Rheinische Friedrich-Wilhelms-Universität Bonn

Master Course Computer Science

Written Exam

Semester: Summer 2020	Exam Period: 1. x 2. □
Module Name: IT Security	
Module Number: MA-INF 3236	Date of Exam: 27.07.2020
Examiner: Prof. Dr. Michael Meier	

To be filled by the Student:

Last name:	Matriculation number:
First name:	
Course of Study Master in Computer Science □ Master in Education □ secondary subject □ other □	
For me, there were no technical problems with the exam.	Signature:

To be filled by the Examiner:

1	2	3	4	5	6	7	8	9	10	Σ
10	10	10	10	10	10	10	10	10	10	100

To be filled by the Examiner:

Grading:

***Grades: very good (1,0; 1,3) good (1,7; 2,0; 2,3) satisfactory (2,7; 3,0; 3,3) sufficient (3,7; 4,0) not sufficient (5,0)**

Date:

Signature of Examiner

Task 1: (Wireless Security) 2+2+2+2+2 points

a) Name the three antenna types presented in the lecture. Point out one of those types that is used more frequently by attackers that aim to attack wireless communication. Explain why this type is usually preferred over the others.
b) Name one protocol aware jamming attack and one protocol oblivious jamming attack.
c) Explain the differences between a protocol aware jamming attack and a protocol oblivious jamming attack with regards to 802.11a Wi-Fi.
d) What are drawbacks for an attacker when using a protocol aware jamming attack over a protocol oblivious jamming attack?
e) What makes the WPA2 handshake vulnerable?

Task 2: (Side Channels) 3+2+5 points

a) List at least two types of side channels that we can observe when treating the system as a black box.
b) Are these attacks typically passive or active?
c) What side channel enables the padding oracle attack presented in the lecture? Which information was leaked?

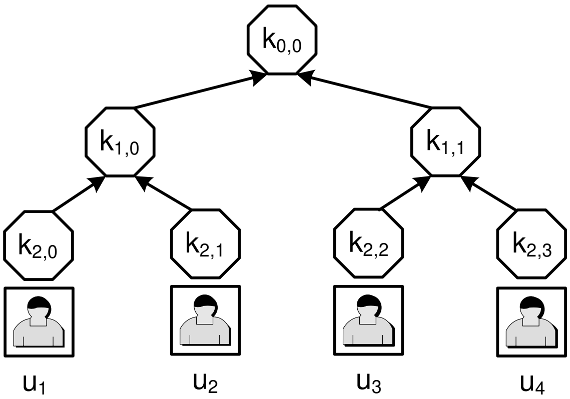
Task 3: (Threat Intelligence) 3+2+2+3 points

a) To which step of the "Intrusion Kill Chain" does footprinting belong? Explain that step.
b) What characteristics of Indicators of Compromise are visualized by the "Pyramid of Pain"?
c) What is so special about Insider Threats?
d) What is the idea behind Supply Chain Attacks?

Task 4: (Multi-Signature Algorithm) 3+3+3+1 points

a) Write down three features of a multi-signature.
b) Given a 5-out-of-5 RSA signature algorithm with the public key **(e, ñ)**, the secret (private) keys **(d_i, ñ)** of user **u_i, i ∈ {1,2,3,4,5}** and the (RSA) modulus **ñ = p·q** (**p**,**q** large primes). Write down the multi-signature generation equations for a message **m**.
c) Write down the multi-signature verification equation for the 5-out-of-5 RSA signature.
d) Name a sample application for multi-signatures.

Task 5: (Group Key Management) 2+3+2+3 points



The key tree above is used for the key management of a group G with the user $\mathbf{u_i}$, **i** ∈ **{1,2,3,4}.** The members of the group are associated with leafs of the key tree. Each node in the key tree contains a secret key. All members of the sub-tree rooted at node **v** know the key stored in the node **v**. The key $\mathbf{k_{0,0}}$ stored in the root of the tree is the group key.

a) A group controller uses the LKH (Logical Key Hierarchy) protocol and the tree in figure 1 for the key management. Write down the keys known by the user $\mathbf{u_1}$.

b) The user $\mathbf{u_5}$ joins the group and is added to the tree at the position of the user $\mathbf{u_3}$ (in figure 1). Hence, $\mathbf{k_{2,2}}$ moves to $\mathbf{k_{3,4}}$. Draw the modified tree.

c) A group controller uses the LKH protocol (group oriented) for the key update. Specify the broadcast message of the group controller that enables all members to calculate the new group key. Assume that the key $\mathbf{k_{3,5}}$ is established by the Diffie-Hellman algorithm in advance.

d) Now the TGDH (Tree Based Group Diffie Hellman) protocol and the tree in figure 1 is used for the key management. Write down the keys known by the user $\mathbf{u_1}$.

Task 6: (Certificate Revocation) 5+5 points

Serial number	1
Issuer	J
NotBefore	01/01/2015
NotAfter	31/12/2020
Subject	B

Serial number	2
Issuer	J
NotBefore	01/01/2016
NotAfter	31/12/2019
Subject	S

Serial number	3
Issuer	J
NotBefore	01/01/2016
NotAfter	31/12/2019
Subject	H

Serial number	4
Issuer	J
NotBefore	01/01/2015
NotAfter	31/12/2019
Subject	E

Serial number	5
Issuer	J
NotBefore	01/01/2016
NotAfter	31/12/2019
Subject	G

Serial number	6
Issuer	J
NotBefore	01/01/2016
NotAfter	31/12/2019
Subject	T

Table 1: Details about some certificates

The certificate authority J issues the certificates listed in table 1.

a) The certificate authority (CA) J publishes revocation information in the form of CRLs. A complete CRL is always generated at the first day of the month. Please specify the CRLs issued in April, May and June 2019 if the following certificate are revoked.

B	03/05/2019
E	05/05/2019
T	14/05/2019
G	24/05/2019
H	03/06/2019

b) The CA J introduces delta CRLs. The delta CRLs are issued twice a month, on the 10th and 20th of each month. Please write down the delta CRLs in May and June 2019.

Task 7: (Privacy) 6+2+2 points

a) Which of the following statements are true and which are false? Use the symbols T (true) and F (false) to answer this question.

_ After anonymizing a dataset using multivariate microaggregation, anomaly detection is always possible.

_ Pseudonymization always makes it impossible to link an individual to certain data anymore.

_ The GDPR demands that anonymous data is protected from being used for purposes different from the purpose the plaintext data have been collected for.

_ In order to produce a pseudonym that allows for plaintext disclosure on demand, a state-of-the art probabilistic encryption function can be used.

_ A release of data is said to have the k-anonymity property if the information for each person contained in the release cannot be distinguished from at least k -1 individuals whose information also appear in the release.

_ In the context of privacy and data protection, the GDPR is the abbreviation of "guide of data protection and privacy respectation".

b) Explain the difference between the generalization techniques of global and local recoding, respectively. For which kind of data Is this technique appropriate?

c) Considering pseudonymized data is still subject to the GDPR, why should personal data be pseudonymized at all?

Task 8: (Anomaly Detection) 2+8 points

a) Which of the following statements are true and which are false? Use the symbols T (true) and F (false) to answer this question.

_ In general, data deformation can improve the detection quality of k-means and linear SVMs but not for the DBScan algorithm.

_ In a worst case scenario, the runtime of DBScan is in O(#pts^3+dim).

b) Provide the algorithms for DBScan and k-means (including the input parameters). In each of the resulting models, which points are predicted "abnormal"?

Task 9: (Statistics) 4+6 points

Which of the following statements are true and which are false? Use the symbols T (true) and F (false) to answer this question.

_ The values of an ordinal data type do not come with a natural ordering.

_ The Spearman Correlation Coefficient of two ordinal features F and G is defined as the correlation of the ranks of F respectively G.

_ PCA is used to approximate the probability distributions of a family of features.

_ In the U-test, we have to assume that the two given groups are approximately normally distributed.

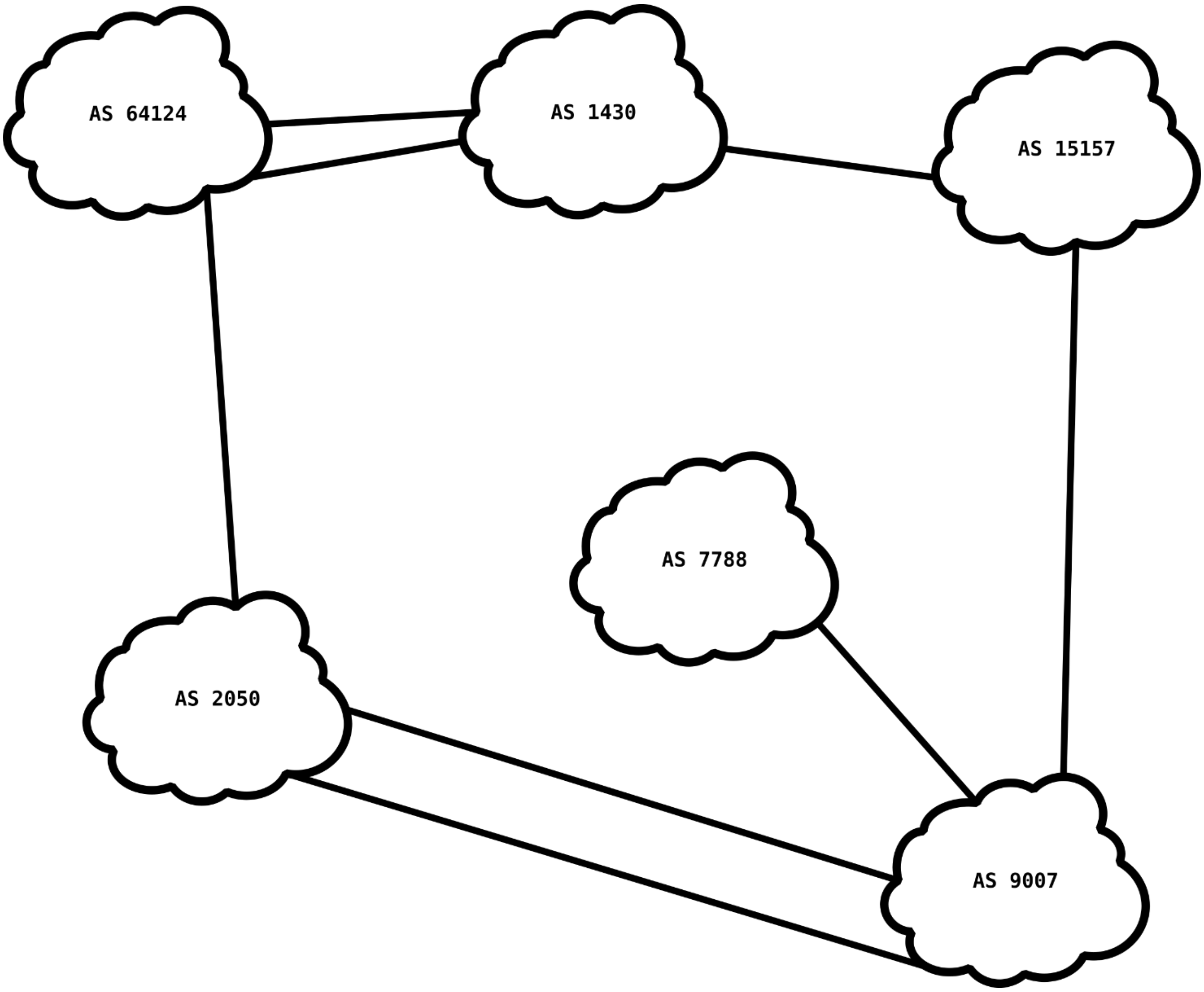
A new virus scanner detects malware with a recall Rec = $T_P/(T_P+F_N)$ of 100% and a specificity Spec = $T_N/(T_N+F_P)$ of 99.9%. A cloud service provider operates a server with 10,030,000 unencrypted files. We assume that 30,000 files are infected. The virus scanner scans all unencrypted files. Fill out the confusion matrix and compute the precision of the virus scanner.

	File is infected	File is not infected
File is reported by the scanner	T_P	F_P
File is not reported by the scanner	F_N	T_N

Name: ____________________________________ *Matriculation number:*______________________________

Task 10: (Internet Routing) 10 points

Given a small Internet as shown in the figure below, calculate the Impact regarding Prefix Hijacking of AS 64124. Provide the corresponding formula and intermediate results of your calculation.


AS 64124
AS 1430
AS 15157
AS 7788
AS 2050
AS 9007