LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LFE Medieninformatik • Katja Hertzschuch

Abschlussbericht Projektarbeit

Entwicklung von softwarebasierten Authentifizierungs-Verfahren zur Vorbeugung gegen shoulder surfing

Verantw. Hochschullehrer: Prof. Dr. Heinrich Hußmann
Betreuer: Dipl. Medieninf. Alexander De Luca

Agenda

- Motivation
- Bisherige Arbeiten
- Neue Pin Verfahren
- Nutzerstudie
- Fazit

Authentifizierung über PIN allgegenwärtig …

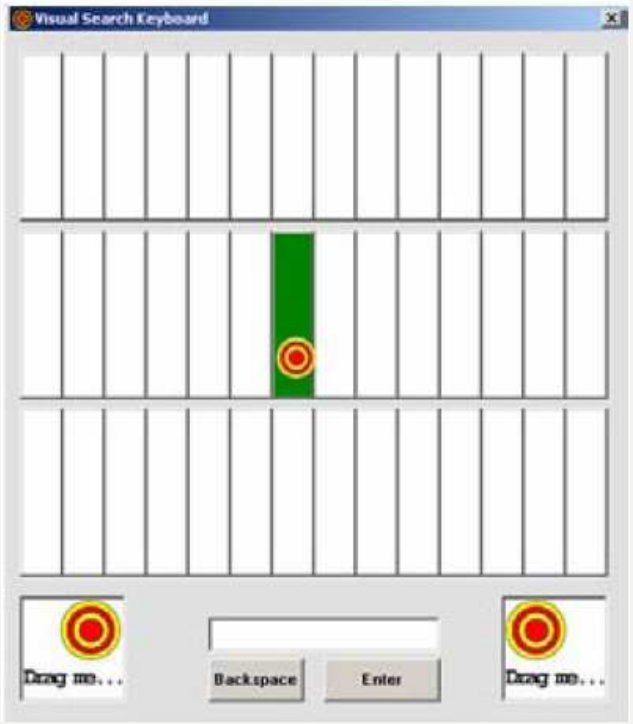
- Bezahlung mit Karte im Supermarkt
- Kartenzahlung einer Fahrkarte am Automaten
- Online-Banking
- Authentifizierung beim Einschalten des Handys

… genau wie shoulder surfing

Agenda

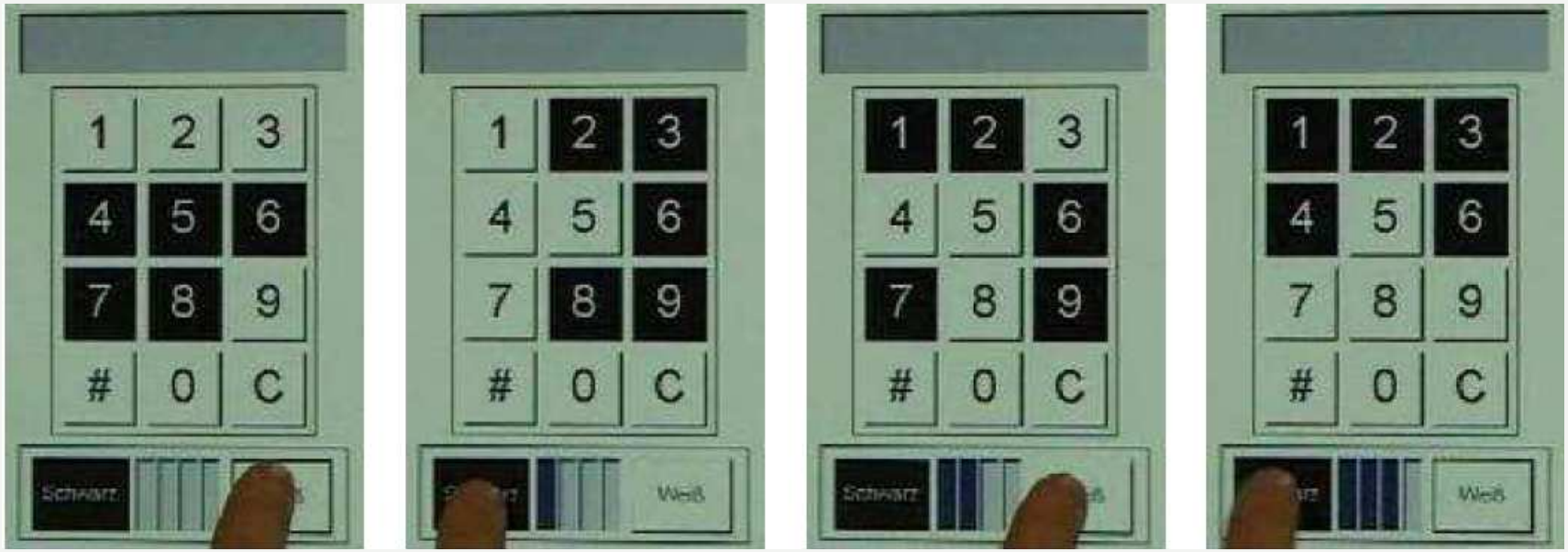
- Motivation
- Bisherige Arbeiten
- Neue Pin Verfahren
- Nutzerstudie
- Fazit

Textbasierte Ansätze wie „Spy-Resistant Keyboard“



[Desney, 2005]

Mischformen wie „cognitive trapdoor games“



[Roth, 2004]

Grafische Ansätze wie „Convex Hull Click“

[Wiedenbeck, 2006]

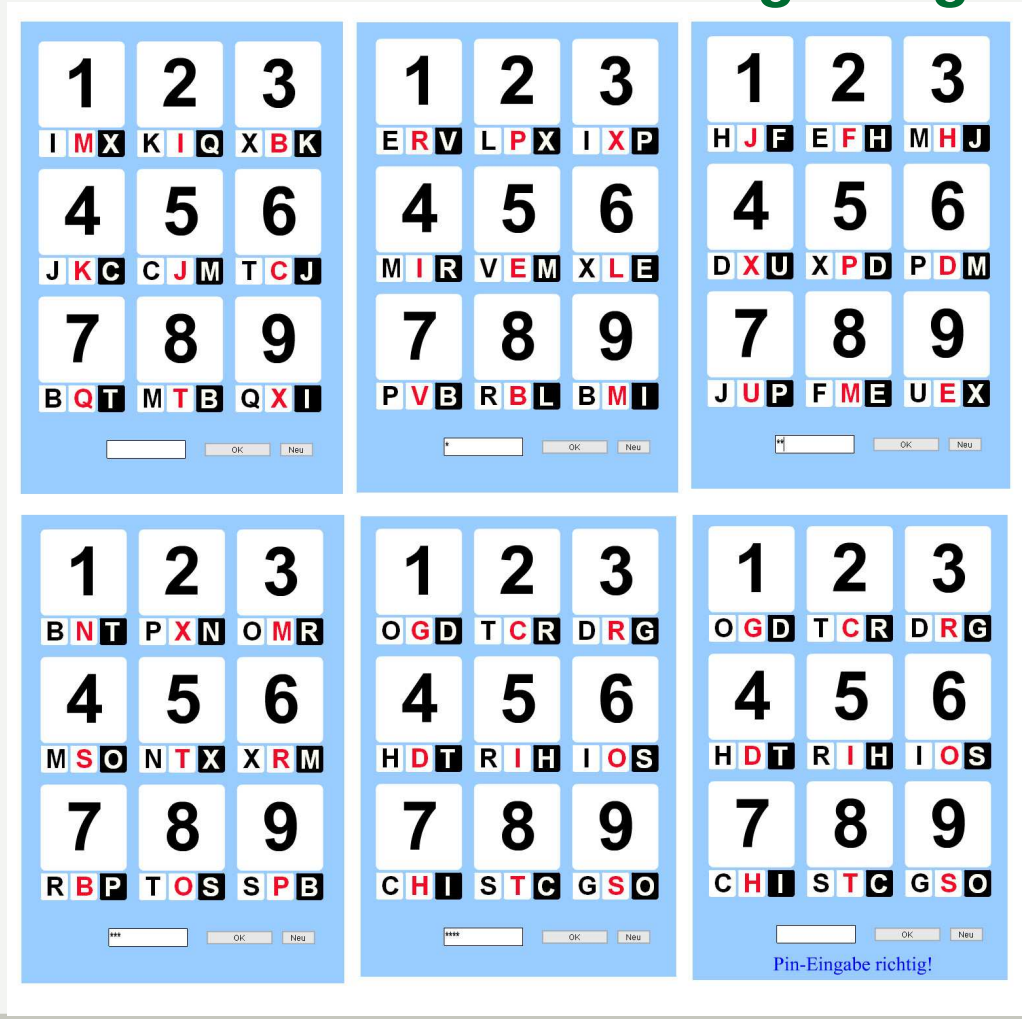
Agenda

- Motivation
- Bisherige Arbeiten
- **Neue Pin Verfahren**
- Nutzerstudie
- Fazit

Color PIN - Idee

- PIN besteht aus Zahlen und Farben z.B. 1(s) 2(r) 3(w) 4(s)
- Stellvertretend für die PIN-Zahl wird der Buchstabe eingegeben
- Buchstabe ist durch Farbe eindeutig bestimmt
- Jeden Buchstaben gibt es in den drei Farben
- Nach jeder Eingabe werden die Buchstaben neu angeordnet

Color PIN - Authentifizierungsvorgang



Beispiel: 1(s) 2(r) 3(w) 4(s)

Eingabe: I, P, J, M

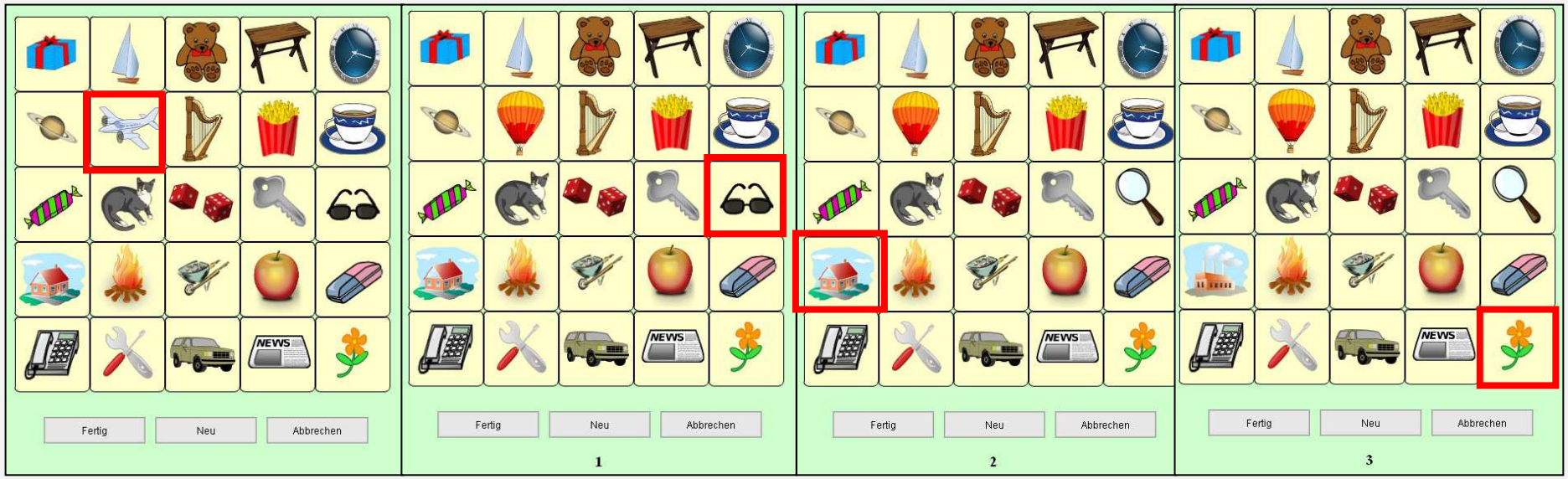
Memory PIN - Idee

- Authentifizierungs-Token besteht aus vier Bildern z.B. Hund, Tasse, Motorrad, Lupe
- Karten sind durchgemischt
- Karten werden per Klick umgedreht
- Vorder – u. Rückseite haben stehen im Zusammenhang
- Am Ende müssen alle vier PIN-Bilder sichtbar/aufgedeckt sein
- min. sechs Klicks →Lügen soll Angreifer verwirren

Memory PIN – Authentifizierungsvorgang

Bsp. Hund, Tasse, Motorrad, Lupe

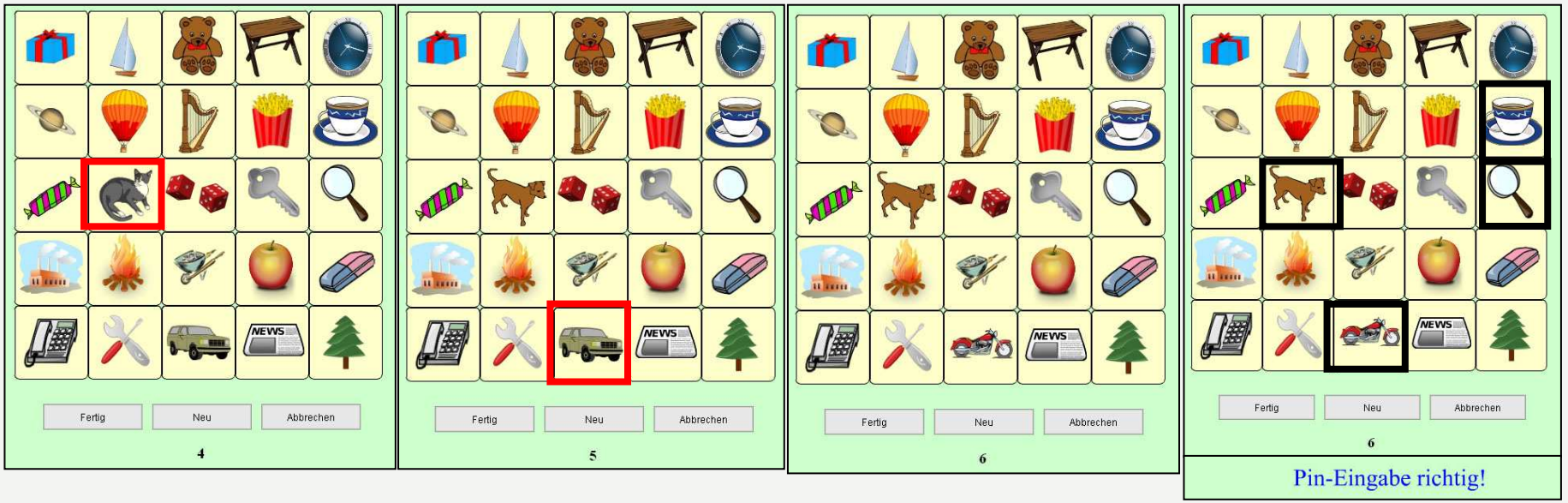
Umgedrehte Bilder: Flugzeug (Lüge), Brille, Haus (Lüge), Blume (Lüge), Katze, Auto



Memory PIN – Authentifizierungsvorgang

Bsp. Hund, Tasse, Motorrad, Lupe

Umgedrehte Bilder: Flugzeug (Lüge), Brille, Haus (Lüge), Blume (Lüge), Katze, Auto



Vergleich der Verfahren

	PIN	Memory	Color
PIN Art	Zahlen (0-9)	Bilder (4 aus 50)	Zahlen (1-9) und drei Farben
PIN Bsp.	1234	Hund, Tasse, Lupe, Motorrad	1(s),2(r),3(w),4(s)
Theoretisch mögliche Kombinationen	10.000	211.925	531.441
Wahrscheinlichkeit nach einmaligem shoulder surfing	1:1	bester Fall: 1:1 schlechtester Fall: 1:11.285	1:81
Hängt Sicherheit vom User ab?	Nein	Ja →„Lügen“	Nein

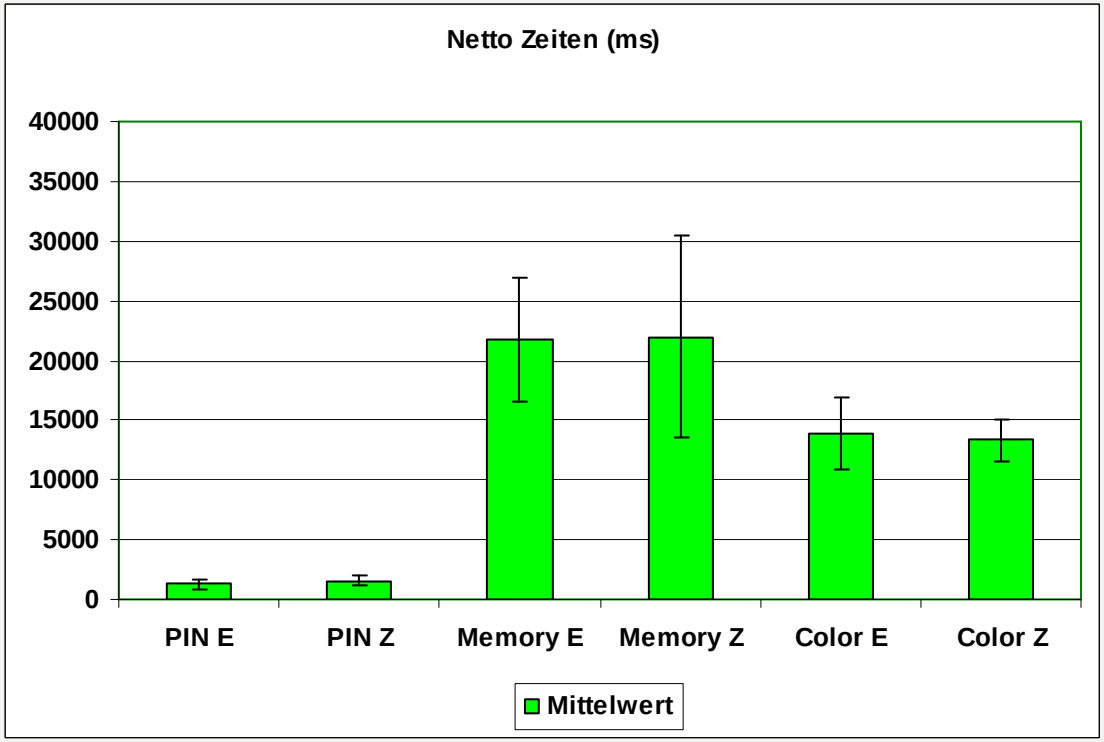
Agenda

- Motivation
- Bisherige Arbeiten
- Neue Pin Verfahren
- **Nutzerstudie**
- Fazit

Es wurde eine Nutzerstudie mit 24 Personen durchgeführt

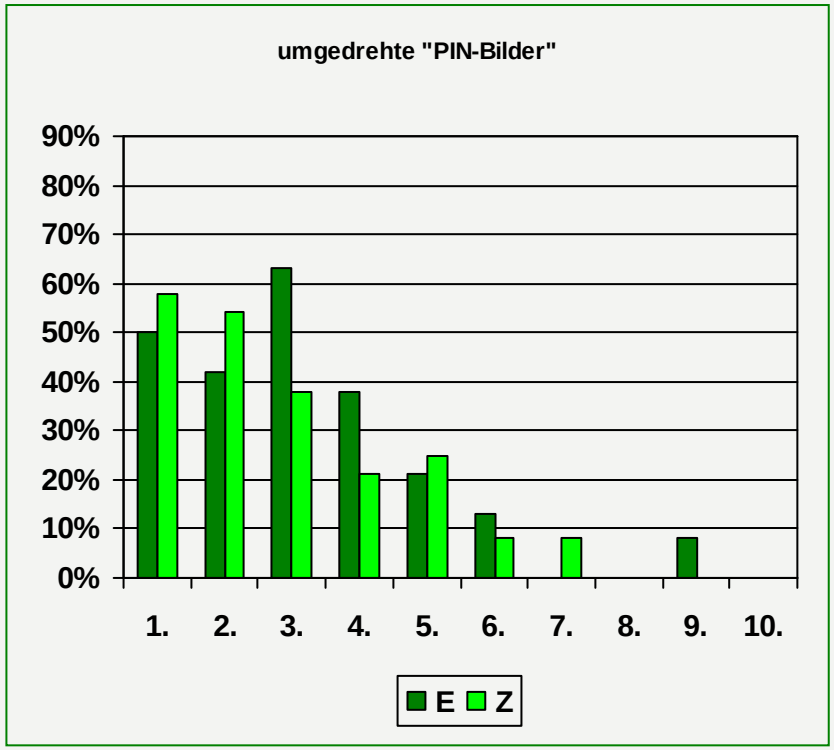
- Alter 15 – 57 (Mittelwert 27,71)
- davon 18 männlich, 6 weiblich
- PIN, Color PIN, Memory PIN
  (je zwei Durchgänge – eigene u. zufällige PIN)
- Fragebogen, Logdatei und Kameraaufzeichnung

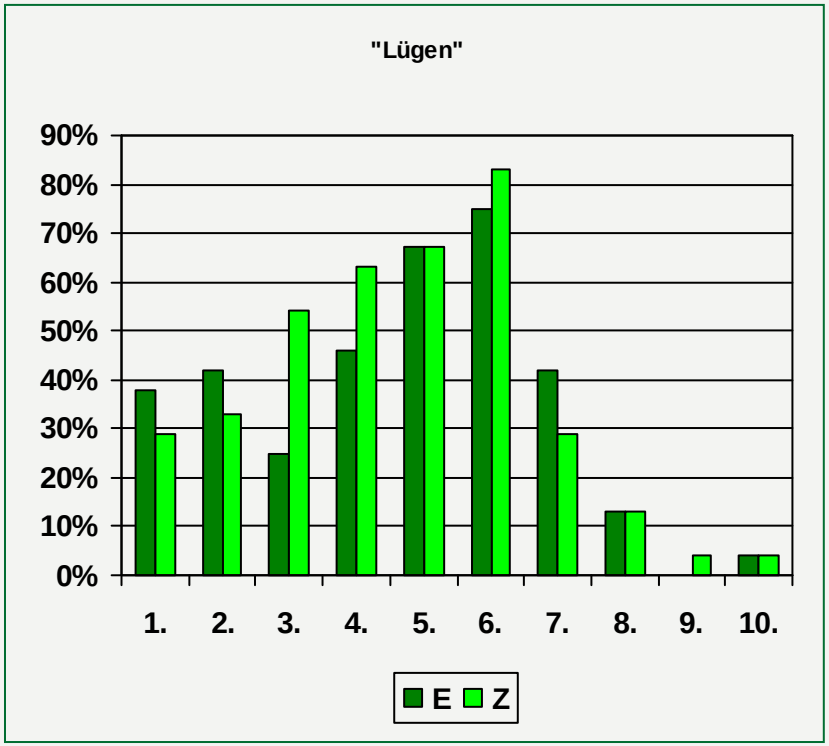
Memory PIN ist das langsamste Verfahren



- Die Zeitdifferenzen zwischen den drei Verfahren sind höchst signifikant
- Die Zeitdifferenzen zwischen der eigenen u. der zufälligen PIN sind nicht signifikant

User klicken zuerst die notwendigen Bilder an



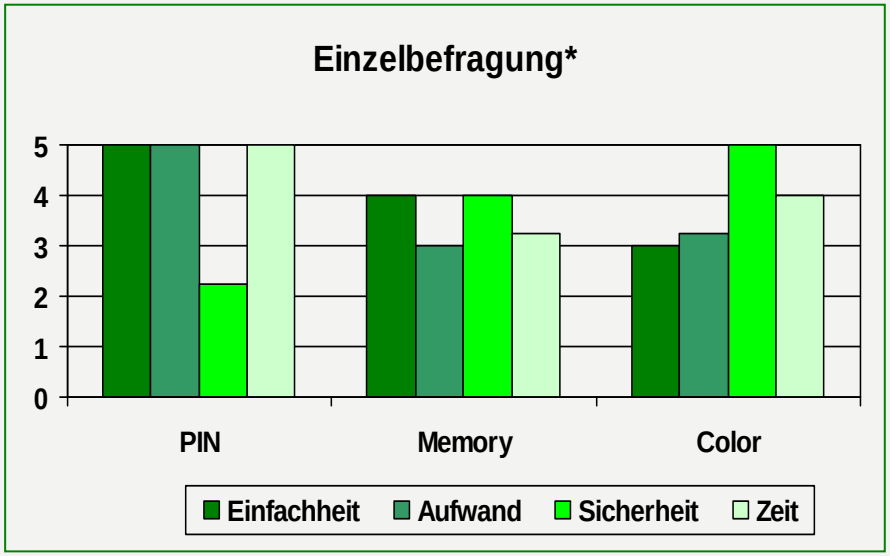


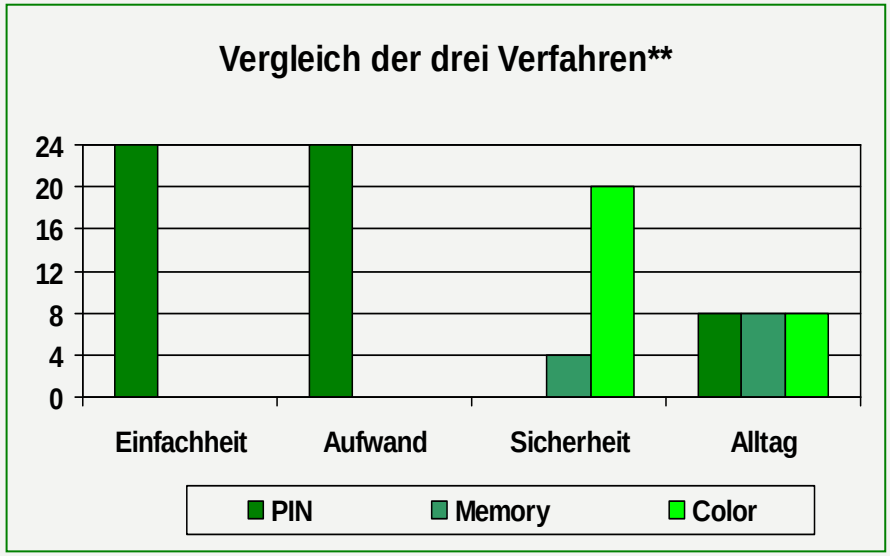
→ Nutzer klicken 6 mal (Median)

Nutzer verraten ihre PIN-Bilder durch schlechte „Lügen“

- Ein PIN-Bild, das schon bei Beginn „aufgedeckt“ ist, wird zweimal umgedreht
- Ein PIN-Bild wird mehrmals „umgedreht“
- Nutzer bewegen die Maus über bereits „aufgedeckte“ PIN-Bilder
- wenn alle PIN-Bilder sichtbar sind, wird kurz gezögert und danach gelogen

Color Pin wird als sicherstes Verfahren eingestuft





→ PIN empfinden die Nutzer am einfachsten und es hat für sie den geringsten Aufwand

→ Color Pin wird am sichersten eingeschätzt

→ Alle drei Verfahren sind gleich beliebt

* Skala 1 (sehr schlecht) - 5 (sehr gut)

** Anzahl befragte Personen

Agenda

- Motivation
- Bisherige Arbeiten
- Neue Pin Verfahren
- Nutzerstudie
- Fazit

Fazit

→Nutzern ist Sicherheit grundsätzlich sehr wichtig

→bei mehr Sicherheit darf Autorisierung auch länger dauern

→Color PIN ist sicherer

→Color PIN u. Memory PIN sind gleich beliebt

→PIN und Color PIN sind sich relativ ähnlich, wodurch der Nutzer die Option erhalten könnte, zwischen beiden Verfahren zu wählen, falls die Umgebung „unsicher“ erscheint


NEWS

???


1 2 3
E R V L P X I X P
4 5 6
M I R V E M X L E
7 8 9
P V B R B L B M I

Quellen

Desney S. Tan, Pedram Keyani, Mary Czerwinski. Spy-resistant keyboard: more secure password entry on public touch screen displays. In: OZCHI '05: Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction. Canberra, Australia, 2005, 1-10.

Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean-Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In:AVI '06: Proceedings of the working conference on Advanced visual interfaces. Venezia, Italy, 2006, ACM, 177-184.

Volker Roth, Kai Richter, Rene Freidinger. A PIN-entry method resilient against shoulder surfing. In: CCS '04: Proceedings of the 11th ACM conference on Computer and communications security. Washington DC, USA, 2004, ACM, 236-245.