IT-Sicherheit
Prof. Dr. Michael Zohner
Wintersemester 2021/2022

Hochschule Fulda
University of Applied Sciences

Übung Kapitel 7: Passwörter und Challenge-Response Protokolle v1.3*

Aufgabe 1 Berechnen Sie die Entropie der folgenden Passwortwahlstrategien. Die Entropie wird berechnet als $\log_2(AnzahlKombinationen)$. Nutzen Sie als Basis zur Berechnung die Angaben in Tabelle 1.

A) Deutsche Wörter mit mindestens 10 Buchstaben und einer Ziffer am Ende

B) Deutsche Wörter mit mindestens 10 Buchstaben sowie einer Ziffer und einem Sonderzeichen am Ende, die in beliebiger Reihenfolge stehen können (also ;4 oder 4;)

C) Vier hintereinander folgende Deutsche Wörter mit mindestens 10 Buchstaben

D) Deutsche Wörter mit genau 10 Buchstaben wobei jeder Buchstabe zufällig groß oder klein geschrieben wird

E) Deutsche Wörter mit genau 10 Buchstaben wobei 4 zufällige ausgewählte Buchstaben basierend auf der Reihenfolge substituiert werden (Buchstabe 1 durch 1 oder !, Buchstabe 2 durch 2 oder ", Buchstabe 3 durch 3 oder §, Buchstabe 4 durch 4 oder $).

F) Ein zufälliges 10-stelliges Passwort bestehend aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen

Menge	**Anzahl Elemente**
Deutsche Wörter mit genau 10 Buchstaben	15.674
Deutsche Wörter mit mindestens 10 Buchstaben	137.465
Kleinbuchstaben	26
Klein- und Großbuchstaben	52
Ziffern	10
Sonderzeichen	30
Substitutionsmöglichkeiten	2 pro Buchstabe (also z.B. a $\mapsto \{1, !\}$)

Table 1: Gegebene Häufigkeit bestimmter Wörter und Buchstaben.

Aufgabe 2 Beim Challenge-Reponse Protokoll, welches in Figure 1 dargestellt ist, sendet ein Server eine Challenge C an Alice, die basierend auf einem Geheimnis G und einer Funktion f eine Response $R = f(C, G)$ berechnet, welche sie dem Server sendet um sich zu authentifizieren.

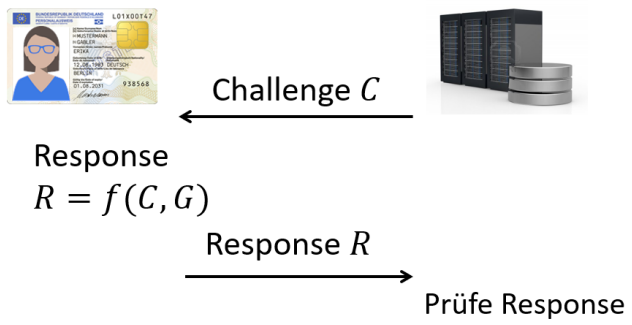

Figure 1: Challenge-Response Protokoll zwischen Alice's Smartcard und einem Server.

Ihre Aufgabe ist, die Eigenschaften der Werte im Challenge-Response Protokolls zu analysieren und kryptographische Verfahren zu nutzen, um das Protokoll konkret zu instanziieren.

A) Worauf müssen Sie bei der Wahl der folgenden Werte achten:

- Die Challenge C?
- Die Funktion f?
- Das Geheimnis G?
- Die Reponse R?

B) Wie könnte ein Challenge-Response Protokoll auf **symmetrischer** Verschlüsselung aufgebaut werden?

- Welche Partei muss welchen Schlüssel kennen?

- Wie sieht die Funktion f aus mit der die Response berechnet wird?
- Wie wird die Response verifiziert?
- Wie können die benötigten Sicherheitseigenschaften aus Punkt A) auf die genutzte Verschlüsselung reduziert werden?

C) Wie könnte ein Challenge-Response Protokoll auf **asymmetrischer** Verschlüsselung aufgebaut werden?

- Welche Partei muss welchen Schlüssel kennen?
- Wie sieht die Funktion f aus mit der die Response berechnet wird?
- Wie wird die Response verifiziert?
- Wie können die benötigten Sicherheitseigenschaften aus Punkt A) auf die genutzte Verschlüsselung reduziert werden?

Aufgabe 3 - Bonuspunkteaufgabe (TaskID 7A) Bob ist sehr stolz auf ein selbst entwickeltes Verfahren um sichere Passwörter zu generieren, welche von allen Passwort Policies akzeptiert werden:

A) Wähle ein deutsches Wort mit mindestens 10 Zeichen aus einer gegebenen Liste (verfügbar auf: `https://elearning.hs-fulda.de/ai/pluginfile.php/93431/mod_assign/introattachment/0/Wortliste_Deutsch.txt?forcedownload=1`)

B) Schreibe den ersten oder zweiten Buchstaben des Wortes groß

C) Substituiere einen beliebigen kleingeschriebenen Vokal durch eine Zahl

D) Substituiere einen anderen, beliebigen kleingeschriebenen Vokal durch ein Sonderzeichen

E) Füge eine Zahl am Ende des Passworts ein, die, beginnend bei 1, mit jedem Update des Passworts hochgezählt wird (max. 20)

Obwohl die so erstellten Passwörter den meisten Empfehlungen folgen, möchten Sie Bob davon überzeugen, dass durch die Preisgabe des Verfahrens die erstellen Passwörter unsicher werden. Bob fordert Sie heraus Ihre These zu beweisen und gibt Ihnen einen Hashwert h der wie folgt berechnet wurde:

$$h = SHA256(pw||salt)$$

wobei pw das Passwort, $salt$ ein zufälliger Wert und || der Konkatenationsoperator ist. Beweisen Sie Ihre These indem Sie auf das Passwort pw via Brute-Force ermitteln und auf das Moodle Element "Abgabe Übung 7: Passwort Brute-Force" hochladen. Sie erhalten den Wert $salt$, die genutzte Substitution der Vokale sowie den Hashwert h aus der Übungsumgebung.

Hinweise:

- Beispielwerte für das SHA256 Passwort Hashing
  - Passwort (als String): aBg0schn/ertem10
  - Passworts (Bytedarstellung als Hex): 614267307363686e2f657274656d3130
  - Salt (Bytedarstellung als Hex): f8791d3120f151961a66c84449c3e72c
  - Hashwert (Bytedarstellung als Hex): 9bf2f4b49961a4a37e9517fbd54589c3f37eeb151d61971ebdcd507419d0559a
- Sie können das gefundene Passwort mit der Aufgaben-ID "7AV" verifizieren (Antwort als OK/NOK). Geben Sie das Passwort als String an.
- Die Berechnung sollte etwa 10 Minuten dauern.
- Die Abgabefrist ist der 10/Januar/2022, 23:59 Uhr. Ein erfolgreiches Bestehen wird via Moodle mitgeteilt.

***Versionshistorie** V1.0: Initiale Version. v1.1: Updated Wording in Aufgabe 2. v1.2: Beispielhashwerte und Informationen für Aufgabe 3 geupdated. v1.3: Aufgabe 1 E geupdated und die Reihenfolge der Substitution in die Kombinationen mitaufgenommen.