TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2021/22

12. Aufgabenblatt – Sicherheit I

Geplante Bearbeitungszeit: 17.01.2022 – 21.01.2022

Aufgabe 12.1 Grundlagen

(a) Angenommen, Ihre Aufgabe ist es, ein sicheres IT-System zu entwerfen. Bezogen auf die Sicherheit, was sind die drei wesentlichen Aspekte, die Sie bei Ihrem Entwurf berücksichtigen müssen?

(b) Was sind Schutzziele? Nennen und erläutern Sie mindestens drei Schutzziele.

(c) Was ist ein Angreifermodell? Warum ist es notwendig, ein Angreifermodell festzulegen?

(d) Nennen und erläutern Sie Eigenschaften, die zur Beschreibung eines Angreifermodells verwendet werden können.

Aufgabe 12.2 Authentikation

(a) Welche unterschiedlichen Faktoren können benutzt werden, damit sich ein Mensch gegenüber einer Maschine authentifizieren kann? Nennen Sie Beispiele für die einzelnen Faktoren.

(b) Was ist bei Passwort-basierter Authentikation im Internet zu beachten? Wie sollten Passwörter übertragen und gespeichert werden?

(c) Nehmen wir an, einem Angreifer steht ein System mit 8 Grafikkarten zur Verfügung, wobei jede Grafikkarte 32 Gigahashes je Sekunde (GH/s) berechnen kann bei dem gewählten Hashing-Algorithmus (z.B. MD5). Wie lange dauert es (Erwartungswert), um ein zufällig gewähltes Passwort zu brechen (d. h. der Hashwert des Passwortes liegt vor), welches

   (a) 8 Zeichen lang ist, wobei nur Kleinbuchstaben verwendet werden

   (b) 8 Zeichen lang ist, wobei Kleinbuchstaben, Großbuchstaben und Ziffern verwendet werden

   (c) 12 Zeichen lang ist, wobei nur Kleinbuchstaben verwendet werden

   (d) 12 Zeichen lang ist, wobei Kleinbuchstaben, Großbuchstaben und Ziffern verwendet werden

(d) Wie ändern sich die Zeiten aus (c), wenn als Hashalgorithmus `scrypt` verwendet wird (1 MH/s)?

(e) Inwiefern sind Ihre Berechnungen aus (c) und (d) aus Sicherheitssicht richtig und inwiefern nicht?

Aufgabe 12.3 Diskussion von IT-Sicherheit an Hand ausgewählter Beispiele Diskutieren Sie Schutzziele, Angreifermodelle und mögliche Sicherheitsmaßnahmen für folgende beispielhafte Anwendungsfälle:

(a) Betrieb einer öffentlichen Web-Seite zur Informationsverbreitung (etwa Wikipedia)

(b) IT-System, welches eine elektronische Patientenakte umsetzt

(c) Einbindung eines IoT-Temperatursensors in eine Smart Home Umgebung, um beispielsweise die Heizung zu regeln.

(d) Ein IT-System, welches es Rettungsfahrzeugen durch Übermittlung entsprechender Nachrichten erlaubt, die Ampelschaltungen an Kreuzungen so zu beeinflussen, dass die Rettungsfahrzeuge freie Fahrt haben.