Masterarbeit - Aufgabenstellung

Name, Vorname: _____

UniBw-E-Mail-Adresse: _____

Matrikel Nummer: _____

Studiengang: _____

Thema: **Dezentrale Passwortmanager**
Voraussetzung: Vorlesung: Middleware und mobile Cloud Computing

Anforderungen und Zielstellung:

Regelmäßig findet man in den Medien Berichten zu Datenleaks, bei denen Nutzerdaten abhandenkommen. Eine Mehrfachverwendung des gleichen Passworts bei unterschiedlichen Accounts kann dementsprechend schwerwiegende Folgen haben, sollte das Passwort nur einer dieser Accounts in falsche Hände geraten. Wie geht man jedoch damit um, sich dutzende verschiedener Passwörter merken zu können? Abhilfe schaffen sogenannte Passwort-Manager, die eine Vielzahl von Passwörtern in einer verschlüsselten Datei speichern können und diese mittels eines Master-Passworts schützen, so dass man sich nur ein einziges Passwort merken braucht.

In manchen Hochsicherheitsbereichen kommt das sogenannte 4-Augen-Prinzip zum Einsatz, bei dem mindestens 2 Personen nötig sind, um einen Vorgang durchzuführen. Dieses Prinzip stellt sicher, dass eine Person alleine niemals einen Vorgang starten kann. Dieses Prinzip könnte auch durch verteilte Passwortmanager umgesetzt werden, bei denen ein geheimer Schlüssel nur dann herausgegeben wird, wenn mehrere Personen dies autorisieren. Unter anderem im Bereich der Server-Administration durch ein Team von Admins ist dies wünschenswert. Dazu werden oft auch Zertifikate verwendet anstelle von Passwörtern.

Die Bachelorarbeit adressiert dieses Handlungsfeld, indem ein Passwort-Management-System geschaffen werden soll, welches auch den Anforderungen von verteilten Nutzern gerecht wird. Ziel ist die Konzeptionierung und Entwicklung einer verteilten Passwortmanagement Software. Hierbei ist ein funktionsfähiger Demonstrator zu erstellen. Weiterhin ist das System so auszurichten, dass es erweiterbar und flexibel auf verschiedene Anwendungsbereiche anpassbar ist. Insbesondere, dass neu erstellte Passwörter eines Knotens automatisch und gesichert auf die anderen Knoten des Quorums verteilt werden. Mit dem System werden hauptsächlich die folgenden Nutzen verfolgt. Passwörter kryptographisch sicher speichern, verteilen und abrufen. Funktionalität für den Zugriff nach dem 4-Augen-Prinzip auf Passwörter ermöglichen.

Institut: Angewandte Informatik – INF 4
1. Verantwortlicher Hochschullehrer: Prof. Dr.-Ing. Andreas Karcher
2. Verantwortlicher Hochschullehrer: _____
Betreuer: Dr. Peter Hillmann
Ausgehändigt am: _____
Einzureichen bis: _____

Detaillierte Aufgabenstellung

1. Beschreibung der Motivation der Thematik und Erläuterung des Problems anhand eines selbstgewählten Beispiels. Aufstellen von wissenschaftlichen Fragestellungen und Anforderungen, welche zur Lösung des Problems zu beachten sind. Ermittlung von einsatzrelevanten Daten und Diensten auch unter Berücksichtigung zukünftiger Einsatzszenarios. Aufstellen von Anforderungen hinsichtlich einer cloudbasierten und verteilten Anwendung.

2. Umfassende Literaturrecherche zu Anforderungen und Richtlinien hinsichtlich Erstellung, Nutzung, softwarebasierte Generierung und Sicherheit von Passwörtern. Vergleich gängiger Passwort-Manager (PC/Handy-App) und derer Funktionsweisen. Umfassende Literatur- & Softwarerecherche und Analyse derzeitiger Lösungsansätze und Möglichkeiten zur Entwicklung von verteilten Passwortmanagern. Bewertung der verfügbaren Technologien hinsichtlich der aufgestellten Anforderungen (Multi-User-Fähigkeit, Sicherheit, Performance beim Zugriff auf das System).

3. Entwurf eines theoretischen Konzeptes mittels Schichtenarchitektur zur Umsetzung der aufgestellten Anforderungen an eine dezentrale Software zur Speicherung und Multi-User-Zugriff auf Passwörter. Aufzeigen gängiger Technologien zur späteren Implementierung. Beschreibung der Möglichkeiten zur praktischen Umsetzung des konzeptionierten Systems.

4. Evaluation des theoretischen Konzeptes. Prototypisches Aufzeigen, Umsetzen und Nachweisen des Konzeptes mittels einer programmtechnischen Implementierung. Beschreibung der gewählten Software-Architektur samt Programmfluss sowie der gewählten Datenstrukturen. Beschreibung und Evaluierung des Sicherheitskonzeptes des Konzeptes.

5. Praktischer Nachweis anhand eines selbstgewählten Beispiels. Zusammenfassende Betrachtung und Diskussion der Ergebnisse. Bewertung der praktischen Umsetzung und ziehen von Rückschlüssen auf das Konzept. Beschreibung von Verbesserungsvorschläge und Abschätzung des weiteren Implementierungsbedarfs.

6. Zusammenfassung der Ergebnisse sowie Diskussion möglicher zukünftiger Erweiterungen und Anwendungsgebiete.

Literatur

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Passwort_Manager/Passwort_Manager_node.html
- https://www.chip.de/test/Die-besten-Passwort-Manager-2019_128580641.html
- https://csrc.nist.gov/publications/detail/sp/800-63b/final
- https://blog.wuermkanal.de/was-ist-ein-sicheres-passwort/
- https://dl.acm.org/doi/pdf/10.1145/359168.359176
- https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
- https://www.schneier.com/blog/archives/2017/10/changes_in_pass.html