Goethe-Universität Frankfurt am Main
Lehrstuhl für Mobile Business & Multilateral Security

Wintersemester / ~~Sommersemester~~ .....2010.....

Matrikelnummer: ..... (Bitte auch auf jedes Lösungsblatt oben rechts eintragen!)

Fach: Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle (SEC)
Themensteller: Prof. Dr. Kai Rannenberg
Punktezahl: 90 Zugelassene Hilfsmittel: Keine

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 keine Hilfsmittel erlaubt
- 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 deutlich und **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.

Die Bearbeitung der Klausur erfolgt direkt innerhalb dieses Klausurheftes. Beantworten Sie jede Frage an den dafür vorgesehenen Stellen unterhalb der Aufgabenstellung. Sollten der Platz nicht ausreichen verwenden Sie die zusätzlichen Ersatzblätter am Ende der Klausur nur, wenn der Platz nicht ausreicht, und machen Sie auf dem Aufgabenblatt kenntlich, auf welcher Seite die Weiterbearbeitung der Aufgabe erfolgt.

Bitte für die Korrektur freilassen!

Aufgabe:	1	2	3	4	5	6	7	8	9	Summe
Punkte:										

Punkte: ..... Note: .....

Unterschrift des Prüfers: .....

Exercise 1: Authentication (10 Points)

Alice is a customer of the *Bank of Duckburg* and she regularly uses online banking. She receives an e-mail with the subject „Bank of Duckburg – 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 “Bank of Duckburg - 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.

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

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.

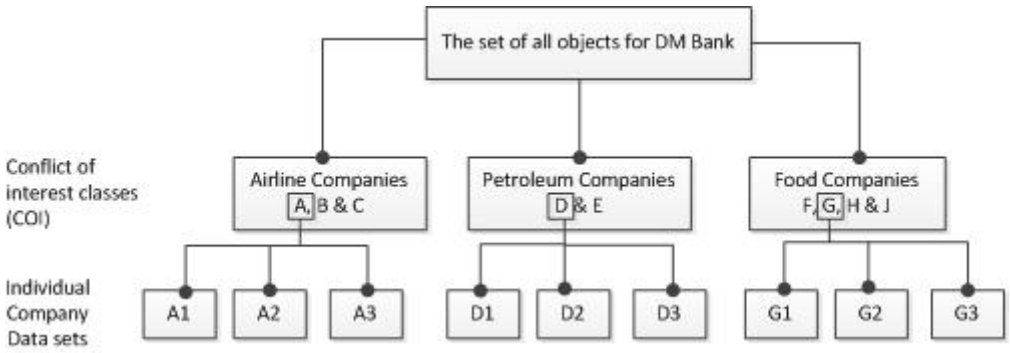
Gegenseitige Authentifizierung:
- Auch das System muss sich gegenüber dem Nutzer authentifizieren.

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.

Exercise 2: Access Control (10 Points)

Consider the database of an investment house. It consists of companies' records about investment data. The following *Chinese Wall Model* shows the datasets for each company in the database and the conflict of interest (COI) classes. Let us assume that Bob just joined DM Bank as analyst and gains access to Airline Company A's data sets first; at this stage, he possesses information concerning Airline Company A's data sets.



a) Can Bob gain access to Airline Company B's data set? Justify your answer (2 points).

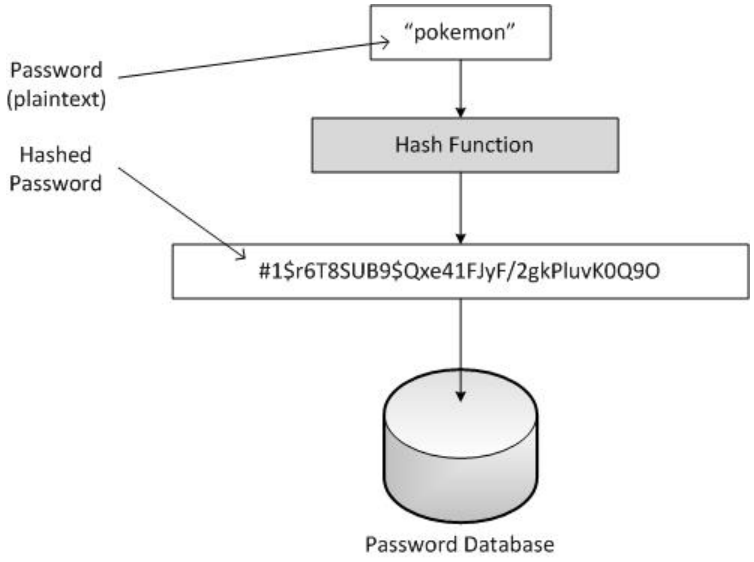
b) Can Bob gain access to Petroleum Company D's data set? Justify your answer (2 points).

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

d) Let's assume now that besides Airline Company A, Bob gains access also to Food Company G. Name all the companies in all CIR classes, where Bob cannot get access (now or in the future) (3 points).

Exercise 3: Cryptography / Electronic Signatures (10 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.



a) Explain, why this is safer? That is, explain why someone who gets access to the database and retrieves the hash values cannot find out the passwords of the users (2 points).

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

c) Given that we don't store the passwords themselves in the database. When the user tries to log-in and enters his password, how can we still check that the password is the correct one (5 points)?

Exercise 4: Data Protection & Privacy (12 Points)

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

- **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. The anonymous credential system „Idemix“ is one of them. What is the purpose of anonymous credentials (2 points)? Name the four requirements to be met by anonymous credential systems (1 point per requirement).

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

- 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

Exercise 5: Biometrics (8 Points)

a) Given a biometric system with a *False Acceptance Rate (FAR)* of 0,01. With 100 authentication attempts, what is the probability that a person gets falsely accepted at least one time (2 points)?
$p(n) = 1 - (1-p)^n$
$p = FAR = 0{,}01$
$n = 100$

➔ $p(100) = 1 - (1 - 0{,}01)^{100} = \underline{0{,}63 = 63\%}$

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

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) Chose any 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).

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 6: Computer System Security (10 Points)

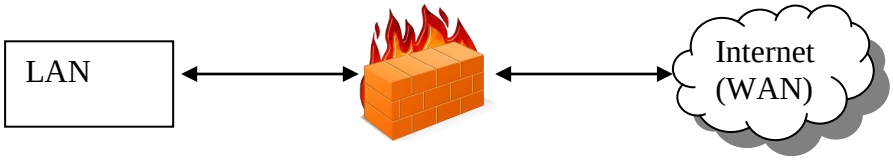
Name and describe five types of computer viruses (10 points).

Exercise 7: Network Security (10 Points)

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

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.

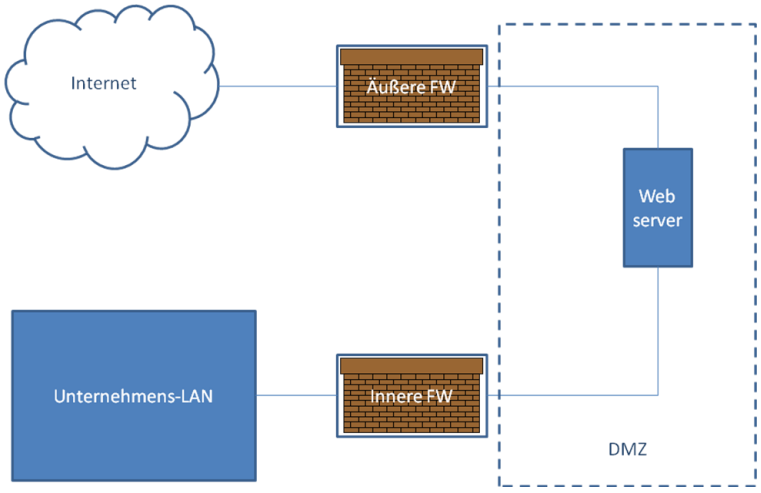
b) Sketch where a firewall is usually placed in a network infrastructure (1 point).



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

- 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.

d) 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 (4 points).



e) You plan to connect a branch of your company in another city to your corporate network, so that the local employees can access the data on the servers in the central office. For cost reasons, you connect the locations over the Internet. How can you assure confidentiality for the communicated data (1 point)?

VPN, Verschlüsselung, IPSec.

Exercise 8: Security Engineering (12 Points)

a) Complete the „Secure System Development Process“, by entering the missing descriptions of the points 1 – 4 (2 points). Further, explain in note form (bullet points) the functions of step 1 and step 3 (2 points).

1: Threat Analysis / Bedrohungsanalyse

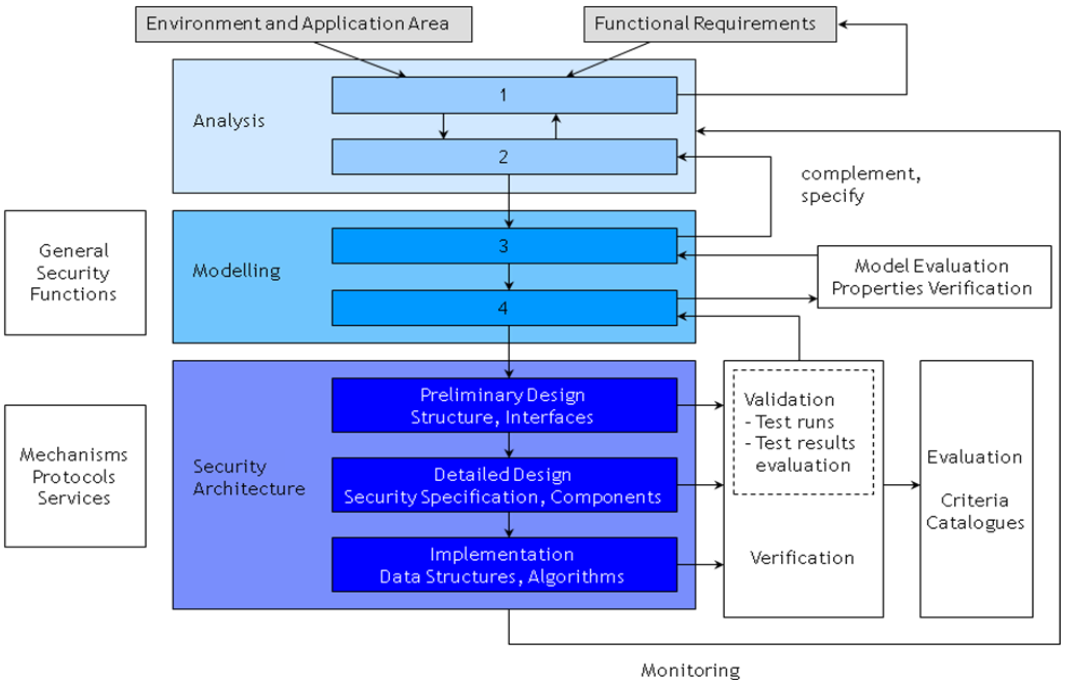
Aufgabe(n): Untersuchung von System Schwächen/Verletzlichkeiten/Verwundbarkeiten hinsichtlich bekannter Bedrohungsquellen zur Bestimmung existierender Bedrohungen für ein definiertes System in seiner spezifischen Einsatzumgebung.

2: Risk Analysis / Risikoanalyse

3: Security Policy / Sicherheitsleitlinie

Aufgabe(n): Modellierung abstrakter Sicherheitsanforderungen, Abbildung Beziehungen zwischen konkreten Sicherheitsleitlinienelementen und Basis Sicherheitsfunktionen

4: Security Model / Sicherheitsmodell



b) Explain the structure of an „attack tree“ (3 points). What is the purpose of an attack tree (1 point)?

Aufbau:

- Wurzel: symbolisiert das Angriffsziel
- Folgende Ebene(n): beinhalten als Knotendargestellte Zwischenziele die erreicht werden müssen, damit das Angriffsziel erreicht wird.

UND-Knoten müssen gemeinschaftlich erreicht/erfüllt werden, ODER-Knoten hingegen alternativ.

- Blätter: stellen möglich Angriffswege zur Erreichung des Angriffszieles dar

Verwendung:

- *System Bedrohungen* können als Angriffsbäume dargestellt werden außerdem dienen als *Hilfsmittel zur Risikoanalyse*.

c) You have to perform a risk analysis. What types of approaches for exist? How do they differ (2 points)?

Quantitativ Analyse

- Versucht realistische Zahlenwerte allen Elementen des Risikoanalyseprozesses zuzuordnen.
- Jedes Element wird quantifiziert und in Berechnungen zur Ermittlung des Restrisikos eingesetzt.
- Eine rein quantitative Risikoanalyse ist nicht möglich, da die Methode versucht qualitativen Werten Zahlenwerte zu zuordnen was immer mit Unschärfe/subjektiver Bewertung verbunden ist.

Qualitative Analyse

- Risiken werden in der Regel auf eine zwei bis vier stufigen Skala qualitativ bewertet (niedrig, mittel, hoch, katastrophal).

d) What is UMLsec (1 points)?

Eine Erweiterung der UML zur Unterstützung sicherer Softwareentwicklung.

e) Name one advantage of UMLsec (1 point).

- Evaluate UML specifications for weaknesses in design.
- Zusammenfassen etablierter Regeln zum sicheren entwickeln in Checklisten.
- Sicherheitsüberlegungen werden für Entwickler ohne entsprechende Spezialisierung verfügbar gemacht.
- Berücksichtigung von Sicherheitsanforderungen im Systemkontext schon in frühen Entwicklungsphasen.
- Unterstützung für kosteneffektive Zertifizierung.

Exercise 9: Security Management (8 Points)

a) Name two tasks of the Information Security Management (2 points).
- Notwendige Prozesse implementieren (Get relevant Processes in place).
- Entwickeln einer verbindlichen Organisationsstruktur (Create a responsible organizational structure).
- Sicherheit zum Unternehmensziel machen. (Make IT-Security a Business objective).

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