Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

2. Aufgabenblatt

Ziel dieser Übung ist es, einen Einblick in die Abgründe von Sicherheitslöchern zu geben. Die Sammlung von teils kuriosen, in der Regel aber recht schwerwiegenden Vorkommnissen soll Beispiele für typische Motive von Angreifern, die eingesetzten Angriffsmethoden und die dabei ausgenutzten Schwachstellen informationstechnischer Systeme zeigen. Durch das aufgezeigte breite Spektrum der Motive und Methoden soll insbesondere das Bewußtsein für die Notwendigkeit einer strukturierten Risikoanalyse geschaffen werden. Ein weiteres Thema, dem wir uns zuwenden, ist die Steganographie. Schließlich betrachten wir noch den Sicherheitsaspekt hinsichtlich der Verfügbarkeit.

Aufgabe 2.1

Eine Firma führt eine Datenbank mit den Gehältern ihrer Angestellten. Der Zugriff hierauf ist lediglich privilegierten Personen der Gehaltsbuchhaltung möglich. Allerdings existieren auf dieser Datenbank Zugriffsmöglichkeiten, die es den (unprivilegierten) Mitarbeitern der Abteilung für Unternehmensstatistik erlauben, das Durchschnittsgehalt einer Gruppe von mindestens zehn benennbaren Personen auszulesen.

a) Ist es einem Mitarbeiter dieser Abteilung unter dieser Sicherheitsstrategie möglich, die individuellen Gehälter einzelner Mitarbeiter zu extrahieren?

b) Wenn ja, auf welche Weise? Wenn nein, welche zusätzlichen Rechte bräuchte er?

c) Auf welche möglichen Motive der Angreifer lässt dieses Beispiel schließen? Nennen Sie mindestens vier?

d) Welche der abstrakten Werte der Informationssicherheit wurden durch den Angriff bedroht?

Aufgabe 2.2

a) Was versteht man unter Steganographie?

b) Welche Prinzipien und Verfahren werden in der Steganographie angewandt.

c) Was sind die beiden Hauptziele der Steganographie?

d) Was verbirgt sich hinter den folgenden drei Chiffren?

i) DSSGHISCE AITEEMAH

ii) SCHS! PUHCLESL RSUE

iii) RASEAC SUILUJ SUIAG

Aufgabe 2.3

a) Beschreiben Sie anhand eines Schaubildes oder mittels mathematischer Gleichungen die Arbeitsweise einer synchronen XOR-Stromchiffre! Nennen Sie je einen Vor- und einen Nachteil!

b) Was ist bezüglich des Schlüssels speziell bei Verwendung einer XOR-Stromchiffre immer zu beachten, außer dass der Schlüssel hinreichend lang und geheim sein muss? Begründung anhand eines Beispiels.

Aufgabe 2.4

Ihr Studentenwohnheim bietet vernetze Rauchmelder an, welche über WLAN und die Cloud im Bedarfsfall einen Alarm auf Ihr Handy auslösen. Wie hoch ist die System-Verfügbarkeit der Alarmierung, wenn in Ihrer Ein-Zimmer-Studentenwohnung zwei redundante Rauchmelder angebracht sind, die eine Verfügbarkeit von 90 % besitzen, und sowohl WLAN als auch die Cloud eine Verfügbarkeit von 98 % bzw. 96 % aufweisen?

Aufgabe 2.5

a) Aus welchen fünf Grundelementen besteht ein Kryptosystem?

b) Erläutern Sie den Unterschied zwischen einer Quellencodierung und Kanalcodierung.

c) Aus welchen Parametern setzt sich der Schlüsselraum eines kryptographischen Schlüssels zusammen?

d) Was ist der Unterschied zwischen einer Blockchiffre und einer Stromchiffre?

e) Worin unterscheidet sich eine Hashfunktion von einem Message Authentication Code?