SIGCHI Conference Proceedings Format

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 Brute-Force 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

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

INTRODUCTION

Statistik über Angriffe, Sicherheitslücken Was ist genau das Problem, welches gelöst werden soll. (Der Angreifer weiss, dass Login fehlgeschlagen ist)

RELATED WORK

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)

METHODIK

Idee beschreiben

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. 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 einen Authentifizierung mittels eines Codes, welcher per SMS zugesandt wird, mittels Push-Benachrichtigung am Mobiltelefon oder mittels biometrischer Daten. Unabhängig davon, ob E-Mail Adresse, Passwort, die Wahl des Verfahrens oder die Durchführung des Verfahrens korrekt waren, gelangt der Nutzer in das Netzwerk. Doch nur im Falle eines vollständig korrekten Vorgangs befindet sich der Nutzer in seinem Account im "echten" Netzwerk. Andernfalls gelangt der Nutzer in ein täuschend echt aussehendes Fake-Profil, welches nur vom Inhaber als solches enttarnt werden kann. 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. Welche Informationen er hierfür verwendet, ist ihm überlassen.
BILD
In der zweiten Variante erstellt der Nutzer lediglich sein echtes Profil. Er kann jedoch für jede Information, beispielsweise

dem Namen, seinem Alter oder dem 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. BILD
In der dritten Variante werden alle Fake-Profile automatisch generiert. Die Nutzer können den Prozess hierbei nicht beeinflussen. BILD
In der vierten Variante werden die Fake-Profile, analog zu Variante 3 automatisch generiert. Hierbei wird der Nutzer jedoch aufgefordert Bilder für die Fake-Profil Generierung zur Verfügung zu stellen. Dadurch soll erreicht werden, dass die Fake-Profile für einen Angreifer authentischer Wirken. BILD

Fokusgruppe

Aufbau der Umfrage, des Experimentes...

Einzelbefragungen

Aufbau der Umfrage, des Experimentes...

Herausforderungen bei der Umsetzung

Was hat die Befragung ergeben? Auswertung der Fokusgruppe.. Was sind die wichtigsten Punkte, Erkentnisse..

Vorschlge fr die Umsetzung

Lösungsansätze der vorher beschriebenen Probleme vorstellen.

Vorschlag 1
Vorschlag 2
Vorschlag 3

ZUSAMMENFASSUNG

AUSBLICK