bestehenden Notizen
- Bei Veränderung von privaten Schlüsseln, Anpassung von bestehenden Notizen
- Automatische Entschlüsselung, falls schon genügend Informationen vorhanden sind
- Massenentschlüsselung

Literatur:

Adi Shamir. How to share a secret. Commun. ACM, 22(11):612-613, November 1979

Wolfgang Konen. Lecture: 'Das Teilen von Geheimnissen (Secret Sharing)'. http://www.gm.fh-koeln.de/~konen/DisMa/secret-sharing.pdf [Retrieved 15.03.2012].