TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Professur für Privacy and Security, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2024/25

10. Aufgabenblatt – Sicherheit II

Besprechungszeitraum: 14.01.2025 – 17.01.2025

Aufgabe 10.1 Kryptographie - Verständnis

(a) Welche Schutzziele erreicht Kryptographie typischerweise?

(b) Was ist der Unterschied zwischen Nachrichtenvertraulichkeit und Nachrichtenintegrität?

(c) Wofür braucht man Signaturen?

(d) Was bedeutet es für ein signiertes Dokument verifizierbar und nicht veränderbar zu sein?

(e) 8 Mitarbeiter:innen einer Firma sollen miteinander vertrauliche Nachrichten austauschen. Niemand sollte in der Lage sein, die Kommunikation der anderen Paare zu lesen.

1. Wie viele Schlüssel braucht man bei der Verwendung von symmetrischer Verschlüsselung?
2. Wie viele Schlüsselpaare braucht man bei der Verwendung asymmetrischer Verschlüsselung

Aufgabe 10.2 Kryptographie - Caesar Eine sehr einfache Verschlüsselungstechnik ist die Caesar-Verschlüsselung. Die Grundidee besteht darin, dass jeder Buchstabe eines geordneten Alphabets durch einen Buchstaben ersetzt wird, der eine bestimmte Anzahl von Buchstaben entfernt ist. Beispielsweise bei einem Schlüssel $k = 2$, wird A zu C, B zu D, Z zu B usw.

(a) Schreiben Sie eine Funktion in einer Programmiersprache Ihrer Wahl, die eine Zeichenkette s sowie eine Zahl k als Eingabe erhält und s mit dem Caesar-Algorithmus verschlüsselt. Nehmen Sie dafür an, dass s nur aus Großbuchstaben des lateinischen Alphabets bestehen darf.

(b) Kann Ihre Funktion zum Verschlüsseln ohne Änderungen auch zum Entschlüsseln verwendet werden? Falls ja, wie? Falls nein, was müsste geändert werden?

(c) Welche Strategie(n) kann man anwenden um einen verschlüsselten Text zu entschlüsseln, wenn der Key unbekannt ist? Implementieren Sie eine Strategie und überprüfen Sie Ihre Funktion, in dem Sie `GUVF VF ZL FRPERG ZRFFNTR` entschlüsseln. *Hinweis: Es handelt sich um einen englischen Satz.*

Aufgabe 10.3 Kryptographie - RSA Rivest-Shamir-Adleman (RSA) ist ein Verfahren zur asymmetrischen Verschlüsselung. Es besteht somit aus einem öffentlichen und einem privaten Schlüssel. Für die Aufgabe gilt: A-Z entsprechen den Werten 01-26 und die Zahlen 0-4 den Werten 27-31. Benutzen Sie die Formeln aus der Vorlesung.

(a) Was sollte man bei der Wahl von p und q beachten?

(b) Gegeben sei: $p = 3$, $q = 11$, $e = 3$. Wie groß sind n, z und d?

(c) Vervollständigen Sie die Tabellen mit den gegebenen und berechneten Parametern.

Symbol	Nummer	C
B	02	
E	05	
T	20	
R	18	
I	09	
E	05	
B	02	
S	19	
Y	25	
S	19	
T	20	
E	05	
M	13	

C	Nummer	Symbol
28		
03		
27		
17		
26		
24		
17		
26		
03		
14		
15		
07		
02		

Aufgabe 10.4 Monster in the Middle (MitM)

(a) Was ist eine sogenannte MitM Attacke? Was ist die Gefahr?

(b) Was ist der Unterschied zwischen einer passiven und aktiven Angreifer:in?

(c) Wie kann man sich davor schützen?

(d) Was erreicht der Diffie-Hellman (DH) Schlüsselaustausch? Unter welchen Bedingungen ist er sicher?

(e) Kann der DH-Schlüsselaustausch einem MitM standhalten? Wenn ja, begründen Sie Ihre Antwort. Wenn nein, skizzieren Sie einen MitM-Angriff auf DH.

Aufgabe 10.5 Digitale Zertifikate

Gegeben ist der Ausschnitt eines digitalen Zertifikats.

```
Subject Name
Country DE
State/Province Sachsen
Organization Technische Universitaet Dresden
Common Name tu-dresden.de

Issuer Name
Country NL
Organization GEANT Vereniging
Common Name GEANT OV RSA CA 4

Validity
Not Before Mon, 28 Oct 2024 00:00:00 GMT
Not After Tue, 28 Oct 2025 23:59:59 GMT

Subject Key ID
Key ID 88:6C:38:91:DC:D9:3C:36:5F:C4:19:E0:48:63:40:67:79:9E:BD:C9
Authority Key ID
Key ID 6F:1D:35:49:10:6C:32:FA:59:A0:9E:BC:8A:E8:1F:95:BE:71:7A:0C
```

(a) Was ist ein digitales Zertifikat und welchen Zweck erfüllen sie?

(b) Wer garantiert, dass das Zertifikat korrekt ist? Welche Rolle hat diese Instanz?

(c) Angenommen Sie besuchen am 27. Oktober 2024 die Seite `tu-dresden.de` und erhalten das abgebildete Zertifikat. Was ist das Problem?

Aufgabe 10.6 Sicherheitsprotokolle

(a) Was ist ein Challenge-Response Protokoll?

(b) Was ist eine Nonce und was ist ihr Zweck in einem Authentisierungsprotokoll?

(c) Angenommen in Protokoll `ap4.0` (siehe Vorlesung) muss sich Alice nicht nur gegenüber Bob authentifizieren, sondern Bob auch gegenüber Alice. Beschreiben Sie ein Szenario bei dem sich Trudy gegenüber Bob als Alice ausgeben kann.
Hinweis: Berücksichtigen Sie die Reihenfolge der Operationen von `ap4.0` - Trudy und Bob initiieren das Protokoll und es kann beliebig verschachtelt werden. Beachten Sie besonders die Nonce und dass man sie bei Unachtsamkeit missbrauchen kann.

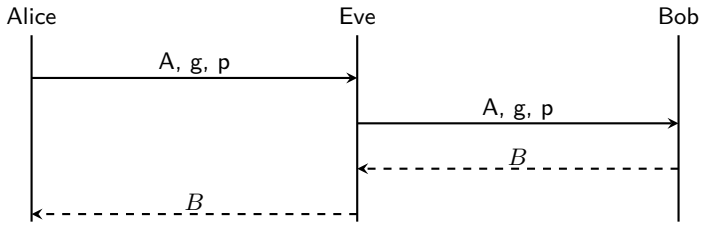
Klausuraufgabe I

In der folgenden Abbildung versucht Eve einen Monster-in-the-Middle-(MitM-)Angriff auf den Diffie-Hellmann-(DH-)Schlüsselaustausch von Alice und Bob durchzuführen.

Gehen Sie von der Notation aus der Vorlesung aus. Zur Erinnerung:

- a ist eine geheime Zufallszahl von Alice
- b ist eine geheime Zufallszahl von Bob
- g ist der sog. Primzahlgenerator
- p ist eine Primzahl
- $A = g^a \mod p$ und $B = g^b \mod p$

HINWEIS: Sie dürfen Ihre Angaben auch direkt in der Abbildung ergänzen.



a) Was macht Eve falsch? Beschreiben und skizzieren Sie einen erfolgreichen MitM-Angriff.

b) Wie kann man den DH-Schlüsselaustausch zuverlässig gegenüber Eve absichern? Nennen Sie hierzu die erforderlichen Schutzziele.

c) Unter welchen Bedingungen ist ein ungesicherter DH-Schlüsselaustausch sicher?

d) Welche datenschutzrelevanten Informationen kann Eve beobachten? Sie dürfen von einem sicheren DH-Schlüsselaustausch ausgehen. Begründen Sie Ihre Antwort.

Klausuraufgabe II

Gehen Sie von einer 2-Bit Blockchiffre mit der in Tabelle 1 dargestellten Schlüsseltabelle aus.

Tabelle 1: Schlüsseltabelle

In	Out
00	01
01	11
10	00
11	10

a) Verschlüsseln Sie den Klartext 01010000 mit der Betriebsart CBC (Cipher Block Chaining). Der Initialisierungsvektor ist 00.

b) Nennen Sie zwei Unterschiede von CBC gegenüber Electronic Codebook (ECB).

c) Welches Problem haben beide Verfahren (CBC und EBC)?