Aufgabenblatt Nr. 5

Aufgabe 1 V

Ein Unternehmen schützt seinen Zugang mit einem biometrischen Zugangskontrollsystem. Das System ist so konfiguriert, dass es 99, 8% aller legitimen Benutzer korrekt erkennt, dass bedeutet, die Wahrscheinlichkeit für einen Type 1 Error (false rejection) beträgt 0, 2%. Das Systeme erkennt eine nicht-autorisierte Person mit einer Wahrscheinlichkeit von 99%, die Wahrscheinlichkeit für einen Type 2 Error (false acceptance) beträgt also 1%.

Untersuchungen haben ergeben, dass 1 von 1.000 Personen, die versucht, durch das Zugangskontrollsystem zu gehen, dafür nicht autorisiert ist (meist ein Besucher, der sich verlaufen hat).

Aufgabe 1.1

Jeden Tag gehen 200 Personen durch das Zugangskontrollsystem. Wie häufig wird dabei im Schnitt einer Person der Zugang verweigert?

Aufgabe 1.2

Eine Person wurde soeben vom Zugangskontrollsystem zurückgewiesen. Wie hoch ist die Wahrscheinlichkeit, dass es sich um eine nicht-autorisierte Person handelt?

Aufgabe 2 K & V

In einem Unternehmen sind die möglichen Zeichen eines Passworts Großbuchstaben, Kleinbuchstaben, Ziffern sowie die beiden Sonderzeichen '(' oder ')', also insgesamt 64 Zeichen. Die Passwortrichtlinie sieht vor, dass jedes Passwort genau 8 Zeichen lang ist.

Aufgabe 2.1

Wie viel Bit Entropie enthält jedes Passwort, wenn man davon ausgeht, dass jedes Passwort echt zufällig gewählt wurde?

Aufgabe 2.2

Ein Hacker kann $2^{30} \approx 1.000.000.000$ Passworte pro Sekunde ausprobieren. Wie lange dauert es höchstens, bis der Hacker ein Passwort durch Ausprobieren gebrochen hat?

Aufgabe 2.3

Die Passwortdatei enthält statt der Passwörter selbst die Hashwerte des Passworts gespeichert. Ein Hacker möchte für ein Passwort zurückrechnen und legt dafür eine Tabelle an. Jeder Eintrag in der Tabelle ist 40 Byte lang (32 Byte für den Hashwert und 8 Byte für das Passwort). Wie groß ist die Tabelle mit allen möglichen Passworten, die der Passwortrichtlinie entsprechen?

Aufgabe 2.4

Der Hacker möchte in der angelegten Tabelle effizient suchen können. Wie muss die Tabelle dafür sortiert sein und wie lange (wie viele Schritte) dauert eine Suche in diesem Falle?

Aufgabe 3 K & V

Die meisten Betriebssysteme der Linux-Familie haben eine Zugriffskontrolle nach dem Prinzip der Disrectionary Access Controll.

Aufgabe 3.1

Was macht Discretionary Access Control aus und wie unterscheidet es sich von Mandatory Access Control?

Aufgabe 3.2

Nennen Sie eine Möglichkeit, sich unter Linux anzeigen zu lassen, welche Benutzer(-gruppen) welche Berechtigungen auf eine Datei haben.

Aufgabe 3.3

Nennen Sie eine Möglichkeit, wie ein Benutzer die Berechtigungen auf eine Datei ändern kann.

Aufgabe 4 K

SSH und TLS sind beides Protokolle, die jeweils eine sichere Verbindung zwischen Server und Client etablieren sollen. Dazu führen sie zu Beginn der der Verbindung einen *Handshake* durch.

Aufgabe 4.1

Wie viele Nachrichten tauschen Server und Client bei einem SSH-Handshake aus? Wie vielen RTT (Round Trip Time) entspricht das?

Aufgabe 4.2

Wie viele Nachrichten tauschen Server und Client bei einem TLS-Handshake aus? Wie vielen RTT (Round Trip Time) entspricht das?

Aufgabe 4.3

Bei einem SSH-Handshake authentifiziert sich der Client in der Regel, bei einem TLS-Handshake authentifiziert sich der Client in der Regel nicht. Stellen Sie kurz die unterschiedlichen Anwendungsgebiete für SSH und TLS dar und erklären Sie damit die Unterschiede bei der Clientauthentifizierung bei SSH und TLS.

Aufgabe 4.4

Warum ist sowohl bei SSH als auch bei TLS eine Authentifizierung des Servers üblich?