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: .....

Aufgabe 1: Authentication (15 Punkte)

a) Was ist eine "Multifaktor-Authentifizierung (MFA)"? Warum ist ein Angriff auf ein MFA-System schwieriger durchzuführen als auf ein System mit Einfaktor-Authentifizierung? Geben Sie ein typisches Beispiel für MFA.
(5 Punkte)

- MFA ist der gleichzeitige Einsatz von mehr als einem Authentifizierungsmechanismus, um ein höheres Sicherheitsniveau zu erreichen. (2 Punkte)
- Ein Angreifer muss mehr wissen/besitzen, als bei einer Ein-Faktor-Authentifizierung. (2 Punkte)
- Beispiel: Geldautomat → Bankkarte (Besitz) + PIN (Wissen) (1 Punkt)

b) Alice ist Kunde bei der *Entenhausener Sparkasse* und nutzt regelmäßig Onlinebanking. Sie erhält eine E-Mail mit dem Betreff „Entenhausener Sparkasse – Aktualisierung Ihrer persönlichen Informationen". Im Textkörper der E-Mail wird Alice aufgefordert, sich auf der Onlinebanking-Plattform einzuloggen und ihre Stammdaten auf Korrektheit zu prüfen, da eine Wartung des Systems durchgeführt wurde. Unter diesem Text befindet sich auch gleich ein Hyperlink mit dem Titel „Onlinebanking Plattform der Entenhausener Sparkasse - Login". Alice klickt auf diesen Link. Auf der dann erscheinenden Webseite gibt Alice ihre Login-Daten ein und klickt auf „Login". Daraufhin erscheint eine Fehlermeldung, die ihr mitteilt, dass der Login fehlgeschlagen ist und wiederholt werden muss. Ein paar Sekunden später wird sie automatisch wieder zur Login-Seite weitergeleitet. Der zweite Login-Versuch ist erfolgreich.

i. Welchem Angriff ist Alice höchstwahrscheinlich zum Opfer gefallen? **(2 Punkte)**
Password Spoofing oder Phishing.

ii. Welche Schwächen eines solchen Authentifizierungsschemas (Nutzername/Passwort) ermöglichen diese Art von Angriffen? **(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.

iii. Nennen und beschreiben Sie zwei Gegenmaßnahmen für diesen Angriff.
(5 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.

Aufgabe 2: Access Control (10 Punkte)

Gegeben sind die Vertraulichkeitsstufen TOP SECRET, SECRET, CONFIDENTIAL und UNCLASSIFIED (in absteigender Reihenfolge) und die Kategorien A, B und C. Geben Sie an, welche Zugriffe (lesen/schreiben) in den folgenden Situationen erlaubt sind. Tragen Sie hierfür „ja“ (=Zugriff erlaubt) oder „nein“ (=Zugriff nicht erlaubt) in die entsprechende Zelle ein. Gehen Sie davon aus, dass das **Discretionary Access Control** (**DAC**)-Modell jedem Zugriff gewährt, so lange nichts anderes spezifiziert ist. **(10 Punkte)**

Für jeden richtigen Eintrag gibt es +1 Punkt, für jeden falschen Eintrag -1. Für leere Felder gibt es 0 Punkte. Insgesamt können nicht weniger als 0 Punkte erreicht werden.

Case	Read	Write
Paul mit Genehmigung (TOP SECRET, {A, C}), möchte auf ein Dokument mit Klassifizierung (SECRET, {A, C}) zugreifen.	Ja	Nein
Anna mit Genehmigung (CONFIDENTIAL, {C}), möchte auf ein Dokument mit Klassifizierung (CONFIDENTIAL, {B}) zugreifen..	Nein	Nein
Jesse mit Genehmigung (CONFIDENTIAL, {C}), möchte auf ein Dokument mit Klassifizierung (SECRET, {C}) zugreifen.	Nein	Nein
Sammi mit Genehmigung (SECRET, {A, C}) möchte auf ein Dokument mit Klassifizierung (TOP SECRET, {A}) zugreifen.	Nein	Nein
Robin, der keine Genehmigungen hat (und somit auf Stufe UNCLASSIFIED arbeitet), möchte auf ein Dokument mit Klassifizierung (TOP SECRET, {B}) zugreifen.	Nein	Nein

Aufgabe 3: Cryptography / Electronic Signatures (13 Punkte)

a) Verwenden Sie die "Vigenère-Chiffre", um das Wort „RANNENBERG" mit dem Schlüssel "KAI" zu verschlüsseln. **(10 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

Solution / Lösung (1 point per letter / 1 Punkt pro korrektem Buchstaben)

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) Ist es möglich, dass zwei verschiedene Zeichenketten bei Anwendung einer Hashfunktion in einem identischen Hashwert resultieren? Begründen Sie Ihre Antwort. **(3 Punkte)**

Ja, da der Eingaberaum (undendlich) größer ist als der Ausgaberaum (endliche Anzahl an Werten mit fixer Länge).

Aufgabe 4: Identity Management (15 Punkte)

a) Nennen Sie fünf Prinzipien des EU-Datenschutzrechts**. (5 Punkte)**

- 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) Der Klassifizierung von Identitätsmanagementsystemen liegen die verschiedenen Schichten der Identität nach Durand zugrunde (Tier 1-3 Identities). Nennen und beschreiben Sie diese kurz. **(6 Punkte)**

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

- 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)

Aufgabe 5: Biometrie (12 Punkte)

a) Ein biometrisches System habe eine *False Acceptance Rate (FAR)* von 0,01. Wie groß ist die Wahrscheinlichkeit, dass eine Person bei 100 Authentifizierungsversuchen mindestens einmal unberechtigterweise akzeptiert wird? **(4 Punkte)**

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

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

b) Nennen und beschreiben Sie vier **Eigenschaften** von Merkmalen zur biometrischen Identifikation. **(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) Wählen Sie ein beliebiges physiologisches Merkmal aus, das für biometrische Systeme genutzt werden kann. Nennen Sie je zwei Vor- und Nachteile von biometrischen Systemen, die auf diesem physiologischen Merkmal aufbauen **(4 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

Aufgabe 6: Computer System Security (10 Punkte)

a) Nennen und beschreiben Sie vier Typen von Malware in Computersystemen. **(6 Punkte)**

- Viren: ...
- Würmer: ...
- Trojanische Pferde: ...
- Logische Bomben: ...

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

b) Wodurch wird ein "Buffer Overflow" verursacht? Welchen Effekt hat es auf den „procedure call stack" ? **(4 Punkte)**

- Durch das Schreiben eines Wertes, der größer ist, als der dafür reservierte Speicherplatz. (2 Punkte)
- Die Rückgabeadresse wird überschrieben. (2 Punkte)

Aufgabe 7: Network Security (15 Punkte)

a) Nennen und beschreiben Sie drei Typen von *Intrusion Detection* Systemen. **(6 Punkte)**

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

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

b) Was ist das Authentifizierungs-Token eines GSM-Teilnehmers? **(1 Punkt)**

Die SIM-Karte.

c) Welche Art von Protokollen wird bei der Authentifizierung von GSM-Teilnehmern eingesetzt? Bietet GSM gegenseitige Authentifizierung? Begründen Sie Ihre Antwort. **(3 Punkte)**

Challenge-Response Protokoll. (1 Punkt)
Nein (1 Punkt). Nur der Teilnehmer authentifiziert sich gegenüber dem Netzwerk. Das Netzwerk authentifiziert sich nicht gegenüber dem Teilnehmer. (1 Punkt)

d) Wie wird Vertraulichkeit bei der Kommunikation in GSM-Netzen gewährleistet? Skizzieren Sie, wie der Session Key erstellt wird. **(5 Punkte)**

Inhalte werden zwischen dem Teilnehmer und dem Netzwerk verschlüsselt übertragen. (1 Punkt)

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!