TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2023/24

10. Aufgabenblatt – Sicherheit II

Geplante Bearbeitungszeit: 18.12.2023 – 05.01.2024

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 Fri, 01 Dec 2023 00:00:00 GMT
Not After Sat, 30 Nov 2024 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 30. November 2023 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.

Aufgabe 10.7 Privatsphäre

(a) Was sind „personenbezogene Daten“?

- ☐ Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren juristischen Person
- ☐ Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person
- ☐ Angaben über eine Person, wie z.B. Name, Blutgruppe, Bankdaten

(b) Was bedeutet „Datenschutz“?

- ☐ Alle Maßnahmen zum Schutz von Daten vor missbräuchlicher Verwendung
- ☐ Der Schutz des Rechts auf informationelle Selbstbestimmung
- ☐ Maßnahmen die verhindern sollen, dass Daten durch Feuer oder Wasser beschädigt werden

(c) Was bedeutet „Datensicherheit“?

- ☐ Alle Maßnahmen zum Schutz von Daten vor Verlust, Zerstörung oder Verfälschung
- ☐ Nur Maßnahmen die verhindern sollen, dass Daten durch Feuer oder Wasser beschädigt werden
- ☐ Maßnahmen die u.a. verhindern sollen, dass Daten durch Alterung verloren gehen

(d) Was beinhaltet die „Anonymisierung“ von Daten?

- ☐ Die Verschlüsselung von Daten
- ☐ Nutzer:innen geben bei Onlinebestellungen keinen Daten an und bestellen stattdessen anonym
- ☐ Die Veränderung von Daten, sodass diese nur mit hohem Aufwand einer natürlichen Person zugeordnet werden können

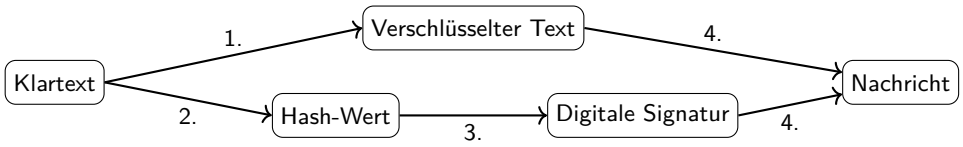
(e) Mit welchen der folgenden Möglichkeiten sollte man Daten sichern?

- ☐ Verschlüsselte Sicherheitskopien anlegen, die getrennt von Daten gespeichert werden
- ☐ Eine Kopie der Daten auf eine frei zugängliche Cloud-Server hochladen
- ☐ Die Daten möglichst vielen Mitarbeiter aushändigen, damit die Daten wieder zu erhalten sind, falls diese verloren gehen

Klausuraufgabe I

Ein Chat-System zum Austausch von kurzen Nachrichten soll die Vertraulichkeit und Integrität der übertragenen Daten sicherstellen. Jeder Teilnehmer besitzt ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel. Für jede Kommunikationsbeziehung wird außerdem ein sicher ausgehandelter symmetrischer Schlüssel vorausgesetzt.

Das Chat-System verwendet das folgende Design:



1. Der Klartext der Nachricht wird mit dem symmetrischen Kommunikationsschlüssel verschlüsselt.
2. Parallel dazu wird die Nachricht von einer kryptografischen Hash-Funktion zusammengefasst.
3. Dieser Hash-Wert wird mit dem privaten Schlüssel des Senders in eine digitale Signatur umgewandelt.
4. Beide Nachrichtenteile werden zusammengefügt und über ein unsicheres Netz zum Empfänger gesendet.

a) Nennen Sie konkrete kryptografische Algorithmen, mit denen die Schritte 1, 2 und 3 jeweils umgesetzt werden können.

b) Diskutieren Sie die Sicherheit des gegebenen Verfahrens unter den genannten Schutzzielen. Wie ließe sich die Sicherheit des Verfahrens verbessern?

c) Wir nehmen an, dass durch Fortschritte bei Quantencomputern alle kryptografischen Algorithmen unsicher werden, die auf Faktorisierung oder diskreten Logarithmen beruhen. Nennen Sie einen kryptografische Algorithmus, der von dieser Entwicklung betroffen wäre und einen, der nicht betroffen wäre.

Klausuraufgabe II

Alice und Bob kommunizieren über ein verschlüsselndes Chatsystem. Dafür haben beide vor Beginn der Kommunikation asymmetrische Schlüsselpaare erstellt und die geeigneten Teilschlüssel sicher miteinander ausgetauscht. Im laufenden Chat wird jede Nachricht sowohl verschlüsselt als auch signiert.

a) Sind die folgenden Aussagen korrekt? *Falls ja, genügt eine einfache Angabe ohne Begründung.* Falsche Aussagen sind zu inhaltlich entsprechenden, sinnvollen Aussagen zu berichtigen.
HINWEIS: Bei Korrekturen von falschen Aussagen genügt es Teile der vorgegebenen Sätze zu streichen bzw. zu ergänzen. Eine einfache Negation der Aussage ist jedoch nicht zulässig.

1. Alice und Bob verwenden jeweils das Verfahren AES für die Erstellung der Schlüsselpaare.
2. Alice hat vor Beginn der Kommunikation Bob ihren privaten Schlüssel zur Verfügung gestellt.
3. Beim Schlüsselaustausch musste auf mögliche Man-in-the-Middle-Angriffe geachtet werden.
4. Ein passiver Angreifer kann den Klartext-Inhalt der verschlüsselten Chat-Nachrichten nicht lesen.
5. Ein passiver Angreifer erhält keinerlei Informationen über den Chatverlauf.
6. Durch Prüfen der Signatur kann Alice sicher erkennen, dass eine Chatnachricht von Bob stammt.
7. Gelangt ein Angreifer an den geheimen Schlüssel von Alice, so kann er damit alle zukünftigen und vergangenen Nachrichten entschlüsseln, die an Alice gerichtet sind.
8. Besitzt ein Angreifer lediglich die öffentlichen Schlüssel, so kann er unter keinen Umständen die Vertraulichkeit des Chatsystems brechen.

b) Alice und Bob möchten über das Chatsystem auch Dateien austauschen, die potenziell mehrere Gigabyte groß sind. Schlagen Sie eine geeignete Erweiterung des Chatsystems vor, die dies effizient ermöglicht und begründen Sie ihren Vorschlag!