LFE Medieninformatik • Stefan Karl

SmartTiles Authentication Game

21.04.2009

Problematik

- Authentifizierung gegenüber Computersystemen zunehmend notwendig

- Bisherige Systeme (z.B. PIN) haben Defizite:
  - Sicherheit vs. Usability
  - Nicht resistent gegen Shoulder-Surfing

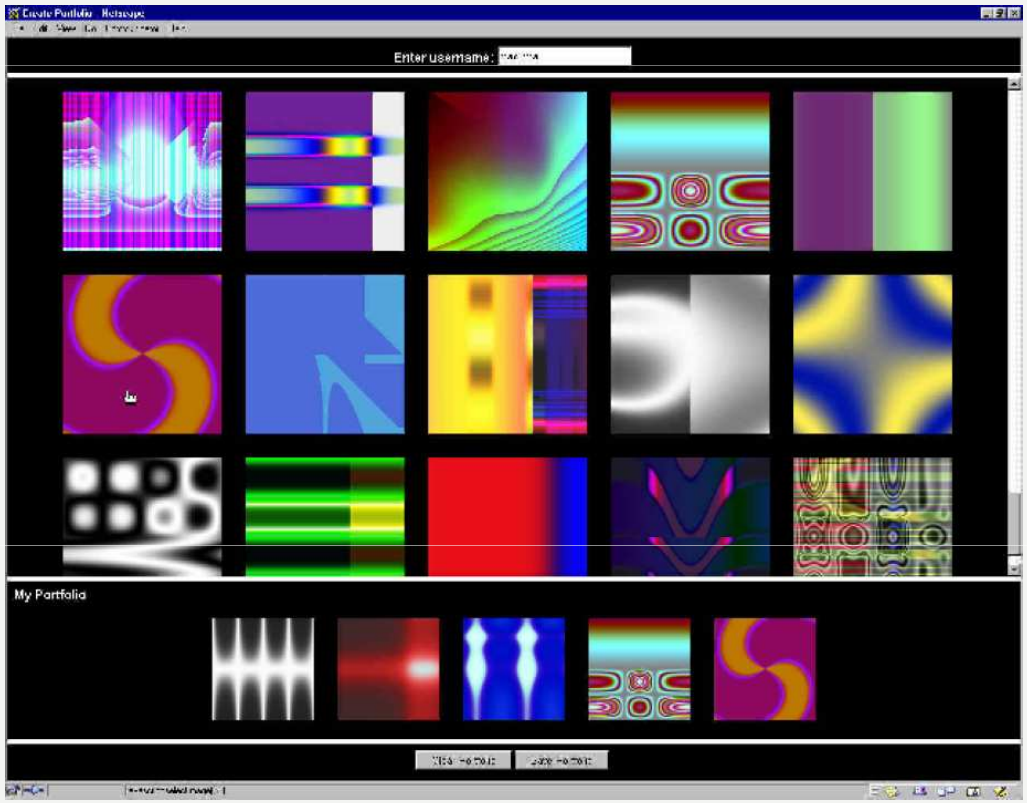
→ Neues System notwendig, das Sicherheit und Usability vereint und resistent gegen Shoulder-Surfing ist

Verwandte Arbeiten (1)

- Passfaces und Deja Vu
  - Bilderbasierend: Gesichter bei Passfaces, abstrakte Bilder bei Deja Vu
  - Passwort: Portfolio aus bestimmten Bildern
  - Login: Benutzer muss seine Portfolio-Bilder in einer Menge wiedererkennen
- Convex Hull Click (CHC)
  - Wie Deja Vu, aber Auswahl durch enthalten sein in gewählter konvexer Hülle

  → Besser gegen Shoulder-Surfing

Verwandte Arbeiten (2)

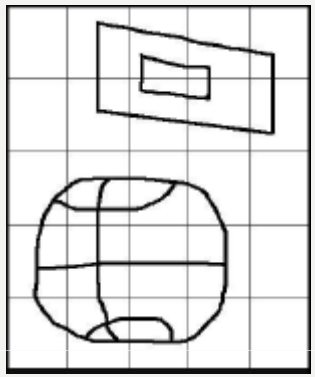


Deja Vu (Dhamija 2000)

CHC (Wiedenbeck 2006)

Verwandte Arbeiten (3)

- Draw a Secret (DAS) und Pass-Go
  - Passwort: gezeichnete Linien und Punkte
  - Abtastung:
    - DAS: durchlaufene Zellen der Zeichenfläche
    - Pass-Go: Schnittpunkte eines Gitternetzes
  - Login: Nachzeichnen mit etwas Toleranz
  - Nicht resistent gegen Shoulder-Surfing



Passwörter bei DAS (Dunphy 2007)

Verwandte Arbeiten (4)

- Auf kognitiven Fähigkeiten basierende Systeme
  - Cognitive Trapdoor Games
    - PIN-orientiert, mehrere Challenges pro PIN-Stelle
    - Pro challenge: PIN-Ziffer gehört zu einer von zwei dargestellten Gruppen (schwarz oder weiß), Benutzer muss Gruppe auswählen

    → Resistent gegen Shoulder-surfing

Challenge bei Cognitive Trapdoor Game
(Roth 2004)

Verwandte Arbeiten (5)

- Spy-resistant Keyboard
  - Drei Buchstaben/Ziffern/Symbole auf jeder Taste
  - Shift-State (unterstrichen) veränderbar durch antippen von „Drag-Me“
  - Auswählen einer Taste durch ziehen von „Drag-Me“ auf diese
  - Beschriftung der Tasten verschwinden bei Beginn des Ziehens von „Drag-Me“

  → Resistent gegen Shoulder-Surfing aber nicht gegen Videoaufzeichnung

Spy-resistant Keyboard
(Tan 2005)

Verwandte Arbeiten (6)

- Weitere Systeme
  - Biometrische Verfahren
    - Identifizierung mittels biometrischer Merkmale
  - Einmal verwendbare PIN
    - Berechnung aus alter PIN und Secret
  - Eye-Tracking
    - Aufzeichnung der Bewegung der Augen und Berechnung des aktuellen Fokus auf dem Interface

Idee

- Authentifizierung durch Spiel
- Passwort: selbst definierte Spielregeln
- Login:
  - mehrmaliges Spielen des Spiels
  - zufälliges Spielfeld
  - Lösungsmöglichkeiten einberechnet (→ lösbar)
- Art des Spiels
  - Möglichst einfach → Brettspiel

Gedanken zur Umsetzung

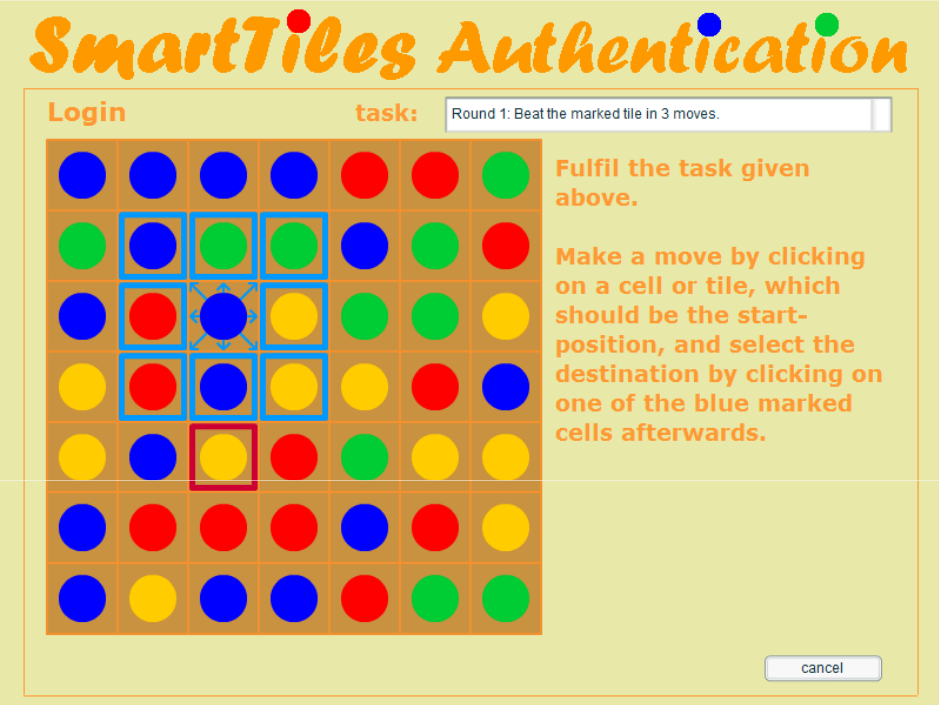
- Fragen:
  - Felder- oder Gitternetz-Design?
  - Welche Arten von Spielregeln möglich?
  - Welche Darstellungen?
- Kleine Design-Studie mit Mockups zur Klärung der Fragen

Umgesetztes Konzept (1)

- Brettspiel mit 7 mal 7 Feldern bzw. Zellen
- Vier verschiedene Spielsteine (verschiedene Farben: rot, blau, grün und gelb)
- Registrierung: Festlegung der Spielregeln
- Login: Spielen des Spiels (drei Runden)
- Erfolgreicher Login: Dreimaliges erfolgreiches Spielen des Spiels gemäß der eigenen Spielregeln

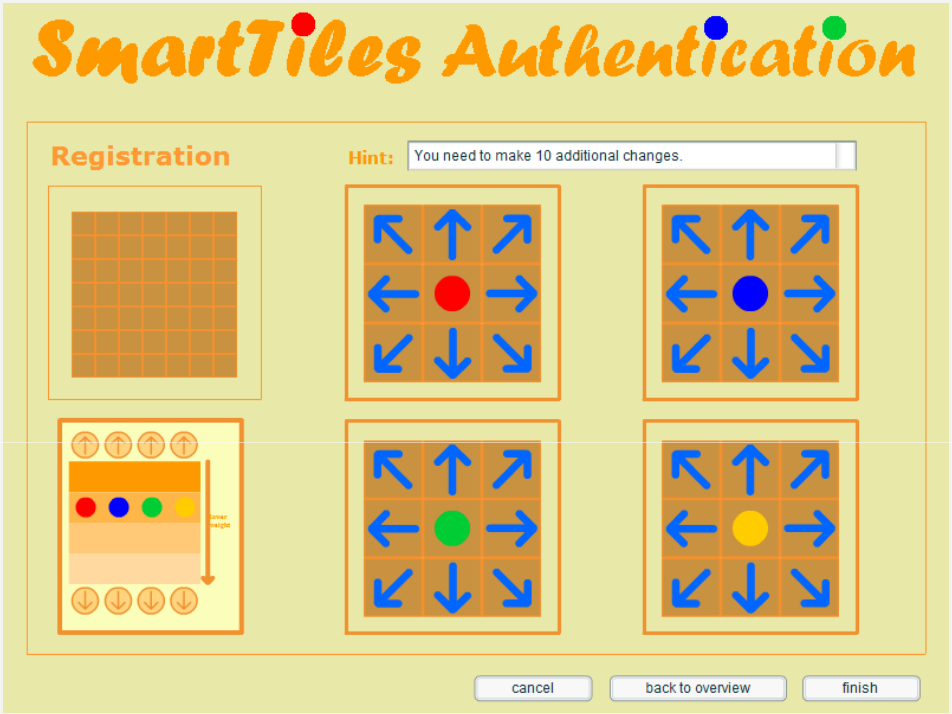
Umgesetztes Konzept (2)

- Aufgabe in der Form „Schlage den markierten Stein in x Spielzügen“
- Pro Spielzug darf sich der Stein nur auf ein Nachbarspielfeld bewegen
- Spielzug: erst zu bewegenden Stein anklicken, dann Ziel-Feld der Bewegung



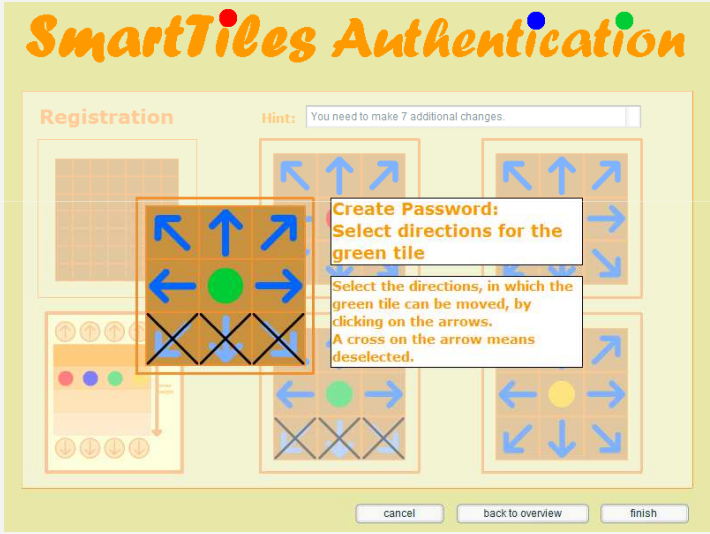
Umgesetztes Konzept (3)

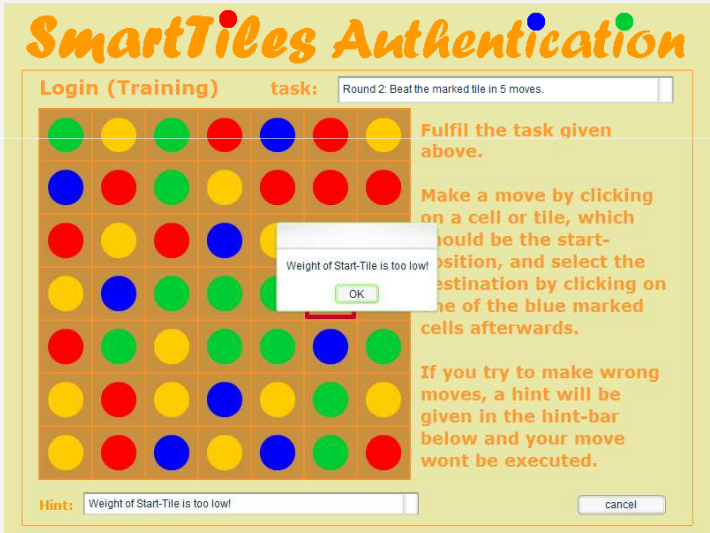
- Festlegbare Spielregeln:
  - Zellen, auf die sich ein Stein nicht hinbewegen darf
  - Richtungen, in die sich eine bestimmte Steinfarbe nicht bewegen darf
  - Wertigkeit der Steinfarben: Steine können nur gleich- oder niedriger-wertige Steine bei einem Spielzug schlagen



Umgesetztes Konzept (4)

- Registrierungsarten:
  - Wizard
  - Übersicht mit veränderbarer Großdarstellung durch Klick in der Übersicht
- Trainings-Modus nach Registrierung
  - Benutzer wird durch „Hint“-Zeile und Pop-ups auf Fehler hingewiesen





Evaluierung (1)

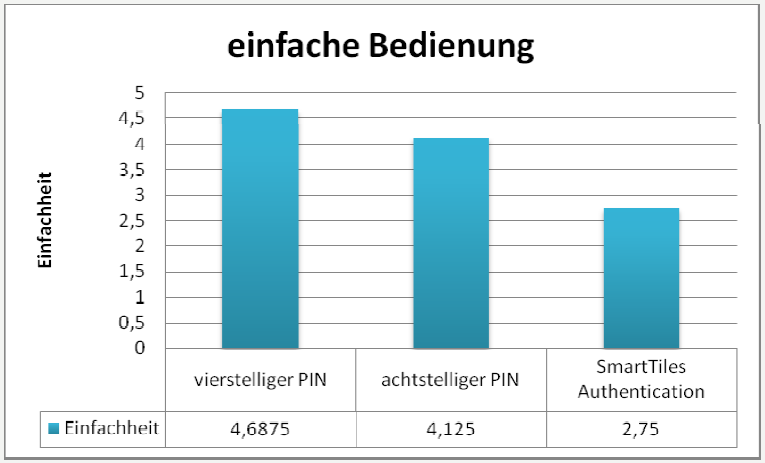
- Evaluierung in Bezug auf
  - Sicherheit
  - Einfachheit der Bedienung
  - Schnelligkeit der Authentifizierung
  - Aufwand für den Benutzer
  - Fehleranfälligkeit
  - Akzeptanz durch die Benutzer

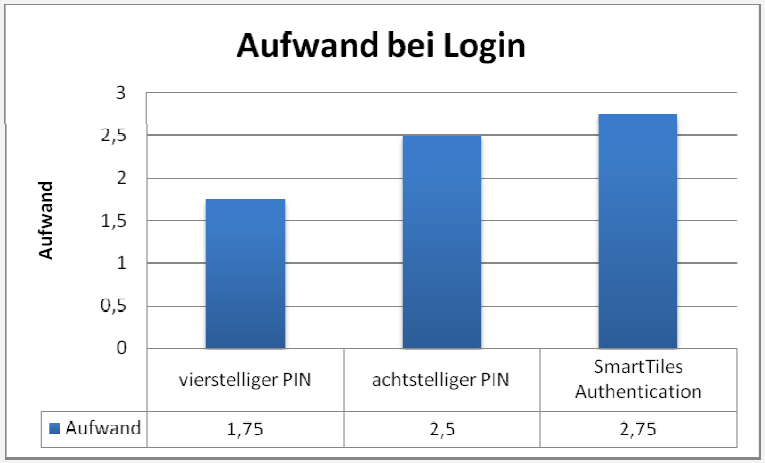
Evaluierung (2)

- Benutzerstudie
  - 16 Teilnehmer
  - Fragebogen zur Einschätzung durch den Benutzer
  - Praktischer Teil: Registrierung und Login bei…
    - System mit vierstelliger PIN
    - System mit achtstelliger PIN
    - SmartTiles Authentication

Evaluierung (3)

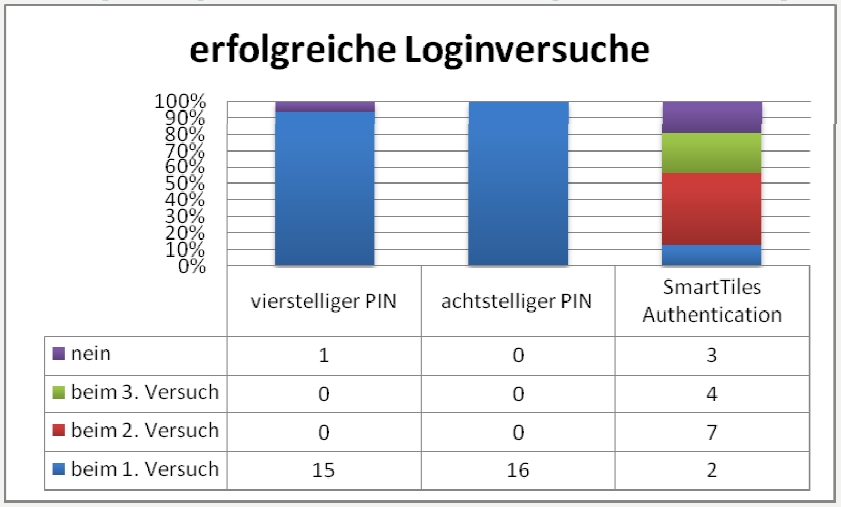
- Einschätzung durch Benutzer:
  - SmartTiles ist schwieriger zu bedienen als PIN-Systeme
  - Der Login bei SmartTiles ist aufwändiger als bei PIN-Systemen



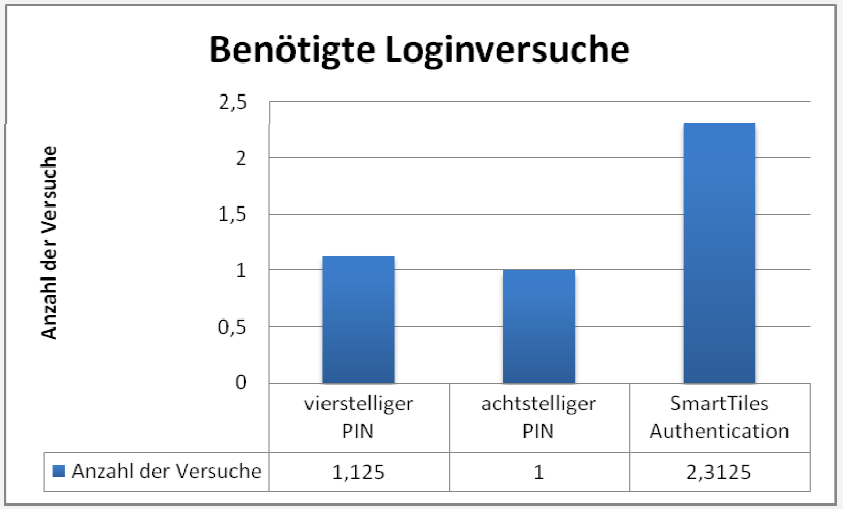


Evaluierung (4)

- SmartTiles ist deutlich fehleranfälliger als PIN-Systeme
- Zu komplizierte Spielregeln bei manchen Benutzern (kognitive Fähigkeiten!)



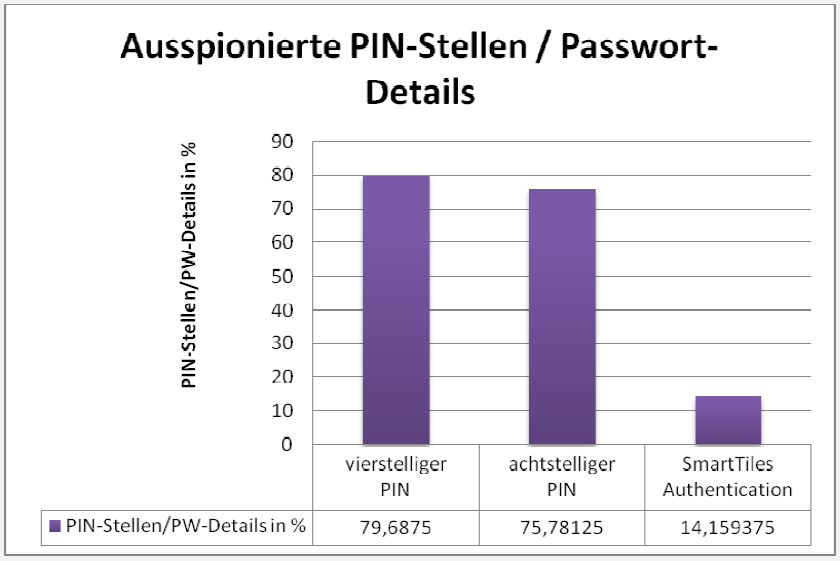
	vierstelliger PIN	achtstelliger PIN	SmartTiles Authentication
nein	1	0	3
beim 3. Versuch	0	0	4
beim 2. Versuch	0	0	7
beim 1. Versuch	15	16	2

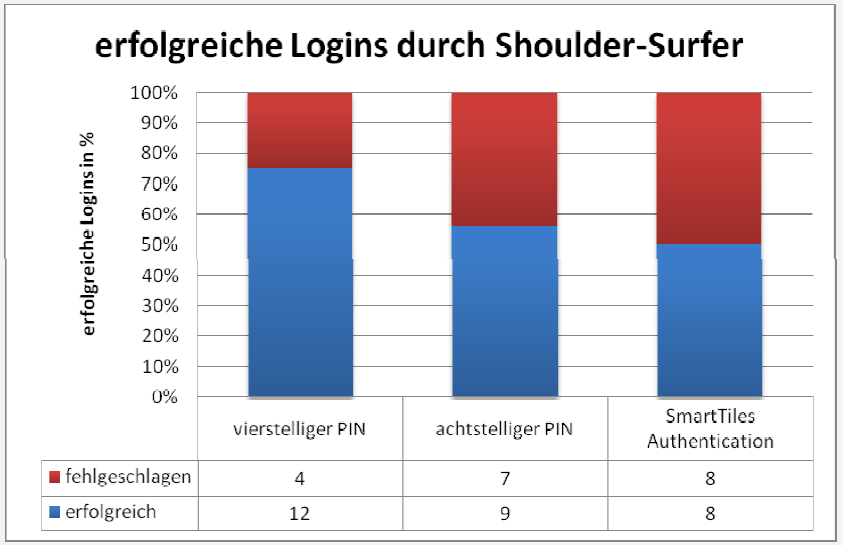


	vierstelliger PIN	achtstelliger PIN	SmartTiles Authentication
Anzahl der Versuche	1,125	1	2,3125

Evaluierung (5)

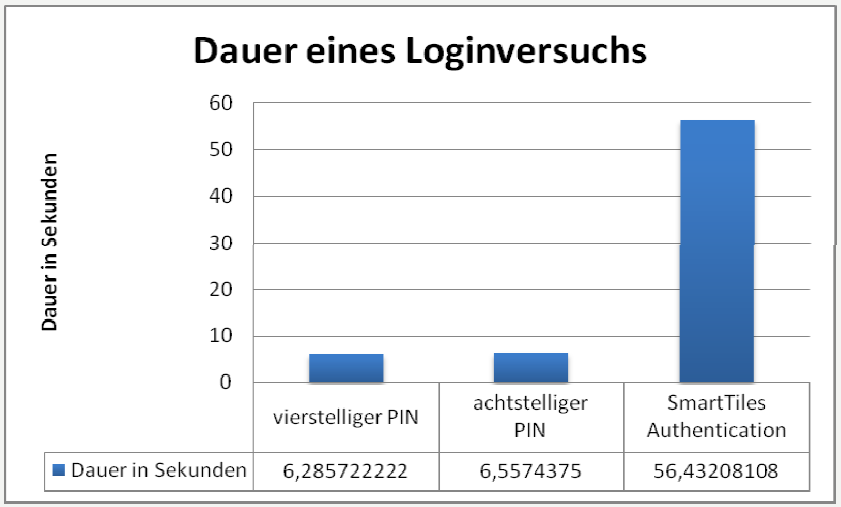
- Die Sicherheit ist bei SmartTiles am höchsten (deutlich höher als bei vierstelligem PIN)

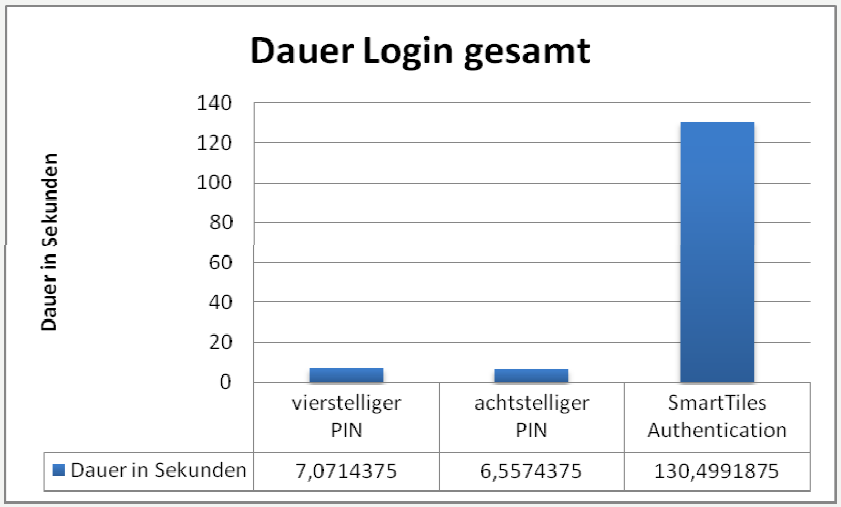




Evaluierung (6)

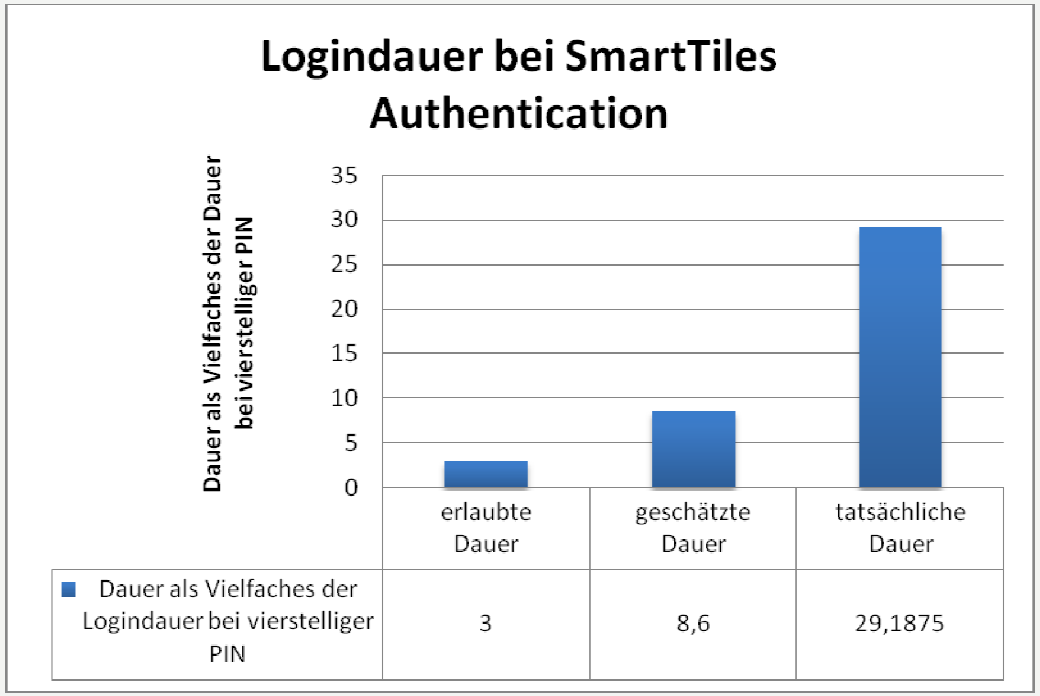
- Die Authentifizierungsdauer ist bei SmartTiles deutlich höher als bei PIN-Systemen





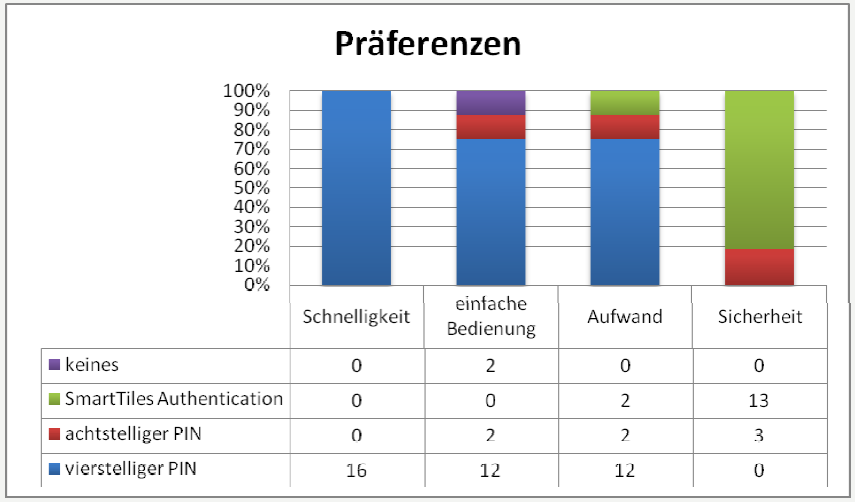
Evaluierung (7)

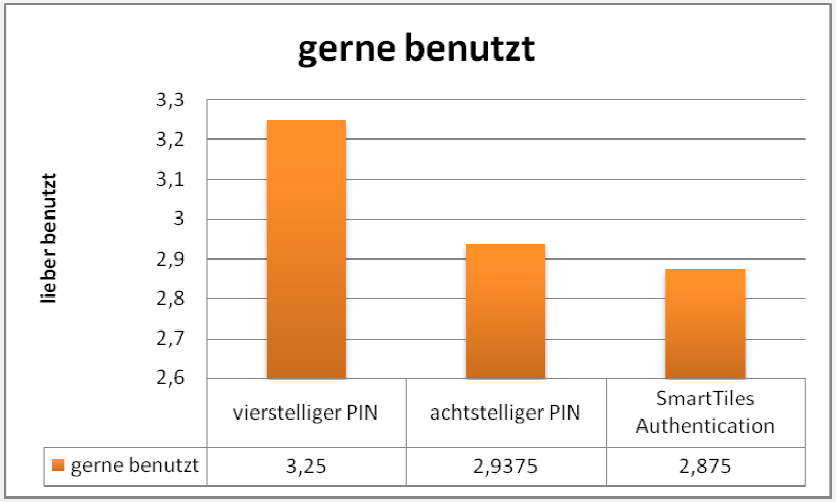
- Die Authentifizierungsdauer im Vergleich zu Systemen mit vierstelliger PIN ist deutlich höher als die Benutzer schätzen und erlauben



Evaluierung (7)

- SmartTiles ist lediglich bei der Sicherheit die Präferenz vieler Benutzer





- Aufgrund der zu hohen Authentifizierungsdauer wird SmartTiles von den Benutzern nicht angenommen

Schlussfolgerung

- SmartTiles kann nur bei Sicherheit punkten
- Spiel scheint Authentifizierung weniger langweilig zu machen (da Dauer deutlich kürzer eingeschätzt)
- Dauer des Authentifizierungsvorgangs und Umgang mit kognitiven Fähigkeiten der Benutzer sind sehr kritische Werte