Parallel World

Daniel Graf
Hochschule München
München
graf12@hm.edu

Ludwig Wagner
Hochschule München
München
wagner43@hm.edu

Dimitrie Diez
Hochschule München
München
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.

Quelle

Bei zahlreichen Onlineplattformen, wie beispielsweise Yahoo, SchülerVZ oder Sony wurden Millionen Kundendatensätze gestohlen und im Darknet veröffentlicht.

Quelle

Somit fehlen Angreifern lediglich die Passwörter um in die Accounts zu gelangen. Angreifer versuchen häufig diese durch BruteForce Angriffe zu ermitteln.

Quelle

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,

deutsch Soziale Netzwerke

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.

täuschend echt 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

CHI'16, May 07–12, 2016, San Jose, CA, USA

 ISBN 123-4567-24-567/08/06…$15.00

DOI: http://dx.doi.org/10.475/123_4

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

Authentifizierungsmechanismus; Fake-Profile; Authentifizierungskonzept; Parallel World

Überarbeiten/ weitere ergänzen

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)

WEITERFÜHRENDE LITERATUR

Literatur zu diesem Thema und beschreiben des Ergebnisses in einem bis zwei Sätzen. Was haben andere rausgefunden? ISBN: 978-1-4799-6364-5 (IEEE Passwords are Dead)
Überarbeitung der Copy Right (siehe anfang des tex Dokuments) Überarbeitung der Umlaute in den Kapitelüberschriften

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 „echten“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,

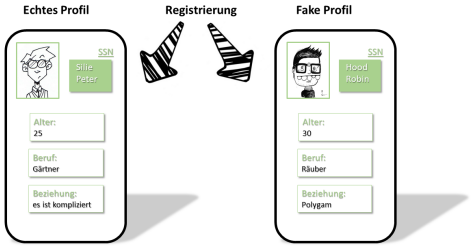

Figure 1. User legt das Fake Profil selbst an

möglichst authentische Fake-Profile 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 durch die Zu-

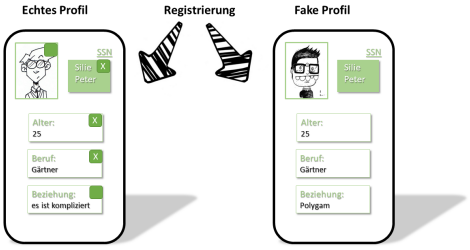

Figure 2. Vom User ausgewählte Informationen werden für die Fake-Profile verwendet.

satzangaben 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.

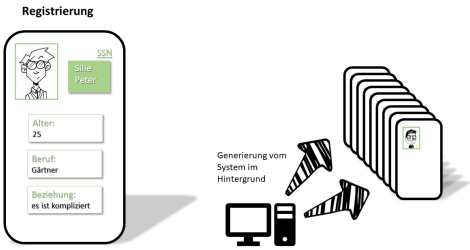

Figure 3. Fake-Profile werden vom System generiert.

Variante 4 stellt eine Kombination aus den bisherigen drei Varianten dar. Die Fake-Profile werden, analog zu Variante 3 automatisch generiert. Es besteht jedoch für jeden Nutzer die Möglichkeit Daten, wie beispielsweise Bilder für die Fake-Profil Generierung zur Verfügung zu stellen. Somit ist einerseits kein Nutzer gezwungen Daten bereit zu stellen, andererseits können authentischere Fake-Profile als z.B bei Variante 3 generiert werden. Eine Veranschaulichung dieser Umsetzungsvariante ist am Beispiel von Profilbildern in Abbildung 4 aufgeführt.

METHODIK

Für eine Diskussion, welche der Varianten bei Nutzern bevorzugt werden könnte und bei welchen Teilaspekten des Konzepts es möglicherweise Probleme bei der Umsetzung geben könnte, wurde eine Fokus Gruppe organisiert. Basierend auf den Ergebnissen der Fokus Gruppe

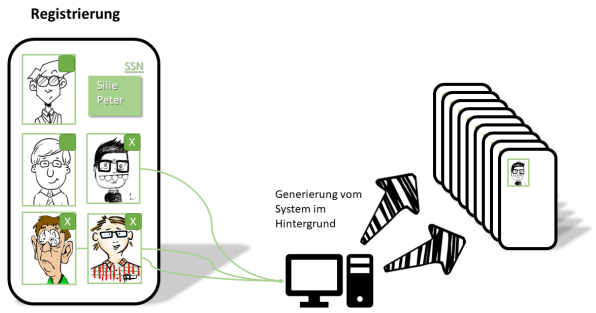

Figure 4. Fake-Profile werden vom System generiert. Der User kann freiwillig Daten zur Verfügung stellen.

wurden interessante Aspekte im Zuge einer Umfrage qualitativ vertieft. Sowohl für die Fokus Gruppe, als auch für die Umfrage wurden ausschließlich Personen in Betracht gezogen, welche mindestens ein soziales Netzwerk aktiv nutzen. Dadurch soll eine erhöhte Vergleichbarkeit zwischen dem Sicherheitskonzept herkömmlicher Netzwerke und dem in Kapitel 3 beschriebenen Konzept erzielt werden. In diesem Kapitel werden zunächst der Aufbau der Fokusgruppe (vgl. Abschnitt 4.1) und der Einzelbefragungen (vgl. Abschnitt 4.2) erläutert. Anschließend werden im Abschnitt 4.3 die Ergebnisse von beiden zusammengefasst. Im Abschnitt 4.4 werden mögliche Herausforderungen für die Umsetzung des Konzepts diskutiert, bevor schließlich im Abschnitt 4.5 konkrete Handlungsempfehlungen für die Umsetzung beschrieben werden.

Fokusgruppe

Die Fokus Gruppe bestand aus dem Projekt Team und 8 Studenten der Hochschule München. Zu Beginn der Fokus Gruppe wurden den Teilnehmern allgemeine Fragen zu sozialen Netzwerken gestellt und über potenzielle Schwachstellen bzgl. Sicherheit in vorhandenen Netzwerken diskutiert. Im zweiten Schritt erfolgte die Erläuterung der Konzeptidee und eine anschließende Diskussion bzgl. Machbarkeit, Usability und Sicherheit. Anschließend wurden den Teilnehmern stufenweise alle 4 Umsetzungsvarianten erläutert. Nach jeder Variante erfolgte erneut eine (kurze) Diskussion bezüglich der Machbarkeit, Usability und Sicherheit der jeweiligen Variante. Abschließend erfolgte eine freie Diskussion über die nicht berücksichtigten Aspekte und es wurden weitere Umsetzungsideen erfragt.

Einzelbefragungen

Insbesondere Aspekte, bei denen Uneinigkeit zwischen den Teilnehmern der Fokus Gruppe geherrscht hat, wurden im Zuge von Einzelbefragungen vertieft. Hierfür wurden insgesamt 9 Befragungen durchgeführt. Der gesamte Fragebogen ist im Anhang angefügt.

Fragebogen in Anhang

Ergebnisse

In Abbildung 5 ist ein Ausschnitt aus den Ergebnissen der Fokus Gruppe und der anschließenden Einzelbefragungen zu sehen. Die gesamten Ergebnisse sind in einem MindMap im Anhang aufgeführt. Die wichtigsten Aspekte sind im folgenden genauer beschrieben.

Mindmap in Anhang einfügen UND aufbereiten

Testen ob Mindmap lesbar ist, oder weiter gekürzt werden muss

1. Für die Usability des Netzwerkes ist es essenziell zu definieren, wann eine Authentifizierung des Nutzers erforderlich ist. Beispielsweise bei wiederholtem Login vom gleichen Gerät sagen die Teilnehmer von Fokus Gruppe und Umfrage einstimmig, darf keine erneute Authentifizierung gefordert werden.

2. Viele Teilnehmer sehen nicht das Sicherheitskonzept als ausschlaggebend, ob sie sich in einem Netzwerk registrieren würden. Andere Aspekte, wie Bekanntheit des Netzwerkes und Anzahl der registrierten Personen, insbesondere der jeweiligen Freunde, wird bei der Wahl eines Netzwerkes als bedeutend wichtiger angesehen.

3. Der tiefere Sinn dieses Sicherheitskonzeptes ist insbesondere für Personen ohne technische Kenntnisse meist nicht zu verstehen. Folglich wird nur der Mehraufwand bei der Registrierung oder beim Login in das Netzwerk betrachtet. Die Mehrheit der Personen ohne technischen Hintergrund empfangen folglich den Mehraufwand als unnötig. Für die Mehrheit der Personen mit technischem Hintergrund war das Ziel des Konzeptes offensichtlich. Diese wären auch mehrheitlich bereit einen gewissen Mehraufwand für eine erhöhte Sicherheit in Kauf zu nehmen. Andererseits beurteilte die Mehrheit der Teilnehmer, unabhängig vom technischen Hintergrund, die Sicherheit bestehender sozialer Netzwerke als nicht ausreichend.

4. Viele Teilnehmer gaben an, dass sie nicht bereit wären Daten für die Erstellung von Fake Profilen zur Verfügung zu stellen. Darüber hinaus wären auch nur wenige Teilnehmer bereit Zeit für die Erstellung und Verwaltung von Fake-Profilen zu investieren. Ca. 20% der Teilnehmer wären weder bereit Daten bereit zu stellen, noch Zeit für die Erstellung der Fake-Profile zu investieren.

5. Für die Umsetzung des Konzeptes ist zu klären, wie bei Passwortverlust vorgegangen werden soll. Insbesondere ein Zurücksetzen des Passworts über eine E-Mail wurde von vielen Teilnehmern als kritisch angesehen, da man die sicherere Authentifizierung in das Netzwerk und eine ëinfacheÄuthentifizierung mittels E-Mail und Passwort aushebeln könnte.

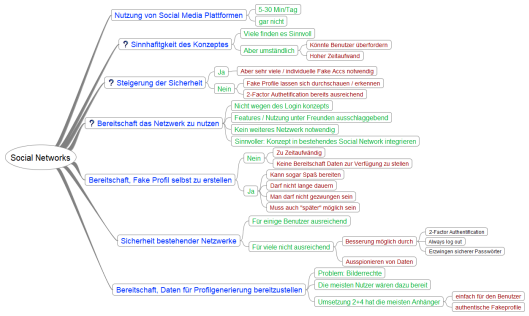

Figure 5. Ausschnitt aus den Ergebnissen von Fokus Gruppe und Einzelbefragung

6. Eine genaue Auflistung aller Verfahren für den zweiten Authentifizierungsschritt ist zu definieren. Viele Teilnehmer sehen eine Zwei-Wege Authentifizierung über ein Gerät, in der Regel das Mobiltelefon, als kritisch.

7. Insbesondere der Umgang mit den Fake-Profilen führte zu vielen Fragen und Diskussionen. Diese werden im Abschnitt 4.4 näher erläutert.

Diskussion der Herausforderungen bei der Umsetzung des Konzepts

1. Eine große Herausforderung bei der Umsetzung ist die Generierung der Fake-Profile. Einerseits wirken diese authentischer, wenn Mitglieder des Netzwerkes Daten hierfür bereit stellen. Andererseits ist nicht jedes Mitglied bereit Daten bereitzustellen sodass eine Generierung der Fake-Profile ermöglicht werden muss. Darüber hinaus ist es für eine wirkliche Verwirrung des Angreifers durch die sog. "Parallel World"nicht ausreichend, wenn es pro echtes Profil ein Fake-Profil (statische Generierung) gibt. Versucht ein Angreifer beispielsweise das Passwort für ein Konto zu erraten, muss er pro falsches Passwort in einem anderen Fake-Profil landen. Sonst kann ein Fake-Profil zu schnell als solches identifiziert werden. Es müssen folglich für jedes Profil alle falsch eingegebenen Passwörter (und weitere Authentifizierungsverfahren wie z.B falsche Codes) generiert, gespeichert und mit dem entsprechend erstelltem Fake-Profil verknüpft werden (dynamische Generierung).

2. Die Lösung der im vorherigen Punkt beschriebenen Herausforderung führt zu einem weiteren Problem. Gerade durch die Vielzahl möglicher Fake-Profile pro echtes Profil, muss eine große Menge Daten gespeichert werden. Dies führt zu einem enormen Bedarf an Speicherkapazität, was wiederum einen Anstieg der Kosten für den Betrieb eines solchen Netzwerkes bedeutet.

3. Auch mögliche Handlungen in die Fake-Profilen müssen ins Detail definiert und durchdacht werden, um die Verwirrung für den Angreifer aufrecht zu erhalten. Eine Kommunikation zwischen Fake-Profilen, sowie zwischen Fake- und echten Profilen muss aus Gründen der Tarnung möglich sein. Dies stellt jedoch eine Gefahr dar, da mittels des Fake-Profils z.B Nachrichten mit Links zu schadhaften Seiten versendet werden können. Andererseits muss sicher gestellt sein, dass jeder Nutzer aus seinem echten Profil auch die echten Profile seiner Kontakte finden kann. Werden aus einem Fake-Profil Nachrichten versendet, müssen diese ebenso wie erstellte oder angezeigte Statusnachrichten oder Bilder im entsprechenden Fake-Profil gespeichert werden. Gelangt man zu einem späteren Zeitpunkt erneut in das Fake-Profil, kann dieses ansonsten enttarnt werden. Es ist jedoch essenziell, dass der Zugriff auf persönliche Daten eines (echten) aus einem Fake-Profil unterbunden wird.

4. Es ist zu definieren, ob Fake-Profile mittels Suchmaschinen gefunden werden könnte. Beispielsweise kann nahezu jedes Facebook Profil z.B mittels google gefunden werden. Findet man jedoch lediglich echte Profile, können Fake-Profile auf diese Weise enttarnt werden. Eine mögliche und umsetzbare Lösung hierfür wäre, wenn jedes Fake-Profil alle öffentliche Informationen eines echten Profils verwendet. Sucht man nun nach dem Profil, ist es ausreichend wenn die öffentlichen Daten es echten Profils angezeigt werden. Da lediglich die öffentlichen Daten sichtbar sind, kann folglich nicht zwischen einem Fake- und einem echten Profil unterschieden werden.

5. Eine identifizierte Schwachstelle des Netzwerkes sind Personen, die das Mitglied (gut) kennen. Je besser jemand ein Mitglied des Netzwerkes kennt, desto einfacher ist es für diese Person ein potenzielles Fake-Profil dieser Person zu enttarnen. Grund hierfür ist, dass die Person möglicherweise Freunde, Bekannte oder Familienmitglieder des Mitgliedes kennt. Befindet sich die Person nun in einem potenziellen Fake-Profil in welchem sich keinerlei Nachrichten oder Bilder von besagten Personen befinden, kann dieses als Fake-Profil enttarnt werden. Eine direkte Lösung für diese Problematik konnte nicht identifiziert werden. Eine Art Brute-Force Schutz für die Konten, könnte die Ermittlung des echten Profiles jedoch erschweren. Werden Beispielsweise nur drei fehlgeschlagene Login Versuche pro Stunde zugelassen, steigert dies die Dauer für die Ermittlung des Passwortes enorm. Wird darüber hinaus eine weitere Authentifizierungsmethode (z.B Push-Benachrichtung auf das Handy oder Biometrische Daten) verwendet, steigt der Schutz nochmals

erheblich. Auch die Menge der Fake-Profile, welche gespeichert werden muss reduziert sich durch den Brute-Force Schutz erheblich.

Handlungsempfehlungen

Lösungsansätze der vorher beschriebenen Probleme vorstellen. + Diskussion der Umsetzbarkeit 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

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

What ist please ein Sozial Network... dann lieber Social Netzwerk

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 Erläuterung 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 für 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

Diese Arbeit beschäftigte sich mit der Umsetzung des Konzeptes aus der Sicht des Nutzers. Zusammenfassend lässt sich sagen, dass zwei wichtige Aspekte für die erfolgreiche Umsetzung dieses Konzeptes zu beachten sind. Zum einen ist es die möglichst einfache Einrichtung und Benutzung des Netzwerks durch den Nutzer. Dabei sollte der Nutzer möglichst wenig Einfluss in die Einrichtung der Sicherheit haben. Dadurch soll die Usability sichergestellt werden und gleichzeitig eine mögliche Fehleinrichtung durch den Nutzer verhindert werden. Die gewohnten Funktionen wie das Verschicken von Nachrichten oder das Teilen von Bildern dürfen durch das neue Konzept nicht eingeschränkt werden.

Dem gegenüber steht die Generierung von Fakeprofilen. Der Erfolg dieses Konzeptes hängt maßgeblich von der Generierung von möglichst authentischen Profilen ab. Die echte Welt und die Parallelwelt sind keine eigenständigen Konstrukte, sondern müssen mit einander kommunizieren. So können sich zum Beispiel die echten Profile und die dazugehörigen Fake-Profile die öffentlichen Daten teilen. Dabei müssen klare Schnittstellen zwischen echter und Parallelwelt geschaffen werden. Letztendlich lässt sich sagen, dass dieses Konzept in bereits bestehende Netzwerke integriert werden muss. Es hat sich gezeigt, dass Nutzer nicht bereit wären sich nur wegen diesem Sicherheitskonzept in einem Netzwerk zu registrieren.

Fehlt: Zusammenfassung und Fazit

AUSBLICK

Die Arbeit hat bei der Betrachtung des Konzeptes den Fokus auf den Nutzer gelegt. Es sind jedoch auch weiterführende Aufgaben bei der Umsetzung des Konzeptes notwendig. Das Angreifermodell muss genauer analysiert werden. Dabei gilt es zu betrachten, ob das Konzept robust gegen bereits bekannte Angriffsszenarien ist. Darüber hinaus ist es notwendig zu untersuchen, ob diese Konzept neue Angriffsszenarien eröffnet.

Viele Fragen stellen sich jedoch erst bei der technischen Umsetzung des Konzeptes. Dafür ist es notwendig einen Prototypen zu erstellen. Die ausgearbeiteten Angriffsmodelle sowie die Useability müssen dann an diesem Prototypen getestet werden.

Fehlt: QUELLEN