Berner Fachhochschule
Hochschule für Technik und Informatik

Abteilung Informatik
Diplomarbeit

Autoren: Graber Johnny, Müdespacher Andreas
Thema: Sicherheitstool für USB-Sticks
Datum: 23. Oktober 2006

geht an: Dubois Jean-Paul
Fuhrer Claude

Projekthandbuch

AtaraxiS

Dok.-Nr:	2
Version:	1.2
Status:	Abgeschlossen
Klassifizierung:	intern
Ausgabedatum:	14. Dezember 2006
Projektbeginn:	23. Oktober 2006
Projektende:	15. Dezember 2006
Dok.-Name:	Projekthandbuch_AtaraxiS.pdf
SVN-Ablage:	/documents/

1 Inhaltsverzeichnis

2 Zweck des Dokuments

Das Projekthandbuch dient als einheitliche Handlungsgrundlage für alle Projektbeteiligten und legt damit den allgemeingültigen technischen und organisatorischen Rahmen fest.
Das Projekthandbuch ist soweit als möglich als statisches Dokument zu führen. Dennoch ist es zu Beginn und am Schluss jeder Phase zu überprüfen und an die neuen Erkenntnisse anzupassen.

3 Projektbeschreibung

3.1 Ausgangssituation

USB-Sticks werden immer beliebter. Die Speicherkapazität wächst rasant, die Preise sinken und das Handling ist sehr einfach. Dies führt dazu, dass immer mehr Leute Dateien darauf abspeichern und damit transportieren.

Was passiert, wenn man so einen Stick verliert? Nicht nur die Hardware geht verloren, auch die Daten, die sich darauf befanden. Je wichtiger diese Dateien waren, desto grösser wird die Ungewissheit, was mit ihnen passiert. Werden sie von einem Finder unversehrt zurückgebracht? Werden die Dateien gelöscht? Oder werden sie gar detailliert untersucht?
Dies wird man erst erfahren, wenn es zu spät ist. Als Vorsorge für so einen Fall würde eine Verschlüsselung der darauf abgespeicherten Dateien helfen. So verliert man im schlimmsten Fall die Hardware, die Daten aber blieben geschützt.

Es gibt ein grosses Bedürfnis nach einem einfach zu handhabenden Programm für die Dateiverschlüsselung. Bisher erhältliche Programme sind aber an spezifische USB-Sticks gebunden, laufen nur auf einem Betriebssystem oder benötigen zusätzliche Software, die auf jedem PC installiert sein muss, bevor man die Verschlüsselung nutzen kann.

Mit der Diplomarbeit AtaraxiS wollen wir ein Programm zur Steigerung der Datensicherheit von USB-Stick Benutzern schreiben. Es soll unabhängig von Betriebssystemen funktionieren und keine Installation von zusätzlicher Software ausserhalb des USB-Sticks benötigen.

3.2 Ziele

In der Projektarbeit wurde von uns die zur Verschlüsselung notwendigen Basisklassen sowie ein erster Prototyp für die Dateiver- und Entschlüsselung erstellt. In der Diplomarbeit wollen wir auf den Ergebnissen der Projektarbeit aufbauen und AtaraxiS um die untenstehenden Punkte ergänzen.

Wir unterscheiden zwischen 2 Arten von Zielen:

- Muss-Ziele (M), die in der Diplomarbeit erreicht werden müssen
- Kann-Ziele (K), die als Vertiefung angegangen werden können

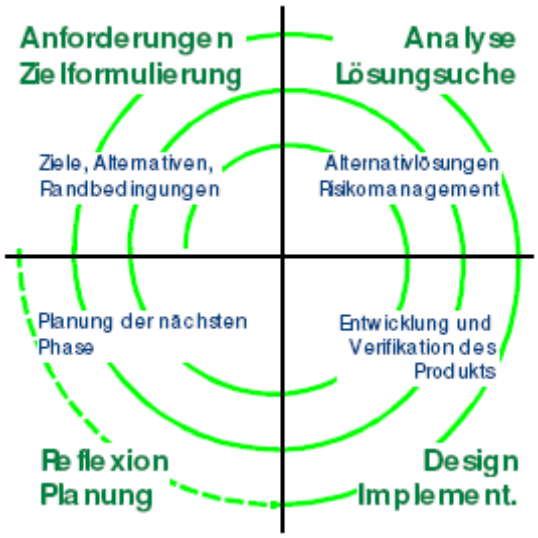
Nummer	Ziel	Art
1.1	mehrsprachiges GUI	M
1.2	Taskbar-Icon mit den wichtigsten Funktionen	M
2.1	Passwort- und Accountverwaltung	M
2.2	Passwort-Generator	M
3	Datenschredder (sicheres Löschen von Dateien)	M
4.1	Funktion zur Verschlüsselung von Verzeichnissen	M
4.2	komprimierte Verschlüsselung von Dateien und Verzeichnissen	M
5	einfaches Deployment-Verfahren für Endbenutzer	M
6.1	Public-/Private-Key Verschlüsselung für Texte / E-Mails	K
6.2	Import- / Exportmöglichkeit für Public-Key Zertifikate	K
7.1	Hashbasierte Dateiverifikation	K
7.2	Kontrolle des Ver- und Entschlüsselungsvorgangs	K
7.3	Einbinden von portabler Applikationen	K

Für jedes der Zielgruppen wird eine Iteration im Spiralmodell durchgeführt. Die Dauer der Iterationen variiert zwischen 3 bis 10 Tagen. Im Kapitel „Projektspezifisches Vorgehensmodell“ haben wir die detaillierte Beschreibung und den vorgesehenen Inhalt für diese Ziele beschrieben.

4 Vorgehensstrategie

Für die Diplomarbeit verwenden wir wie in der Projektarbeit das iterative Spiral-Modell. Eine schrittweise Annäherung an die Ziele des Projekts und möglichst früh verfügbaren Prototypen erscheint uns angesichts der Thematik des Projekts als angebracht.

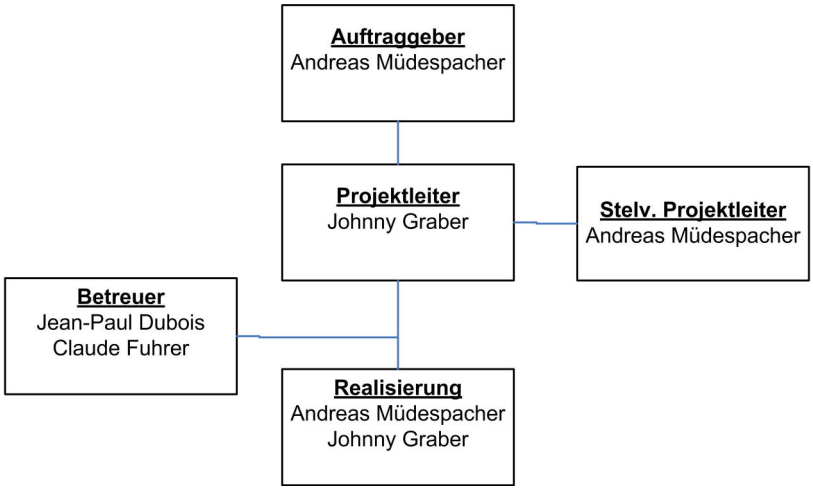
4.1 Phasenmodell & Kurzbeschreibung



Jede Iteration beginnt mit dem definieren der Ziele und dem aufnehmen der Randbedingungen. Anhand dieser wird nach Lösungen gesucht und Analysen durchgeführt. Diese werden umgesetzt und verifiziert. Zum Abschluss wird die gemachte Arbeit reflektiert und mit der Planung der nächsten Phase begonnen.

4.2 Projektrollen

Die Projektrollen sind nach dem in Hermes definierten Organigramm organisiert. Angesichts der Grösse des Projektteams haben die Studenten mehrere Rollen gleichzeitig besetzt.



	Betreuer Implementation	Betreuer Implementation	Student	Student
Name	Fuhrer Claude	Dubois Jean-Paul	Graber Johnny	Müdespacher Andreas
Tel.	032 321 63 36	032 321 62 82	076 336 02 93	076 502 36 63
E-Mail	claude.fuhrer@bfh.ch	jean-paul.dubois@bfh.ch	grabj@bfh.ch	mudea@bfh.ch

5 Projektspezifisches Vorgehensmodell

Die geplanten Iterationen laufen vom Aufbau her sehr ähnlich ab. Der detaillierte Lösungsansatz wird jeweils in der Phase Analyse erstellt, wodurch hier die Lösungen nur oberflächlich beschrieben werden. Die Ergebnisse jeder Phase werden im Abschlussbericht dargelegt.

Die einzelnen Iterationen werden durch den Auftraggeber bewilligt.

5.1 Initialisierung

In der Initialiserungsphase erstellen wir die für die Projektführung benötigten Dokumente.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Projekt vorbereiten	Diplomaufgabe	Nein	erledigt	
	Pflichtenheft	Ja	erledigt	
	Projekthandbuch	Ja	erledigt	
	Projektplan	Ja	erledigt	

5.2 1. Iteration (Basis-GUI)

Ziel der 1. Iteration ist die Erstellung des Basis-GUI, in das die Ergebnisse der folgenden Iterationen integriert werden können. Dies bedeutet im speziellen, dass hier die Grundlagen für die Mehrsprachenfähigkeit und das Logging gelegt werden müssen.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	erledigt	
Analyse	Lösungsvariante ausgewählt	Ja	erledigt	
Design	Klassendiagramm	Ja	erledigt	
	Manueller Funktionstest	Ja	erledigt	
Implementierung	Java-Klassen	Ja	erledigt	
	Erstellung Basis-GUI	Ja	erledigt	

5.3 2. Iteration (Passwort und Accountverwaltung + Passwortgenerator)

Ziel dieser Iteration ist die Erstellung Passwort- und Accountverwaltung sowie dem Passwortgenerator. In der Analyse muss geklärt werden, wie die Account-Daten gespeichert und gesichert werden sollen.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	erledigt	
Analyse	Lösungsvariante ausgewählt	Ja	erledigt	
Design	Klassendiagramm	Ja	erledigt	
	Manueller Funktionstest	Ja	erledigt	
Implementierung	Java-Klassen	Ja	erledigt	
	Einbindung in GUI	Ja	erledigt	
	Integrationstest	Ja	erledigt	

5.4 3. Iteration (Datenshredder)

Der Datenschredder soll das sichere Löschen von Dateien ermöglichen. Welchen Ansatz wir in AtaraxiS benutzen wollen, muss in der Analyse-Phase geklärt werden.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	erledigt	
Analyse	Lösungsvariante ausgewählt	Ja	erledigt	
Design	Klassendiagramm	Ja	erledigt	
	JUnit-Test	Ja	erledigt	
Implementierung	Java-Klassen	Ja	erledigt	
	Einbindung in GUI	Ja	erledigt	
	Integrationstest	Ja	erledigt	

5.5 4. Iteration (Verschlüsselung)

Im Prototypen aus der Semesterarbeit haben wir eine Verschlüsselung von Dateien implementiert. Auf dem bauen wir in dieser Iteration auf und ergänzen die Funktionalität um eine Verschlüsselungsfunktion für Verzeichnisse sowie die Möglichkeit, vor dem verschlüsseln die Daten zu komprimieren.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	erledigt	
Analyse	Lösungsvariante ausgewählt	Ja	erledigt	
Design	Klassendiagramm	Ja	erledigt	
Implementierung	Java-Klassen	Ja	erledigt	
	Einbindung in GUI	Ja	erledigt	
	Integrationstest	Ja	erledigt	

5.6 5. Iteration (Deployement-Prozess und Benutzerdokumentation)

Da die Sicherheit für den Endbenutzer nur bei guter Dokumentation und einfachem Deployement der Software gesteigert werden kann, ist diese Iteration sehr wichtig.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	erledigt	
Analyse	Lösungsvariante ausgewählt	Ja	erledigt	
Implementierung	Java-Klassen	Ja	erledigt	
	Integrationstest	Ja	erledigt	

5.7 [Optional] 6. Iteration (Public-/Private Key Verschlüsselung)

Je nach Vorschritt der ersten 5 Iterationen bleibt uns noch Zeit für eine Erweiterung von AtaraxiS um eine Public-/Private Key Verschlüsselung.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Anforderungen & Ziele	Anforderungen definiert	Ja	offen	
Analyse	Lösungsvariante ausgewählt	Ja	offen	
Design	UseCases	Ja	offen	
	Klassendiagramm	Ja	offen	
	Sequenzdiagramm	Ja	offen	
	JUnit-Test	Ja	offen	
Implementierung	Java-Klassen	Ja	offen	
	Einbindung in GUI	Ja	offen	
	Integrationstest	Ja	offen	

5.8 [Optional] 7. Iteration (Diverse Erweiterungen)

Über die bisher genannten Erweiterungen heraus haben wir noch zahlreiche weitere Ideen:

- einbinden von portablen Applikationen in AtaraxiS.
- Hashbasierte Dateiverifikation
- Detailliertere Kontrolle des Ver- und Entschlüsselungsvorgangs

5.9 Projektabschluss

Die Diplomarbeit AtaraxiS wird mit dem Abschlussbericht, der Verteidigung der Diplomarbeit, einer Präsentation am Finaltag sowie einer CD mit den erarbeiteten Ergebnissen beendet.

Hauptaktivität	Ergebnis	Erstellen	Status	Bemerkung
Projektabschluss	Abschlussbericht	Ja	erledigt	
	Verteidigung Diplomarbeit	Ja	offen	
	Präsentation AtaraxiS	Ja	offen	
	Ergebnis-CD	Ja	erledigt	

6 Methoden und Werkzeuge

Alle erzeugten Dokumente und der Sourcecode werden im SVN-Repository der HTI abgelegt. Die definitiven Versionen der Dokumente werden auf der Webseite des Projekts unter der URL http://projects.hti.bfh.ch/ataraxis publiziert.

Die Zeiterfassung wird im Wiki geführt.

Die verwendete Software ist entweder im Besitz der HTI und uns gratis zur Verfügung gestellt worden oder als OpenSource lizenziert.

7 Zeit und Ablaufplanung

Die Zeit- und Ablaufplanung der einzelnen Iterationen haben wir im Dokument Ablaufplan_AtaraxiS.xls eingetragen. In der Analyse-Phase der Iterationen wird die Zeitplanung jeweils verfeinert und für die einzelnen Aufgaben ausgewiesen.

8 Dokumentenliste

Die Liste der Dokumente wird fortlaufend erweitert.

- Pflichtenheft (Anforderungen)
- Projekthandbuch (Vorgehen, Inhaltliche Planung)
- Ablaufplan (Zeitliche Planung)
- Endbericht (Ergebnisse)
- Benutzerhandbuch (Handbuch für den Endbenutzer)