Neue Ansätze für Grafische Passwörter

Roland Schmitz

Hochschule der Medien, Nobelstrasse 10, 70569 Stuttgart
schmitz@hdm-stuttgart.de

Zusammenfassung Grafische Passwörter und das von ihnen gebotene Verhältnis von Sicherheit und Usability sind seit einiger Zeit Gegenstand intensiver Forschung. In diesem Beitrag werden zwei neuartige Konzepte für grafische Passwörter, Pass-Fractals und Pass-Maps, vorgestellt. Die Sicherheit und Usability beider Konzepte werden anhand einer groß angelegten Nutzerstudie, die über einen längeren Zeitraum mit Studenten an zwei verschiedenen Hochschulen durchgeführt wurde, bewertet.

1 Einführung

Seit den 90er Jahren werden in der Literatur grafische Passwörter untersucht, in der Hoffnung, dass diese ein besseres Verhältnis von Security und Usability bieten als textuelle Passwörter. Bei einem grafischen Passwort besteht das Geheimnis aus einem Objekt, das vom Nutzer visuell wieder erkannt werden kann und gleichzeitig vom Computer einfach erzeugt und verarbeitet werden kann. Einen guten Überblick über die bisherigen Ansätze bietet die Arbeit [1].
Leider hat sich bei diesen Ansätzen gezeigt, dass auch hier die gewählten Passwörter, ähnlich wie bei textuellen Passwortern, nicht gleichmässig über den zur Verfügung stehenden Password Space verteilt sind, sondern durch persönliche Präferenzen der Nutzer beeinflusst werden.
Im vorliegenden Beitrag werden zwei neue Ansätze für grafische Passwörter vorgestellt, die beide auf dem neuartigen Konzept einer *Pass-Region* basieren. Dabei wählt der Nutzer durch mehrfaches Zoomen eine kleine Teilregion eines Datenobjekts (z.B. ein hochaufgelöstes Bild) als sein Geheimnis aus; zur Authentifikation reicht es aus, in eine Teilmenge der Pass-Region hinen zu zoomen. Beim ersten Ansatz namens *Pass-Fractals* hat der Nutzer die Möglichkeit, beliebig tief in ein Fraktal hinein zu zoomen und so seine Pass-Region festzulegen. Der zweite Ansatz namens *Pass-Maps* funktioniert ähnlich, basiert aber auf einer Weltkarte und Google Maps.

2 Pass-Fractals

Bei diesem Ansatz ist die wohlbekannte Mandelbrotmenge, eine Teilmenge der komplexen Zahlenebene, die zu Grunde liegende Struktur. Die Mandelbrotmenge besitzt, wie andere Fraktale auch, einige interessante Eigenschaften, die sie für den Einsatz im Rahmen des Pass-Region Konzepts besonders geeignet erscheinen lassen. So kann der Zoom-Prozess im Prinzip beliebig oft wiederholt werden, wobei sowohl bereits bekannte als auch neue Muster auftauchen, an denen sich der Nutzer orientieren kann. Da die Definition der Mandelbrotmenge auf einer einfachen mathematischen Vorschrift beruht, können die benötigten Teilmengen einfach und schnell dynamisch generiert

werden. Gleichzeitig ist zu erwarten, dass aufgrund der mathematisch-abstrakten Natur der Mandelbrotmenge persönliche Präferenzen der Nutzer keine Rolle spielen bei der Definition der Pass-Region. Um diese Annahme zu überprüfen, haben wir zwei Pass-Fractals Prototypen (einen Web-basierten und ein Smartphone-basierten) entwickelt und einer Nutzerstudie unterzogen.

3 Pass-Maps

Bei Pass-Maps liegt dem System eine zoombare Weltkarte, basierend auf Google Maps, zu Grunde. In diesem Fall wurde lediglich ein Web-basierter Prototyp entwickelt. Um Pass-Fractals und Pass-Maps möglichst gut vergleichbar zu halten, wurde nicht das normale Zoom-Interface von Google Maps genutzt, sondern dieselbe Technik wie bei Pass-Fractals, d.h. der Nutzer legt mit der Maus ein Quadrat fest, in welches dann hinein gezoomt wird. Bei diesem System war natürlicherweise zu erwarten, dass die Pass-Regions nicht gleichmässig über die Welt verteilt sind, sondern zu einem gewissen Grad mit der Herkunft der Nutzer korrespondieren.

4 Nutzerstudie

Insgesamt haben 85 Nutzer (Informatikstudenten der beteiligten Hochschulen) über einen Zeitraum von mehreren Monaten das Web-basierte Pass-Fractals System zum Login auf einen Server mit Unterrichtsmaterialien genutzt. Pass-Maps wurde von 24 Nutzern, zumeist Mitarbeiter der Hochschulen, getestet. Im Rahmen der Nutzerstudie wurden Daten wie Erfolgsquote beim Login, Login-Zeiten, sowie Verteilung und Größe der gewählten Pass-Regions gemessen. Der mobile Pass-Fractals Prototyp wurde nur über einen kurzen Zeitabschnitt von wenigen Nutzern getestet. Hier stand die Realisierbarkeit des Konzepts auch für mobile Endgeräte im Vordergrund.
Die Nutzerstudie hat im wesentlichen die in den Abschnitten 2 und 3 getroffenen Annahmen bestätigt. Pass-Fractals hat sich als zwar ein sicheres, aber wenig intuitiv merkbares System erwiesen, dessen Nutzer eine gewisse Eingewöhnungszeit benötigen. Wie erhofft, sind die Pass-Regions relativ gleichmäßig über das Fraktal verteilt. Zudem bietet das System einen exponentiell mit der Anzahl der Zoom-Vorgänge anwachsenden Password-Space.
Auf der anderen Seite ist Pass-Maps sofort intuitiv nutzbar und hat eine hohe Login-Erfolgsrate aufzuweisen, weist aber eine schlechte Sicherheit gegen Social-Engineering Attacken und Shoulder Surfing auf. Insbesondere besteht eine hohe Korrelation zwischen Herkunftsland der Nutzer und gewählter Pass-Region.
Wir werden in Zukunft die Nutzeroberflächen beider Systeme weiter optimieren und weitere Instanzen des Pass-Region Konzeptes untersuchen. Dabei werden wir insbesondere neben dreidimensionalen Datenstrukturen auch hörbare Objekte (etwa eine Musikdatenbank) betrachten, um sehbehinderten Menschen eine Alternative bei der Authentifikation anbieten zu können.

Literatur

1. Biddle, R., Chiasson, S., van Oorschot, P.C.: Graphical passwords: Learning from the first generation. Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada (2009) verfügbar unter `http://people.scs.carleton.ca/~schiasso/chiasson_gp_survey_techreport.%pdf`.