Parallel World

Daniel Graf
Hochschule Mnchen
Mnchen
graf12@hm.edu

Ludwig Wagner
Hochschule Mnchen
Mnchen
wagner43@hm.edu

Dimitrie Diez
Hochschule Mnchen
Mnchen
diez@hm.edu

ABSTRACT
In der heutigen Zeit gibt es viele verschiedene Authentifizierungsverfahren, die den Menschen vertraut sind. Der Mensch nutzt heute verschiedene Plattformen und Devices um Informationen aufzubewahren oder mit anderen Personen zu teilen. Der Zugang zu diesen Daten muss durch Authentifizierungsverfahren bestmöglich geschützt werden. Die am häufigsten verwendeten Methoden sind E-Mail Adresse und Passwort. Bei zahlreichen Onlineplattformen, wie beispielsweise Yahoo, SchülerVZ oder Sony wurden Millionen Kundendatensätze gestohlen und im Darknet veröffentlicht. Somit fehlen Angreifern lediglich die Passwörter um in die Accounts zu gelangen. Angreifer versuchen häufig diese durch BruteForce Angriffe zu ermitteln. Dies ist möglich, da der Angreifer bei fehlerhaften Login Informationen informiert wird. Um dies zu verhindern wurde ein Konzept für einen Authentifizierungsvorgang entwickelt, bei dem der Angreifer genau diese Informationen nicht erhält. Das Konzept wurde für Social Networks ausgelegt, ist jedoch vielseitig, beispielsweise auch für E-Mail Accounts, verwendbar. Bei einem fehlgeschlagenen Authentifizierungsvorgang wird ein erfolgreicher Login, durch die Anzeige eines täuschend echt aussehenden Fake-Kontos, vorgetäuscht. Für die Umsetzung des Konzepts wurden verschiedene Handlungsempfehlungen erarbeitet und limitierende Faktoren aufgezeigt. Basierend auf diesen Aspekten erfolgt eine Bewertung des Konzepts hinsichtlich Sicherheit, Umsetzbarkeit und Benutzbarkeit.

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; AUS BENUTZERSICHT

KONZEPT dagegen ... Durch ein geschicktes Konzept wird dieser Angriffsvektor unterbunden. Konzept ursprünglich für Social Network jedoch vielseitig verwendbar Es lohnt sich nicht ein eigenes Netzwerk mit dem Konzept zu entwickeln Viele Leute sind nicht bereit

ACM Classification Keywords
H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous; See http://acm.org/about/class/1998/ for the full list of ACM classifiers. This section is required.

Author Keywords
Authors' choice; of terms; separated; by semicolons; include commas, within terms only; required.

EINLEITUNG
Einleitung mit einer Statistik über Angriffe und Sicherheitslücken aktueller Social Media Plattformen, Identifikation des Problems bei aktuellen Authentifizierungsverfahren (Der Angreifer weiss, dass Login fehlgeschlagen ist)

WEITERFHRENDE LITERATUR
jeder sucht Literatur zu diesem Thema und beschreibt Ergebnis in einem bis zwei Sätzen. Was haben andere rausgefunden? ISBN: 978-1-4799-6364-5 (IEEE Passwords are Dead)

BESCHREIBUNG DES KONZEPTS
Kernpunkt des Konzept ist die Erschaffung eines parallelen Fake-Netzwerkes. Dadurch soll verhindert werden, dass ein Angreifer in das Netzwerk gelangt oder Informationen über die Mitglieder des Netzwerkes gewinnen kann. Die Sicherheit wird somit durch Verwirrung erzeugt. Im folgenden wird der Aufbau des Netzwerkes anhand eines Login-Vorgangs beschrieben.
Auf der Startseite des Netzwerkes werden die Nutzer zunächst aufgefordert E-Mail Adresse und Passwort einzugeben, bevor sie zum zweiten Schritt der Authentifizierung gelangen. Hierfür muss jeder Nutzer bei der Registrierung eines, oder mehrere Authentifizierungsverfahren hinterlegen. Zur Auswahl stehen beispielsweise ein Code, welcher per SMS zugesandt wird, eine Push-Benachrichtigung am Mobiltelefon oder die Verwendung biometrischer Daten (z.B Fingerabdruck).
Unabhängig davon, ob E-Mail Adresse, Passwort, die Wahl des zusätzlichen Verfahrens oder die Durchführung des gewählten Verfahrens korrekt waren, gelangt der Nutzer in das Netzwerk. Doch nur im Falle eines vollständig korrekten Authentifizierungsvorgangs befindet sich der Nutzer in seinem Account im ëchten"Netzwerk. Andernfalls gelangt der Nutzer in ein täuschend echt aussehendes Fake-Profil, welches nur vom Inhaber als solches enttarnt werden kann.

Bild des Loginvorgangs

Der Angreifer erfährt dadurch weder ob seine eingegebenen Angaben korrekt waren bzw. welche nicht korrekt waren, noch

kann er sich sicher sein, ob er im echten Netzwerk ist. Sämtliche, für ihn sichtbaren Informationen sind folglich nicht verifizierbar und daher nahezu wertlos.
Die größte Herausforderung bei der Umsetzung des Konzeptes stellt die Generierung des Fake-Netzwerkes dar. Hierfür wurden 4 unterschiedliche Umsetzungsvarianten definiert, welche im Folgenden beschrieben werden.
In der ersten Variante, muss jeder Nutzer bei der Registrierung neben seinem echten Profil auch ein Fake Profil anlegen. Ob er hierbei korrekte oder falsche Angaben macht kann jeder Nutzer selbst entscheiden. Abbildung 1 zeigt ein Beispiel hierfür. Ziel dieser Variante ist es, möglichst authentische Fake-Profile

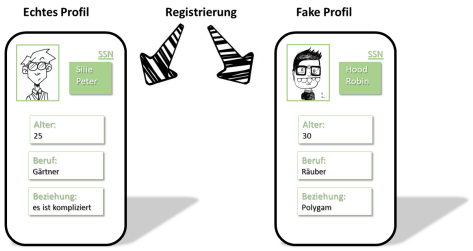

Figure 1. User legt das Fake Profil selbst an

zu erstellen. Je authentischer diese auf einen Angreifer wirken, desto sicherer sind die ëchten"Daten der Nutzer.
In der zweiten Variante erstellt der Nutzer lediglich sein echtes Profil. Er kann jedoch für jede Information, beispielsweise bei seinem Namen, seinem Alter oder seinem Profilbild durch setzen eines Hakens entscheiden, ob diese Information für die Erstellung des Fake-Profils verwendet werden darf, oder nicht. Restliche Daten werden durch das System zufällig generiert. Abbildung 2 veranschaulicht diese Variante. Dadurch sollen

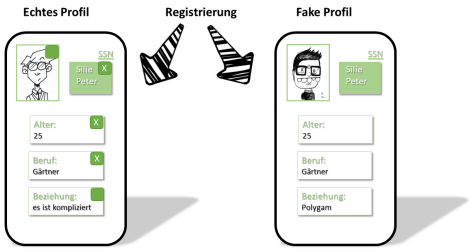

Figure 2. Vom User ausgewählte Informationen werden für die Fake-Profile verwendet.

durch die Zusatzangaben einerseits authentische Fake-Profile erzeugt werden können und andererseits der zeitliche Aufwand für die Nutzer reduziert werden.
In Variante 3 verläuft der gesamte Vorgang automatisiert. Der User hat keinen Einfluss auf die Erstellung der Fake Profile. Sie werden vm System m Hintergrund generiert. Der Ablauf ist in Abbildung 3 dargestellt.
Variante 4 stellt eine Kombination aus den bisherigen drei Varianten dar. Die Fake-Profile werden, analog zu Variante 3 automatisch generiert. Es besteht jedch für jeden Nutzer die Möglichkeit Daten, wie beispielsweise Bilder für die

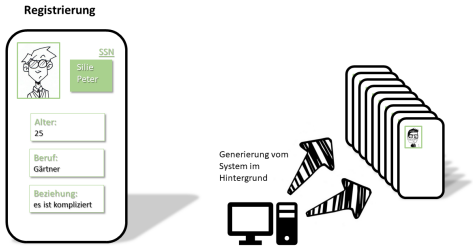

Figure 3. Fake-Profile werden vom System generiert.

Fake-Profil Generierung zur Verfügung zu stellen. Somit ist einserseits kein Nutzer gezwungen Daten bereit zu stellen, andererseits können authentischere Fake-Profile als z.B bei Variante 3 generiert werden.

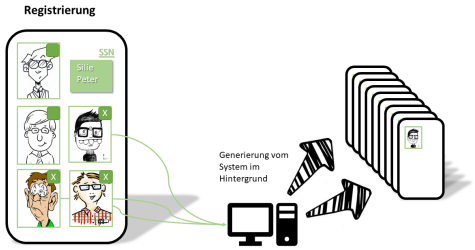

Figure 4. Fake-Profile werden vom System generiert. Der User kann freiwillig Daten zur Verfügung stellen.

METHODIK

Fokusgruppe
Aufbau der Umfrage, des Experimentes...

Einzelbefragungen
Aufbau der Umfrage, des Experimentes...

Ergebnisse
auch das Mindmap reinnehmen... Oder CLusterbildung... usw.

Diskussion der Herausforderungen bei der Umsetzung des Konzepts
Ergebnisse von Fokusgruppe + Einzelbefragungen, Diskussion der wichtigsten Aspekte

Handlungsempfehlungen
Lösungsansätze der vorher beschriebenen Probleme vorstellen. + Diskussion der Umsetzbarkeit

Speichern des Logins
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.

Integration in ein bestehendes Sozial Network statt Entwicklung eines neuen
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.

Klare Erluterung des Sicherheitskonzeptes
Durch attraktiv gestaltete Grafiken, Illustrationen, Videos oder Tutorials muss der Benutzer in kurzer Zeit über die Vorteile des Konzepts informiert werden.

Automatische und manuelle Fakeprofil Erstellung
Die Fakeprofil Erstellung 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.

Umgang mit Passwortverlust
Das Zurücksetzen des Passworts muss möglich sein.

Auswahl unterschiedlicher Verfahren fr die 2-Wege Authentifizierung
Dem Nutzer muss eine große Anzahl an hinterlegbaren Authentifizierungsmechanismen zur Auswahl gestellt werden

Kommunikation im Netzwerk
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.

ZUSAMMENFASSUNG UND FAZIT

Was wurde gemacht, Handslungsempf zusammenfassen.. Die Wichtigsten erläutern

AUSBLICK