UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Übungsblatt 2

Passwortsicherheit, Hashfunktionen und Authentifizierung

Abgabe bis 02. Mai 2023 um 12:00 Uhr im Moodle

Cybersecurity im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

Einführung

Dank Ihrer Unterstützung bei der Klärung von grundlegenden kryptographischen Konzepten ist ITS bei seiner *IT-Sicherheits-Offensive* gut im Zeitplan. Das Unternehmen möchte nun als ersten konkreten Schritt ein neues internes Authentifizierungssystem einführen, und bittet Sie darum, das in einem aufwendigen Verfahren erarbeitete Konzept zu prüfen. Grundlage für das System bildet eine Datenbank mit Benutzernamen und Passworthashes, die von einem Authentifizierungsserver verwaltet wird; dieser generiert bei erfolgreicher Anmeldung ein sogenanntes *Ticket*, welches anschließend bei jedem weiteren Netzwerkdienst als Authentifizierung verwendet werden kann.

Aufgabe 1 Passwortstärke beurteilen (9 Punkte) *[optional bei bestandenem Praktikum]*

Diese Aufgabe muss nicht bearbeitet werden, wenn Sie stattdessen das "Passwörter"-Praktikum bestehen. Bitte geben Sie Ihren Gruppennamen aus dem Praktikum an, um die Korrektur zu erleichtern.

Um auch für den Fall eines Datenlecks vorzusorgen, sollen nur die Hashwerte der Passwörter in der Datenbank abgelegt werden. Die verwendeten Passwörter sollen so stark sein, dass ein Angreifer im Random-Oracle-Modell (also bei einer perfekten Hashfunktion) nur mit enormen Aufwand an die Klartextpasswörter herankommt. Für eine geeignete Passwortrichtlinie wurden daher fünf zu überprüfende Vorschläge entwickelt:

1. Ein Passwort soll aus genau vier Ziffern bestehen (vierstellige PIN)
2. Ein Passwort soll aus genau zwei Großbuchstaben (A-Z), fünf Kleinbuchstaben (a-z) und drei Ziffern (0-9) bestehen, die in einer zufälligen Reihenfolge verkettet werden.
3. Ein Passwort soll einem aus einer Wortliste mit 10.000 Einträgen zufällig gewähltem Wort entsprechen.
4. Ein Passwort soll einem aus einer Wortliste mit 10.000 Einträgen zufällig gewähltem Wort mit zwei angehängten Ziffern (0-9) entsprechen.
5. Ein Passwort soll vier aus einer Wortliste mit 10.000 Einträgen zufällig gewählten Wörtern entsprechen.

Die Wortliste in Vorschlag 3 bis 5 ist jeweils öffentlich und in der Sprache des Benutzers verfasst. Sie können annehmen, dass die jeweiligen Passwörter perfekt zufällig erzeugt werden (mit Zurücklegen, also Dopplungen möglich). Bestimmen Sie für jeden dieser Vorschläge die erwartete Passwortstärke in Bits (Shannon-Entropie), wenn ein potenzieller Angreifer das zur Erzeugung verwendete Verfahren kennt. Welches dieser Verfahren würden Sie empfehlen? Begründen Sie Ihre Antwort.

Aufgabe 2 Eigenschaften von Hashfunktionen (7 Punkte)

Im zweiten Schritt geht es um die Wahl einer möglichst starken Hashfunktion zum Sichern der Passwörter. Hierzu wurde der folgende Vorschlag erarbeitet (Java-Code):

```java
public static String hash(String input)
{
    // Use large factors for good distribution
    final BigInteger a1 = new BigInteger("485440633518672411");
    final BigInteger a2 = new BigInteger("14381932621899831683");

    // Fit result into 64 bits
    // m = 2^63
    final BigInteger m = new BigInteger("2").pow(63);

    // Sum up ASCII values of input characters
    // e.g. for "pw123": sum = 112 + 119 + 49 + 50 + 51 = 381
    long sum = 0;
    for(char c : input.toCharArray())
        sum += (int)c;
    BigInteger sumAsBigInt = new BigInteger("" + sum);

    // Calculate hash value as linear congruence
    // v1 = a1 * sum  mod m
    // v2 = a2 * sum  mod m
    byte[] v1 = a1.multiply(sumAsBigInt).mod(m).toByteArray();
    byte[] v2 = a2.multiply(sumAsBigInt).mod(m).toByteArray();

    // Return hash value as hex string
    return javax.xml.bind.DatatypeConverter.printHexBinary(v1).toLowerCase()
         + javax.xml.bind.DatatypeConverter.printHexBinary(v2).toLowerCase();
}
```

Die Eingabe `password123` ergibt beispielsweise den Hashwert `2f286bca1af286f35fdc150fdbdff19b`, die Eingabe `password124` den Hashwert `35e50d79435e510e2772f89533d10b1e`.

Untersuchen Sie die beschriebene Hashfunktion im Hinblick auf die drei in der Vorlesung beschriebenen zentralen Eigenschaften. Würden Sie die Benutzung dieser Hashfunktion empfehlen? Haben Sie Ideen für Verbesserungen, oder alternative Ansätze? Begründen Sie Ihre Antwort.

Hinweis: Versuchen Sie eine Zahl $b_1 \in \mathbb{N}$ zu finden, sodass

$$a_1 \cdot b_1 \equiv 1 \mod m$$

bzw. äquivalent

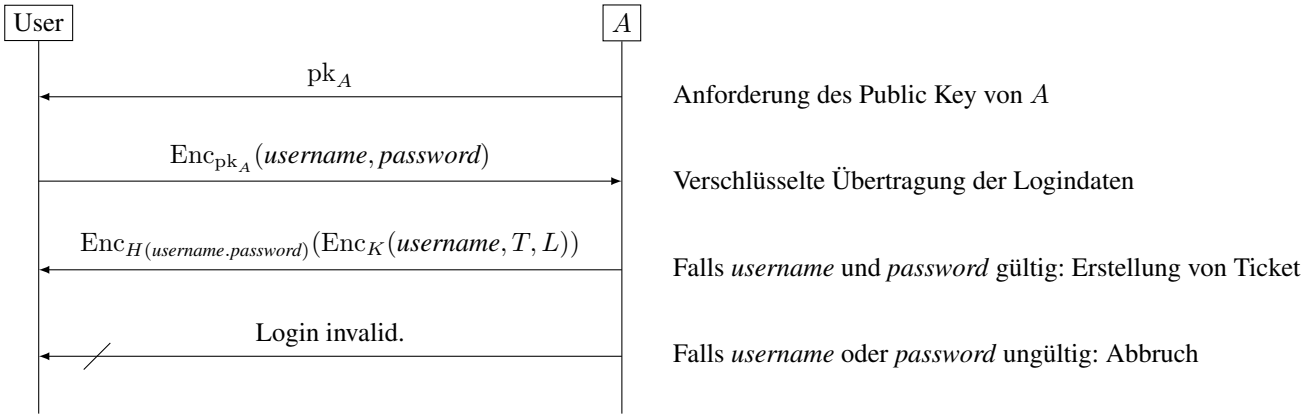
$$\exists k \in \mathbb{N}\colon a_1 \cdot b_1 = k \cdot m + 1$$

gilt.

Aufgabe 3 Authentifizierungsprotokolle (4 Punkte)

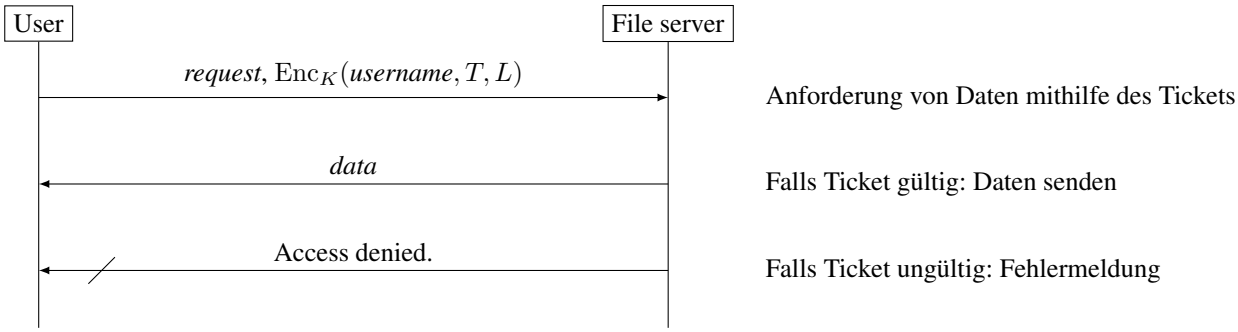
Zum Schluss muss nun noch die oberste Ebene des neuen Systems betrachtet werden, das Authentifizierungsprotokoll. Wie schon in der Einführung beschrieben, stellt ein zentraler Authentifizierungsserver A nach Login mit Benutzername und Passwort ein Ticket aus, welches anschließend im gesamten Netzwerk benutzt werden kann. Der Unterschied zu anderen Protokollen wie z.B. Kerberos ist hier, dass Benutzerschlüssel aus dessen Namen und Passwort erzeugt werden, sodass der Benutzer kein eigenes Schlüsselmaterial mehr pflegen muss.

In grafischer Darstellung sieht der Login im Detail wie folgt aus:



$H\colon \{0,1\}^* \to \{0,1\}^n$ ist eine perfekte kryptographische Hashfunktion nach dem Random-Oracle-Modell; T ist ein Zeitstempel, L die Lebensdauer des Tickets. Jede Komponente des Systems kennt einen internen symmetrischen Key K, der zur Entschlüsselung des Tickets benutzt wird und für Angreifer als unbekannt angenommen werden kann.

Eine Benutzung des Tickets um beispielsweise Daten von einem Dateiserver abzurufen gestaltet sich wie folgt:



Überprüfen Sie das Protokoll auf Sicherheit gegenüber Angreifern auf Netzwerkebene, und beschreiben Sie mögliche Schwachstellen.

Aufgabe 4 Alternative Authentifizierungsverfahren (6 Punkte)

Neben klassischen Passwörtern gibt es noch weitere Authentifizierungsverfahren, die sich ebenfalls gut in das Protokoll aus Aufgabe 3 einbetten ließen. Versprechen diese möglicherweise höhere Sicherheit?

Beschreiben Sie ganz kurz das jeweilige Verfahren und nennen Sie jeweils einen Vorteil und einen Nachteil.

1. TAN-Liste
2. Security Token
3. Biometrie