Vorbemerkungen und Abgabe

Das SVS-Übungsblatt besteht aus Pflicht-Aufgaben und optionalen Aufgaben. Nur die Pflicht-Aufgaben müssen von Ihnen abgegeben werden. Wir erwarten, dass Sie diese eigenständig lösen. In den optionalen Aufgaben behandeln wir ausgewählte Detailaspekte, die Inhalte aus der Vorlesung erweitern bzw. vertiefen. Die optionalen Aufgaben müssen nicht abgegeben werden. Die Auseinandersetzung mit diesen Aufgaben ist jedoch u. U. zur Beantwortung der Pflicht-Aufgaben erforderlich, in jedem Fall aber eine gute Vorbereitung auf die Klausur. Nur die Pflicht-Aufgaben werden korrigiert und für den Erhalt des Übungsscheins herangezogen (50%-Regel). Der Inhalt aller Aufgaben ist klausurrelevant.

Der Besuch der Vorlesung ist für das Verständnis der Inhalte und die erfolgreiche Teilnahme an der Klausur essenziell. Die Termine finden Sie unter **https://www.inf.uni-hamburg.de/de/inst/ab/svs/courses/bachelor/gss.html**

Die Abgabe erfolgt online unter **https://svs.informatik.uni-hamburg.de/submission/for/gss16-1**; bitte nicht per E-Mail abgeben! Abgaben müssen exakt eine PDF-Datei umfassen und können bis zum Ablauf der Frist mittels eines Zugriffscodes (GSSxx-xxxx-xxxx-xxxx-xxxx), der beim 1. Hochladen angezeigt wird, beliebig oft aktualisiert werden. Eine spätere Abgabe ist nicht möglich. Wird kein Zugriffscode angezeigt wird, war das Hochladen wahrscheinlich nicht erfolgreich. Versuchen Sie es in diesem Fall erneut. Falls das System nicht erreichbar ist, können Sie zur Wahrung der Frist ihre Lösung notfalls per E-Mail an ezimmer@informatik.uni-hamburg.de schicken. Die Bewertungen sind rechtzeitig vor den Übungen (spätestens am Tag der Übung morgens) ebenfalls online einsehbar. Bitte bringen Sie ggf. selbst einen Ausdruck Ihrer Lösung zum Übungstermin mit.

Aufgabe 1: Allgemeine Aussagen zur IT-Sicherheit

1. **Verteilte Systeme (Optional)** – Was ist ein verteiltes System? Nennen Sie drei Beispiele für verteilte Systeme!
2. **Sicherheit verteilter Systeme (Optional)** – Welche Vor- bzw. Nachteile bzgl. der Sicherheit bietet ein verteiltes System gegenüber einem nicht-verteilten System?
3. **Ursachen (Optional)** – Nennen Sie die Ihrer Meinung nach drei häufigsten Ursachen für mangelnde IT-Sicherheit in Unternehmen. Wo finden Sie belastbare Referenzen für Ihre Vermutungen?
4. **Digitale Signaturen (Optional)** – Was ist der Unterschied zwischen einer Signatur und einer digitalen Signatur?

Aufgabe 2: Schutzziele

1. **Abgrenzung I (Pflicht, 5 Punkte)** – Erläutern Sie die folgenden Schutzziele indem Sie sie jeweils voneinander abgrenzen! Definitionen sind unzureichend.

   a) Anonymität, Pseudonymität und Unbeobachtbarkeit

   b) Vertraulichkeit und Verdecktheit

2. **Abgrenzung II (Pflicht, 4 Punkte)** – Erläutern Sie die folgenden Schutzziele indem Sie sie jeweils voneinander abgrenzen! Definitionen sind unzureichend.

   a) Integrität und Zurechenbarkeit

   b) Verfügbarkeit und Erreichbarkeit

3. **Techniken (Pflicht, 4 Punkte)** – Nennen Sie für jedes der obigen Schutzziele eine geeignete Technik, mit der das Schutzziel umgesetzt bzw. adressiert werden kann.

Aufgabe 3: Angreifermodell

1. **Angreifermodell (Optional)** – Was versteht man unter einem Angreifermodell und warum stellt man es auf? Welche einen Angreifer beschreibenden Kriterien werden in einem Angreifermodell berücksichtigt? Geben Sie zu jedem Kriterium auch die konkreten Ausprägungen an.

2. **Praxisbeispiel (Pflicht, 10 Punkte)** – Stellen Sie das Angreifermodell für das Abheben von Bargeld an Geldautomaten mit einer EC-Karte auf.

Aufgabe 4: Angriffsformen

In der Vorlesung wurden verschiedene Angriffsformen beschrieben (siehe Folie Nr. 24, Foliensatz „Einführung in die IT-Sicherheit“ unter **https://www.inf.uni-hamburg.de/de/inst/ab/svs/courses/material/slides.html**). Lesen Sie sich die beiden untenstehenden Situationsbeschreibungen durch. Überlegen Sie sich dann, wie diese Systeme auf aktive oder passive Angriffe reagieren und welche Schutzziele dadurch bedroht sind. Für welche Angriffsart bzw. Angriffsarten sind die Systeme anfällig? Was wären mögliche Gegenmaßnahmen?

1. **Essenslieferungen (Optional)** – Unmittelbar vor der Durchführung eines militärischen Kampfeinsatzes steigt die Anzahl der Essenslieferungen (Pizza, Burger, Croques, Sushi, ...), die an die Adresse des Verteidigungsministeriums geliefert werden, massiv an.

2. **Liste bekannter WLAN-AP SSIDs (Optional)** – Viele öffentliche WLAN-Access-Points (APs) teilen allen Stationen (Clients) in Reichweite ihren Netznamen (SSID) mit. Der Nutzer einer Station wählt aus der Liste aller Stationen anhand der SSID das Netz mit dem er sich verbinden will. Damit der Nutzer diese Auswahl nicht jedes Mal wieder treffen muss, verbinden sich die Stationen automatisch mit Access Points, mit denen sie bereits verbunden waren. Hierzu wird eine Liste der bereits bekannten SSIDs auf der Station aufbewahrt. Stehen an einem Ort mehrere APs mit derselben SSID zur Auswahl, verbindet sich eine Station i.d.R. mit dem AP mit der größten Signalstärke.

Aufgabe 5: Passwortsicherheit

1. **Eigenschaften kryptographischer Hashfunktionen (Optional)** – Erläutern Sie drei der sechs Eigenschaften kryptographischer Hashfunktionen!

2. **Einfaches Hash-Verfahren (Optional)** – Durch kryptographische Hash-Funktionen können Kennwörter sicherer als im Klartext hinterlegt werden. Nennen Sie zwei Gründe, warum die Kennwörter in einem IT-System nicht im Klartext abgespeichert werden sollten.

   Wie funktionieren Kennwortspeicherung und -prüfung unter Verwendung einer Hash-Funktion im einfachsten Fall? Warum ist dieses Verfahren sicherer als die Abspeicherung im Klartext?

3. **Brute-Force-Angriff (Pflicht, 3 Punkte)** – Bei vielen Unix-Betriebssystemen wurden früher lediglich die ersten acht Stellen eines Kennwortes verwendet. Wie lange benötigt ein Passwort-Cracking-Tool in diesem Fall maximal, das eine Million Passwörter pro Sekunde prüfen kann, wenn bekannt ist, dass das Passwort lediglich aus alphanumerischen Zeichen besteht. Wäre es im Vergleich dazu für das Passwort-Cracking-Tool aufwändiger, wenn das Betriebssystem keine Beschränkung der Kennwortlänge hat und bekannt ist, dass das Passwort nur aus Zahlen und maximal 16 Stellen besteht?

4. **Time-Memory-Trade-Off (Optional)** – Eine leistungsfähige Technik, mit der auf Basis eines Hashwerts ein dazu passendes Passwort ermittelt werden kann, stellen sogenannte *Rainbow Tables* dar. Zur Beantwortung können Sie **http://www.h-online.com/security/features/Cheap-Cracks-Of-dictionaries-and-rainbows-746217.html** heranziehen.

   Was versteht man in diesem Zusammenhang unter dem Begriff *Time-Memory-Trade-Off*? Was ist die grundsätzliche Idee von Rainbow Tables bzw. den Vorgänger-Verfahren. Was haben Rainbow Tables mit dem Regenbogen zu tun?

5. **Salting (Optional)** – Einen wirksamen Schutz gegen Rainbow Tables stellt das Hinzufügen einer zufälligen Zeichenkette (auch „Salt“ genannt) vor dem Anwenden der Hash-Funktion h auf ein Kennwort dar, was als $h(\mathrm{SALT}|\mathrm{PASSWORD})$ ausgedrückt werden kann. Warum?

6. **Dictionary-Attack (Optional)** – Schreiben Sie ein Programm (z. B. in Java, Ruby, Python oder Perl) zum Ermitteln eines Kennworts anhand eines Hashwerts mit einem Wörterbuch-Angriff. Besorgen Sie sich dazu ein deutsches Wörterbuch aus dem Internet. Testen Sie Ihre Implementierung mit den unten angegebenen Daten. Über das gespeicherte Kennwort sind die folgenden Fakten bekannt: Es ist ein deutsches Wort, steht im Wörterbuch, ist kleingeschrieben und nicht länger als 5 Zeichen. Das Salt wird beim Hashen vor das Passwort gestellt. Bei der Hash-Funktion handelt es sich um MD5.

   ```
   # user;salt:hash
   berta;xohth4dew5p8:199f066a0bac4140e792d1d4a434ae44
   ```

   Welches Kennwort konnten Sie ermitteln? Skizzieren Sie die Funktionsweise Ihres Programms anhand der wichtigsten Stellen Ihres Programms (bitte nicht separat abgeben, sondern ins PDF einfügen). Achten Sie dabei auf Verständlichkeit und Übersichtlichkeit.

   Wie müsste das Programm erweitert werden, wenn das Salt im Vorfeld nicht bekannt wäre?