Prüfungsamt
Fachbereich Wirtschaftswissenschaften

Professur/Chair: Rannenberg

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Winter Semester 2012/2013

Matrikelnummer:
Student ID:

Bitte auch auf jedes Lösungsblatt oben rechts eintragen! *Please also record this on each page in the top right corner!*

Modulkürzel/ *Module Code*: INKO

Themensteller/*Lecturer:* Dr. Martin Reichenbach

Modultitel/*Module Title:*

Wichtig: **Durch Ihre Unterschrift in der Teilnehmerliste bestätigen Sie, folgende Prüfungsvorschriften zu beachten:**

- Sie haben den nachfolgenden Text gelesen und stimmen allen Punkten zu.
- Sie fühlen sich gesund und sind in der Lage, an der Prüfung teilzunehmen.
- Sie haben sich über die Vorschriften der PO, die Teilnahme an Klausurprüfungen betreffend, informiert.
- Sie haben zur Kenntnis genommen, dass Sie für die ordnungsgemäße Abgabe der Klausur vor Verlassen des Prüfungsraumes selbst verantwortlich sind. Dazu gehört, dass Sie auf Ihrem Platz bleiben, bis alle Klausuren eingesammelt sind, und den Prüfungsraum nicht verlassen, bevor die Klausuren gezählt und die Vollständigkeit festgestellt wurde.
- Es sind folgende Hilfsmittel erlaubt:
  Taschenrechner
- Das Mitbringen eines Mobiltelefons oder anderer elektronischer Kommunikationsmedien in die Klausur ist verboten. Zuwiderhandeln gilt als Täuschungsversuch.
- Bitte lassen Sie ausreichend Korrekturrand, und schreiben Sie **nicht** mit Bleistift oder roter Tinte.

Im Falle einer **Erkrankung** während der Klausur beachten Sie bitte:

1. Vermerken Sie die Erkrankung in Ihrer Klausur (Unterschrift!) und informieren Sie die Aufsicht unverzüglich.
2. Geben Sie die Klausur und alle Prüfungsblätter ab und achten Sie darauf, daß die Abgabe in der Anwesenheitsliste vermerkt wird.
3. Falls Sie Hilfe benötigen, wenden Sie sich an die Aufsicht.
4. Gehen Sie **unmittelbar** zum Arzt und reichen Sie innerhalb von drei Arbeitstagen ein Attest, das Ihnen die Prüfungsunfähigkeit bescheinigt, beim Prüfungsamt ein.
5. Bei **wiederholter Erkrankung** im selben Studienabschnitt ist ein **amtsärztliches** Attest erforderlich, das die Prüfungsunfähigkeit bescheinigt:
   - Lassen Sie sich von der Aufsicht oder im Prüfungsamt ein Aufforderungsformular zur Vorstellung beim Amtsarzt geben.
   - Suchen Sie den Amtsarzt am selben Tag oder am nächsten Arbeitstag auf.

Important: **with your signature on the signature list you confirm to comply with the following examination requirements**

- You have read the follow text and agree to all points.
- You feel healthy and able to participate in the examination.
- You have informed yourself with the examination regulations regarding the participation of exams.
- You have taken notice that you are responsible to hand in your examination orderly before you leave the examination room. This includes that you remain quietly seated until all examinations have been counted and it is determined that all examinations have been submitted.
- The following resources and aids are allowed:
  Calculator
- Carrying mobile phones or other electronic communication devices during the exam is forbidden. Violating this rule will be counted as an attempt to cheat.
- Please leave sufficient space in the margin for marking, please do **not** write with a **pencil** or **red ink**.

In case you fall ill and become unfit for examination during the course of examination please note the following:

1. Please record this in writing including your signature on your examination documents and inform an invigilator immediately.
2. Submit your examination and all examination documents and ensure that the information is declared on the signature list.
3. In case you need help please inform an invigilator.
4. Please see a doctor immediatley on the day on which you discontinued the examination. Submit the required medical certificate which confirms your inability to participate in the examination to the examination office within 3 working days.
5. In case of **repeated illness** during the same official aera of study you are required to to submit a medical certificate from a public health medical office**r:**
   - Please collect the medical examination request form for the public health medical officer from an invigilator or the examination office.
   - Please go and see a public health medical officer on the same day or on the next working day.

Bitte für die Korrektur freilassen! / *Please leave blank for grading purposes!*

Ergebnis/*Result*:

Aufgabe/Question:	1	2	3	4	5	6	7	8	9	10	Summe/Sum
Punkte/Points:											

Punkte ***Points***	**Note** ***Grade***	**Unterschrift des Prüfers** ***Examinar's Signature***

Exercise 1: Authentication (12 Points)

Alice is a customer of the *D-Bank* and she regularly uses online banking. She receives an e-mail with the subject „D-Bank – Please update your personal information“. In the text of the e-mail she is informed that a system maintenance has been performed and that she should login to the online banking platform and check her personal information for correctness. Below this text, there is a hyperlink with the title “D-Bank - Online Banking Portal - Login“. Alice clicks on this link. On the website that appears, Alice enters her login credentials and clicks on „Login“. An error message appears that tells her that the login has failed and has to be repeated. A few seconds later, the browser automatically gets redirected to the login page. The second login attempt succeeds.

Alice ist Kunden der D-Bank und nutzt regelmäßig Onlinebanking. Sie erhält eine Email mit dem Thema "D-Bank - Bitte aktualisieren Sie Ihre persönlichen Daten". Im Text der Email wird sie darüber informiert, dass aus Wartungsgründen ein Update durchgeführt wurde und sie sich anmelden sollte, um die Korrektheit ihrer persönlichen Daten zu überprüfen. Unter diesem Text ist ein Hyperlink sichtbar mit dem Titel "D-Bank - Online Banking Portal - Login". Alice klickt auf diesen Link, und auf der folgenden Webseite gibt sie ihren Nutzernamen und ihre Kennung ein. Eine Fehlermeldung weist sie darauf hin, dass der Anmeldeversuch gescheitert ist und wiederholt werden sollte. Ein paar Sekunden später wird der Browser automatisch auf die Anmeldeseite weitergeleitet, ein weiterer Anmeldeversuch gelingt jetzt.

a) With a high probability, to what kind of attack Alice has fallen victim (2 points)?

   Welcher Angriffsart ist Alice wahrscheinlich zum Opfer gefallen? (2 Punkte).

   Password Spoofing or Phishing.

b) What are the weaknesses of such an authentication scheme (username/password) that make such kind of attacks possible (3 points)?

   Was sind die Schwachstellen eines auf Nutzernamen/Kennung basierenden Authentifizierungsverfahrens, das solche Angriffe möglich macht (3 Punkte).

   Identifizierung und Authentifizierung mittels Nutzername und Passwort bieten nur einseitige Authentifizierung.
   Der Nutzer weiß nicht, wer Nutzername und Passwort erhält.
   Der Nutzer kann nicht (mit Sicherheit) beurteilen, wer auf der anderen Seite der Verbindung sitzt.

c) Name and describe two countermeasures for this kind of attack (4 points).

   Nennen und beschreiben Sie bitte zwei Gegenmaßnahmen gegen diese Angriffsart (4 Punkte).

   Anzahl der gescheiterten Login-Versuche anzeigen:
   Wenn der erste Login-Versuch scheitert, man beim zweiten Versuch aber angezeigt bekommt, dass es bisher keine Authentifizierungsversuche ohne Erfolg gab, sollte man misstrauisch werden.

Gegenseitige Authentifizierung:
Auch das System muss sich gegenüber dem Nutzer authentifizieren.

Trusted path:
Beispiel: Strg+Alt+Entf in Windows (Task Manager) kann sicherstellen, dass der Nutzer mit dem Betriebssystem kommuniziert und nicht mit einer Schadenssoftware (spoofing program).

Multifaktor-Authentifizierung:
Multifaktor-Authentifizierung mit zusätzlichem Authentication-Token, da Angriff dann allein mit Nutzername/Password nicht möglich.

d) Why is an attack to multifactor authentication is more difficult than single factor authentication? Give an example of a typical 2 factor authentication. **(3 points)**

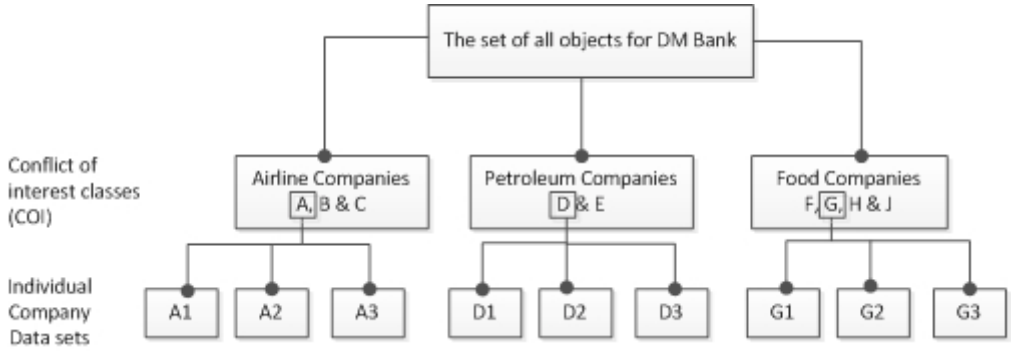
Warum ist ein Angriff auf ein Multifaktorauthentifizierung deutlich komplizierter als ein Angriff auf ein System mit einfacher Authentifizierung? Geben Sie ein Beispiel für eine typische zwei-Faktor-Authentifizierung. (3 Punkte)

- Multi factor authentication is when two or more authentication mechanisms are used jointly to provide more security (2 points).
- The attacker needs to know more, or possess more, than is required to spoof a single layer (2 points).
- ATM cards which requires PIN as well (1 point).

Exercise 2: Access Control (12 Points)

After successfully finishing your studies you manage to get contracted by a major Investment firm. Consider the database of this investment house. It consists of companies' records about investment data. You immediately see that your company is following the Chinese Wall Model to secure their data. The following *Chinese Wall Model* shows the datasets for each company in the database and the conflict of interest (COI). classes.

Nach erfolgreich absolviertem BWL-Studium schaffen Sie den Direkteinstieg in eine Investmenbank. Dort finden Sie die Datenbank mit Kunden-/Unternehmensdaten in Bezug auf Investmentaktivitäten und Sie erkennen auf Anhieb, dass die Security Policy der Bank auf dem *Chinese Wall Modell* basiert, das sie bereits während ihres Studiums kennen gelernt haben. Das folgende Modell zeigt die Datensätze für jedes Unternehmen in der Datenbank und die Conflict of Interest Klassen (COI).



a) You receive your first tasks and access provisions. At this moment, are there any access restrictions to objects, where you don't have access to due to the Chinese Wall Policy? (2 points)

Sie stehen kurz vor ihrem ersten Arbeitsauftrag und Systemzugriff. Gibt es zum jetzigen Zeitpunkt bereits Objekte, auf die Sie grundsätzlich wegen der Chinese Wall Policy nicht zugreifen dürfen? (2 Punkte)

Nein

b) Let us assume that you as your first task gain access to Airline Company A's data sets first; at this stage, you possess information concerning Airline Company A's data sets. Can you gain access to Airline Company B's data set? Justify your answer (2 points).

Nehmen Sie an, dass Sie ale ersten Arbeitsauftrag Zugriff auf die Daten der Airline A bekommen. Können Sie daraufhin auch auf Daten der Airline B zugreifen? Begründen Sie ihre Antwort. (2 Punkte)

Nein, weil im gleichen COI class.

c) Could you gain access to Petroleum Company D's data set? Justify your answer (2 points).

Würden Sie danach Zugriff auf die Daten des Ölunternehmens D bekommen? Begründen Sie Ihre Antwort. (2 Punkte)

Ja, weil in einem anderen COI class.

d) What is the minimum number of analysts (including you) needed to access the data sets from all companies in the Airline Companies Class (3 points)?

Wieviele Analysten (inklusive Ihrer Person) müssten es sein, um die Datensätze aller Unternehmen der Klasse "Airline" zugreifen zu können? (3 Punkte)

3

e) Let's assume now that besides Airline Company A, during your work you gain access also to Food Company G. Name all the companies in all COI classes, where you cannot get access (now or in the future) (3 points, if all named correctly).

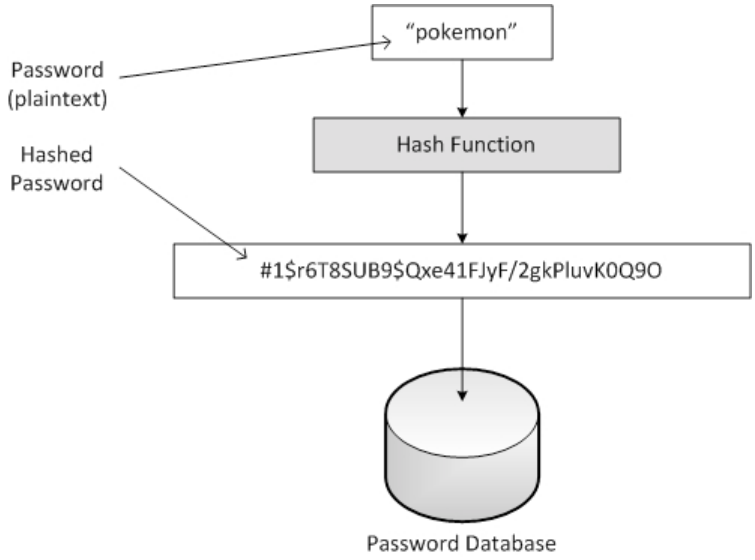
Nehmen wir an, dass Sie neben der Airline A während Ihrer Arbeitstätigkeit auch Zugriff auf die Nahrungsmittelfirma G erhalten. Nennen Sie alle Unternehmen in allen COI Klassen, auf die Sie jetzt oder in Zukunft KEINEN Zugriff mehr hätten. (3 Punkte, wenn alle korrekt genannt werden)

B, C, F, H, J

Exercise 3: Cryptography / Electronic Signatures (7 Points)

It's a bad idea to store passwords for computer systems in plaintext (in their original form), because if the attacker can somehow get to where they're stored, he has access to all the passwords. A more secure way is to store a hash of the password, rather than the password itself. This is depicted in the figure below.

Es ist keine gute Idee, Passworte für Computer im Klartext zu speichern (in ihrer ursprünglichen Form), weil ein Angreifer, sobald er Zugriff auf diesen Rechner bekäme, dann auch Zugriff auf alle Passworte im Klartext hätte. Ein sicherer Weg ist es, einen "HASH" als Fingerabdruck des Passwortes zu speichern. Dieses Vorgehen sehen Sie im folgenden Bild.



a) Explain, why this is safer. How much safer? Explain how someone who gets access to the database and retrieves the hash values can find out the passwords of the users (2 points).

Erklären Sie, warum dieses Vorgehen sicherer ist. Wieviel sicherer? Erklären Sie, warum/wie jemand mit Zugriff auf die Datenbank mit dem Hashwerten auch die ursprünglichen Passworte herausfinden kann. (2 Punkte)

Das Geheimnis Passswort wird so nicht im Klartext gespeichert. Wenn aber jemand Zugriff auf die Hashwerte bekommt, kann er durch Brute Force und Dictionary Attacks aus den Hashwerten auf die zugrundeliegenden Passworte zurückschließen.

b) Is it possible that two different passwords produce the same hash value? Justify your answer (3 points).

Ist es möglich, dass zwei unterschiedliche Passworte den gleichen Hashwert ergeben? Begründen Sie Ihre Antwort (3 Punkte)

Yes (1 point). Since the input space (infinite size) is larger than the output space (finite size), there exist different words that have the same hash value. (2 points)

c) Due to which attack scenario, conducted using public key systems, emerges the need for Certification? (2 points)

Welcher Angriff, der mittels öffentlicher Schlüssel durchgeführt werden kann, macht Zertifizierung notwendig? (2 Punkte)

Um Man in the Middle-Angriffe zu verhindern, wird eine Zertifizierung nötig.

Exercise 4: Cryptography / Electronic Signatures (8 Points)

e) Use the Vigenère Chiffre to encrypt the word “REICHENBACH” by using the key “SEC”. **(5 points)**

Verwenden Sie die Vigenère-Chiffre für die Verschlüsselung des Wortes “REICHENBACH” und verwenden Sie dabei den Schlüssel “SEC”. (5 Punkte)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

R	E	I	C	H	E	N	B	A	C	H
S	E	C	S	E	C	S	E	C	S	E
J	**I**	**K**	**U**	**L**	**G**	**F**	**F**	**C**	**U**	**L**

b) Which approach is used to bypass the inherent challenges of symmetric and asymmetric cryptography? Name the approach and describe a setup for a generic and secure Client Server Communication protocol. Use current cryptosystems to depict your solution. (1 point for naming, 2 points for describing the example)

Welchen pragmatischen Ansatz wählen Designer von Sicherheitslösungen, um die logistischen Probleme der Verwendung symmetrischer und asymmetrischer Kryptografie zu umgehen? Nennen Sie den Ansatz und beschreiben Sie die Vorgehensweise anhand eines allgemein verwendbaren, sicheren Protokolls für Client-Server-Kommunikation anhand je eines gängigen Verschlüsselungs- und Signaturalgorithmusses (1 Punkte fürs Nennen, 2 Punkte fürs Beispiel).

Hybridverfahren, die jeweiligen Nachteile ausschließen (Nachteile sichere Schlüsselverteilung bei Symm., Performance bei asymm. Kryptosystemen).Symmetrisch: AES, Triple DES; Asymmetrisch: RSA, Elliptic Curve

1) Schlüsselerzeugung symm.
2) Verschlüsselung der Nachrichten mit symm Schlüssel
3) Anforderung Public Key des Empfängers
4) Schlüsselverteilung des symm.

Keys per asymm. Krypto, d.h. Versenden des mit dem Symm. Schlüssel verschlüsselten Nachricht PLUS des mit dem Public Keys des Empfänger verschlüsselten Symm.Keys an Empfänger 5) Der Empfänger entschlüsselt das Paket mit seinem Privaten Schlüsselteil, erhält so den Symmetrischen Schlüssel zur Entschlüsselung der ursprünglichen Nachricht

Exercise 5: Data Protection & Privacy (14 Points)

a) Name and describe four principles of the European Data Protection Directive (0,5 points per naming, 1 point per description).

Nennen Sie 4 Prinzipien des EU-Datenschutzrechts. (0,5 Punkte) fürs Nennen, 1 Punkt je Beschreibung)

Intention and notification: The processing of personal data must be reported in advance to a Data Protection Authority.

· Transparency: The person involved must be able to see who is processing her data for what purpose.

· Finality principle: Personal data may only be collected and processed for specific, explicit and legitimate purposes.

· Legitimate grounds of processing: The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.

· Quality: Personal data must be as correct and as accurate as possible

· Data subject's rights: The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.

· Processing by a processor: This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.

· Security: A controller must take all meaningful and possible measures for guarding the personal data.

· Transfer of personal data outside the EU: The traffic of personal data is permitted only if that country offers adequate protection.

b) Different „Privacy Enhancing Technologies (PET)“ where introduced in the lecture. Name four PETs suitable to secure your Privacy and Identy (0,5 points per PET).

Sie haben ein Semester lang regelmäßig die Vorlesung Informations- und Kommunikationssicherheit besucht. Jetzt beschließen Sie, Ihre eigene Identität und Privatsphäre im Internet besser zu schützen. Nennen Sie vier der in der Vorlesung vorgestellten Privacy Enhancing Technologies. (0,5 Punkte je PET)

·Anonymous Credentials are used to prove privileges or attributes of their owner without revealing its identity, e.g. to prove, that

·Anonymiser
· a device contains an unrevoked Trusted Platform Module (TPM); this is also called Direct Anonymous Attestation

· the owner possesses a subscription and is of the required age, e.g. for an identity management system supporting anonymous video download

Such a system needs to have the following properties:

· Unforgeability of credentials

· Unlinkability of credentials

· No credential sharing

· Consistency of credentials

c) The categorization of Identity Management Systems can be based on the three-tier model introduced by Durand (Tier 1-3 Identities). Name these three tiers and give a brief description of each one. (3 Points)

Der Klassifizierung von Identitätsmanagementsystemen liegen die verschiedenen Schichten der Identität nach Durand zugrunde („Tier 1-3 Identities"). Nennen und beschreiben Sie diese kurz (3 Punkte).

Pro Nennung und pro Beschreibung jeweils 1 Punkt.

- Tier 1: True („My") Identity
  1. Meine tatsächliche und persönliche digitale Identität
  2. Wird ausschließlich von mir kontrolliert
  3. (Bspl. Selbsterstelltes Profil in einer Social Community)
- Tier 2: Assigned („Our") Identity
  1. Digitale Identität, die uns zugeordnet wird.
  2. Zuordnung erfolgt durch 3. Parteien (implizit klar)
  3. (Bspl. Sozialversicherungsnummer)
- Tier3: Abstracted („Their") Identity
  1. Aus Identitätsattributen Abgeleitet
  2. Zuordnung zu einer Gruppe / Zuordnung einer Gruppenidentität

d) What factor distinguishes the three identity tiers from each other? Describe, based on this factor, how the three tiers are different from each other. (3 Points)

In Bezug auf welchen Faktor unterscheiden sich die verschiedenen Schichten der Identität voneinander? Erläuter Sie anhand dieses Faktors, wie sich die Schichten voneinander abgrenzen. (4 Punkte)

1) Kontrolle (1 Punkt)
2) Tier 1 Identity wird komplett vom Individuum kontrolliert. Die Tier 2 Identität kann nur zum Teil vom Individuum kontrolliert werden (die Attribute der Tier 2 Identität sind dem Individuum allerdings bekannt). Die Tier 3 Identität kann nicht vom Individuum kontrolliert werden (das Vorhandensein einer Tier 3 Identität kann, muss aber nicht zwingend, dem Individuum bekannt sein). (3 Punkte)

Exercise 6: Biometrics (9 Points)

a) Given a biometric system with a *False Acceptance Rate (FAR)* of 0,5. With 3 authentication attempts, what is the probability that a person gets falsely accepted at least one time (2 points)?

Gegeben sei ein biometrisches Authentifikationssystem mit einer False Acceptance Rate (FAR) von 0,5. Wie hoch ist die Wahrscheinlichkeit bei 3 Authentifizierungsversuchen, dass eine unautorisierte Person mindestens einmal akzeptiert wird? (3 Punkte)

$p(n) = 1 - (1-p)^n$
$p = FAR = 0,5$
$n = 3$
$p(3) = 1 - (1 - 0,5)^3 = \underline{0,875 = 87,5\%}$

b) Name and describe four properties of characteristics for biometric authentication (4 points).

Nennen und beschreiben Sie kurz vier physische und menschliche Eigenschaften, welche für biometrische Authentifikation verwendet werden können. (4 Punkte)

Eigenschaften von Merkmalen zur biometrischen Identifikation:

- **Universalität**: Merkmal ist bei jeder Person vorhanden.
- **Einzigartigkeit**: Merkmal ist bei jeder Person anders.
- **Permanenz**: Merkmal ändert sich über die Zeit nicht oder nur minimal.
- **Erfassbarkeit**: Merkmal lässt sich quantitativ erheben.

c) Choose any (only 1) physiological characteristic that can be used for biometric systems. Name two advantages and two drawbacks of biometric systems that base on this physiological characteristic (2 points).

Wählen Sie eine physische und menschliche Eigenschaften, welche für biometrische Authentifikation verwendet werden könnte. Nennen Sie zwei Vor- und zwei Nachteile von biometrischen Systemen, die auf dieser Eigenschaft aufbauen (2 Punkte)

Fingerabdruckanalyse:
Vorteile:

- Sehr gut erforschtes Verfahren
- Hohe Einzigartigkeit des Merkmals
- Billige Sensoren
- Verfahren zur Identifikation geeignet

Nachteile:

- Gute Lebenderkennung relativ aufwendig
- Hygienische Bedenken
- 5% aller Personen haben keine sinnvoll nutzbaren Fingerabdruckmerkmale
- Nicht fälschungssicher
-

Iris Scanner:
Vorteile:

- Hohe Einzigartigkeit
- Hohe zeitliche Konstanz
- Einfache Lebenderkennung durch Pupillenreflex
- Verfahren zur Identifikation geeignet

Nachteile:

- Merkmalsveränderung durch Krankheit
- Beleuchtung, Brille, Kontaktlinsen
- Kosten

- Nutzerakzeptanz
- Benutzerverhalten bei aktiven Systemen

Gesichtserkennung:
Vorteile:
- Hohe Benutzerfreundlichkeit
- Hohe Akzeptanz
- Gesicht ist immer (wenigstens teilweise) sichtbar
- Kann unbeobachtet aufgenommen und überprüft werden

Nachteile:
- Geringe relative zeitliche Konstanz
- Niedrige Einzigartigkeit
- Keine Kooperation erforderlich
- Kann unbeobachtet aufgenommen und überprüft werden

Exercise 7: Computer System Security (10 Points)

a) Name four types of malware in computer systems and briefly describe each one of them. **(6 points, 0,5 for naming, 1 for describing)**

Nennen Sie 4 gängige Kategorien (Typen) von Schadsoftware, und beschreiben Sie kurz.deren Angriffspunkt bzw. Wirkung (6 Punkte, 0,5 fürs Nennen, 1 fürs Beschreiben).

- Viruses: …
- Worms: …
- Trojan horses: …
- Logic Bombs: …

b) What can cause a Buffer Overflow and what would be the effect on the procedure call stack? **(4 points)**

Was kann einen "Buffer Overflow" verursachen und was würde der Effekt auf den "Programmausführungs-Stack" sein? (4 Punkte)

- Moving a value into a storage location which is larger than the space allocated for a variable (2 points)
- It would overwrite the return address in the procedure call stack (2 points)

Exercise 8: Network Security (12 Points)

a) In the context of network security, what is a firewall (2 points)?

Was versteckt sich hinter dem Begriff "Brandmauer" im Netzwerkkontext? (2 Punkte)

Eine Firewall ist ein spezialisierter netzwerkverbindender Rechner (Internetwork Gateway) der die Kommunikation zu und von einem der verbundenen Netze beschränkt/überwacht (inneres Netze/LAN) und dadurch die Ressourcen des Netzwerks gegen Bedrohungen von außen (WAN/Internet) schützt. Paketfilterung auf Basis von Regeln. Sketch where a firewall is usually placed in a network infrastructure (1 point).

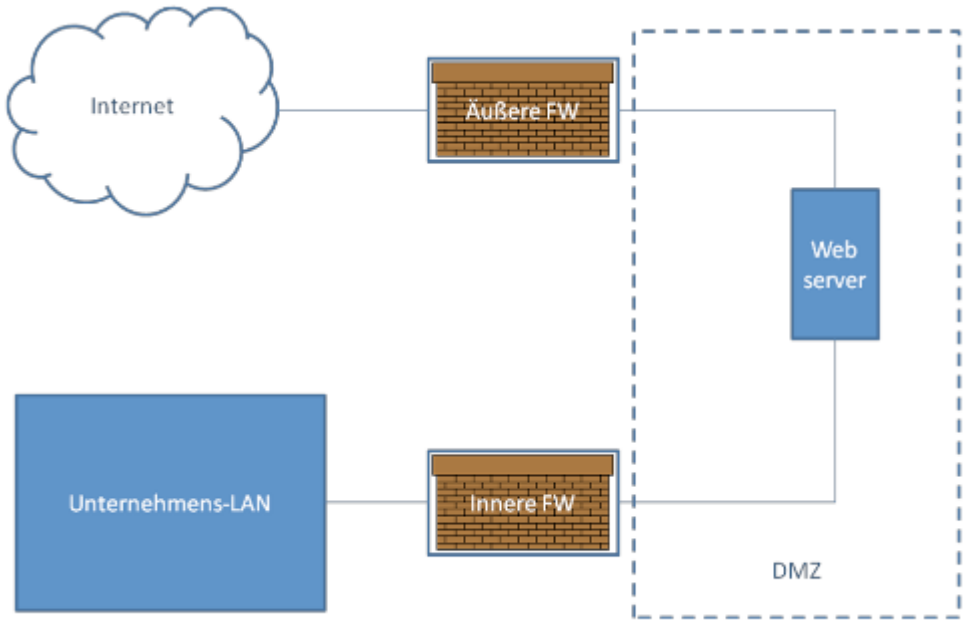
b) What is a demilitarized zone (DMZ) (2 points)?

Was ist eine demilitarisierte Zone (DMZ)? (2 Punkte)

Unter einer DMZ versteht man einen Netzwerkabschnitt/Segment in welchem eine Separation zwischen internem und externem Netzwerk stattfindet. Die “äußere Firewall” befindet sich zwischen dem Internet/WAN und der DMZ eine “innere Firewall” zwischen der DMZ und dem LAN Die DMZ stellt einen limitierten/kontrollierten öffentlichen Zugang und einen ebenso limitierten/kontrollierten Zugang aus dem LAN zu Servern in der DMZ zur Verfügung schottet den öffentlichen Zugang aber gegen das LAN vollständig ab.

c) You want to avoid connecting your corporate web server directly to the corporate local area network (LAN). But you still want it to be accessible from the Internet and from the corporate LAN. Sketch how such an infrastructure could look like. Label the used components, networks, and zones (5 points).

Sie wollen Ihren Unternehmens-Webserver direkt ans Unternehmensnetzwerk (LAN) anschließen. Er soll aber trotzdem gleichzeitig vom Internet und vom Unternehmensnetz aus zugreifbar sein. Skizzieren Sie, wie solch eine Infrastruktur sicher aufgestellt werden könnte. Kennzeichnen Sie die skizzierten Komponenten, Netzwerke und -zonen) (5 Punkte)



d) Secure Socket Layer (SSL) is one of the most applied Security Protocols to secure Communication. What are the main two threats, it is addressing? (2 points)

SSL ist ein weit verbreitetes Sicherheitsprotokoll für die Sicherung Ihrer Kommunikation. Gegen welche zwei Angriffsarten richtet sich SSL hauptsächlich? (2 Punkte)

Eavesdropping
Spoofing, Compromise of DNS

Exercise 9: Security Management (6 Points)

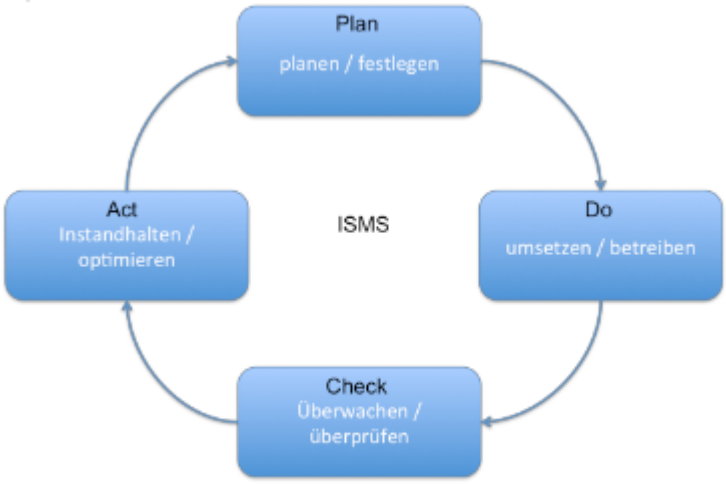
a) Name two tasks of the Information Security Management (2 points).

Nennen Sie zwei Aufgaben des Informationssicherheitsmanagements. (2 Punkte)

Get relevant processes in place.
Create a responsible organizational structure.
Make Information Security a business objective

b) Sketch the ISMS 4-step life-cycle (2 points). List in note form the activities performed in each step (0,5 points each).

Skizzieren Sie den ISMS-Lebenszyklus (2 Punkte). Kennzeichnen Sie in Notizform die Hauptaktivitäten, die in jedem Schritt ausgeführt werden (0,5 Punkte je Schritt)


Plan
planen / festlegen
Do
umsetzen / betreiben
Check
Überwachen /
überprüfen
Act
Instandhalten /
optimieren
ISMS