JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit
www.m-lehrstuhl.de

Prof. Dr. Kai Rannenberg

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306

Abschlussklausur Vorlesung „Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle“, WS 2006

Punktezahl: 90
Mindestpunktezahl zum Bestehen: 45
Veranstalter: Prof. Dr. Kai Rannenberg
Zugelassene Hilfsmittel: Keine

Achtung – geben Sie das Aufgabenblatt zusammen mit der Klausur ab!

Wir wünschen viel Erfolg!

Matrikelnummer *(Bitte eintragen!)*	

Aufgabe:	**1**	**2**	**3**	**4**	**5**
Punkte:					

Aufgabe:	**6**	**7**	**8**	**9**	**Gesamt**
Punkte:					

Punkte insgesamt:	**Note:**

1 Schutzziele (10 Punkte)

1.1 Nennen Sie die vier klassischen technischen Schutzziele der IT-Sicherheit. **(2 Punkte)**

1.2 Geben sie für jedes Schutzziel entweder eine kryptographische Funktionen an, mit der dieses üblicherweise erreicht wird, oder begründen Sie kurz, dass eine solche Primitive nicht existiert. **(8 Punkte)**

2. Authentifizierung (13 Punkte)

Da verschiedene Angriffe gegen Passwortsysteme denkbar sind, gelten diese in der Literatur nicht als besonders sicher. Andere Authentifizierungsfaktoren werden oftmals als sicherer betrachtet.

2.1 Vor welcher Schwäche von z.B. Passwortsystemen schützen Challenge-Response-Protokolle? **(2 Punkte)**

2.2 Beschreiben sie kurz Angriffe gegen 3 verschiedene Komponenten eines biometrischen Signaturerkennungssystems **(9 Punkte)**

2.3 Warum wird im Zusammenhang mit bestimmten Authentifizierungsfaktoren oftmals Multi-Faktor-Authentifizierung verwendet? Erklären sie dies anhand eines Beispiel-Faktors **(2 Punkte)**

3. Kryptographie (25 Punkte)

Der Lehrstuhl für Mobiles Leben und Arbeiten hat sich entschieden, für seine Studenten eine interne Zertifizierungsstelle einzurichten. Grund dafür ist, dass während der Klausurvorbereitung immer häufiger falsche Lösungen zweifelhafter Herkunft verbreitet wurden, was verhindert werden soll. Aus diesem Szenario ergeben sich die folgenden Entitäten:

1. Ein besonders eifriger Student, der Musterlösungen bereitstellt
2. Student(en) die diese Lösung erhalten sollen
3. Zertifizierungsstelle des Lehrstuhls

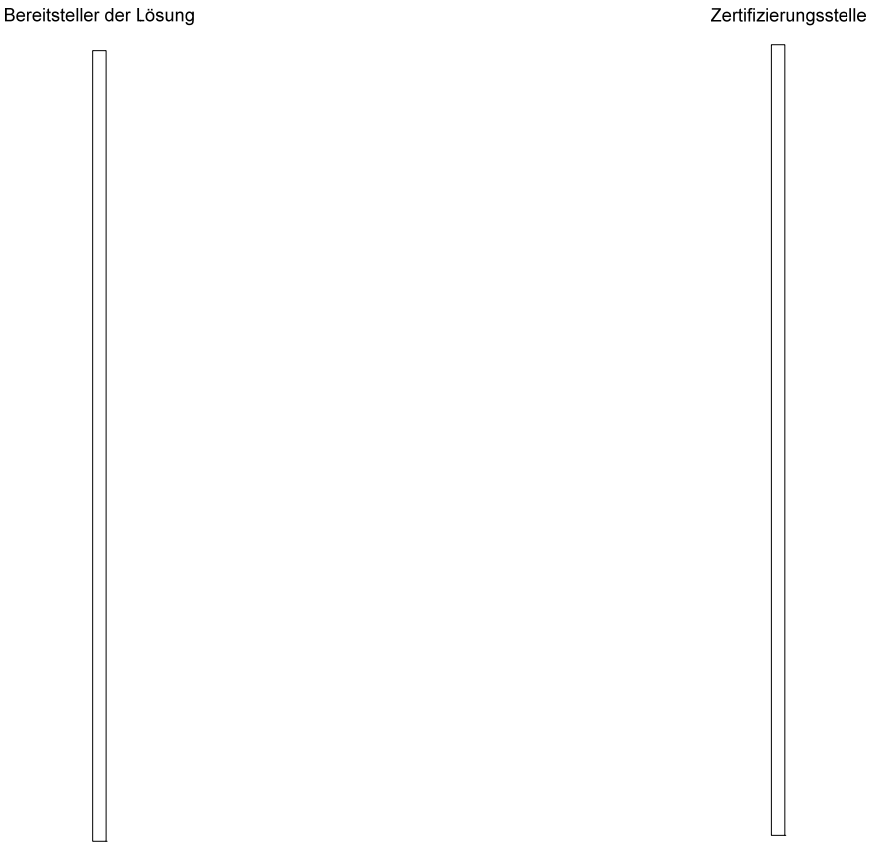
Verwenden Sie bitte das folgende Symbol für Vorgänge im Bereich derselben Entität:

Für den Übergang von einer Entität zur anderen verwenden Sie bitte eine Variation dieses Symbols:

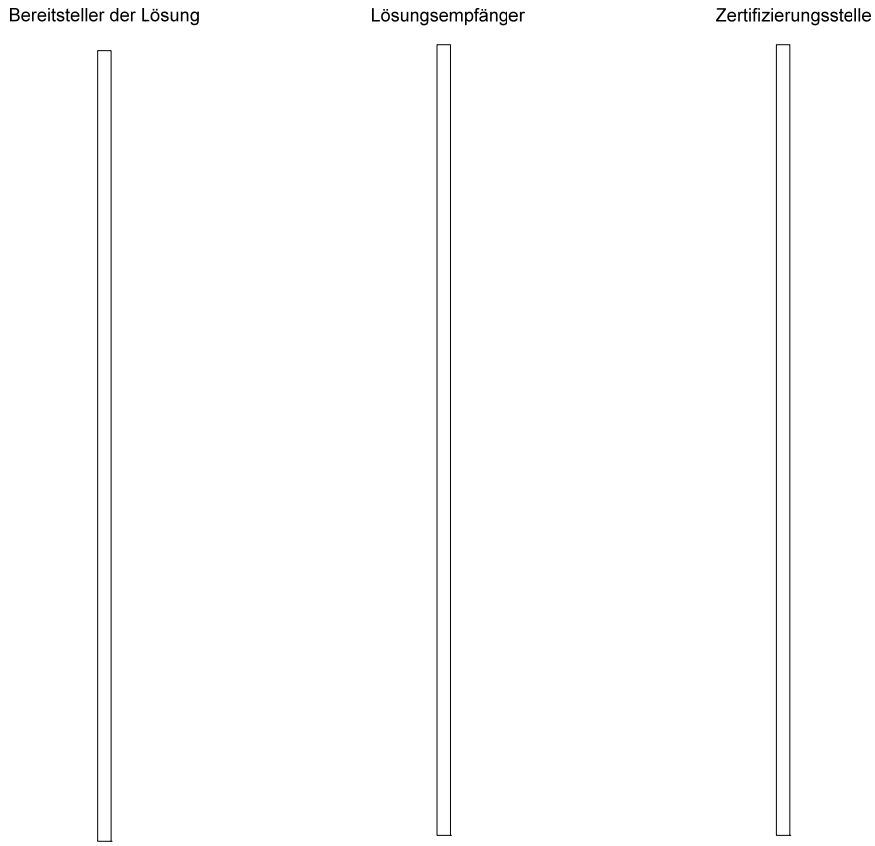
Die Übermittlung der Musterlösungen soll über E-Mail, Webspace, Newsgroups und Diskussionsforen möglich sein, und die gewählte Technologie soll möglichst viele Schutzziele erfüllen.

3.1 Welche Technologie würden Sie wählen, und welche Schutzziele erfüllt sie? **(3 Punkte)**

3.2 Übertragen Sie das folgende Schaubild in Ihr Lösungsheft, und beschreiben Sie dabei den Ablauf für die Zertifizierung. **(10 Punkte)**



3.3 Übertragen sie das folgende Schaubild in Ihr Lösungsheft und beschreiben Sie dabei die sicheren Übermittlung der Musterlösung. **(12 Punkte)**



4. Netzsicherheit (12 Punkte)

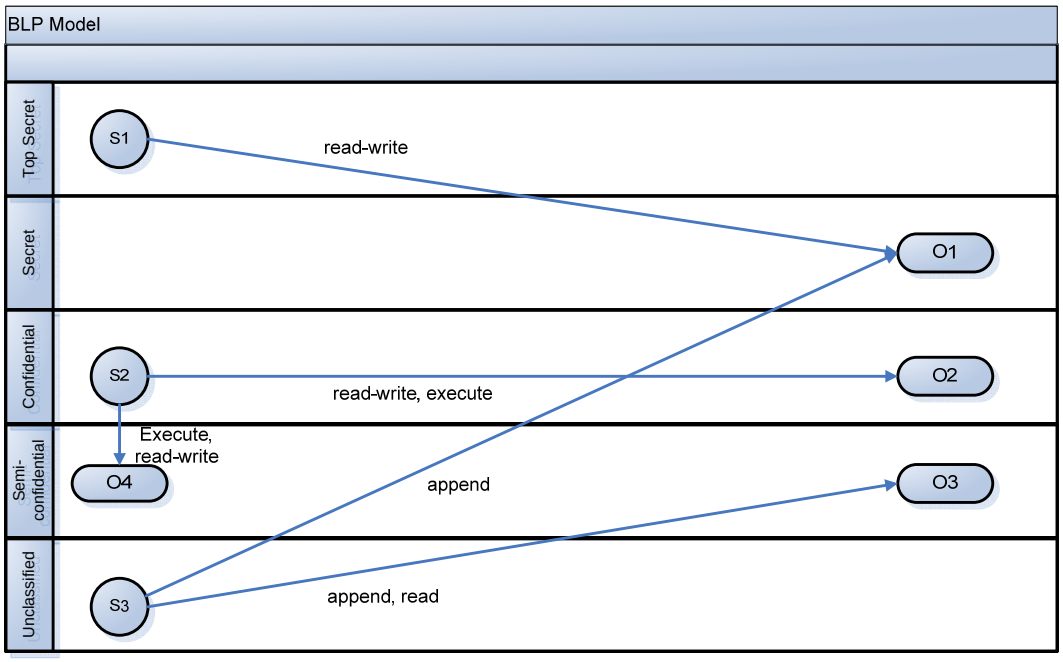
Ein verbreiteter Angriff auf die Netzwerksicherheit ist das sogenannte DNS-Spoofing, gegen welches man sich beispielsweise mit SSL schützen kann.

4.1 Welche Schutzziele im Sinne von Aufgabe 1 werden durch SSL gewahrt? **(2 Punkte)**

4.2 Zeichnen Sie ein Diagramm, vergleichbar mit den Diagrammen aus Aufgabe 3), in dem der Kommunikationsablauf während einer DNS-Spoofing-Attacke dargestellt ist. **(10 Punkte)**

5. Zugangskontrolle (10 Punkte)

5.1 (Bell-LaPadula) Markieren Sie im folgenden Bild die nach Bell-LaPadula zulässigen Zugriffe mit einem Haken an den entsprechenden Verbindungen. **(6 Punkte)**



5.2 (Role-based access control) Sind folgende Aussagen wahr oder falsch? Begründen Sie kurz. **(4 Punkte)**

- Ein Subjekt kann zur selben Zeit nur eine Rolle innehaben.
- Transaktionen können im Rahmen von role-based access control niemals aufgrund der Rolle eines Subjektes autorisiert werden.

6. Systemsicherheit (15 Punkte)

6.1 Welcher Typ von Malware kann von einem Mitarbeiter in einer Organisation so platziert werden, dass er erst nach seinem Ausscheiden (automatisch) ausgelöst wird (, selbst wenn dieses Ereignis für den Mitarbeiter nicht vorhersehbar war)? Beschreiben Sie kurz das Angriffsszenario. **(6 Punkte)**

6.2 Nennen Sie zwei Typen von Viren, die spezielle Eigenschaften haben, die ihr Aufspüren oder ihre Entfernung durch Virenscanner beeinträchtigen. Begründen Sie kurz. **(4 Punkte)**

6.3 Wie nennt man super user unter Unix üblicherweise (noch)? **(1 Punkt)**

6.4 Nennen Sie zwei Sicherheits-Funktionalitäten, die von heutigen Trusted-Computing-Implementierungen oftmals unterstützt werden. **(4 Punkte)**

7. Identity Management (5 Punkte)

7.1 Wofür stehen die 4A, die sie in der Vorlesung kennengelernt haben? Nennen Sie die Begriffe und jeweils ein Beispiel für Funktionen oder Funktionalitäten, die in diesem Bereich anzusiedeln sind. **(4 Punkte)**

7.2 Nennen Sie zwei Verbesserungen der Sicherheit, die durch die Einführung eines SSO-Systems erreicht werden können. **(1 Punkt)**