# Prüfungsamt
# Fachbereich Wirtschaftswissenschaften

Professur/Chair: Chair of Mobile Business & Multilateral Security

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Summer Semester 2016

| Matrikelnummer:<br>*Student ID number:* |
|---|

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:* Prof. Dr. Kai Rannenberg

Modultitel/*Module Title:* Information and Communication Security: Infrastructures, Technologies, and Business Models

**Wichtig:** **Durch Ihre Unterschrift in der Teil-nehmerliste 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 **Prüfungsordnung**, 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 nur die vom Themensteller aufgeführten **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 **nicht** mit Bleistift oder roter Tinte.

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

1. Vermerken Sie die Erkrankung auf Ihrer Klausur schriftlich und unterschreiben dies. Informieren Sie die Aufsicht unverzüglich und erklären Sie bitte ausdrücklich den Abbruch der Klausur wegen Erkrankung.
2. Geben Sie die Klausur und alle Prüfungsblätter ab und achten Sie darauf, dass die Abgabe in der Unterschriftenliste vermerkt wird.
3. Falls Sie Hilfe benötigen, wenden Sie sich an die Aufsicht.
4. Gehen Sie am Tag des Prüfungsabbruches **ohne Verzögerung** zum Arzt und reichen Sie **unverzüglich** ein Attest beim Prüfungsamt ein, in welchem Ihre Krankheitssymptome detailliert beschrieben werden.
5. Wenn Sie trotz gesundheitlicher Probleme Ihre Klausur mitschreiben und abgeben, geht das Risiko einer eventuell verminderten Prüfungsleistung zu Ihren Lasten.

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

- You have read the following 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.
- 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 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 of your discontinuance due to illness explicitly.
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 **without delay** on the day on which you discontinued the examination. Submit the required medical certificate which describes your symptoms in detail to the examination office **immediately**.
5. If you write and hand in your examination despite your health problems, the risk of eventual diminished examination performance will be at your own expense.

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

**Ergebnis/*Result*:**

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

| **Punkte**<br>***Points*** | **Note**<br>***Grade*** | **Unterschrift des Prüfers**<br>***Examinar's Signature*** |
|---|---|---|

# 1. Authentication / Biometrics (14 points)

A. In a gaming website, users are requested to insert their password to login into the website. Consider that you are only allowed to use a combination of letters, numbers and one or more symbols from the five non alphabetical symbols to construct a password. For the letters, let us assume we are using the English alphabet, which consists of 26 different characters, for the numbers the Arabic numbers from 0-9, and the five symbols are *,@,#,$, and %.

1. How many different passwords are possible if a password is exactly n characters long, and passwords are case not sensitive? **(2 points)**

   **Answer: $41^n$**

2. How many different passwords are possible when we have a distinction between case-sensitive and non-case-sensitive characters? **(2 points)**

   **Answer: $67^n$**

3. Name three ways to attack a password system? **(3 points)**

   **Answer:** 1) Threatening the subject 2) Password guessing 3) Password spoofing 4) Compromise of password file 5) Social engineering

4. What is the advantage of increasing the password length? **(1 point)**

   **Answer:** It is more difficult to break the password using bruit force (exhaustive search) attack.

B. What is multi-factor authentication? What makes an authentication system with multi-factor authentication better than an authentication system with single factor authentication? Give an example of multi-factor authentication. (**3 points)**

**Answer**:

- Authentication mechanisms can be combined, or multiple methods can be used (Multi-factor authentication). (1point)
- The multiple layers of authentication require an attacker to know more, or possess more, than is required to spoof a single layer. (1point)
- Example: combination of ATM cards with password (PIN) (1 point)

C. Fill out the following table with three different features of behavioural biometrics features and three physiological biometric features. **(3 points)**

| No | behavioural biometrics features | physiological biometric features |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |

Answer:

- Fingerprint, face, iris, retina, hand geometry, vein pattern, ear geometry, DNA
- Signature (dynamic/static), Gestures (facial expression while speaking), walk, lip movement, voice (speech behavior), keystroke

## 2. Access Control (12 points)

A. Assume Alice and Bob are working in a company where access control needs to be enforced using the Bell-LaPadula model. The capability lists of the two subjects Alice and Bob, and the three objects bill.doc, edit.txt and financial.xls are:

| | | |
|---|---|---|
| CList (Alice) = bill.doc: {read, write} | edit.txt: {read, append} | financial.xls: {} |
| CList (Bob) = bill.doc: {read, append} | edit.txt: {append, write} | financial.xls: {read} |

Extending to the capability list, consider the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest). The subjects' security levels are $L_{Alice}$ = CONFIDENTIAL and $L_{Bob}$ = SECRET. The objects' security levels are $L_{bill.doc}$ = UNCLASSIFIED, $L_{edit.txt}$ = SECRET, and $L_{financial.xls}$ = TOP SECRET.

1. Rewrite the capability lists (CList) above using access control lists (ACL). **(3 points)**

**Answers:**
ACL (bill.doc) =Alice: {read, write}, Bob: {read, append}
ACL (edit.txt) = Alice: {read, append}, Bob {append, write}
ACL (financial.xls) = Alice: {}, Bob {read}

2. Using the Bell-LaPadula model, which of the following actions are allowed? Explain and justify your answer. (Hint: In order to help you understand the question, you can draw the Bell-LaPadula model which visualises the access control matrix and then check whether it is allowed for the following actions.) **(9 points)**
   i. Alice writes bill.doc

**Answer:**
This action is **NOT ALLOWED** because:
- Even though Write is $\in$ M (Alice, bill.doc), where M is the access control matrix, the next statement is not true.

- Based on the "No write down" rule, $L_{Alice} \leq L_{bill.doc}$ **doesn't** hold, where $L_{Alice}$ = CONFIDENTIAL, $L_{bill.doc}$ = UNCLASSIFIED

ii. Alice appends edit.txt

**Answer:**

This action is **ALLOWED** because

- Append $\in$ M (Alice, edit.txt), where M is the access control matrix and
- Based on the "No write down" rule, $L_{Alice} \leq L_{edit.txt}$ holds, where $L_{Alice}$ = CONFIDENTIAL, $L_{edit.txt}$ = SECRET

iii. Bob reads financial.xls

**Answer:**

This action is **NOT ALLOWED** because

- Read is not a member of the Matrix M(Bob, financial.xls)
- Based on the "No read up" rule $L_{financial.xls} \leq L_{Bob}$ **doesn't** hold, where $L_{Bob}$ = SECRET, $L_{financial.xls}$ = TOP SECRET

## 3. Cryptography and Electronic Signatures (13 points)

A. Describe the following attacks. **(3 points)**
   1. Cipher text only
   2. Known plain text
   3. Chosen plain text

**Answer**: **(1 point for each correct answer)**

- In a ***ciphertext only*** attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.
- In a ***known plaintext*** attack, the adversary has the plaintext and the ciphertext that was enciphered. Her goal is to find the key that was used.
- In a ***chosen plaintext*** attack, the adversary may ask that specific plaintexts be enciphered. She is given the corresponding ciphertexts. Her goal is to find the key that was used.

B. Given a cipher text "**LTTI QZHP**" and key = 5,

**1.** Find out the corresponding plain text using Caesar cryptosystem. Show the decryption steps for one of the letters. Use the table below when necessary. **(2 points)**

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Answer: (1 point for the correct plain text and 1 for an example of decryption step)**

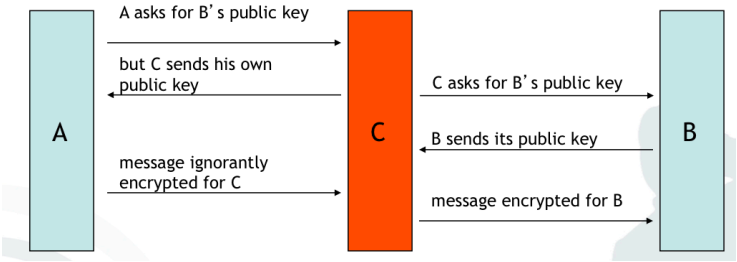
A decryption function D for an input x; D = (x - k) mod 26
e.g. for "L" which is 11,
D = (11 - 5) mod 26 =6
6 in the table is "G"
The plain text is: GOOD LUCK

2. Give an example of an attack for the Caesar scheme above. **(1 point)**

**Answer:**
**Statistical ciphertext-only attack**
**Brute force**

C. Draw a diagram to describe the Man–in-The-Middle attack scenario. **(3 points)**

**Answer**: (1 point for the idea of man in the middle attack, for the description between a and c and c and b awards 1 point each)



D. List two characteristics of cryptographic hash functions. **(2 points)**

**Answer**: **(1 point for each requirement)**

For a hash function h and an input string s

- *One way cryptographic schemes, which produce fixed size hash values*
- Virtual collision freedom: In terms of figures it is difficult to create collisions h (s1) = h (s2).

E. Name two security properties of digital signatures. **(2 points)**

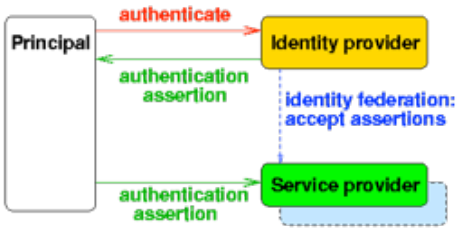
**Answer:**

Message Authentication (data origin authentication): The origin of the message matches the identifier of the public key.
Integrity: Messages have not been modified in transit.
Non-repudiation: The creator of the signature cannot deny the signing of the signed message.

## 4. Identity Management & Privacy Protection (23 points)

A. Sketch a diagram with the main entities in a federated identity management scheme and briefly describe their roles. **(6 points)**

**Answer:**




Identity Provider is an entity, which vouches for the attributes of the Principal.
The Principal is typically a User (person), who wants to access the services offered by a Service Provider. In order to do so, the Principal must authenticate towards the Service Provider by claiming an assertion. The Service Provider trusts (accepts identities asserted by) the Identity Provider for a certain Principal. This way, the Principle can use services of main Service Providers by using a federated identity from a single or more Identity Providers.

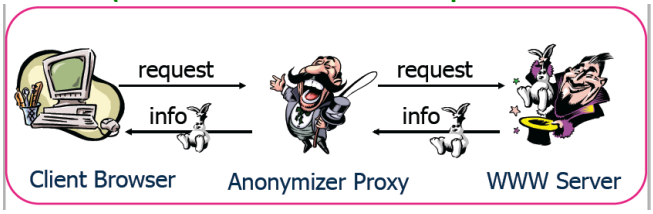
B. Two most common methods of technical privacy protection were discussed in the lecture. Name these two types and specify one example of technologies for each of them. **(4 points)**

**Answer:**

1. *Communication systems*, e.g. the Anonymizer, Tor, Cookie Cooker, etc. or
2. *Transaction systems*, e.g. credential technologies (Idemix, U-Prove, etc.), or reachability management techniques.

C. Depict a typical Anonymizer architecture and mention two drawbacks with respect to privacy. **(5 points)**

**Answer: (1 for each of the three components in the architecture, 1 for each of the drawbacks)**




1. *Anonymizer learns about client's activities / interests.*
2. *No protection against attackers with global view.*

**D.** Name two features that differentiate Mix Cascade from Mix Network. **(2 points)**

**Answer:**

1. *Fixed Path through the network*
2. *No mix addresses required in messages*
3. *All traffic flows over the same mixes.*

E. On April 14, 2016 the European Parliament adopted the EU General Data Protection Regulation (GDPR) on the protection of personal data. Name and describe three principles of the GDPR. **(6 points)**

**Answer:**

1. *Lawfulness, fairness and transparency: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.*
2. *Purpose limitation: personal data must collected for specified explicit and legitimate purposes.*
3. *Data minimisation: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
4. *Accuracy: personal data must accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

5. *Storage limitation: personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*
6. *Integrity and confidentiality: personal data must be processed in a way that ensures appropriate security of the personal data.*
7. *Accountability: The controller shall be responsible for and be able to demonstrate compliance to the principles mentioned above.*

## 5. Computer Systems Security (9 points)

A. Name and briefly describe four types of malicious logic. **(4 points)**

**Answer**:

- Trojan Horses – programs with a covert purpose, non-spreading
- Viruses – self-spreading program – it replicates relying on user activity
- Worms – Propagate autonomously from system to system

Logic Bombs - hidden code, triggered by external event

B. Briefly describe what Ransomware is. **(2 points)**

**Answer:**

It is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

C. In the Unix operating system security paradigm, there is a concept of root and kernel space. What is the main difference between the two? **(2 points)**

**Answer**:

the difference between kernel and root access:

- Kernel processes can access anything.
- Root processes can order the kernel to access anything

D. Briefly describe what buffer overflow is. **(1 point)**

**Answer**

Buffer overflow software bug

- data larger than the variable allocated for it

can overwrite a procedure return address in the procedure call stack in memory

## 6. Network Security (9 points)

A. Different network security protocols were discussed in the lecture, one of them being SSL/TLS. In the table below, put a right mark (✓) where it applies and an X mark where it doesn't. **(5 points)**

| **Security goal** | **http** | **https (SSL/TLS)** |
|---|---|---|
| Authenticity | | |
| Non-repudiation | | |
| Confidentiality | | |
| Integrity | | |
| Date documentation | | |

**Answer: (half point each)**

| **Security goal** | **http** | **https (SSL/TLS)** |
|---|---|---|
| **Authenticity** | **x** | ✓ |
| **Non-repudiation** | **x** | **x** |
| **Confidentiality** | **x** | ✓ |
| **Integrity** | **x** | ✓ |
| **Date documentation** | **x** | **x** |

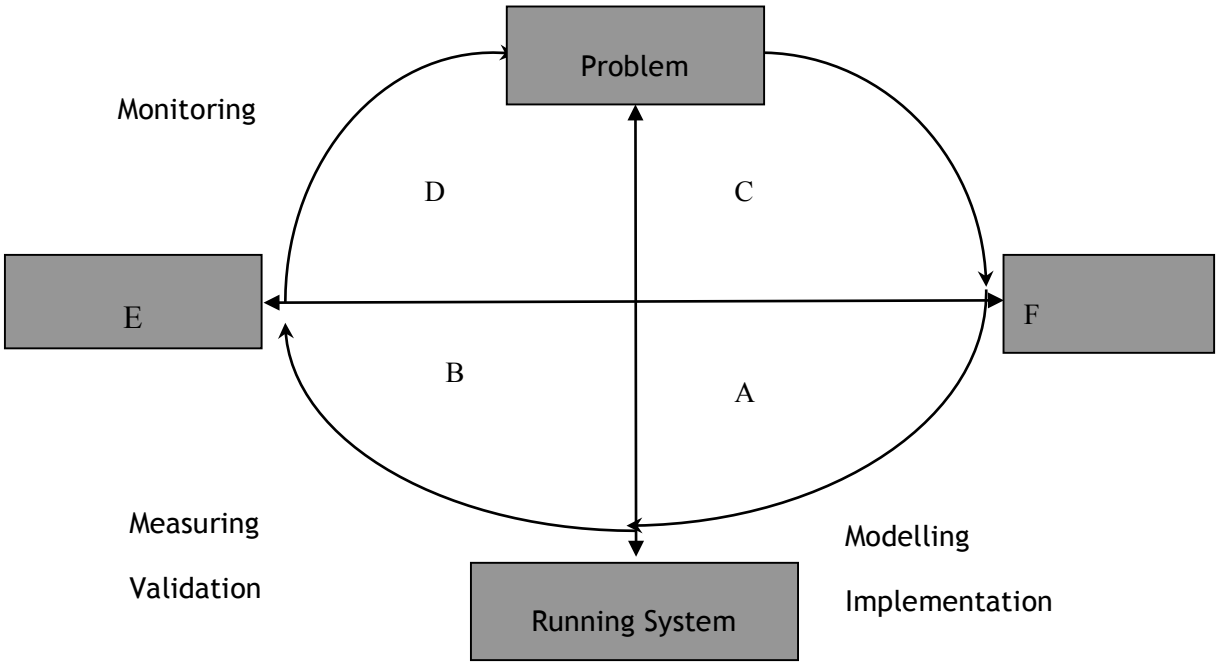
B. Name and describe two application layer security attacks. **(4 points)**

**Answer:**

- **Insertion attacks involve the introduction of unauthorized content or devices to an otherwise secured infrastructure, e.g., SQL injection.**
- **SQL injection is an attack that inserts unauthorized code into a script hosted on a Web site**
- **Buffer overflow an attack against poor programming techniques and a lack of quality control. An attacker injects more data into a buffer than it can hold.**
- **XSS Similar to SQL injection, but attacks visitors to a website ratherthan grant access to the back-end database**
- **DDoS attacks advance DoS attacks through massive distributed processing and sourcing with Bots (zombies) as malicious code implanted on victim systems across the Internet with the Command and Control server controlling the bots.**

## 7. Security Engineering (6 points)

Security engineering is a discipline to build secure systems. In the lecture, the iterative security engineering process was highlighted. Name the missing words/phrases of the diagram below. **(6 points)**




| | |
|---|---|
| A | |
| B | |
| C | |
| D | |
| E | |
| F | |

### Answers

| | |
|---|---|
| A | Execution/ Realisation |
| B | Controlling |
| C | Planning |
| D | Improvement and adoption |
| E | Evaluation |
| F | Measures |

## 8. Information Security Management (4 points)

Information Security Management System (ISMS) is a systematic approach to manage sensitive company information so that it remains secure. Name the typical ISO/IEC 27001 ISMS processes. Briefly describe each of them. **(4 points)**

**Answers**

- Plan - Define the ISMS guidelines, objectives, processes and procedures
- Do - Implement and execute the ISMS guidelines, objectives, processes and procedures
- Check - Asses the ISMS at the guidelines, objectives and check results
- Act - Take corrective actions based on the check results