Stefanie Jasser

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Nachklausur Modul IT-Sicherheit (A106)

Quartal: (1/2018)

Name des Prüflings: **Matrikelnummer:** **Zenturie:**

Dauer: 90 Min. Seiten der *Klausur* **ohne** Deckblatt: 15 Datum: 02.02.2018

Hilfsmittel:

- Keine (auch kein Taschenrechner)

Bemerkungen:

- **Bitte prüfen Sie zunächst die Klausur (alle Teile) auf Vollständigkeit.**
- **Bitte lösen Sie nicht die Heftung.**

Es sind 90 Punkte erreichbar!

Zum Bestehen der Klausur sind 45 Punkte ausreichend!

Aufgabe:	1	2	3	4	5	6	7	8	Summe:
Erreichbare Punkte:	6	14	6	8	13	21	8	14	90
Erreichte Punkte:									

Note: _____ Prozentsatz: _____ Ergänzungsprüfung: _____

Datum: _____ Unterschrift: _____

Datum: _____ Unterschrift: _____

Aufgabe 1 (6 Punkte)

	Beantworten Sie die folgenden Fragen:	stimme zu	stimme nicht zu
a)	Autorisierung ist ein klassisches Sicherheitsziel der Kryptographie. Es bedeutet, dass der Urheber einer Information bekannt ist.		
b)	Ende-zu-Ende-Sicherheit bedeutet, die gesamte Übertragungsstrecke eines Netzwerkpakets vom Endgerät des Senders bis zum Endgerät des Empfängers bezüglich der vorher festgelegten Schutzziele abzusichern. Sie ist Verbindungssicherheit vorzuziehen.		
c)	Passive Angriffe können die Integrität einer Nachricht nicht verletzen oder deren Verfügbarkeit beeinträchtigen.		
d)	Phishing ist eine verbreitete Methode des Social Engineering, um Nutzer zu bestimmten Handlungen zu verleiten, z. B. der Preisgabe sensibler Informationen oder dem Kauf eines Produkts.		
e)	Steganographische Systeme, die mit Bildern und Audiodateien arbeiten, bringen Informationen in den niederwertigsten Bits unter. Änderungen sind so kaum sichtbar/hörbar.		
f)	Die Nutzung von Fingerabdrücken bzw. Fingerabdruckscannern gilt als heute sicheres biometrisches Authentifizierungsverfahren, da die Fälschung von Fingerabdrücken sehr aufwendig ist.		

Jede richtige Antwort wird mit je 1 Punkt, jede falsche oder nicht gegebene Antwort mit 0 Punkten bewertet.

Aufgabe 2 (14 Punkte)

(2.1) (2 Punkte) Welche Aussage kann über das Monotonieverhalten der Vertraulichkeit sowie ihrer Teilziele getroffen werden? Begründen Sie Ihre Antwort!

(2.2) (4 Punkte) Nennen Sie vier Wechselwirkungen zwischen Schutzzielen, bei denen eine Stärkung oder Schwächung mindestens eines der Schutzziele erfolgt.

(2.3) (4 Punkte) Definieren Sie ein geeignetes Angreifermodell für die Erfassung und Auswertung von Biometriedaten auf einer Intensivstation. Begründen Sie jeweils kurz die Eignung und Konsistenz der Bestandteile des Angreifermodells.

(2.4) (4 Punkte) Grenzen Sie folgende Malware-Begriffe voneinander ab: Computervirus, Computerwurm und Trojanisches Pferd. Beschreiben Sie den Zusammenhang zu Backdoors.

Aufgabe 3 (6 Punkte)

(3.1) (2 Punkte) Was ist ein VPN?

(3.2) (2 Punkte) Warum ist TLS nicht (direkt) für ein VPN geeignet?

(3.3) (2 Punkte) Erläutern Sie, warum das Problem bei IPSec nicht besteht. Gehen Sie auch darauf ein, was Sie in IPSec-basierten VPNs zusätzlich benötigen.

Aufgabe 4 (8 Punkte)

Anlageberaterin Alice versucht Bob als neuen Kunden zu gewinnen.

Alice: Meine Anlage-Empfehlungen sind äußerst wertvoll: Letzten Monat habe ich meinen Kunden diese fünf Aktien empfohlen. Sie haben ihren Wert seitdem verdoppelt.

Bob: Aha. Aber woher weiß ich, dass du mir nicht einfach fünf Aktien genannt hast, die im letzten Monat gut gelaufen sind? Sag mir doch einfach, welche Aktien du momentan empfiehlst. In einem Monat überprüfe ich dann die Qualität deiner Empfehlung – und wenn ich zufrieden bin, dann beauftrage ich dich.

Alice: Das kann ich leider nicht machen. Schließlich könntest du dein Geld mit meiner Empfehlung einfach selbst anlegen – ohne mich zu bezahlen.

Bob: Das mache ich nicht, vertrau mir!

Alice: Das ist mir zu riskant. Aber ich kann dir versichern, dass ich meine Empfehlung nicht nachträglich verändert habe. Vertrau mir!

So kommen Alice und Bob nicht weiter. Entwerfen Sie ein geeignetes Protokoll, bei dem keiner der beiden betrügen kann. Verzichten sie dabei — falls möglich -– auf eine dritte Partei.

Aufgabe 5 (13 Punkte)

(5.1) (6 Punkte) Erläutern Sie Abuse Case Diagramme. Gehen Sie dabei mindestens auf folgende Fragen ein:

- Was sind Abuse Case Diagramme und was stellen sie dar?
- Wann und zu welchem Zweck werden sie eingesetzt?
- Wie ist das Vorgehen zu ihrer Erstellung?

(5.2) (7 Punkte) Erstellen Sie ein vollständiges Abuse Case Diagramm für einen Geldautomaten. Geben Sie mindestens zwei verschiedene Angriffe an.

Aufgabe 6 (21 Punkte)

(6.1) (2 Punkte) Welche grundsätzlichen Ansätze für Identifikation und Authentifikation können beim Systementwurf unterschieden werden?

(6.2) (9 Punkte) Welchen der beiden Zugriffskontrollmechanismen **Full Access with Errors** und **Limited Access** würden Sie für die folgenden Szenarien im Entwurf Ihres Softwaresystems vorsehen:

Begründen Sie Ihre Antwort!

Szenario 1: Sie wollen Amazon Konkurrenz machen und entwickeln einen Online-Shop. Sie haben sich auch einen USP überlegt: Ihr Online-Shop soll von allen IOT-Geräten auf dem Markt bedienbar sein. D. h. zusätzlich zu einer herkömmlichen Web-Oberfläche, soll beispielsweise ein smarter Kühlschrank Lebensmittel oder eine smarte Heizung Öl nachbestellen können.
Natürlich müssen Sie sich an die gängigen Gesetze halten: Beispielsweise können Sie nicht einfach an jeden Kunden Zigaretten oder Alkohol verkaufen. Dafür muss zunächst sein Alter verifiziert werden.

Szenario 2: Dass Netflix im vergangenen Jahr seine Gewinne verdreifachen konnte, weckt auch bei Ihnen den Wunsch, in den Streaming-Markt einzusteigen. Zunächst wollen Sie einen Musik-Streamingdienst und das Streaming von Sport-Events konzentrieren, die in Deutschland sonst nur auf Nebensendern zu empfangen sind. Sobald Sie ausreichend Gewinne machen, wollen Sie dann auch Rechte an größeren Sport-Events erwerben.

Szenario 3: Ihre Marketing-Abteilung ist vom häufigen Tool-Bruch genervt. Um Ihre Mitarbeiter optimal zu unterstützen, wollen Sie Ihren Online-Shop daher um eine fachliche Administrationsmöglichkeit für alle Ihre Fachabteilungen erweitern. Beispielsweise sollen hier die Artikelbeschreibungen, die Lagerbestände auf Basis der Inventur aktualisiert oder auch Nachbestellungen vom Hersteller oder Großhändler angestoßen werden können.

(6.3) (5 Punkte) Leiten Sie mindestens 5 konkrete Architekturvorgaben aus den in der Vorlesung besprochenen Top Ten Security Design Flaws ab.

(6.4) (5 Punkte) Geben Sie für jede der definierten Architekturvorgaben an, wie Ihre Einhaltung durch die Quellartefakte geprüft werden kann: Gehen Sie auch auf die benötigten Artefakte und den Zeitpunkt der Prüfung ein.

Aufgabe 7 (8 Punkte)

(7.1) (3 Punkte) Analysieren Sie folgenden Code und benennen Verwundbarkeiten. Gehen Sie dabei davon aus, dass die genutzten Variablen korrekt deklariert und initialisiert wurden.

Hinweis: Die Methode `getParameter()` des Interface `ServletRequest` gibt eine Zeichenkette zurück.

```
public void loadMemos(ServletRequest request) {
   String memoQuery = "SELECT lastmodified, memocontent, owner " +
                      "FROM memos " +
                      "WHERE owner = " + request.getParameter("user");
   try {
      Statement statement = connection.createStatement();
      ResultSet rs = statement.executeQuery(memoQuery);
      while (rs.next()) {
         page.addTableRow(rs.getDate("lastmodified"),
         rs.getString("memocontent"),
         rs.getString("user"),
         MemoState.valueOf(rs.getString("state")));
      }
   } catch (SQLException e) {
      LOG.warning(e.getMessage());
   }
}
```

(7.2) (5 Punkte) Wägen Sie Vor- und Nachteile von Entwurfs- und Code-Reviews gegeneinander ab. Ist die Durchführung eines Entwurfs- oder Code-Reviews wichtiger? Begründen Sie Ihre Antwort!

Aufgabe 8 (14 Punkte)

(8.1) (2 Punkte) Grenzen Sie Schwachstellenscans und Penetrationtests voneinander ab!

(8.2) (3 Punkte) Beschreiben Sie eine Möglichkeit, den Aufwand von Secure Code Reviews auch in kritischen Softwaresystemen sinnvoll zu begrenzen. Stellen Sie dies anhand eines Beispiels dar.

(8.3) (9 Punkte) Was ist eine Dynamic Taint Analysis? Beschreiben Sie, welche Schritte zu ihrer Durchführung notwendig sind.

Geben Sie außerdem zwei Beispiele für Schwachstellen an, die mittels Dynamic Taint Analysis aufgedeckt werden können. Begründen Sie Ihre Antwort!