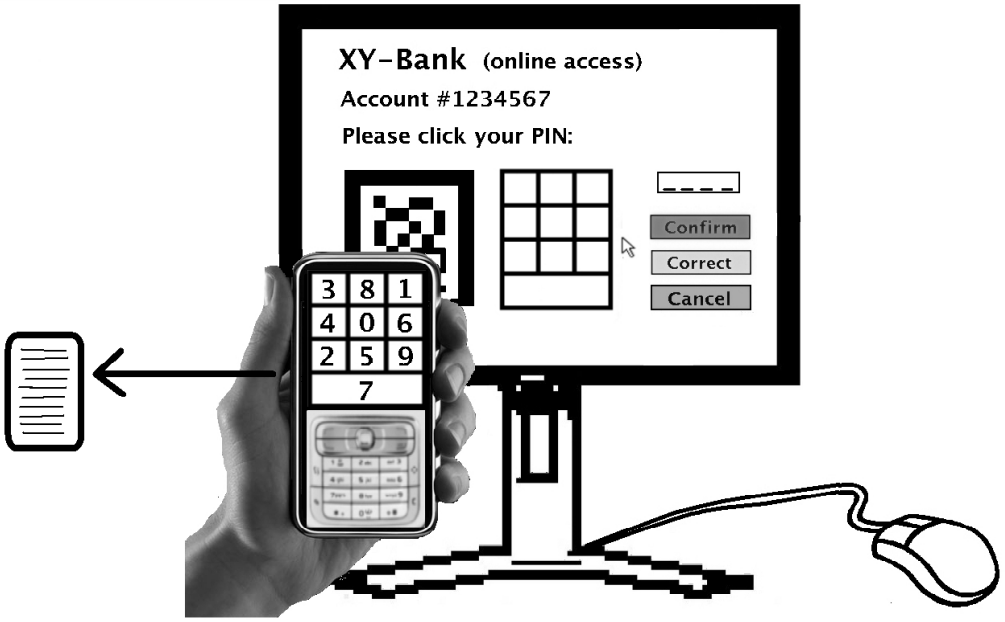
Eberhard Karls Universität Tübingen
Wilhelm-Schickard-Institut für Informatik (WSI)
Arbeitsbereich für Theoretische Informatik/Formale Sprachen

15.1.2011 Thema für eine studentische Arbeit (Stud., Dipl., Bach., Master)

Back-Up für das Fotohandy-Verfahren

Das Open-Sesame/Foto-PIN Verfahren erlaubt den komfortablen und abhörsicheren Zugang zu Online Accounts. Der Benutzer benötigt dafür ein internetfähiges Smartphone. Ein Prototyp für das Open-Sesame/Foto-PIN Verfahren Verfahren ist schon implementiert worden:
http://www.ekaay.com/sesame



Für den Fall des Diebstahls, des Verlusts oder der Zerstörung des Fotohandys braucht der Benutzer ein Back-Up Verfahren für die auf dem Handy abgespeicherten geheimen Schüssel. Bislang wird dem Benutzer ein "low-tech" Back-Up empfohlen: der Benutzer legt sich die Papier-Ausdrucke mit den QR-Codes, mit denen die Accounts initialisiert werden, ab. Im Falle der Wiederherstellung scannt er dann einfach alle QR-Codes nochmal wieder ein.

Es soll eine elektronische Back-Up Version konzipiert und implementiert werden. Die Aufgabe einer Studien - oder Bachelor-Arbeit ist es, ein benutzerfreundliches Back-Up Verfahren zu implementieren, mit dem die geheimen Informationen in einer dump Datei, z.B. zunächst auf dem Handy, gespeichert und wieder eingelesen werden können, sinnvollerweise verschlüsselt. Die Aufgabe einer Diplom- oder Master-Arbeit ist es, weitere Konzepte für ein sicheres und benutzerfreundliches Back-Up beim Fotohandy-Verfahren zu entwerfen und zu analysieren. Es soll das geeignetste der Verfahren implementiert werden. Zum Beispiel ist eine Variante zu betrachten, bei der die verschlüsselten dumps vom Handy selbständig an eine feste Stelle ins Internet gestellt werden, so dass sich der Benutzer nur wenig um das Thema Back-Up kümmern muss.

Implementierungen sollen in der Android oder in der iPhone Programmierumgebung geschrieben werden und ggfs. in das entsprechende bestehende Open Sesame Paket integriert werden. Anleitung und Unterstützung für die Programmierung für Android bzw. iPhone wird geboten.

Betreuer: Dr. Bernd Borchert
http://www-fs.informatik.uni-tuebingen.de/~borchert/Troja/