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

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Winter Semester 2011/2012

Matriculation number: ..... (Please also write this on each answer sheet in the top right corner!)

Course: Information and Communication Security: Infrastructures, Technologies and Business Models (SEC)
Held by: Prof. Dr. Kai Rannenberg

Total points: 90

Important:

With your signature on the signature list you confirm to observe 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 in 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.
- Only the resources and aids listed on the examination paper are allowed.
- 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 and 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:

- Please record this in writing, including your signature on your examination documents, and inform an invigilator immediately.
- Submit your examination and all examination documents and ensure that the information is declared on the signature list.
- In case you need help please inform an invigilator.
- Please see a doctor immediately 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.

In case of repeated illness during the same official aera of study you are required to submit a medical certificate from a public health medical officer:

- 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.

Please leave free for marking purposes! ----------

Question:	1	2	3	4	5	6	7	8	Sum
Points:									

Points ..... Grade: .....

Examiner Signature: .....

Exercise 1: Authentication (7 Points)

a) What is a multifactor authentication? Why an attack to such an authentication system is more difficult compared to an attack to a system with single factor authentication? Give an example of a typical two-factor authentication. **(4 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 of defense (2 points).
- ATM cards which requires PIN as well (1 point).

b) What is a challenge-response technique? Describe shortly how it works and its main advantage. **(3 points)**

In a challenge-response authentication system, *Alice* sends a random message *m* (the challenge) to Bob and *Bob* replies with the transformation $r = f(m)$ (the response). The fact that Bob is able to compute f (m) shows to *Alice* that Bob is authentic.

.

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" (=access allowed) or "No" (=access not allowed) 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 (SECRET, {A, C}), wants to access a document classified (TOP SECRET, {A, C}).	No	Yes
Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B, C}).	No	Yes
Jesse, cleared for (CONFIDENTIAL, {A, C}), wants to access a document classified (SECRET, {C}).	No	No
Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {A, B}).	No	No
Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (TOP SECRET, {B})	No	Yes

Exercise 3: Cryptography / Electronic Signatures (15 Points)

a) Use the Vigenère cipher to encrypt the word "INFORMATION" by using the key "SEC". **(6 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

SOLUTION:

I	N	F	O	R	M	A	T	I	O	N
S	E	C	S	E	C	S	E	C	S	E
A	R	H	G	V	O	S	X	K	G	R

b) What is a public-key (asymmetric) crypto system? Argue about the advantages of public-key schemes over private-key ones with regard to key management. **(5 points)**

In a public key system, each party owns a key pair consisting of a private key and the corresponding public key. Public key can be made public and is used for encryption, while the private key has to be kept secret and is used to decrypt the ciphertext. The advantage is that only the public key must be shared and the server storing the keys does not know the secrets.

c) In a typical Public Key Infrastructure (PKI), a third person/institution certifies public keys, confirming the affiliation of the public key to a person. Why is such a certification important (what does it protect from)? **(4 points)**

To avoid attacks, such as Man in the Middle attack.

Exercise 4: Identity Management (13 Points)

a) Name 6 of 9 principles of EU privacy law. **(3 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 is an Anonymous Credential? **(1 Point)**

`Anonymous Credentials are used to prove privileges or attributes of their owner without revealing her owner.

d) Name 3 of 4 properties of Anonymous Credential Systems. **(3 Points)**

- Unforgeability of credentials
- Unlinkability of credentials
- No credential sharing
- Consistency of credential

Exercise 5: Biometrics (10 Points)

a) List four different physical human characteristics that can be used for biometric authentication. **(2 points)**

Fingerprints, iris, face or speaker recognition.

b) Briefly argue about three challenges in using biometrics for authentication. (**3 points)**

- Patterns will hardly ever match precisely.
- A new problem occurs: *false positives* and *false negatives.*
- If a potential attacker can copy data, identity fraud can occur.
- Replay attacks are possible.
- Biometric attribute cannot be easily revoked.

c) Given a biometric system with a *False Acceptance Rate (FAR)* of 0,05. With 50 authentication attempts, what is the probability that an unauthorized person gets falsely accepted at least one time? **(5 points)**

$p(n) = 1 - (1-p)^n$
$p = FAR = 0{,}05$
$n = 50$

➔ $p(100) = 1 - (1 - 0{,}05)^{50}$

Exercise 6: Computer System Security (10 Points)

a) Name and describe five types of viruses in computer systems. **(5 points)**

- Slide 10 and 11 from lecture 9

b) Describe what is a logic bomb? Illustrate your answer with an example. **(2 point)**

Slide 13 from lecture 9

c) What is the difference between kernel and root access in Unix? **(1 point)**

Kernel processes can access anything but root processes can order the kernel to access anything.

d) What access control mechanism is used in the Windows NT security model to protect resources? **(1 point)**

Access Control List - ACL

e) What is the name for the piece of hardware added to the client devices to enable Trusted Computing? **(1 point)**

Trusted Platform Module - TPM

Exercise 7: Network Security (15 Points)

a) What is the encryption mechanism used in the first version of the IEEE 802.11 standard? Is it secure? Justify your answer. **(2 points)**

- WEP.
- No, it was easily broken due to the bad initialization. Problem with key management and RC4 algorithm.

b) How can access control be applied in the first version of IEEE 802.11 standard? Is it secure? Justify your answer.
(2 points)

- Rule-based access control based on MAC address.
- No, it's easy to fake the MAC address.

c) Specify what security goals are supported by each protocol. Put a "Yes" or "No" into the corresponding cell: **(3 points)**

Each correct answer is +0.5 and each wrong answer is -0.5. Leaving a cell blank gives you 0 points. The total points you can get will not go less than zero.

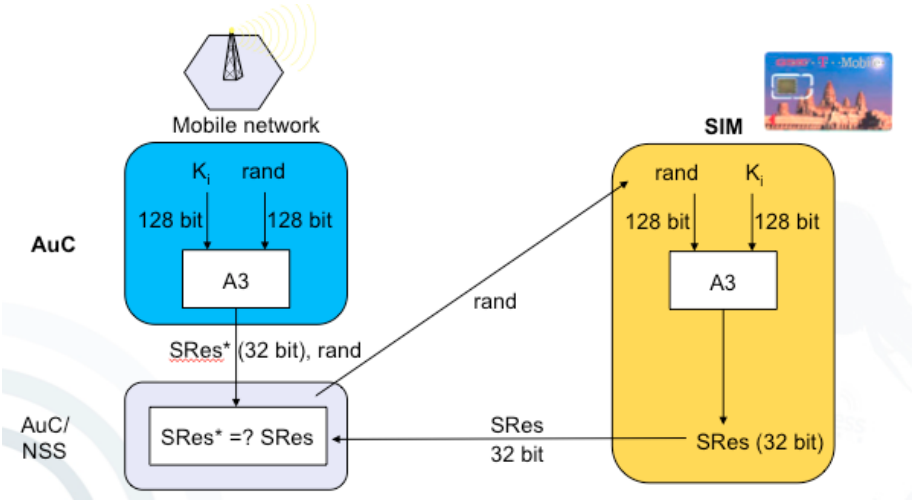
Security Goal	http	https (SSL/TLS)
Non-Repudiation	No	No
Integrity	No	Yes
Confidentiality	No	Yes

d) 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. What mechanism do you use to enable the communication and how can you assure confidentiality for the data transfer **(2 point)?**
VPN, Verschlüsselung, IPSec

e) What is the authentication token for a GSM network subscriber? **(1 point)**
The SIM Card

f) Sketch how authentication of a subscriber is done in a GSM network. **(5 points)**

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 using A3 (1 point) Sending back SRes and comparison on the network side (1 point)


Mobile network
SIM
AuC
K_i
rand
128 bit
128 bit
A3
rand
K_i
128 bit
128 bit
A3
rand
SRes* (32 bit), rand
AuC/
NSS
SRes* =? SRes
SRes
32 bit
SRes (32 bit)

Exercise 8: Security Engineering (10 points)

a) For a security system, it is important to be designed following specific design principles, which are built upon simplicity and restriction. List and describe five General Design Principles. **(5 points)**

1. **Economy of Mechanism:** The protection mechanism should have a simple design without overhead.
2. **Fail-safe Defaults:** The protection mechanism should deny access by default, and grant access only when explicit permission exists.
3. **Complete Mediation:** The protection mechanism should check every access to every object.
4. **Open Design:**
    a. The strength of protection mechanisms should not depend on attackers being ignorant of their design.
    b. It may however be based on the attacker's ignorance of specific information such as passwords or cipher keys.
5. **Separation of Privilege:** The protection mechanism should decide on access based on more than one piece of information.
6. **Least Privilege:** The protection mechanism should force every process to operate with the minimum privileges needed to perform its task.
7. **Least Common Mechanism:** The protection mechanism should be shared as little as possible among users.
8. **Psychological Acceptability:** The protection mechanism should be easy to use (at least as easy as not using it).

b) What is an "attack tree"? Describe its main components and how it constructed. **(5 points)**

Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes.
Components:

- **Tree root**: symbolizes the attack goal
- **Next level(s)**: contain(s) provisional goals (as nodes) required to reach the final attack goal
- **Nodes**

"Or" nodes (standard): represent alternatives
"And" nodes: have to occur in common
Leaves: contain options to attack the goal