30. April 2021

Alexander Schmiedl, Nils Steinlein, Nastassia Vysotskaya, Johannes Gasthuber, Paul Gerhart, Rümeysa Gel, Tobias Krieg

Human Factors in Security and Privacy

Übungsblatt 01

Aufgabe 1 Users are not the enemy

1.1 Forschungsziele:

Der Fokus des Artikels liegt auf den menschlichen Einflüssen von Computer Security im hinblick auf Passwörtern. Das Ziel ist herauszufinden weshalb Sicherheitsrichtlinien von Menschen (in diesem Fall Arbeitnehmern) nicht bzw schlecht umgesetzt werden, welche Gründe dazu führen und welche Gegenmaßnahmen es gibt.

1.2 Motivation der Forschung:

Da viele Sicherheitssysteme nicht nutzerfreundlich designt sind scheinen sich viele Anwender nicht an die Sicherheitsmechanismen zu halten. Wenn das Problem der Nutzer verstanden ist, können nutzerfreundliche Systeme zu einer deutlich besseren Sicherheit führen.

1.3 Befragungsmethoden:

Es wurde ein Webbasierter Fragebogen genutzt um Daten über das Verhalten von Nutzern im Bezug auf Passwörter zu sammeln. Anschließend wurden semi-strukturierte Interviews geführt um Themen aus dem Fragebogen aufzuarbeiten und Informationen der Teilnehmer zu sammeln.

1.4 Teilnehmer der Studie:

Insgesamt gab es 139 Reaktionen auf den Fragebogen. Etwa die Hälfte von Angestellten der Organisation A einer Technologiefirma. Die andere Hälfte von Firmen Weltweit. In den Interviews wurden Mitarbeiter der Organisation A (Technologie) und der Organisation B (Baugewerbe) befragt. Man könnte annehmen, dass Angestellte einer Technologiefirma tendenziell besser mit dem Thema Cybersicherheit vertraut sind als andere.

1.5 Nutzer Strategien:

Passwort aufschreiben: Nutzer müssen sich viele unterschiedliche Passwörter für unterschiedliche Anwendungen merken und teilweise öfters wechseln. Daraus folgt eine verringerte Sicherheit da Angreifer den Zettel finden könnten. Schlechte(einfache) Passwörter: Die Anwender haben viele unterschiedliche Passwörter, die regelmäßig geändert werden müssen. Die Folge sind Passwörter die einfach zu erraten/cracken sind. Passwörter mit kleinen Veränderungen: Um Security Guidelines bei vielen Passwörtern zu erfüllen werden Passwörter die sich nur durch einzelnen Zahlen unterscheiden verwendet. Die Folge ist noch schlechtere Merkbarkeit der Passwörter was zum aufschreiben der Passwörter führt und wiederum die Sicherheit verringert.

1.6 Need to know:

Das need to know Prinzip kommt aus dem Militär und besagt, dass je mehr über ein Sicherheitssystem bekannt ist, desto einfacher es ist das System anzugreifen. Auf die IT Sicherheit angewendet wird den Nutzern also so wenig wie möglich über die genutzten Mechanismen gesagt um das System so vermeintlich Sicherer zu machen. Die Autorinnen sind der Meinung, dass fehlendes Wissen und Aufklärung auf Seite der Anwender der Grund für unsicheres Verhalten sind, und dass diese aufgrund ihrer Unwissenheit die Mechanismen missachten. Die Studie zeigt den Fall auf, dass die

Firmen ihre Passwörter von system auf benutzergeneriert umstellen, den Anwendern aber nicht die Sicherheitskriterien für sichere Passwörter nennen. Was wiederum zu unsicheren Passwörtern geführt hat.

1.7 Sicherheits- Bedrohungsmodelle:

Nutzer denken Passwort cracking sind Angriffe auf einzelne Persönlichkeiten und schätzen ihre in Platz im System als zu unbedeutend ein. Daraufhin missachten diese Personen oft die Sicherheitsmechanismen. Einige verstehen die ID im Authentifikationsprozess als eine andere Art Passwort welche sicher ausgewählt und gemerkt werden muss. Das verdoppelt die zu merkenden Daten was wiederum die Motivation der Angestellten senkt. Hier werden Smartcards oder Biometrische Merkmale als alternative zur ID vorgestellt. Die Folgen eines Security Breaches wird von einigen Nutzern bezüglich der vermeintlich unwichtigen Daten als nicht bedenklich eingeschätzt. Die Folge sind schlechte sicherung der Zugänge oder Daten.

1.8 Schlussfolgerung der Ergebnisse:

Die Sichereheitsfeatures sind nicht mit nach den Möglichkeiten des Benutzers Designt. Viele Mechanismen fordern einen großen Overhead an Arbeit die von vielen Arbeitnehmern nicht geleistet werden kann. Schlechte Kommunikation der Security Abteilung bezüglich der Mechanismen und deren Gründe sind ein Grund für den Motivationsverlust der Arbeiter. Sicherheits Workshops könnten die Menschen für das Thema IT Sicherheit sensibilisieren.

1.9 Ergebnisse in der Heutigen Zeit:

Viele Menschen haben immer noch wenig Berührungspunkte mit der digitalen Welt und sind dementsprechend unvorsichtig mit ihren Daten und Passwörtern. Themen wie social engineering sind durch social media immer populärer geworden. Oft müssen Angestellte sich immer noch viele Passwörter merken, auch wenn die Verbreitung von single sign on, Smart Cards, Two Factor Authentication und Passwort Managern stetig zunimmt. Viele (größere) Firmen bieten Workshops an, die das Thema IT Sicherheit verständlicher machen sollen.

1.10 Gefahren durch Forschung:

Die gesammelten Daten sollten nicht direkt mit den Angestellten in Verbindung gebracht werden. Ein eventuell schlechter Umgang mit dem Thema Sicherheit könnte für die betroffenen personelle Konsequenzen nach sich ziehen und eventuell zu Jobverlust, Mobbing oder Diskriminierung am Arbeitsplatz führen. Die gesammelten Daten könnten in den Händen von Kriminellen ein Sicherheitsrisiko für die Firmen darstellen und Optionen für Human Engineering oder anderes Hacking eröffnen. Gegenmaßnahmen: Ein annonymisieren bzw pseudonymisieren der Daten von Mitarbeitern und Unternehmen sollte von den Studienerstellern sorgfältig durchgeführt werden. Die Daten sicher speichern und den Zugriff einschränken. Keine Rückschlüsse auf Personen durch angegebene Daten zulassen.

Aufgabe 2 Passwortrichtlinien

2.1

Richtlinie A:
mögliche Zeichen: 26 [Kleinbuchstaben] + 10 [Ziffern] = 36
mögliche Passwortlängen: 8
Rechnung: $36^8 = 2,82 * 10^{12}$

Richtlinie B:

mögliche Zeichen: 26 [Kleinbuchstaben] + 10 [Ziffern] + 35 [Sonderzeichen] = 71
mögliche Passwortlängen: $10, 11, 12$
Rechnung: $71^{10} + 71^{11} + 71^{12} = 1,66 * 10^{22}$

Richtlinie C:
mögliche Zeichen: 26 [Kleinbuchstaben] + 26 [Großbuchstaben] + 10 [Ziffern] + 35 [Sonderzeichen] = 97
mögliche Passwortlängen: $6, 7, 8$
Rechnung: $97^6 + 97^7 + 97^8 = 7,92 * 10^{15}$

2.2

Passwörter pro Sekunde als Zehnerpotenz: 100 Millionen = 10^8

Durch die Vereinfachungen ergeben sich:

- $3 * 10^{12}$ mögliche Passwörter für Richtlinie A:

$$\begin{aligned} \frac{3*10^{12}}{10^8} \frac{PW}{PW\ pro\ Sekunde} &= 3 * 10^4 Sekunden \\ &= 8,33\ Stunden \end{aligned} \quad \big) : 3600\ Sekunden/Stunde$$

- $1.5 * 10^{22}$ mögliche Passwörter für Richtlinie B:

$$\begin{aligned} \frac{1.5*10^{22}}{10^8} \frac{PW}{PW\ pro\ Sekunde} &= 1.5 * 10^{14}\ Sekunden \\ &= 4,166 * 10^{10}\ Stunden \\ &= 1736111111\ Tage \\ &= 4756468,798\ Jahre \\ &= 4,76 * 10^6\ Jahre \end{aligned} \quad \begin{matrix} \big) : 3600\ Sekunden/Stunde \\ \big) : 24\ Stunden/Tag \\ \big) : 365\ Tage/Jahr \end{matrix}$$

- $8 * 10^{15}$ mögliche Passwörter für Richtlinie C:

$$\begin{aligned} \frac{8*10^{15}}{10^8} \frac{PW}{PW\ pro\ Sekunde} &= 8 * 10^7\ Sekunden \\ &= 22222,2222\ Stunden \\ &= 925,93\ Tage \\ &= 2,54\ Jahre \\ &= 2,54 * 10^0\ Jahre \\ &= 0,254 * 10^1\ Jahre \end{aligned} \quad \begin{matrix} \big) : 3600\ Sekunden/Stunde \\ \big) : 24\ Stunden/Tag \\ \big) : 365\ Tage/Jahr \end{matrix}$$

2.3

Durch die Vereinfachungen ergeben sich:

- $3 * 10^{12}$ mögliche Passwörter für Richtlinie A:

$$\begin{aligned} 3 * 10^{12}\ PW * 256\ Bits\ pro\ PW &= 7,68 * 10^{14}\ Bits \\ &= 9,6 * 10^1 3\ Byte \\ &= 96 * 10^0\ Terabyte \end{aligned} \quad \begin{matrix} \big) : 8\ Bits/Byte \\ \big) : 10^{12}\ Byte/Terabyte \end{matrix}$$

- $1.5 * 10^{22}$ mögliche Passwörter für Richtlinie B:

$$\begin{aligned} 1.5 * 10^{22}\ PW * 256\ Bits\ pro\ PW &= 3,84 * 10^{24}\ Bits \\ &= 4,8 * 10^{23}\ Byte \\ &= 4,8 * 10^{11}\ Terabyte \end{aligned}$$

$\big)$ *:8 Bits/Byte*

$\big)$ *: 10^{12} Byte/Terabyte*

- $8 * 10^{15}$ mögliche Passwörter für Richtlinie C:

$$\begin{aligned} 8 * 10^{15}\ PW * 256\ Bits\ pro\ PW &= 2,048 * 10^{18}\ Bits \\ &= 2,56 * 10^{17}\ Byte \\ &= 256000\ Terabyte \\ &= 2,56 * 10^{5}\ Terabyte \end{aligned}$$

$\big)$ *:8 Bits/Byte*

$\big)$ *: 10^{12} Byte/Terabyte*

2.4

Wenn man für eine Webseite zwischen Richtlinie A und C entscheiden müsste, würden wir Richtlinie C empfehlen. Da diese alle Zeichen erlaubt und nicht eine exakte Länge, sondern eine innerhalb eines Längenintervall verlangt, ist dies die benutzerfreundlichere Variante – gerade im kommerziellen Bereich, wo die Konkurrenz groß ist, ist dies ein wichtiger Aspekt. Auch vom Sicherheitsstandpunkt ist C besser, da hier die Zahl möglicher Passwörter größer ist.

2.5

Usability:
Die Usability von Richtlinie C ist vermutlich die beste, da User nicht eingeschränkt, was die Wahl ihrer Zeichen innerhalb des gesetzten Passworts angeht – weder Richtlinien A, noch B erlauben die Nutzung von Großbuchstaben. Zudem ist man bei der Richtlinie C etwas flexibler, was die Zeichenkettenlänge betrifft, da sie zwischen 6 und 8 liegen kann und sie in Richtlinie A fix bei 8 liegt. Richtlinie B hat zwar auch einen Toleranzbereich von 10 bis 12 Zeichen, allerdings ist eine kürzere Zeichenkette einfacher zu merken und verringert so unter Umständen das Risiko, das Passwort zu vergessen. Allerdings muss zu allen Richtlinien gesagt werden, dass sie alle eine zu geringe Maximallänge erlauben, da längere Passwörter, welche allerdings leicht einprägbar sind, nicht erlaubt sind.

Security: Richtlinie A scheint die am wenigsten sichere Richtlinie zu sein, da nur Kleinbuchstaben und Ziffern verwendet werden dürfen und die Länge auf genau 8 Zeichen festgelegt wird. Dies erleichtert selbstverständlich offline Attacken wie Brute-Force oder Dictionary-Attacken, da sie auch die geringste Anzahl an möglichen Passwörtern aufweist. Richtlinie C erlaubt zwar die meisten möglichen Zeichen, allerdings sind hier sehr kurze Passwörter erlaubt von 6 bis 8 Zeichen, weshalb es aus Security-Sicht einen geringeren Status als Richtlinie B erreicht. Zwar werden hier keine Großbuchstaben erlaubt, allerdings tritt hier das Intervall mit der größten minimalen Länge hervor und auch die Längenvarianz ist (mit der von Richtlinie C) die größte. Dadurch und durch den Fakt, dass hierbei die größte Anzahl an möglichen Passwörtern existiert, ist sie besonders für offline-Attacken geschützt.
Natürlich existiert der bessere Schutz vor offline Attacken nur, wenn vom Provider Salted Hashing verwendet wird. Ansonsten schützt auch das "beste"Passwort nicht vor einem Angriff.

Zusätzliche Maßnahmen: Eine Möglichkeit wäre Blacklisting: Häufige/triviale Passwörter wie 12345678 oder etwa eine Zeichenkette, welche den Website-Namen inkludiert würden somit verboten. Dies erschwert Dictionary Attacken. Zudem könnte man beispielsweise verlangen, von jeder erlaubten Zeichengruppe mindestens eines im Passwort zu inkludieren und das Passwort nicht mit einer Zahl enden zu lassen.

2.6

Bezüglich der Usability bewerten wir dies als kreative Idee, dem Nutzer einen Leitfaden für ein gutes Passwort zu geben. Allerdings müsste man den Nutzer bei der Passworteingabe daran erinnern, dass er unter Umständen daran denken sollte, dass bei dieser Website eventuell ein Merksatz als Passwort-Basis diene. Ansonsten ist es wahrscheinlich, dass der Nutzer vergisst, auf welcher Seite er dazu aufgefordert wurde, sich einen Merksatz heranzuziehen und vergisst sein Passwort trotzdem. Wenn es außerdem bei jeder Website stehen würde, müsste man sich unglaublich viele Merksätze einprägen, was auch schwierig ist.

Aufgabe 3 bcrypt

Aufgabe 4 John The Ripper

4.1 Wie lauten die Passwörter der Benutzer? Welcher Modus ist am besten geeignet, um das jeweilige Passwort zu knacken? Beschreiben Sie, woran das liegt.

- **felix**: fElIx (single)
- **christian**: abygurl69 (wordlist)
- **lena**: abc (incremental)
- **ben**: 1235 (incremental:Digits)

Der **single** Modus verwendet den User Login Namen und testet mithilfe von einschränkenden Regeln, um das Passwort möglichst schnell zu knacken. Für Felix ist dieser Modus am Besten, da das Passwort aus denselben Buchstaben wie der Benutzername besteht. Lediglich die Groß/Kleinschreibung ist verändert.
Der **wordlist** Modus verwendet eine Wordlist, in welcher das Passwort von Christian enthalten ist. Christians Passwort ist somit kompromitiert und sehr schnell zu knacken
Der **incremental** Modus läuft per default mit ASCII Zeichen. Somit ist er besonders gut geeignet, um ohne Vorwissen Passwörter zu knacken. Bei Lena funktioniert dies gut, da ihr Passwort sehr kurz und einfach ist. Für kompliziertere Passwörter und mit etwas Vorwissen/Glück kann man noch genauere Regeln definieren: z.B. john –incremental=alpha –mask='?u?w' –min-length=7 –max-length=9 pw
Der **incremental:Digits** Modus funktioniert bei Ben, da sein Passwort nur aus Zahlen besteht und somit perfekt geeignet zum Knacken ist.

4.2 Was können Sie aus Ihren Beobachtungen in Bezug auf die Eigenschaften eines guten Passwortes schließen?

Ein gutes Passwort verwendet nicht den Login-Namen oder sonstige öffentliche persönliche Informationen, da diese stark die Sicherheit des Passworts kompromittieren. Zudem sollten sie außergewöhnlich genug seien, sodass sie sich nicht auf Wordlisten enthalten sind (d.h. nicht Passwort, admin, abygurl69, etc.). Man sollte dem Angreifer kein Vorwissen über dass Passwort geben (mindestlänge, verschiedene Zeichenarten, etc.), um somit keine einschränkenden Regeln zum Knacken zu erlauben. Ebenfalls sollte man unbedingt möglichst verschiedene Zeichenarten und lange Passwörter verwenden, um nicht Opfer dieser einschränkenden Regeln zum Knacken zu werden. Sowas könnte z.B. bei Angriffen auf mehrere Personen passieren, wo der incremental:Lower Modus verwendet wird, wobei möglichst schnell viele schwächere Passwörter geknackt werden können.

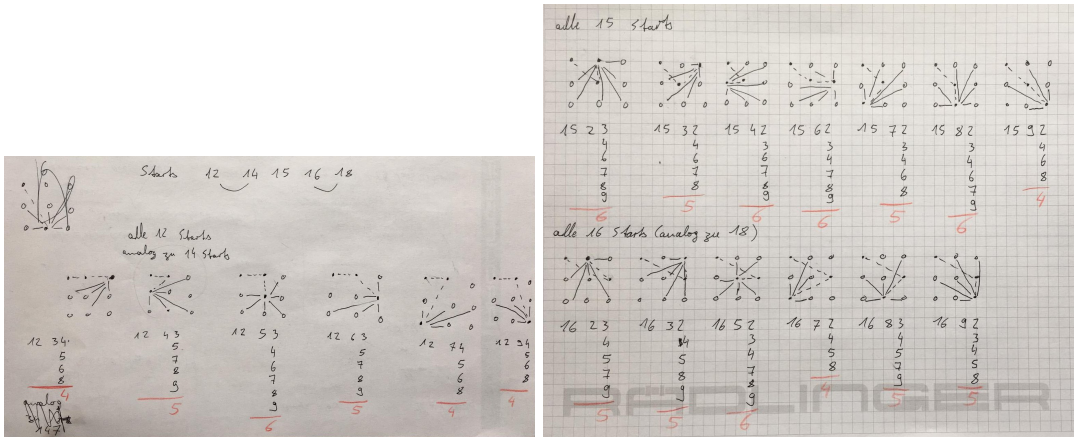

Abbildung 1: kombinatorisches Abzählen der Möglichkeiten

Aufgabe 5 Rainbow Tables

Aufgabe 6 Lock Patterns

6.1 Kombinatorische Aspekte

Entsperrmuster (in Bezug auf Nummerierung auf Abb. 1 der Angabe)

In 1 sind die Überlegungen der Möglichkeiten als grobe Skizze festgehalten. Als Startmöglichkeiten sind die Kombinationen 1-2, 1-4, 1-5, 1-6 und 1-8 möglich. 1-3, 1-7 und 1-9 sind nicht direkt möglich, da auf der geraden Linie zuerst über andere Knoten gelaufen wird, die zuerst markiert werden würden. Die Überlegungen für 1-2 und 1-6 können wegen der Symmetrie entlang der Diagonale für die Starts mit 1-4 bzw. 18 übernommen werden. Damit kommt man auf folgende Anzahl der Möglichkeiten:

$$\begin{aligned} anzahl(1-2)\cdot 2 + anzahl(1-5) + anzahl(1-6)\cdot 2 = \\ (4+5+6+5+4+4)\cdot 2 + (6+5+6+6+5+6+4) + (5+5+6+4+5+5)\cdot 2 = 154 \end{aligned} \tag{6.1}$$

PINn 4 Stellen, erste Ziffer ist 1
Anzahl an Möglichkeiten:

$$1 \cdot 10 \cdot 10 \cdot 10 = 1000 \tag{6.2}$$

6.2 Angriffsmöglichkeiten

- klassischer over-the-shoulder Angriff durch Zuschauen -> direktes Ablesen
- Finger hinterlässt Wischspur auf Bildschirm, wenn dann etwa nur entsperrt wird und nicht auf dem Bildschirm weitergewischt wird, kann der Angreifer den Weg des Musters nachvollziehen
- indirektes Abschauen/Eingrenzen der Möglichkeiten durch Beobachtung der Haltung der Hand, Bewegung des Fingers etc -> allerdings nur begrenzt möglich, da sich das Handy meistens nach zu vielen Fehlversuchen sperrt

6.3 Beispielstudie

zwei Gruppen: Nutzer mit PINn bzw. Lock Pattern Abfrage beim Entsperren des Smartphones Die Teilnehmer werden zu Studienbeginn einer Gruppe (PINn/Pattern) zugeordnet und legen demnach selbst entsprechend ihrer Gruppe einen PIN/Muster fest. Eine App zählt über die Ausführungsdauer der Studie die jeweilige Anzahl an Fehlversuchen bis zum erfolgreichen Entsperren mit (in Bezug

auf Usability der Sicherheitsmaßnahme).
Am Ende der Studie werden die PINns und Muster der Teilnehmer rein stochastisch/kombinatorisch auf Sicherheit ausgewertet. Dazu wird bei einem SZwischengespräch"wird unter nicht-Wissen der Teilnehmer ein over-the-shoulder-Angriff simuliert und auf Erfolg getestet.
Bei der Auswertung werden dann die verschiedenen Faktoren zusammengeführt und verglichen. Sprich, ist ein "rein mathematischßichereres Verfahren für solche Älltagsangriffszenarienäuch wirklich effektiver? Wie verhält es sich mit Benutzbarkeit zwischen den beiden Verfahren, auch im Zusammenhang mit dem Grad an Sicherheit?

Sicherheitsziele und Angreifermodell

- Sicherheitsziel: angemessener Grad an Äufwand"für den Nutzer für Schutz gegen älltäglicheÄngriffe auf Level eines over-the-shoulder Angriffs
- Angreifermodell: im Alltag ist der größte Anteil der Angriffsgefahr auf dem bloßen Zuschauen während des Entsperrens zuzuordnen, weswegen auch nicht stärkere Angreifermodelle in Betracht gezogen werden.

Messung der Sicherheit

- Erfolg des ßimuliertenöver-the-shoulder-Angriff
- mathematisch/kombinatorische Stärke des PINns/Musters

Messung der Benutzbarkeit

- Feedback der Nutzer in Fragebogen
- App auf den Geräten der Teilnehmer, die Fehlversuche beim Einloggen mitzählt

interne und externe Validität

- extern: wichtig zu beachten: wer sind die Studienteilnehmer? Alter? Erfahrung im Umgang mit Smartphones? Berufsfeld?
- intern: die interne Validität ist insofern schwierig zu gestalten, da hier viele Faktoren Einfluss haben können. Nur durch die Teilnahme an der Studie kann bereits schon ein Testeffekt entstehen (Teilnehmer denkt wählen eventuell bewusst ein sicheres Passwort anstatt z.B. einfach ihr Geburtsdatum). Dem könnte man vorbeugen indem man die PINns und Muster zu Beginn der Studie fest zuweist, hier wird dann allerdings Inferenz mit der Benutzbarkeit zu erwarten sein, wenn die Teilnehmer eben NICHT ihr Geburtsdatum zu merken haben, sondern eine zufällige Zahlenfolge.
  Unter Beachtung dieser Aspekte müssen solche Entscheidungen bewusst im Voraus getroffen werden und mögliche Effekte bei der Auswertung in Betracht gezogen werden.

ethische Grundsätze

- ???