1 Whistleblower-Plattform

Im Rahmen dieses Projekts entwickeln Sie ein sicheres Konzept und eine prototypische Implementierung einer anonymen Whistleblower-Plattform namens ***WhistleDrop***, die als Tor Hidden Service bereitgestellt wird. Ziel ist es, sensible Informationen verschlüsselt zwischen einem anonymen Whistleblower und einem Journalisten zu übertragen – unter Einhaltung moderner kryptographischer Prinzipien und unter Berücksichtigung praktischer Aspekte der digitalen Geheimhaltung.

Es gibt in WhistleDrop drei Entitäten, die in der folgenden Tabelle dargestellt werden:

Entität	**Erklärung**
Whistleblower	Der Whistleblower lädt eine Datei, z. B. eine PDF-Datei mit Metadaten, über den Hidden Service hoch. Der WhistleDrop-Server verschlüsselt die Datei unmittelbar nach dem Upload mit einem zufällig generierten symmetrischen Schlüssel.
WhistleDrop-Server	Auf dem WhistleDrop-Server, der als Hidden Service im Tor-Netzwerk angeboten wird, werden die symmetrischen Schlüssel nur verschlüsselt gespeichert. Diese Schlüssel stammen aus einer Datenbank, die nur die öffentlichen Schlüssel von RSA-Schlüsselpaaren enthält. Die dazugehörigen privaten Schlüssel befinden sich ausschließlich beim Journalisten.
Journalist	Die über das Tor-Netzwerk hochgeladenen Daten können nur von dem Journalisten entschlüsselt werden. Bei ihm befindet sich die Datenbank mit den vollständigen RSA-Schlüsselpaaren.

Tabelle 1.1: Entitäten in WhistleDrop.

Entwickeln Sie ein sicheres kryptographisches Konzept zur automatischen Ende-zu-Ende-Verschlüsselung der hochgeladenen Dateien. Die symmetrischen AES-Schlüssel, die beim Upload auf dem WhistleDrop-Server generiert und zum Verschlüsseln der hochgeladenen Daten verwendet werden, dürfen niemals unverschlüsselt auf die Festplatte geschrieben werden. Auch die hochgeladenen Daten dürfen nur verschlüsselt auf die Festplatte geschrieben werden.

Definieren Sie ein passendes Verfahren zum Schlüsselmanagement:

- Die Datenbank beim Journalisten enthält mehrere RSA-Schlüsselpaare.
- Nur die öffentlichen Schlüssel werden in der Datenbank auf dem WhistleDrop-Server gespeichert.
- Jeder der öffentlichen Schlüssel darf beim Upload nur einmal verwendet werden.
- Der verwendete Schlüssel wird markiert oder aus der Datenbank entfernt.
- Die zugehörigen privaten Schlüssel befinden sich ausschließlich beim Journalisten.

Die Plattform soll in der Programmiersprache ***Python*** entwickelt werden. Dokumentieren Sie Ihr Projekt in einem PDF-Dokument, das die folgenden Informationen enthält:

- Eine Erklärung des Whistleblowing-Prozesses mit WhistleDrop.
- Eine grafische Darstellung der Systemarchitektur. Diese soll die Interaktionen der drei Entitäten (Tabelle 1.1) und die kryptographischen Prozesse zeigen.
- Eine Erklärung des Schlüsselmanagements.
- Den Quellcode von WhistleDrop, z. B. als Link zu einem GitHub-Repository.[1]
- Denken Sie wie ein Whistleblower: Was würden Sie von einer solchen Plattform erwarten? Dokumentieren Sie Ihre Überlegungen bzw. Anforderungen an die Plattform.
- Überlegen Sie sich ein Szenario, wie ein Angreifer WhistleDrop attackieren könnte und schlagen Sie eine Gegenmaßnahme vor.
- Dokumentieren Sie mit Screenshots und Text oder in Videoform[2], wie eine PDF-Datei über WhistleDrop als Hidden Service im Tor-Netzwerk hochgeladen wird, wie diese Datei automatisch verschlüsselt und gespeichert wird und wie ein Journalist die Datei abruft und entschlüsselt.
- Geben Sie den kumulierten Zeitaufwand aller Gruppenmitglieder für dieses Projekt an.[3]

---

[1] Sie können den Quellcode auch als .zip-Datei über ILIAS einreichen.

[2] Wenn Sie sich für ein Video entscheiden, dann können Sie dieses in der Dokumentation verlinken.

[3] Diese Information dient statistischen Zwecken und hat keinen Einfluss auf die Bewertung.