2

502470 - Einführung in Sicherheit und Privatheit
Übung: Authentifikation, Identifikation und Zugriffskontrolle
— Disskussion der Lösung während der Übung: 06. Juni 2019 —

1 Authentifikation von Menschen durch IT-Systeme

Frage 1: In der Vorlesung wurden Ansätze zur Authentifizierung von Menschen durch IT-Systeme wie „was der Mensch ist“, „was der Mensch hat/besitzt“ und „was der Mensch weiß“ vorgestellt. Ordnen Sie folgende Punkte den eben genannten Ansätzen zu.

① biometrische Merkmale
② alphanumerische Passwörter
③ Dokument
④ Schlüssel
⑤ graphische Passwörter
⑥ Chipkarte
⑦ kenntnisbasierte Authentifikation

was der Mensch…		
ist:	hat/besitzt:	weiß:

2 Biometrische Merkmale

Frage 2: Biometrische Merkmale lassen sich in physiologische und verhaltensbasierte Merkmale unterteilen. Beschreiben Sie in Ihren eigenen Worten was unter ihnen verstanden wird und führen Sie jeweils zwei Beispiele an.

Frage 3: Rückblickend auf die Vorlesung wurden bereits einige Vor- und Nachteile für biometrische Merkmale genannt. Nennen Sie dennoch zwei Vor- und Nachteile für biometrische Merkmale.

Frage 4: Das Prinzip zur Authentifizierung des Menschen durch biometrische Merkmale basiert auf der Ermittlung und Speicherung der Merkmale sowie dem Vergleich mit den gespeicherten Merkmalen während der Authentifikation. Hierbei kann es zu möglichen Abweichungen kommen. Nennen und beschreiben Sie diese kurz.

Frage 5: In der Vorlesung wurden bereits mögliche Angriffe auf physiologische Merkmale, wie Fingerabdrücke oder Gesichts- und Iris Erkennung, eingegangen. Suchen Sie nun nach möglichen Angriffen auf verhaltensbasierte Merkmale, wie den Gang eines Menschen.

3 Grafische Passwörter

Frage 6: Der picture superiority effect beschreibt, das Nutzer sich Bilder besser merken können als Text. Benennen und beschreiben Sie kurz das in der folgenden Abbildung dargestellte Verfahren für grafische Passwörter. Beschreiben Sie zusätzlich kurz die beiden anderen in der Vorlesung vorgestellten Verfahren.

4 Alphanumerische Passwörter

Frage 7: Alphanumerische Passwörter werden in zahlreichen Bereichen verwendet. Die Wahl des richtigen Passwortes fällt nicht jedem Nutzer leicht. Daher gibt es unterschiedliche Möglichkeiten den Nutzer bei der Auswahl und der Erstellung seines alphanumerischen Passwortes zu unterstützen. Kreuzen Sie richtige Aussagen an und korrigieren Sie ggf. falsche.

- ☐ Eine Richtlinie für Passwörter ist eine ex post Unterstützung.
- ☐ Die Anzeige der Stärke des Passwortes kann eine simultane Unterstützung sein.
- ☐ Die zufällige Änderung des Passwortes zur Erhöhung der Stärke ist eine ex ante Unterstützung.
- ☐ Passwortgeneratoren zählen zu den simultanen Unterstützungen.
- ☐ Die Vorhersage des nächsten Zeichens eines Passwortes ist eine simultane Unterstützung.

5 Authentifikation von IT-Systemen durch Menschen

Frage 8: In der Vorlesung wurde bereits die Man-In-The-Middle-Attack vorgestellt. Definieren Sie daher in Ihren eigenen Worten was unter einer Man-In-The-Middle-Attack verstanden wird.

Frage 9: Voraussetzung für eine Man-In-The-Middle-Attack ist zum einen, dass der Angreifer eine täuschend echte Webseite der Bank betreibt und dieser zum anderen den Kunden dazu bewegt eben diese Seite zu besuchen. Stellen Sie im Zusammenhang mit Online-Banking zunächst kurz die Schwachstellen des TAN-Verfahrens dar. Gehen Sie anschließend auf die Veränderungen durch iTAN und mTAN-Verfahren ein. Wie kommt es durch diese Verfahren zu einer Verbesserung des normalen TAN-Verfahrens?

6 Begrifflichkeiten

Frage 10: Innerhalb der Zugriffskontrolle existieren die Grundbegriffe Objekt, Subjekt und Zugriffsrecht. Definieren Sie diese Grundbegriffe und führen Sie jeweils Beispiele an.

7 Zugriffskontrolle

Frage 11: 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 12: 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

8 Benutzerbestimmbare Zugriffskontrolle

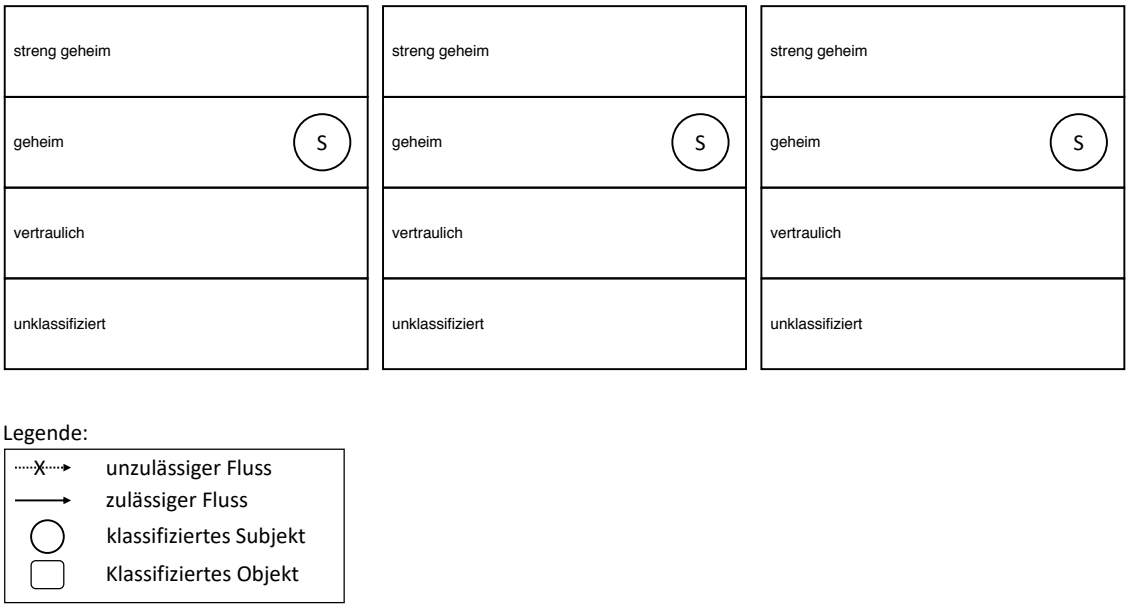
Frage 13: Erläutern Sie das Prinzip von Capabilities und nennen Sie anschließend Vor- und Nachteile.

9 Systembestimmte Zugriffskontrolle

Frage 14: Innerhalb der systembestimmten Zugriffskontrolle (engl. Mandatory Access Control (MAC)) gewährt ein System Zugriffsrechte gemäß systemweiter Richtlinie. Ein Bespiel 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.

a) Welcher Zweck wird mit diesem Modell verfolgt?

b) Nennen und beschreiben Sie die unterschiedlichen Regeln dieses Modells und ergänzen Sie die nachfolgende Abbildung mit den in der Legende definierten Zeichen.



c) Warum reicht die erste Regel in diesem Modell nicht aus?

d) Warum stellt die sukzessive höhere Einstufung der Informationen ein Problem dar?

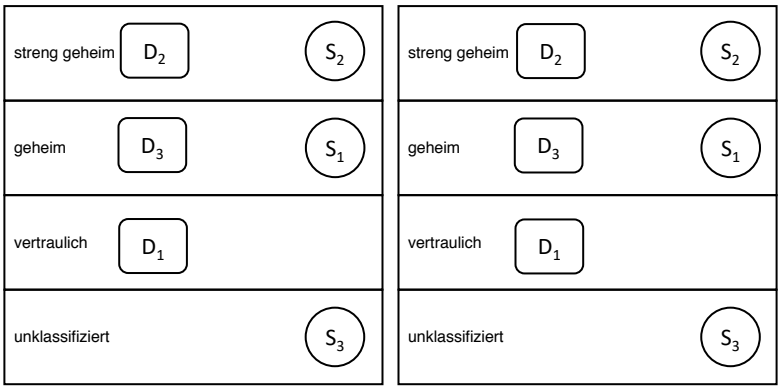
e) Welches Schutzziel verfolgt das Modell?

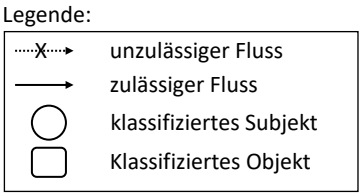
Frage 15: Ein weiteres Beispiel für MAC ist das BIBA-Modell. Dieses Modell wurde 1977 von Ken Biba entwickelt. Es stellt ein duales Modell zum Bell/LaPadula-Modell dar.

a) Welches Schutzziel wird mit diesem Modells verfolgt?

b) Nennen und beschreiben Sie die Regeln dieses Modells.

c) Wenden Sie die Regeln mit allen möglichen Flüssen auf der nachfolgenden Abbildung an.





10 Rechtevergabe

Frage 16: 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. Standardmäßig besitzen o + g keine Rechte.

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 17: 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.