Inhalt

[Gliederung 2](#_Toc410401078)

[Notizen (soch): 5](#_Toc410401079)

[SourceTree: 5](#_Toc410401080)

[GitHub: 5](#_Toc410401081)

[Android Studio: 6](#_Toc410401082)

[1. Einleitung (soch) 7](#_Toc410401083)

[1.1 Ausgangssituation 7](#_Toc410401084)

[1.2 Projektziel 7](#_Toc410401085)

[1.3 Projektabgrenzung 7](#_Toc410401086)

[2. Planung (soch) 7](#_Toc410401087)

[2.1 Geplante Programmentwicklung 7](#_Toc410401088)

[2.2 Geplanter Werkzeugeinsatz 7](#_Toc410401089)

[3. Realisierung 7](#_Toc410401090)

[3.1 Werkzeuge 7](#_Toc410401091)

[3.1.1 GitHub (soch) 7](#_Toc410401092)

[3.1.2 SourceTree (soch) 7](#_Toc410401093)

[3.1.3 Android Studio (lhu) 7](#_Toc410401094)

[3.1.4 Gradle (lhu) 7](#_Toc410401095)

[3.1.5 Unit Testing (lhu) 7](#_Toc410401096)

[3.2 Projektverlauf (nfe) 7](#_Toc410401097)

[4. Bewertung 7](#_Toc410401098)

[4.1 Bewertung der Werkzeuge (lhu) 7](#_Toc410401099)

[4.1.1 GitHub 7](#_Toc410401100)

[4.1.2 SourceTree 7](#_Toc410401101)

[4.1.3 Android Studio 7](#_Toc410401102)

[4.1.4 Gradle 7](#_Toc410401103)

[4.1.5 Unit Testing 7](#_Toc410401104)

[4.2 Bewertung des Projektverlaufs (mkerk) 8](#_Toc410401105)

[4.3 Fazit (alle zusammen) 8](#_Toc410401106)

[5. Ausblick (lhu) 8](#_Toc410401107)

[6. Abbildungsverzeichnis 8](#_Toc410401108)

[7. Quellen 8](#_Toc410401109)

**Notizen von mkerk in rot**

**Notizen von nfe in lila**

**Gliederung:**

* **Aufgabenstellung, Anwendungshintergrund**
* Entwicklung einer App zur Passwortverwaltung
* Sicher (Verschlüsselt, Automatische Generierung)
* Mobil (Deshalb eine App für’s Smartphone)
* Zunehmende Technisierung führt zu vermehrtem Aufkommen von Passwörtern, die verwaltet werden sollten
* Nicht nur Verwaltung sondern auch Nutzung soll erleichtert werden (Copy-Funktion)
* Stabilität der App soll gewährleistet sein
* Backup Funktion (Vergleich Zettel vs. XML-Datei)
* Ein weiteres Ziel des Projekts war die Einarbeitung in die Entwicklung von Android Apps
* Eine Anwendung entwickeln, bei der man Softwaretools einsetzt
* Bei uns konkret: Neuentwicklung einer Android App zur Passwortverwaltung „PWSafe“
* Sichere Verwaltung von eigenen Passwörtern auf dem mobilen Android-Gerät
* das Generieren sicherer Passwörter
* das Ver- und Entschlüsseln der gespeicherten Passwörter
* das Speichern und Lesen von Passwörtern
* **Projektergebnisse**
* eine lauffähige App produziert: die Grundfunktionen umgesetzt
* habe Android-Entwicklung grob kennengelernt: Fokus auf Design einer Maske und Aufrufen einer neuen
  + **Architektur / GUI**
  + Bei der Generierung von Passwörtern ist es derzeitig nicht möglich die zu verwendende Zeichenmenge und die Länge des Passworts anzugeben
    - Wurde nicht umgesetzt, da die Daten zur Generierung von Passwörtern über die Laufzeit der App hinaus in eine zusätzliche Datei mit Einstellungen geschrieben und hieraus wieder gelesen werden müssten
    - Da es neben diesen Einstellungen keine weiteren gab wurde eine feste Zeichenmenge mit Klein-, Großbuchstaben, Sonderzeichen und Zahlen gewählt und die Länge des Passworts fest auf 16 gesetzt
  + Eine Ampel zur Anzeige der Passwortsicherheit wurde nicht implementiert
    - Lediglich bei manuell erstellten Passwörtern ist dies sinnvoll, wenn ein möglicher Angreifer weiß, dass ein bestimmten Passwort manuell erstellt wurde
    - In diesem Fall ist ein Brute-Force Angriff oder sogar ein Wörterbuchangriff durch raten des Masterpassworts möglich
    - Wenn das zuvor manuell erstellte Passwort nicht kryptisch ist und einen Sinn ergibt ist mit hoher Wahrscheinlichkeit das Masterpasswort gefunden und somit sind alle anderen Passwörter auch unsicher
    - Ein direkter Angriff auf das Masterpasswort bringt nichts, da ein Angreifer keine Rückmeldung zur Korrektheit des Passworts erhält
    - Dies hier stellt eine Randsituation dar, weshalb dieses Feature nicht implementiert wurde
  + Wenn ein Passwort in die Zwischenablage kopiert wird, wird es nicht automatisch nach einer bestimmten Zeit wieder hieraus gelöscht
  + Zum Ändern und Löschen der Passwörter ist kein Bearbeitungspasswort möglich
    - Das Merken eines zweiten Passworts wird für den User möglicherweise als lästig empfunden
    - Die Sicherheit, dass keine Passwörter verloren gehen wird hier durch regelmäßige Backups sichergestellt
    - Hierzu sollte die XML-Datei mit den verschlüsselten Passwörtern regelmäßig durch den User gesichert werden
  + Die App ist für die Verwendung auf einem Smartphone optimiert
    - Da Tablets weniger mobil sind wurde hier der Schwerpunkt gelegt
* Eine Aktivität für Eingabe Masterpasswort
* -> Eine Aktivität für Liste mit Passwörtern, Funktionen „Neu“ und Details anzeigen
* Außerdem Settings-Aktivität zum Ändern des Masterpassworts
* Eine Aktivität zum Anzeigen von Details bzw. Neuanlage eines Passworts
* Dort auch Möglichkeit zur Generierung eines zufälligen Passworts und Kopieren des Passworts in die Zwischenablage
  + **Ggf. UML-Diagramme, Screenshots**

s. Repository

* **Projektverlauf**
* Es wurde ein inkrementelles Vorgehen zur Entwicklung der App gewählt
* Die Meilensteine wurden grob nach den Veranstaltungen in Software Engineering ausgerichtet
  + **Besonderheiten**
  + (Siehe Projekttagebuch in den Notizen)
  + Niemand von uns hat bisher Android entwickelt
  + Der Start war recht träge, im neuen Jahr ging es dann besser voran
  + **Schwierigkeiten**
  + (Siehe Projekttagebuch in den Notizen)
  + Zusätzlich: Den Anfang zu finden war schwer: generell und auch als Michaels erster Ansatz schon stand

**In Anhang etc.:**

* **Reflexion Vorgehen**
  + **Was würden wir beim nächsten Mal anders machen?**
  + Mehr auf die Umsetzung von fachlichen Anforderungen achten anstatt die Entwicklung nach technischen Themengebieten auszurichten
    - Das heißt zu Beginn eines Sprints festlegen, welche fachlichen Anforderungen umzusetzen sind und diese als Gruppe umsetzen (Sinnvolle Aufgabenteilung)
    - So entstehen keine technischen Abhängigkeiten und der Blick auf die geforderten Anforderungen geht nicht verloren
  + Mich etwas früher damit befassen, ein anderes Merge-Tool aussuchen
  + **Was war gut?**
  + Anwendung eines inkrementellen Vorgehens da wir den Aufwand zur Entwicklung von Android Apps anfänglich nicht beurteilen konnten
  + Regelmäßige Absprachen ähnlich den Planning Meetings im Vorgehensmodell Scrum
  + Dass jeder seinen Teil beigetragen hat
  + Dass man sich in den Vorlesungen immer mal wieder absprechen konnte
* **Reflexion Tool Einsatz**
  + **Welche Werkzeuge waren hilfreich? Welche nicht?**
  + Git als VCS hatte für unsere Gruppe hauptsächlich den Vorteil, dass es ein zentral verfügbares Repository gab in dem wir unsere Entwicklungsstände zusammenführen konnten
    - Paralleles Arbeiten fand nur in sehr seltenen Fällen statt, wodurch fast keine Merge Konflikte auftraten
    - Die Möglichkeiten von Git als DVCS wurden nicht in Anspruch genommen, da dies den anfänglichen Einstieg nur erschwert hätte (Stichwort: Commit)
  + Aufbauend auf Git als VCS wurde als grafische Oberfläche SourceTree verwendet
    - Gute grafische Aufbereitung der Veränderungen im Repository
    - Weitesgehend intuitive Nutzung
    - Leider wird kein Merge Tool mit ausgeliefert (Allerdings kann mit ein wenig Aufwand ein externes Merge Tool angebunden werden)
    - Die Nutzung von Git Flow zur automatisierten Verwaltung der Branches schlug fehl, da dies in Verbindung mit dem neuen VCS wahrscheinlich Verwirrung schaffte
  + Da die App mit dem Nutzer über visuelles Feedback wie Meldungsfenster kommuniziert war die Implementierung von Logging nicht sinnvoll
  + Unit Tests wurden nur für die Ver- und Entschlüsselung geschrieben, da hierfür keine Drittkomponenten verwendet wurden und so sichergestellt werden musste, dass der Algorithmus korrekt funktioniert
    - Die anderen Funktionen der App wurden durch Tests nach der Umsetzung der einzelnen Funktionen getestet
  + Android Studio war ganz gut, die Konsolen fand ich aber unübersichtlich; das Update war mies, weil Gradle dann auch nicht mehr passte
  + SourceTree bringt für Versionskontrolle nur bedingt was, zum mergen unpraktisch
  + Gradle lief gut, ich habe es aber auch nicht konfiguriert etc.

# Notizen (soch):

## SourceTree:

* Bekommt nicht immer mit, wenn das Respository veraltet ist
* Keine Mergefunktionen

## GitHub:

* Schön, dass kostenloses Zusammenarbeiten so einfach möglich ist
* In kostenloser Version leider für jedermann einsehbar
* Ermöglicht sehr einfache Zusammenarbeit unabhängig vom Standort

## Android Studio:

* In zuerst installierter Version ein wenig fehlerhaft
* Die IDE sollte nicht ohne Absprache aller Beteiligter gehoben werden, da es sonst zu Problemen kommen kann (beispielsweise wird Android Gradle Version mit geupdated, ohne dies zu bestätigen)
* Kostenlos
* Theoretisch direkte GitHub Anbindung möglich
* Umständliches Gestalten der Benutzeroberfläche, da Benutzeroberfläche als XML gespeichert wird und die Ausrichtung eines Elementes immer auf ein anderes Element referenziert wird (sei es Rand, Textbox, Icon etc.)
* UIs hängen sehr stark von Bildschirmgröße ab und verhalten sich auf verschieden großen Smartphones/ Tablets sehr unterschiedlich 🡪 hoher Aufwand zur Gestaltung eines User Interfaces

# Einleitung (soch)

# Ausgangssituation

# Projektziel

# Projektabgrenzung

# Planung (soch)

# Geplante Programmentwicklung

# Geplanter Werkzeugeinsatz

# Realisierung

# Werkzeuge

# GitHub (soch)

# SourceTree (soch)

# Android Studio (lhu)

# Gradle (lhu)

# Unit Testing (lhu)

# Projektverlauf (nfe)

Die erste Besprechung bezüglich des Projekts fand am 10. Oktober 2014 in der Vorlesung Software Engineering statt. Die Gruppenkonstellation war schnell gefunden, da sie sich schon in anderen Arbeiten bewährt hatte. Als Thema wurde aus Ermangelung von kreativen Alternativen zunächst eine Anwendung zum Benchmarking von Datenbanken gewählt. Da die Gruppe davon jedoch nicht gänzlich überzeugt war, wurde noch nach einem anderen Thema gesucht. Es kam schließlich der Vorschlag, eine Android App zur Passwortverwaltung nach Vorlage eines bestehenden Produkts zu entwickeln. Dieser Vorschlag wurde von den anderen Gruppenmitgliedern angenommen und am 26. Oktober wurde die Entscheidung durch Prof. Dr. Convent bestätigt.  
Bei der nächsten Absprache in der Vorlesung am 14. November 2014 wurden die Entwicklungsumgebung sowie die sonstigen benötigten Tools bei allen installiert und eingerichtet, dabei wurde sich gegenseitig unterstützt. Dann wurde die Absprache getroffen, sich bis zur nächsten Vorlesung etwas in die Android-Entwicklung einzulesen und sich ein wenig mit den Tools vertraut zu machen. Außerdem wurde ein grober Entwurf der App erstellt. Dieser umfasste drei Masken: eine zur Eingabe des Masterpassworts, eine zur Anzeige der gespeicherten Passwörter und eine zum Hinzufügen neuer Passwörter. Dieser Grobentwurf sollte zu ersten Erfahrungen mit der App-Entwicklung und einer Diskussion über das Design führen. Passwörter wurden noch nicht auf dem Handy gespeichert und es wurde auch noch keinerlei Verschlüsselung verwendet. Das eingegebene Masterpasswort wurde ebenfalls nicht weiter benutzt.

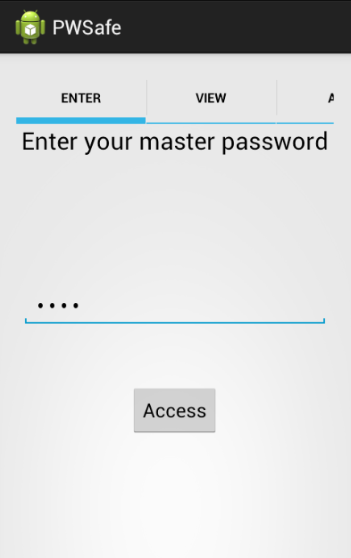
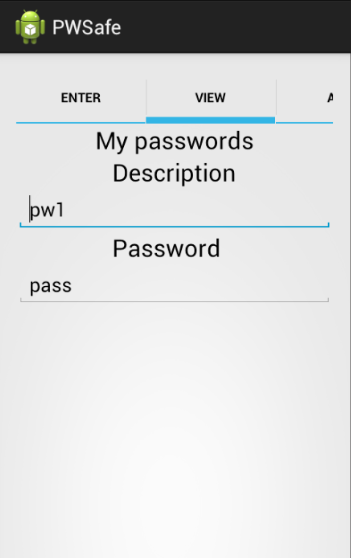
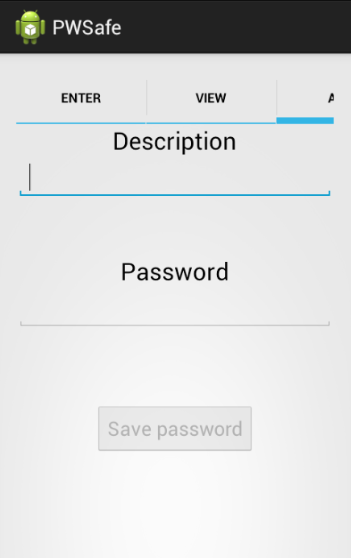
  

Abbildung 1-3: Erster Entwurf

Wie man auf Abbildung 1 bis 3 sieht, ist das Design noch nicht bildschirmgerecht. Außerdem traten bei der Ausführung noch Exceptions auf, weil Elemente im Formular nicht gefunden werden konnten.  
Am 29. November erfolgte die nächste Absprache im Rahmen der Vorlesung. Hier wurde der Entwurf gemeinsam betrachtet und es wurden Überlegungen für ein Re-Design angestellt.

Grafik Design-Plan

Als nächstes wurden die angesprochenen Exceptions beseitigt und die Namensgebung der Elemente wurde optimiert. Weiterhin wurden die Abhängigkeiten der Elemente untereinander verändert. Das Ziel einer ersten lauffähigen Entwurfs-Version wurde damit erreicht.  
Am 13. Dezember 2014 fand eine erneute Besprechung im Rahmen der Vorlesung statt. Zwischen diesem Termin und dem neuen Jahr gab es keine Aktivitäten im Projekt, diese „Weihnachtspause“ war vorher so abgestimmt worden.  
Am 02. Januar 2015 ging es dann weiter: Da der Code für den ersten Entwurf von einer Person erstellt wurde, mussten sich die anderen in diesen einlesen, um ihn nachvollziehen und erweitern zu können. Bis zum 07. Januar wurden das Re-Design durchgeführt: Die drei Tabs wurden aufgelöst und die bisherige Codestruktur wurde überarbeitet. Der Code war bisher vollständig in einer „Aktivität“ (eine Art Klasse für eine Maske in Android) gehalten. Dieser wurde nun auf mehrere Aktivitäten, eine pro Maske, aufgeteilt. Das neue Design hat wir vorher skizziert eine Start-Maske mit einem Eingabe-Feld für das Masterpasswort. Mit einem Klick auf den Button kommt man nun auf die Listenansicht der gespeicherten Passwörter und über den +-Button in der oberen Leiste lassen sich neue Passwörter anlegen. Es wurde außerdem ein „Settings“-Button implementiert, der ebenfalls im Menü der oberen Leiste enthalten ist und auf eine Maske zur Änderung des Masterpassworts führt. Der Button zum Kopieren in die Zwischenablage sowie die Ampel zur Anzeige der Passwortqualität wurden (noch funktionslos) angelegt. Die bisherige Liste der Passwörter wurde insofern erweitert bzw. geändert, dass nun nur noch die Beschreibung in der Liste angezeigt wird und man mit einem Klick auf einen Eintrag auf die Detail-Maske mit den Daten des Passworts gelangt.  
Am 07. Januar hat ein Gruppenmitglied ein angebotenes Update für das Android Studio durchgeführt, was zu Komplikationen führte: Durch das Update war das Projekt mit der bisherigen Gradle Version nicht mehr lauffähig, wodurch einige Konfigurationen angepasst werden mussten. Außerdem mussten die weiteren Gruppenmitglieder das Update dann nachziehen, damit alle daran weiterentwickeln konnten.   
Am 09. Januar wurde außerdem der SplashScreen, also der Startbildschirm, der kurz beim Öffnen der App erscheint, erstellt, sowie das Launcher-Icon ausgetauscht. Bisher hatte die App nur das Standard Android-Icon, dies wurde nun durch ein grünes Schloss ersetzt.  
Als nächstes wurde die Anwendung so erweitert, dass zu jedem Passwort neben der Beschreibung nun auch ein Benutzername eingegeben werden kann. Außerdem wurde nun mit der Speicherlogik angefangen: Ab sofort werden beim Betätigen des "Access"-Buttons auf der ersten Maske die zuvor gespeicherten Daten aus einer XML-Datei ausgelesen, die beim Hinzufügen eines neuen Datensatzes aktualisiert wird.  
Am 10. Januar erfolgte die nächste Absprache im Rahmen der Vorlesung in Bocholt. Hier wurden die noch umzusetzenden Erweiterungen geplant und unter den Gruppenmitgliedern aufgeteilt. Die geplanten Erweiterungen umfassten die tatsächliche Nutzung des eingegebenen Masterpassworts. Dazu musste die Verschlüsselung der Passwörter sowie das Ändern des Masterpassworts umgesetzt werden. Außerdem wurde geplant, eventuell Unit-Tests für die Verschlüsselungslogik zu erstellen. Für die Detail-Maske von Passwörtern wurden ebenfalls Änderungen vorgesehen: Die angefangene „Qualitäts-Ampel“ sollte wieder entfernt werden, da sie nicht mehr wichtig erschien. Außerdem sollte der „Copy to Clipboard“-Buttons mit Funktion versehen und ein Button zur Generierung zufälliger Passwörter erstellt werden. Des Weiteren sollte das eigentliche Passwort von nun an bei Öffnen der Detail-Maske nicht lesbar sein, ein zu implementierender „Show“-Button sollte die Zeichen dann sichtbar machen. Als Deadline für all diese Punkte wurde der 17. Januar definiert.  
Was zur Verschlüsselungswahl sagen  
An diesem Tag fand das nächste Treffen zur Vorlesung statt und die aktuelle Lage wurde besprochen. Jeder hat von seiner Umsetzung berichtet und bis auf die Änderung des Masterpassworts und die Unit-Tests wurden alle Funktionen umgesetzt. Dann wurde erneut geklärt, was im nächsten Schritt, der letzten Stufe, noch umzusetzen war. Das Ändern des Masterpassworts, das Löschen von gespeicherten Passwörtern sowie die Umsetzung der Unit-Tests sollten implementiert werden. Daher wurden diese Aufgaben besprochen und auf die Mitglieder aufgeteilt. Daneben sollten sich alle Gruppenmitglieder Notizen zu allen Punkten der bisher groben Gliederung der Dokumentation machen, sodass die Erfahrungen aller möglichst leicht in die Dokumentation einfließen konnten. Als Deadline hierfür wurde der 24. Januar definiert.  
Dies wurde umgesetzt. Bei Eingabe eines neuen Masterpassworts wird die XML-Datei nun mit dem alten Masterpasswort ausgelesen und mit dem neuen verschlüsselt geschrieben Außerdem wurden die Buttons auf der Detail-Maske umsortiert, da sie nicht auf allen Testgeräten korrekt angezeigt wurden.

Insgesamt wurde also ein inkrementelles Vorgehen zur Entwicklung der App gewählt. Die Meilensteine wurden dabei grob nach den Veranstaltungen in Software Engineering ausgerichtet.

Weitere Screenshots einbinden

Einträge nochmal mit Git abgleichen

# Bewertung

# Bewertung der Werkzeuge (lhu)

# GitHub

# SourceTree

# Android Studio

# Gradle

# Unit Testing

# Bewertung des Projektverlaufs (mkerk)

# Fazit (alle zusammen)

# Ausblick (lhu)

# Abbildungsverzeichnis

# Quellen