Stefanie Jasser

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Klausur Modul IT-Sicherheit (A106)

Quartal: (3/2017)

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

Dauer: 90 Min. Seiten der *Klausur* **ohne** Deckblatt: 19 Datum: 11.10.2017

Hilfsmittel:

- 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	Summe:
Erreichbare Punkte:	6	12	10	11	13	21	17	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)	Durch den Einsatz mehrseitiger IT-Sicherheit schützt eine Partei sich gegen verschiedene Angreifer bzw. Angriffe.		
b)	Die Vertraulichkeit kann nur durch aktive Angriffe beeinträchtigt werden.		
c)	Die Verschlüsselung von Nachrichten schützt deren Integrität.		
d)	Bei einem großen Kreis an Teilnehmern sind symmetrische Verfahren aufgrund der einfacheren Schlüsselverteilung asymmetrischen Verschlüsselungsverfahren überlegen.		
e)	Schalen- und Kettenmodell für die Gültigkeit von Zertifikaten liefern dasselbe Ergebnis, wenn die Gültigkeit des Wurzelzertifikats vor dem Gültigkeitsende der anderen Zertifikate der Hierarchie abläuft.		
f)	Visuelle bzw. auditive Angriffe erlauben die Erkennung und Aufdeckung geheimer Nachrichten, die durch steganographische Verfahren in Hülldaten eingebracht wurden.		

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

Aufgabe 2 (12 Punkte)

(2.1) (1 Punkt) Bei welchem der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit sind die Auswirkungen einer Schutzzielverletzung irreversibel, d.h. unumkehrbar? Begründen Sie Ihre Antwort!

(2.2) (3 Punkte) Auf welchen Schichten des OSI- bzw TCP/IP-Modells kann eine sichere Ende-zu-Ende-Kommunikation stattfinden? Begründen Sie ihre Wahl!

Hinweis: Sichere Kommunikation meint z. B. eine verschlüsselte oder authentifiziert ablaufende Kommunikation.

(2.3) (2 Punkte) Welche Schutzziele können mit IPSec jeweils im ESP- und AH-Modus erreicht werden, welche nicht? Begründen Sie Ihre Antwort!

(2.4) (2 Punkte) Welche Schutzziele werden durch digitale Unterschriften erfüllt? Wie können sie mittels Public-Key-Kryptographie umgesetzt werden?

(2.5) (2 Punkte) Kann ein Dienst verfügbar aber nicht erreichbar sein? Begründen Sie Ihre Antwort!

(2.6) (2 Punkte) Beschreiben Sie ein Verfahren, sichere Passwörter zu generieren, an die Menschen sich dennoch erinnern können.

Aufgabe 3 (10 Punkte)

Der unzufriedene Geheimdienstmitarbeiter Edwin Schneeberger möchte einen streng vertraulichen DES-Verschlüsselungsschlüssel (56 Bit) an die Öffentlichkeit bringen.

Er hat an seinem Arbeitsplatz keinen Internetzugang. Darüber hinaus wird er beim Verlassen seines Arbeitsplatzes jedes Mal auf verdächtige Gegenstände durchsucht. Um den Schlüssel an der Kontrolle vorbei zu schmuggeln, will er eine unauffällige Mineralwasser-Getränkekiste verwenden, die er abends beim Verlassen des Büros mit nach Hause nimmt.

Seine Mineralwasserkiste ist allerdings an einer Ecke leicht beschädigt. In der Kiste lassen sich daher insgesamt nur noch 18 Flaschen transportieren. Edwin überlegt sich folgende Variationsmöglichkeiten, um damit verschiedene Zustände zu kodieren:

- Es können 0 bis 18 Flaschen transportiert werden, d.h. ein Platz in der Kiste kann leer oder mit einer Flasche besetzt sein.
- Eine Flasche kann ganz voll oder ganz leer sein.
- Eine Flasche kann verschlossen (mit aufgeschraubtem Verschlussdeckel) oder offen (ohne Deckel) transportiert werden.
- Eine Flasche kann normal oder verkehrt herum, also auf dem Kopf stehend, transportiert werden.

Kann Edwin mit dieser Kodierung mit einer einzigen Kiste, d. h. auf einmal, den gesamten Schlüssel nach draußen transportieren oder muss er mehrmals gehen? Falls er mehrmals gehen muss, wie oft muss er gehen? Begründen Sie Ihre Antwort!

Aufgabe 4 (11 Punkte)

Zertifizierungsmodelle

Bei der Verschlüsselung und Signierung mithilfe asymmetrischer Kryptographie existieren zwei grundsätzliche Modelle für die Schlüsselzertifizierung: dezentral und hierarchisch-zentral.

(4.1) (1 Punkt) Was ist der Zweck der Schlüsselzertifizierung?

(4.2) (4 Punkte) Erläutern Sie das dezentrale und das hierarchisch-zentrale Zertifizierungsmodell jeweils kurz und prägnant anhand eines Beispiels.

(4.3) (4 Punkte) Nennen Sie zu jedem der beiden Zertifizierungsmodelle je einen Vor- und Nachteil.

(4.4) (2 Punkte) Beschreiben Sie das Konzept der Cross Certification. Welche Vorteile ergeben sich hieraus?

Aufgabe 5 (13 Punkte)

(5.1) (2 Punkte) Stellen Sie dar, wann im Entwicklungszyklus und zu welchem Zweck Attack Trees eingesetzt werden.

(5.2) (6 Punkte) Erstellen Sie einen Attack Tree mit 3-4 Ebenen und mindestens 8 Pfaden für einen Insider-Angriff mit dem Ziel, vertrauliche Informationen zu veröffentlichen.

(5.3) (5 Punkte) Benennen Sie potentielle Gegenmaßnahmen für die möglichen Angriffe und zeichnen Sie diese in den Attack Tree ein. Benennen Sie außerdem diejenigen Angriffe, gegen die keine Gegenmaßnahmen ergriffen werden können.

Aufgabe 6 (21 Punkte)

(6.1) (3 Punkte) Grenzen Sie Security Design Flaws und Security Bugs gegeneinander ab. Welcher Mangel ist kritischer? Begründen Sie Ihre Antwort!

(6.2) (4 Punkte) Welche Art technischer Mängel können neben Entwurfsmängeln und Implementierungsfehlern auftreten? Grenzen Sie diese von den bereits genannten Mängeln ab.
Warum ist die Betrachtung dieser Mängel wichtig für die Sicherheit des Systems? Begründen Sie Ihre Antwort.

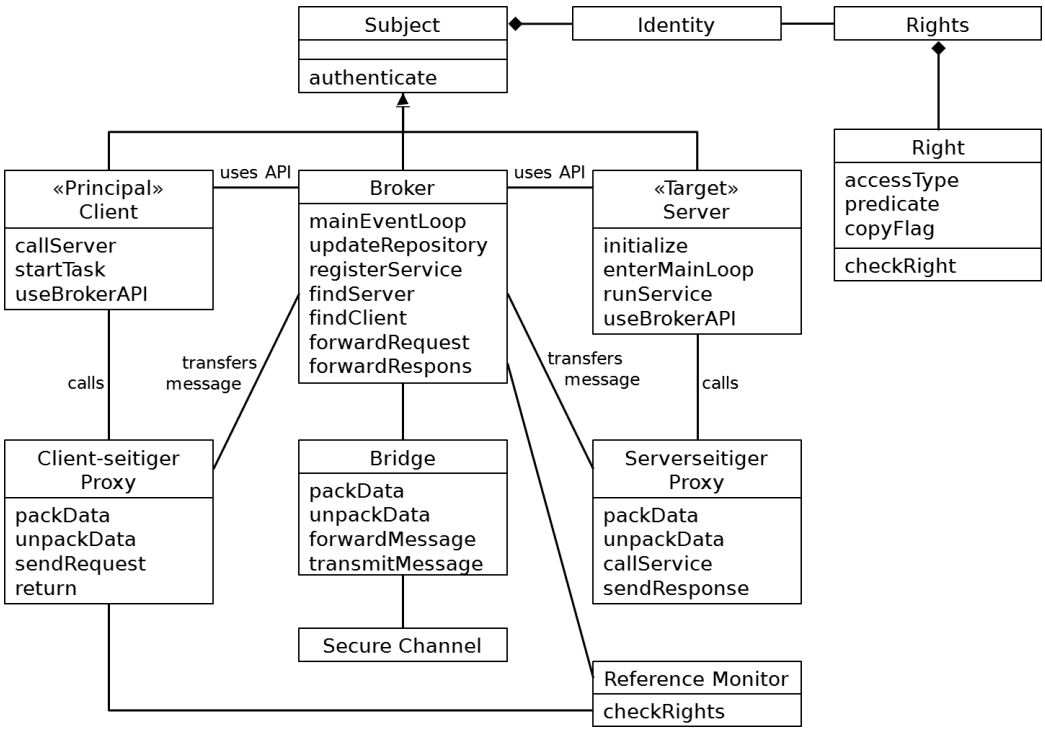
(6.3) (12 Punkte) Analysieren Sie das folgende Security-Entwurfsmuster.
Welchen der verbreiteten Entwurfsmängeln wird entgegengewirkt?
Leiten Sie mindestens 4 sinnvolle, konkrete Architekturvorgaben für die Implementierung ab wie in der Vorlesung besprochen.
Hinweis: Bedenken Sie wie in der Vorlesung ggf. auch implizite Vorgaben, die sich z. B. aus Secure Design Prinzipien ergeben.

Secure Broker:

Das Secure Broker Muster ist eine Variante des Broker Entwurfsmusters: Die Kommunikation unabhängiger Komponenten (Clients, Server) in verteilten Systemen soll abgesichert werden.

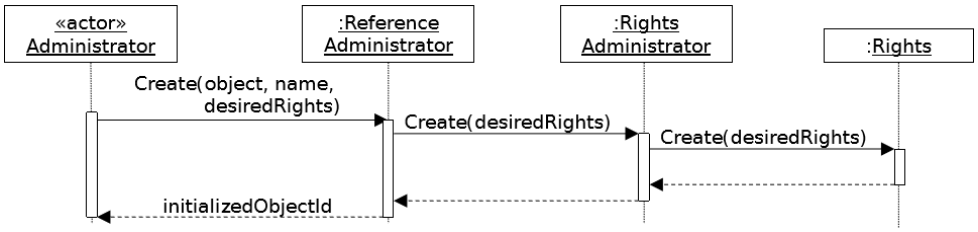
Das Secure Broker Muster implementiert zur Absicherung der Kommunikation die folgende Funktionalität:

- Authentifizierung von Komponenten mittels Identität
- Autorisierung von Anfragen basierend auf der Identität des Anfragenden durch Komponenten selbst, um Verhalten abhängig von Rechten des Anfragenden umzusetzen
- Rechte und Rechtemanagement
- Zugriffskontrolle und Autorisierungsprüfung je Komponente mittels Reference Monitor



Sturktur des Secure Broker Musters

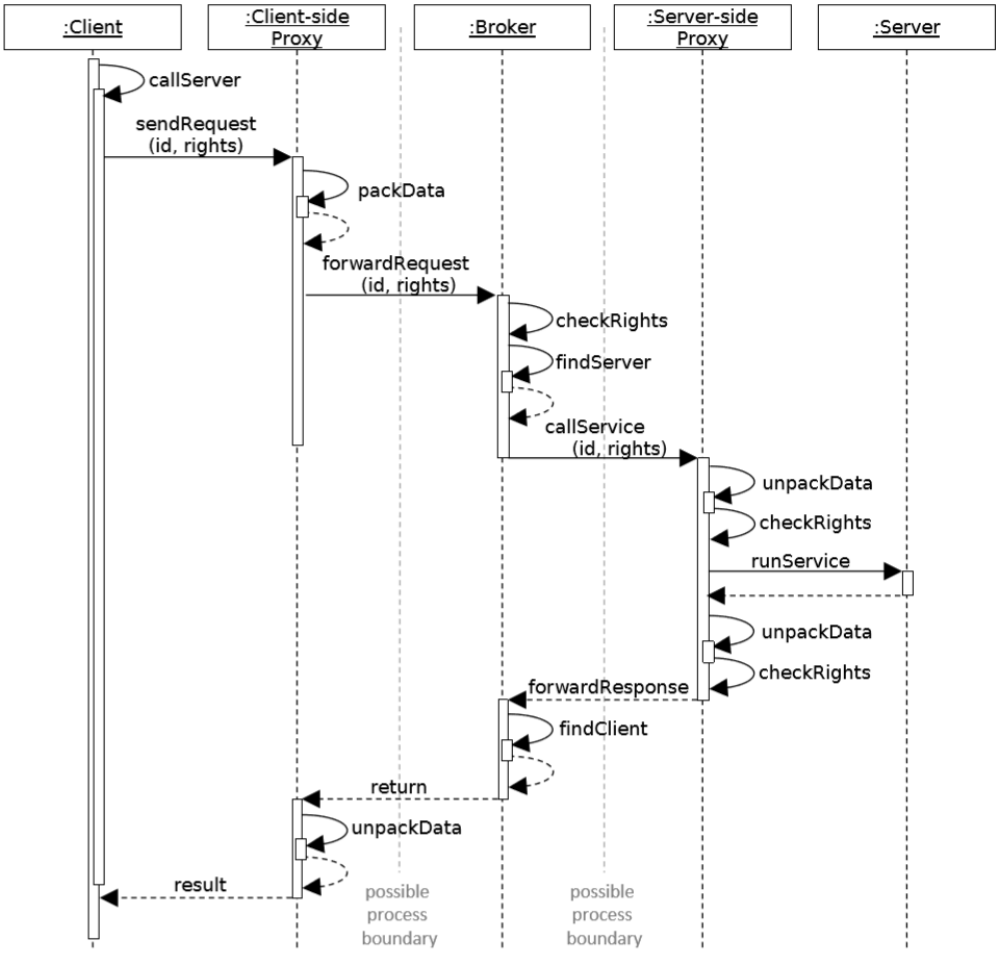
Das Secure Broker Pattern setzt drei zentrale Anwendungsfälle um: Die Erzeugung von Subjekten, die Registrierung und die Anfrage sicherer Services.



Verhalten des Secure Broker Musters bei der Erzeugung von Objekten

Anders als beim ursprünglichen Broker Pattern, bei dem der Broker als vertrauenswürdig gilt, müssen beim Secure Broker Pattern den Hauptkomponenten Server, Clients und Broker Identität und Rechte zugeordnet werden. Dies geschieht während der „Subject Creation“.

Die anschließende Registrierung erfordert – anders als beim klassischen Broker Pattern – eine gegenseitige Authentifizierung.



Verhalten des Secure Broker Musters bei Secure Service Requests

Nach erfolgter Authentifizierung und Registrierung der Hauptkomponenten kann ein Client unter Angabe seiner ID und Rechte Requests senden, die vom client-seitigen Proxy gemarshallt werden. Der Broker leitet den Request nach erfolgreicher Prüfung der Rechte an den server-seitigen Proxy weiter. Der server-seitige Proxy kann nach dem Entpacken ebenfalls eine Prüfung der Client-Rechte durchführen (zusätzlich zum oder anstelle des Brokers) und dann den Service aufrufen. Die Übermittlung der Antwort entspricht dem klassischen Broker Pattern.

Konsequenzen der Verwendung

- Unerwünschter Zugriff auf sensible Daten und Funktionalität kann verhindert werden.
- Gegen unerwünschte Einschränkungen der Schutzziele durch abgefangene Nachrichten(-inhalte) kann Verschlüsselung eingesetzt werden.
- Vorbeugung von Denial-of-Service-Angriffen durch kontrollierten Zugriff auf die am Broker registrierten Server.
- Durch gegenseitige Authentifizierung aller Hauptkomponenten kann Vertrauen zwischen Kommunikationsteilnehmern geschaffen werden.
- Zusätzlicher Overhead und erhöhte Komplexität.

(6.4) (2 Punkte) Warum ist die werkzeuggestützte Identifikation von Verletzungen der Architekturvorgaben für Security problematisch? Welche Maßnahmen können ergriffen werden, um Abweichungen dennoch festzustellen?

Aufgabe 7 (17 Punkte)

(7.1) (4 Punkte) Analysieren Sie folgenden Code und benennen Verwundbarkeiten:

```
private static boolean passwordCompare(char[] a, char[] b){
    if (a.length != b.length) {
        return false;
    }
    for (int i = 0; i < a.length && a[i] == b[i]; i++) {
        ;
    }
    return i == a.length;
}
```

(7.2) (4 Punkte) Erläutern Sie mittels welcher Angriffe solche Verwundbarkeiten ausgenutzt werden können und wie diese durchgeführt werden.

(7.3) (5 Punkte) Wie heißt die von Ihnen angewandte Technik zur Identifikation der Verwundbarkeit? Welche Vor- und Nachteile (je mind. 2) hat sie und wie können die Nachteile eingeschränkt werden?

(7.4) (4 Punkte) Beheben Sie die identifizierten Verwundbarkeiten. Treffen Sie ggf. geeignete Annahmen über die zur Verfügung stehenden Informationen.