Projekt: Authentifizierung im 21. Jahrhundert -Fake World

**Rahmenbedingungen:**

* 6 Seiten
* Studie mit 10 echten Personen & Onlineumfrage mit 70 Personen
* Poster
* Elevator Pitch

**Konzeptideen:**

**Konzept 1**: User legt das Fake Profil im Rahmen der Registrierung selbst an

**Konzept 2:** User teilt durch setzen von Hacken bei der Registrierung mit, welche Informationen zu seiner Person für die Erstellung des Fake Profils verwendet werden dürfen. Das Fake Profil selbst wird vom System erzeugt

**Konzept3:** Fake Profile werden dynamisch generiert. Der User bekommt von der Erstellung nichts mit.

**Konzept 4:** User wird bei der Registrierung gefragt, ob er für eine Erhöhung der Sicherheit seines Kontos Bilder für die Generierung des Fake Profils hochladen möchte.

**Probleme/ Fragen:**

* Trennung zwischen User und Angreifer? Was soll das Konzept beinhalten, was nicht? 🡪 Themenaufteilung so in Ordnung für 3er Gruppe?
* Ist es möglich statt den 2 Umfragen nur eine zu machen und dafür auch die Angreifer Seite zu behandeln?
* Wie Umfangreich soll die Datenanalyse sein? (Insgesamt nur 6 Seiten 🡪 Wenn man die Umfrage genau analysiert braucht man schon mehr Seiten)

Gespräch mit Professor:

Erst: Fokus Gruppe oder Interview: QUALITATV -> Alle Konzeptideen kurz vorstellen, Aussagen aufschreiben und clustern, dann Qualitativ beschreiben 🡪 DANN (nach erneutem Gespräch mit Prof) interessante Aspekte durch Online Umfrage quantitativ erfassen;

Paper: Aspekte die berücksichtigt werden müssen damit man es bauen kann bzw. Empfehlungen zum bauen des Projekts (Bewertung des Konzept im Paper)

Paper: Ausarbeitung welche Teilkonzepte am erfolgversprechendsten sind, welche sind nicht machbar

**Fragen für Umfrage:**

1. Welche Social Media Plattformen nutzen Sie?
2. Falls Sie eine Social Media Plattform nutzen: Wie viel Zeit verbringen Sie dort durchschnittlich?
3. Falls Sie eine Social Media Plattform nutzen: Finden Sie die Sicherheit dort ausreichend?
4. Was könnte man an der Sicherheit der Plattform noch verbessern?

**An dieser Stelle wird unser Konzept erklärt**

1. Finden Sie das Konzept intuitiv?
2. Glauben Sie dieses Konzept steigert die Sicherheit Ihres Kontos?
3. Würden Sie sich in solch einem Netzwerk registrieren?
4. Wären Sie grundsätzlich bereit neben der normalen Registrierung auch ein Fake Profil anzulegen?
5. Wie viel Zeit wären Sie bereit in die Registrierung in das Netzwerk und in die Erstellung des Fake Kontos zu investieren?
6. Wären Sie bereit Daten für eine Fake Profil Generierung bereitzustellen?

**ToDos**

1. Fokus Gruppe organisieren (welche Leute, Raum, Datum/Uhrzeit)

🡪 **Deadline:** 08.01.2018 (Ludwig) -Informieren wann Hochschule geschlossen ist

1. Vorbereitungen für Treffen mit Fokus Gruppe (Dima, Daniel) 🡪**Deadline:** Termin für Treffen
   * Themenvorstellung
   * Konzeptvorstellung
   * Fragebogen/ Fragenkatalog

**Rest ist abhängig von Punkt 1 und 2, daher erst danach genauer auszumachen**

1. Treffen mit Fokus Gruppe
   * Siehe oben
   * Mitschrift der Aussagen
2. Auswertung der Aussagen/ der Ergebnisse der Fokusgruppe (**Deadline:** 21.01.2018)
   * Zusammenfassung
   * Clustern der Einzelantworten
   * Aufbereitung für Treffen mit Prof
3. Schreiben der Arbeit und Vorbereitung des Posters
4. Einleitung/ Beschreibung des Themas (Problemstellung) z.B Meisten Attacken = BruteForce 🡪 Wir haben Lösung
5. Beschreibung der Einzelkonzepte (Beschreibung, Ergebnis der Fokusgruppe, Fazit) 🡪 Für jedes Konzept
6. Zusammenfassung der Bewertung der Einzelkonzepte
7. Diskussion der Umsetzbarkeit
8. Handlungsempfehlung
9. Präsentation

R4.017 um 16:00 Uhr

**Ergebnisse**

1. Klären: Wann werden Authentifizierungen gefordert (bei wiederholtem Login vom gleichen Gerät) 🡪 andernfalls ist keine Usability gegeben
2. Motivation für Nutzer ein Netzwerk zu nutzen ist nicht das Sicherheitskonzept, sondern Kontakte/ Freunde die dort registriert sind
3. Viele Nutzer sehen den Mehrwert (erhöhte Sicherheit) nicht und empfinden den Mehraufwand als unnötig 🡪 Viele Laien verstehen den tieferen Sinn des Konzepts nicht, finden jedoch die Sicherheit in bestehenden Netzwerken nicht als ausreichend
4. Viele Nutzer sind nicht bereit Daten für die Fake Profile zur Verfügung zu stellen
5. Viele Nutzer wären nur bereit wenig Zeit in die Erstellung/ Verwaltung von Fake Profilen zu investieren, einige gar keine Zeit
6. Vielen Details müssen abgeklärt werden
   1. Was passiert wenn man das Passwort vergisst bzw. (wiederholt) falsch eingibt?
   2. Welche zusätzlichen Authentifizierungsmechanismen werden hinterlegt? 2-FA auf gl. Gerät?
   3. Können gezielt Fake Profile angesehen werden? (z.B auch über Google?)
   4. Fake Profile können nicht so „echt“ sein, dass es Person die mich kennt nicht enttarnen kann
   5. Was geschieht mit den Handlungen, die im Fake Profil getätigt werden? Sowohl z.B das Anschrieben anderer, als auch Posten von Neuigkeiten oder Änderungen im Profil 🡪 was wird gespeichert?

**Handlungsempfehlungen**:

Paper: Aspekte die berücksichtigt werden müssen damit man es bauen kann bzw. Empfehlungen zum bauen des Projekts (Bewertung des Konzept im Paper)

Paper: Ausarbeitung welche Teilkonzepte am erfolgversprechendsten sind, welche sind nicht machbar

1. Mechanismen, die es erlauben Logins temporär zu speichern sind State of The Art. Diese Mechanismen müssen auch bei diesem Konzept angewendet werden um eine akzeptable Usability zu gewährleisten.
2. Da Nutzer sich nicht wegen dem Sicherheitskonzept in einem Netzwerk registrieren, sondern wegen Kontakten soll das Konzept in ein bestehendes Netzwerk integriert werden und kein neues Netzwerk entwickelt werden.
3. Durch attraktiv gestaltete Grafiken, Illustrationen, Videos oder Tutorials muss der Benutzer in kurzer Zeit über die Vorteile des Konzepts informiert werden.
4. Die Fakeprofilerstellung muss automatisiert erfolgen. Den Nutzern muss die Möglichkeit gegeben werden Daten für die Generierung des Fake Profils zur Verfügung zu stellen. Den Nutzern muss bewusst gemacht werden, dass die Fake Profile durch die Angaben persönlicher (echter) Daten authentischer wirken.
5. Das Zurücksetzen des Passworts muss möglich sein.
6. Dem Nutzer muss eine große Anzahl an hinterlegbaren Authentifizierungsmechanismen zur Auswahl gestellt werden
7. Die Kommunikation mit Fake Profilen muss möglich sein. Das suchen von Profilen muss möglich sein. Aus Fake Profilen müssen alle Aktionen möglich sein, die auch mit echten Profilen getätigt werden können.

**Bewertung**:

Dieses Verfahren macht alle geklauten Daten nutzlos, da nicht sicher ob sie korrekt sind