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

~~Wintersemester~~ / Sommersemester .....2011.....

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	Summe
Punkte:								

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

Unterschrift des Prüfers: .....

Exercise 1: Authentication (15 Points)

a) What is a multifactor authentication? Why an attack to such an authentication is more difficult than single factor authentication? Give an example of a typical 2 factor authentication. **(5 points)**

- 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).

b) 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 and tells her that the login has failed and it has to be repeated. A few seconds later, the browser automatically gets redirected to the login page. The second login attempt succeeds.

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

Password Spoofing or Phishing.

2) 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.

3) 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 security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C. Specify what type of access is allowed in each of the following situations by putting a "Yes" or "No" into the corresponding cell. Assume that discretionary access controls allow anyone access unless otherwise specified. **(10 points)**

Each correct answer is +1 and each wrong answer is -1. Leaving a cell blank gives you 0 points. The total points you can get will not go less than zero.

Case	Read	Write
Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {A, C}).	Yes	No
Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}).	No	No
Jesse, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (SECRET, {C}).	No	No
Sammi, cleared for (SECRET, {A, C}), wants to access a document classified (TOP SECRET, {A}).	No	No
Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (TOP SECRET, {B})	No	No

Exercise 3: Cryptography / Electronic Signatures (13 Points)

a) Use the Vigenère Chiffre to encrypt the word "RANNENBERG" by using the key "KAI". **(10 points)**

	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	A	N	N	E	N	B	E	R	G
K	A	I	K	A	I	K	A	I	K
B	A	V	X	E	V	L	E	Z	Q

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

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)

Exercise 4: Identity Management (15 Points)

a) Name 5 of 9 principles of EU privacy law. **(5 points)**

- Intention and notification
- Transparency
- Finality principle
- Legitimate grounds of processing
- Quality
- Data subject's rights
- Processing by a processor
- Security
- Transfer of personal data outside the EU

b) 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. **(6 Points)**

Pro Nennung und pro Beschreibung jeweils 1 Punkt.

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

c) What factor distinguishes the three identity tiers from each other? Describe, based on this factor, how the three tiers are different from each other. **(4 Points)**

- Kontrolle (1 Punkt)
- 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 5: Biometrics (12 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? **(4 points)**

$p(n) = 1 - (1-p)^n$
$p = FAR = 0{,}01$
$n = 100$

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

b) Name and describe four **properties of characteristics** for biometric identification. **(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) Choose any physiological characteristic that can be used for biometric systems. Name two advantages and two drawbacks of biometric systems that are based on this physiological characteristic. **(4 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)

a) Name four types of malware in computer systems and briefly describe each one of them. **(6 points)**

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

  0.5 point for the name and 1 point for the description.

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

- Moving a value 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 7: Network Security (15 Points)

a) Name three types of intrusion detection systems and briefly describe each one. **(6 points)**

- Anomaly Detection: ...
- Misuse Detection: ...
- Specification-based Detection: ...

1 point for the name and 1 point for the description.

b) What is the authentication token for a GSM network subscriber? **(1 point)**

The SIM Card

c) What kind of protocol is used for subscriber authentication in GSM networks? Does this protocol offer mutual authentication? Justify your answer. **(3 points)**

Challenge-Response Protocol (1 point)
No (1 point). Because only the subscriber authenticates himself to the network but the network does not provide any proof. (1 point)

d) How content confidentiality is achieved in GSM communication? Sketch how the session key is derived. **(5 points)**

The content is transmitted in an encrypted form between the subscriber and the network operator (1 point).

In the figure: Shared secret key Ki(1 point), rand (1 point), transmission of the rand from the network to SIM (1 point), showing the combination of Ki and rand (1 point)
No algorithm name or key length is required!