

1 Begrifflichkeiten

Frage 1. Innerhalb der Zugriffskontrolle existieren die Grundbegriffe Objekt, Subjekt und Zugriffsrecht. Definieren Sie diese Grundbegriffe und führen Sie jeweils Beispiele an.

2 Zugriffskontrolle

Frage 2. Nachfolgende Sätze stellen unterschiedliche Ansätze für Zugriffsrechte dar. Entscheiden Sie, um welchen Ansatz es sich jeweils handelt.

- ① Im _____ Ansatz können explizite Erlaubnisse als auch explizite Verbote formuliert werden. Hierbei sind jedoch Konfliktlösungsstrategien erforderlich.
- ② Im _____ Ansatz können nur explizite Verbote formuliert werden. Im Standardfall besteht eine Erlaubnis falls Verbot abwesend (default-allow).
- ③ Im _____ Ansatz können nur explizite Erlaubnisse formuliert werden. Im Standardfall besteht ein Verbot falls Erlaubnis abwesend (default-deny).

Frage 3. Entscheiden Sie im Zusammenhang mit Zugriffskontroll-Mechanismen, ob folgende Aussagen richtig sind. Kreuzen Sie diese an und korrigieren Sie ggf. falsche.

- ☐ Eine Anforderung an einen Zugriffskontroll-Mechanismus stellt eine eindeutige und fälschungssichere Identifikation von Subjekten und Objekten dar.
- ☐ Eine Anforderung an einen Zugriffskontroll-Mechanismus ist, dass eine autorisierte Manipulation der Zugriffsrechte und Mechanismen möglich ist.
- ☐ Die Anforderung „Ununterbrechbarkeit“ an einen Zugriffskontroll-Mechanismus bedeutet: Atomarität der Abfolge von Rechteprüfung und Zugriff.
- ☐ Benutzerbestimmbare Zugriffskontrollen werden auch Discretionary Access Control (DAC) genannt.
- ☐ Innerhalb der Benutzerbestimmbaren Zugriffskontrollen entscheidet der Subjekteigentümer über Zugriffsrechte.

- ☐ Eine Variante der systembestimmten Zugriffskontrollen sind die rollenbasierten Zugriffskontrollen (Role-based Access Control (RBAC))
- ☐ Role-based Access Control bedeutet, dass die Zugriffsrechte an Gruppen von Subjekten geknüpft sind.
- ☐ Systembestimmte Zugriffskontrolle wird auch (Discretionary Access Control (DAC)) genannt.
- ☐ Innerhalb der systembestimmten Zugriffskontrolle entscheiden Systemregeln über Zugriffsrechte

3 Benutzerbestimmbare Zugriffskontrolle

Frage 4. Erläutern Sie das Prinzip von Capabilities und nennen Sie anschließend Vor- und Nachteile.

4 Systembestimmte Zugriffskontrolle

Frage 5. Innerhalb der systembestimmten Zugriffskontrolle (engl. Mandatory Access Control (MAC)) gewährt ein System Zugriffsrechte gemäß systemweiter Richtlinie. Ein Beispiel für MAC ist unter anderem das Bell/LaPadula-Modell. Dieses Modell wurde 1973 durch David Bell und Len La Padula auf Initiative der US Air Force entwickelt. Beantworten Sie nachfolgende Fragen zum Bell/LaPadula-Modell.

- Welcher Zweck wird mit diesem Modell verfolgt?
- Nennen und beschreiben Sie die unterschiedlichen Regeln dieses Modells und ergänzen Sie die nachfolgende Abbildung mit den in der Legende definierten Zeichen.

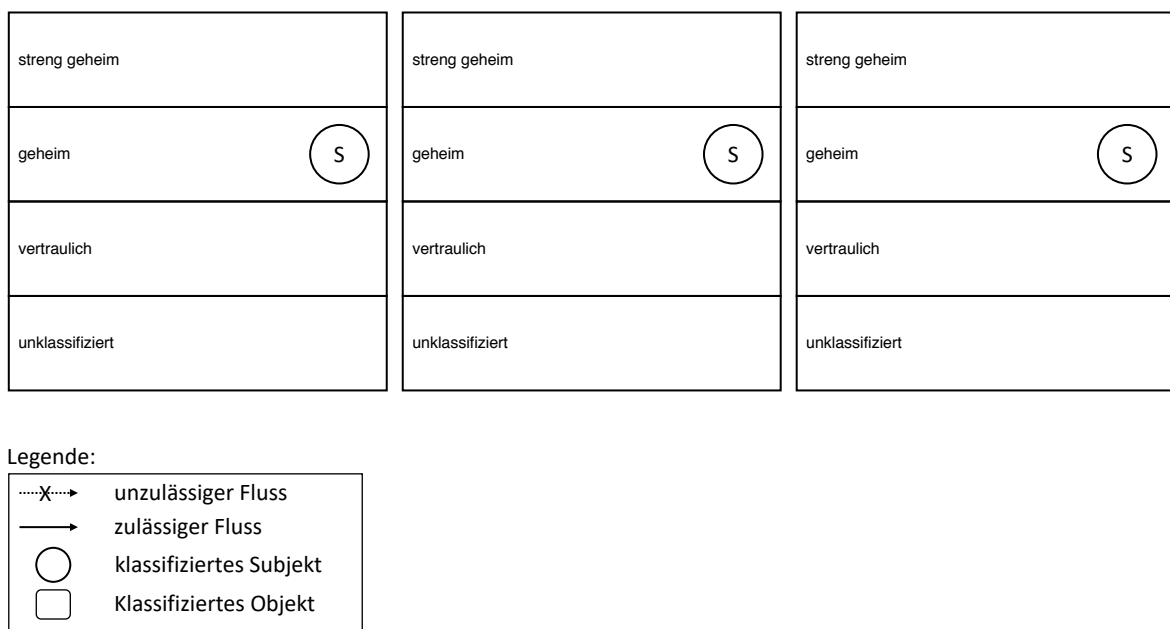


Abbildung 1: Bell/LaPadula-Modell

- Warum reicht die erste Regel in diesem Modell nicht aus?
- Warum stellt die sukzessive höhere Einstufung der Informationen ein Problem dar?
- Welches Schutzziel verfolgt das Modell?

Frage 6. Ein weiteres Beispiel für MAC ist das BIBA-Modell. Dieses Modell wurde 1977 von Ken Biba entwickelt. Es stellt ein duales Modell zum Bell/LaPadula-Modell dar.

- Welches Schutzziel wird mit diesem Modells verfolgt?
- Nennen und beschreiben Sie die Regeln dieses Modells.
- Wenden Sie die Regeln mit allen möglichen Flüssen auf der nachfolgenden Abbildung an.

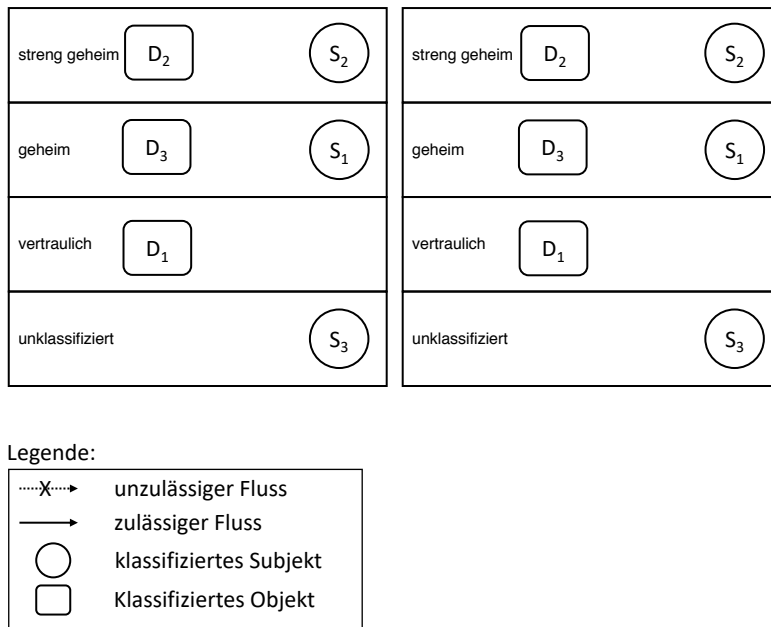


Abbildung 2: BIBA-Modell

5 Rechtevergabe

Frage 7. Sie sind Besitzer eines Verzeichnisses (`/users/username/literature`) in dem sich neben den Dateien (`eBook_Privacy.pdf`) und (`eBook_Security.pdf`) noch weitere Dateien befinden.

- a) Sie besitzen demnach Schreib-, Lese- und Ausführungs-Rechte an der Datei `eBook_Privacy.pdf`. Wie lautet ihre derzeitige ACL an dieser Datei? _____
- b) Sie wollen nun einer Gruppe Lese-Zugriff auf die Datei `eBook_Privacy.pdf` gewähren. Wie lautet die Eingabe, wenn Sie sich bereits im oben genannten Verzeichnis befinden?

- c) Sie stellen nun fest, dass es aufgrund von Anmerkungen innerhalb der Datei besser wäre, wenn die Gruppe die selben Rechte wie Sie besitzen würde. Wie lautet die Eingabe, wenn Sie sich bereit im oben genannten Verzeichnis befinden?

- d) Besitzt die Gruppe nun die selben Rechte an der Datei `eBook_Security.pdf` wie auch an der Datei `eBook_Privacy.pdf` ?

Frage 8. Beantworten Sie folgende Fragen zur Rechtevergabe.

- a) Die Rechte sind derzeit: `- rwx - - - r-x`:
 - Das Objekt ist _____

- Der Eigentümer besitzt _____
 - Mitglieder der Gruppe besitzen _____
 - Alle anderen Benutzer besitzen _____
- b) Innerhalb von Unix erhalten Programme immer die Rechte des Benutzers, der sie startet. Wieso sollten daher Programme aus unsicheren Quellen niemals mit Root-Rechten gestartet werden bzw. Zugriffe auf Verzeichnisse erhalten, die für diese Programme irrelevant sind? Gehen Sie auf diese Problematik ein und nennen Sie mögliche Beispiele.
- c) Erklären Sie kurz was unter den Sonderrechten SUID-Bit, SGID-Bit und Sticky-Bit verstanden wird.

6 Firewalls

Frage 9. Paketfilter, Circuit Level Gateways und Application Level Gateways sind unterschiedliche Typen von Firewalls. Worin bestehen ihre Unterschiede?

Frage 10. Die Kombinationen von Firewall-Komponenten und deren Anordnung wird als Firewall-Architekturen bezeichnet. Benennen und erklären Sie die in der Abbildung dargestellte Firewall-Architektur.

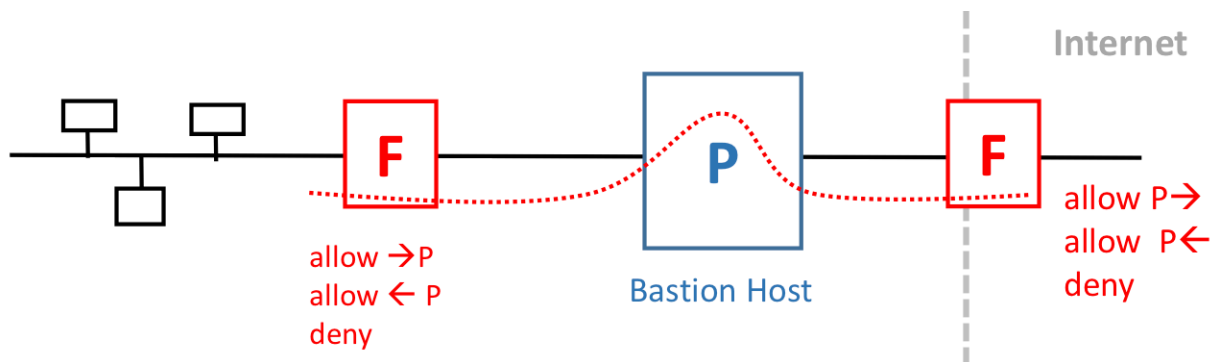


Abbildung 3: _____

Frage 11. Entscheiden Sie, ob folgende Aussagen über die Vorteile sowie Grenzen von Firewalls richtig sind. Kreuzen Sie diese an und korrigieren Sie ggf. falsche.

- ☐ Firewalls tragen zur erhöhten Sicherheit von Netzen bei.
- ☐ Firewalls verbieten die Protokollierung und Erstellung von Nutzer- sowie Dienstprofilen.
- ☐ Firewalls verhindern neben der Ausnutzung von bekannten Schwächen in Netzwerkdiensten oder Kommunikationsprotokollen auch eine Erhöhung der Sicherheit durch eine aufwendige Prüfung mit Paketfiltern.
- ☐ Es bedarf bei Firewalls eines Kompromisses zwischen Schutz und Kosten.

- ☐ Firewalls bieten keinen Schutz vor Angriffen von innen.
- ☐ Firewalls bieten einen perfekten Schutz vor Viren wohingegen sie überhaupt keinen Schutz vor trojanischen Pferden bieten.