502470 - Einführung in Sicherheit und Privatheit Ubung: Authentifikation und Identifikation Diskussion der Lösung während der Übung: 19. November 2018 —

Authentifikation von Menschen durch IT-Systeme 1

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.



Abbildung 1

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 Angriffe zur Ermittlung von Passwörter

Frage 8. Durch welche Verfahren lassen sich Angriffe auf alphanumerische Passwörter durchführen?

Frage 9. Wodurch unterscheidet sich die Zwei-Stufen-Authentifizierung von den bisherigen?

6 Authentifikation von IT-Systemen durch Menschen

Frage 10. 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 11. 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?