# Ziel der Studie

Ziel der Studie ist es neue Pinverfahren zu entwickeln, die sicherer sein sollen als das Standard-Verfahren. Bei traditionellen Verfahren kann man durch Spähen oder Anbringen einer versteckten Kamera die eingetippten Zahlen „ausspionieren“ und erhält somit auch die PIN. Es wurden deshalb 2 Verfahren entwickelt, die selbst wenn man das Eingetippte/Eingegebene erspäht die eigentlich PIN nicht preisgeben. Diese wurden dann mit dem Standard-Verfahren verglichen.

Die entwickelten Verfahren waren:

(Namen frei erfunden und nicht unbedingt die in der Studie benutzten)

## Zahlen, Buchstaben und Farben

In diesem Verfahren bestand die PIN wie üblich aus Ziffern (4), wobei man sich zu jeder einzelnen noch eine von drei Farben (rot, schwarz, weiß) merken musste.

Eine PIN könnte dann folgendermaßen aussehen: 8(schwarz) 4(rot) 2(weiß) 1(rot).

Beim Eingeben der PIN sieht man dann ein Bildschirm mit den Ziffern 0-9 und unter jeder Ziffer stehen 3 Buchstaben, einen roten, einen schwarzen und einen weißen. Wichtig dabei ist, dass jeder Buchstabe unter 3 verschiedene Ziffern steht, und jedes Mal in einer anderen Farbe. D.h. z.B. steht unter der 8 ein schwarzes „s“, dann muss es auch noch eine rotes und ein weißes geben, und die könnte z.B. unter der 4 und der 2 liegen.

Der Nutzer muss dann die aktuelle Ziffer der PIN suchen, sich die dazugehörige Farbe erinnern und dann den Buchstaben mit der richtigen Farbe auf einer Tastatur tippen (es ist klar dass es nicht möglich sein soll mit einem Touch-Display direkt den Buchstaben klicken zu können). Das ist schon um einiges sicherer als ein Standard-Verfahren, da für jeder Buchstabe 3 mögliche Ziffer in Frage kommen.

Zudem wird das Ganze noch sicherer, da das so implementiert wird, dass nach jeder Eingabe die Buchstaben gemischt werden, sie stehen also nicht immer unter der selben Ziffer.

## Memory PIN

In diesem Verfahren besteht die PIN aus einer Reihe von Bildern, also z.B. Katze, Schloss, Tasse und Löffel. Bei der Eingabe sieht der Nutzer dann ein Feld von Bildern (z.B. 10X10). Man kann auf jedes Bild klicken um es praktisch umzudrehen, ähnlich wie beim Memory. Dabei ist es so, dass immer klar ist, was für ein Bild hinter ein anderes steht, da sie irgendwie verwandt sind. So steht z.B. auf einer Karte auf einer Seite eine Katze und auf der anderen eine Maus, oder Tasse/Teekanne, Schloss/Schlüssel, Löffel/Gabel, etc.

Um eine PIN korrekt einzugeben, muss man die Karten solange drehen, bis die Bilder der PIN alle nach oben schauen (Reihenfolge spielt keine Rolle). Zusätzlich gibt es noch ein Paar Bedingungen, es müssen z.B. eine Mindestanzahl gedreht werden und es darf höchstens eine Höchstanzahl gedreht werden, damit einem Späher nicht klar ist, welche Karte jetzt nötig war umzudrehen, und welche umgedreht worden sind um die Mindestanzahl zu erreichen.

Das Ganze wird zudem so implementiert, dass es nie vorkommen kann, dass alle Bilder schon auf der richtigen (oder alle auf der falschen) Seite liegen.

# Ablauf der Studie

Zunächst wurde erklärt, worum es in der Studie ging.

Dann wurden die einzelnen Verfahren vorgestellt und die Bedienmasken erklärt. Schließlich musste man die Studie durchführen, was wie folgt geschah:

Die Versuchsperson bekam von der Versuchleiterin eine PIN, die auf ein Stück Papier gezeichnet war. Die Versuchsperson musste dann über eine Eingabemaske zunächst diese PIN einstellen. Nachdem die PIN eingestellt war, musste man das Eingeben der PIN simulieren, was über eine andere Eingabemaske passierte. Nachdem der Nutzer die PIN korrekt eingegeben hatte und sich somit erfolgreich angemeldet hatte, musste er einen Fragebogen ausfüllen. Dabei wurde nach Einschätzungen des Aufwands des PIN-Verfahrens, der Sicherheit des Verfahrens, ob man es nutzen würde, usw, gefragt. Nach dem Ausfüllen des Fragebogens hat man das gleiche Szenario nochmals durchlaufen, wobei hier der Nutzer sich selbst eine PIN aussuchen durfte, und diese eben nicht vorgeschrieben bekam. Auch nach dem zweiten Durchlauf musste man einen ähnlichen Fragebogen ausfüllen. Die Einstellung und Eingabe der PINs wurde auf Video festgehalten, wobei Bildschirm und Tastatur/Mouse gleichzeitig zu sehen waren.

Das Ganze wurde für die zwei neuen Verfahren und den Traditionellen durchgeführt.

Vor der tatsächlichen Messung, durfte die Versuchsperson Probedurchläufe für jedes Verfahren machen.

# Gemessene Variablen

Während der Studie wurde nicht darauf hingewiesen welche Variablen nun gemessen werden (evtl. absichtlich um mögliche unnatürliche Verhaltensmuster bei der Versuchsperson zu vermeiden).

Da aber Informationen zum Ziel der Studie gegeben wurden, kann man vermuten, dass zumindest Zeit für die Einstellung/Eingabe der PIN und Anzahl der Fehlversuche gemessen wurde. Da die Eingabemasken Flash-Applikationen (oder ähnliches) waren, sind diese Variablen recht einfach zu erheben.

# Kritische Beurteilung

Der Eindruck war, dass Planung und Durchführung gut durchdacht worden sind, es sind also keine Fehler aufgefallen. Eine kleine Anmerkung vielleicht: die Versuchsleiterin hat für das eintippen von Ziffern eine Ziffern-Pad mit „klassicher“ Belegung (also wie auf den Tascherechner) zur Verfügung gestellt. Wie sich aber raustellte, benutzen Banken (zumindest eine Teilmenge davon) Ziffern-Blöcke die wie Telefontasten ausgerichtet sind (die 1 ist also oben links und nicht unten links). Das ist nur zufällig aufgefallen, sollte aber keinen Einfluss auf die Messungen und Konzepte der Studie haben.