SECURITY-Prüfung am 31.3.2006

Name: [redacted]

1.) Welche angegebenen Schutzmethoden eignen sich für den Softwareschutz vor Raubkopien?
- a) Dongle
- b) Hotline
- c) Intrusion Detection System
- d) Zusendung von kostenlosen Updates an den Kunden
- e) Schlechtes Preis-/Leistungsverhältnis
- f) ständige Darstellung des Namens des SW-Lizenznehmers am Bildschirm
- g) keine Dokumentation

2.) Welche Kennwerte (Qualitätsmerkmale) sind bei biometrischen Daten besonders wichtig?
-) wie leicht kann die Eingabe beobachtet werden
-) wie viele Daten werden bei der Merkmalsextraktion weggeworfen
-) wie viele berechtigte Personen werden abgelehnt
-) wie fest muss der Finger bei einem Fingerabdrucksystem auf den Sensor gepresst werden
-) wie viele unberechtigte Personen werden zugelassen
-) Die Referenzdaten können nicht aufgenommen werden, da die Qualität zu gering ist, z.B. schlecht ausgeprägte Papillarlinien der Finger

3.) Sicherheitseigenschaften sind (1) Authentizität (Authenticity), (2) Integrität (Integrity), (3) Vertraulichkeit (Confidentiality), (4) Verfügbarkeit (Availability), (5) Verbindlichkeit (Non-repudiation) und (6) Abrechenbarkeit (Accountability). Welche Sicherheitseigenschaften werden von jedem nachfolgend angegebenen Mechanismus / Verfahren sehr gut erfüllt? Bitte tragen sie maximal 2 geeignete Nummern ein.
- (3) (2) Symmetrische Verschlüsselung
- (1) (3) Passwort
- (5) (1) Digitale Signatur
- (6) (4) Protokollierung

4.) Was ist Steganographie?
- a) mit ihr können Informationen so vermittelt werden, dass ein nicht eingeweihter Dritt die Existenz dieser Information nicht merkt
- b) sie ist eine Form der symmetrischen Datenverschlüsselung
- c) mit ihr kann auf spezielle Form eine Digitale Signatur erzeugt werden
- d) ein Verfahren arbeitet mit Veränderung von Helligkeits- und Farbwerten von Pixel

5.) Ein IT-Sicherheitsmanagement in einem Unternehmen nach dem Grundschutzhandbuch durchläuft mehrere Phasen. Welche nachfolgend angegebener Phasen gehören zu einem üblichen IT-Sicherheitsmanagement?
- X) Erstellung einer Sicherheitspolitik
- X) Festlegung eines Sicherheitsmanagementteams
-) Design und Entwicklung einer Firewall
- X) Analyse (Soll-Ist-Vergleich etc.)
-) Entwicklung von Viren
-) Ernennung einer Geschäftsführung
- X) Aufrechterhaltung im laufenden Betrieb

6.) Welche Angaben über marktübliche Chipkarten (z.B. Bankkarten) sind richtig?
a) sie hat 2 MByte Benutzerspeicher
b) durch die Funktion der gegenseitigen kryptografischen Authentifikation kann auch über große Entfernungen überprüft werden, ob eine Chipkarte echt ist und die Chipkarte kann selbst die Echtheit ihres „Gegenübers" überprüfen
c) sie kann sinnvoll eingesetzt werden, um die Daten der Festplatte z.B. auf einem PC online zu verschlüsseln
d) sie besitzt einen Lautsprecher
e) sie besitzt ein Display
f) sie ist geeignet für kryptografische Aufgaben wie die Digitale Signatur
g) sie hat Sicherheitsmechanismen gegen Hardwareattacken und Datenveränderungen

7.) Welche Eigenschaften/Vorsichtsmaßnahmen soll ein sicheres Passwort aufweisen und was soll der Benutzer dabei berücksichtigen?
) es soll sehr kurz sein (z.B. 3 Zeichen), damit man es sich leichter merkt
) mit der Passworteingabe gibt man eine Willenserklärung ab
c) es soll nur einmal pro Jahr geändert werden
d) es soll ein Tastaturmuster enthalten (z.B sechs nebeneinander liegende Tasten)
e) es soll aus einer Kombination aus Straßenbezeichnung und Hausnummer der eigenen Büroadresse bestehen
f) es soll vor jeder neuen Passworteingabe die letzte erfolgreiche Passworteingabe mit Uhrzeit und Datum angezeigt werden
g) bei einem Passwortwechsel soll eines der letzten drei gewählt werden
h) es soll auf einem Notizzettel notiert werden, damit man es nicht vergessen kann
i) es soll aus Ergebnissen des aktuellen Sports codiert werden (z.B. Name und Punkte des Drittplazierten der deutschen Fußballbundesliga)
) Eliminierung mehrer Zeichen eines längeren bekannten Wortes

8. Ein Dokument wurde mit einer digitalen Signatur versehen und an den Empfänger per Internet übertragen. Der Empfänger überprüft nun die digitale Signatur. Welche Schritte werden dabei auf Empfängerseite unter anderem durchgeführt. Welche unten angegebenen Schritte sind dabei richtig?
a) Dokument wird mit dem öffentlichen Schlüssel entschlüsselt
b) Dokument wird mit dem geheimen Schlüssel entschlüsselt
c) Dokument wird mit einer Hashfunktion komprimiert
d) Dokument wird mit einer Hashfunktion entkomprimiert
e) mitübertragene Signatur wird mit dem öffentlichen Schlüssel entschlüsselt
f) mitübertragene Signatur wird mit dem geheimen Schlüssel entschlüsselt
g) Ergebnis der Hashfunktion wird mit dem öffentlichen Schlüssel entschlüsselt
h) Ergebnis der Hashfunktion wird mit dem geheimen Schlüssel entschlüsselt
i) zuletzt werden zwei der oben angegebenen Ergebnisse verglichen

9.) Welche Angaben über biometrische Authentifizierung sind FALSCH?
) Es werden unberechtigte Benutzer sicher abgelehnt
) Biometrische Daten können auch von speziellen Chipkarten gespeichert und überprüft werden
) Iris-Scan: sehr schlechte Ergebnisse, weil eine geringe Merkmalsvielfalt vorliegt
) Fingerabdruck: geringe Fälschungsmöglichkeiten, Benutzer gibt eine Willenserklärung ab, Ähnlichkeit bei engen Verwandten
) Gesichtserkennung: sehr gute Unterscheidbarkeit, Benutzer gibt Willenserklärung ab
) Handschrift: es geht nicht um das Aussehen, sondern um die Dynamik der Handschr (z.B. Anpressdruck des Schreibstiftes, deren Änderungen, die Geschwindigkeit und Beschleunigung des Schreibstiftes während des Schreibvorganges)

10.) Was ist ein CRC (Cyclic Redundancy Check)
a.) mit dem CRC wird in einem PC in zeitlich zyklischen Abständen überprüft, ob der Code richtig ist
b.) CRC Verfahren enthalten ein sogenanntes Generator-Polynom (z.B. bedeutet CRC-16, dass das Generator-Polynom vom Grad 16 ist)
c.) Im ersten Schritt des Verfahrens werden die zu schützenden Daten mit dem Grad des Generator-Polynoms multipliziert (d.h. an die Daten werden entsprechend dem Grad des Generator-Polynoms NULLEN angehängt; z.B. 16 Nullen bei CRC-16)
d.) Die daraus entstandene neue Bitfolge wird durch das Generator-Polynom geteilt (dividiert) und das Ergebnis der Division ermittelt. Das Ergebnis der Division wird zu den schützenden Daten hinzugezählt
e.) Der Empfänger kann nun die erhaltenen Daten durch das Generator-Polynom ebenfalls teilen (dividieren). Ist das Ergebnis dieser Division 0, sind die Daten korrekt. Ist das Ergebnis der Division ungleich 0, ist ein Fehler in den Daten aufgetreten

11.) Was sind üblicherweise KEINE Angriffspunkte für eine Konkurrenzspionage gegen Unternehmen?
a) Kommunikation mit einer Zweigstelle mit sicher digital signierten Daten
b) Geschäftsführer des Unternehmens
c) Reinigungspersonal
d) Der Papierkorb mit wichtigen ausgedruckten Dokumenten
e) Besucher, die persönlich vom Portier abgeholt und wieder zurück gebracht werden
f) Kompromittierende Abhörung
g) Trojaner

12.) Welche Angaben über Hash-Verfahren sind richtig?
a) Mit einer Hash-Funktion können große Datenmengen in eine kleine Datenmenge (meist fixer Länge) abgebildet werden
b) Hash Verfahren werden für die asymmetrischen Verschlüsselung verwendet
c) Aus dem Hash-Wert kann auf die Quelldaten geschlossen werden
d) Hash-Verfahren werden für die Erzeugung der Digitalen Signatur benötigt
e) Der MT42 ist ein bekanntes und verbreitetes Hash-Verfahren
f) Der SHA-1 ist ein bekanntes und verbreitetes Hash-Verfahren

13.) Was sind spezifische Eigenschaften der symmetrischen Kryptografie?
a) Die Verfahren sind meist viel schneller als bei der asymmetrischen Kryptografie
b) Der Ver- und Entschlüsselungsschlüssel sind identisch
c) Man kann sie für die Erzeugung der Digitalen Signatur verwenden
d) Die Schlüssel sind relativ lang (z.B. 1024 Bit)
e) Der Ver- und Entschlüsselungsschlüssel sind verschieden
f) Der Schlüsselaustausch ist schwieriger als bei der asymmetrischen Kryptografie

14.) Welche Angaben über Patente, Urheberrecht und Markenschutz sind richtig?
a) Ein Patent gilt bis 70 Jahre nach dem Tod
b) Das Urheberrecht muss am Patentamt angemeldet werden und gilt maximal 20 Ja
c) Mit dem Markenschutz schützt man Logos, Namen etc.
d) Eine Marke muss beim Patentamt angemeldet werden
e) Das Urheberrecht gilt sofort ab Schaffung des Werkes und es erfolgt keine Anmel am Patentamt

Name: Matr.Nr.: Kennzahl:

Kommentare / Wünsche / etc.: