COM 402 Final Exam

25.01.2021

1

Name: Anonymous

Sciper: **123456**

Do NOT open this document until instructed to do so.

Instructions

- This is a **closed book** exam. Books, notes and electronic devices are not allowed, except for up to two A4 pages of notes (this amounts for *one* double-sided A4 sheet or equivalent).
- No question will be answered during the exam, except possibly questions related to the understanding of the English language.

Multiple choice questions:

- There are 17 multiple choice questions, counting 1 point each.
- Only one answer per question is correct.
- Ticking the correct answer counts for 1 point.
- Ticking an incorrect answer, more than one answer, or no answer counts for 0 point.
- Make a mark **inside** the box corresponding to your answer.
- Use a black or blue pen to mark your final answers. Pencils are not allowed.
- If you ticked the wrong answer, use a white-out fluid or tape to erase the box completely. **Do not try to re-draw the box**.

Open text questions:

- There are 10 open text questions, counting 1 point each.
- Please write your answers in the corresponding text boxes.
- Do not write more than three lines. Any text outside of the boxes or after three lines will be ignored.
- Do not tick the '0', '0.5', '1' boxes of the top of the text boxes.

Question 1 A web application stores its data in a the database is configured to encrypt all data before we by this configuration?	database on a server. For security reasons, riting it to disks. Which attack is prevented
☐ Database administrators accessing all cleartext data of the users ☐ Users of the application accessing cleartext data of other users through an SQL injection	Server administrators accessing all clear- text data of the users Users of the application accessing clear- text data of other users through an in- secure direct object reference
Question 2 Consider an attacker performing a gras-a-service (MLaaS) in which the machine learning model which one of the following is true?	rey-box attack against a machine learning- nodel is non-linear such as neural networks.
 The attacker must have information about the set or subset of the training data to steal the model. Membership inference attacks are not possible. 	Model stealing attacks are not possible. If MLaaS is using output perturbation, the probability of a successful model stealing attack is reduced.
Question 3 Consider a setting where Alice and Bencrypted using the Paillier homomorphic cryptosystem and Bob (respectively) and pk_A, pk_B be their publicable two secret values held by Alice and Bob (respect $Enc_{pk_B}(m_B)$. If provided with pk_A, pk_B, ct_A and ct_B , which of the the	keys (respectively). Also, let m_A and m_B ively) and $\operatorname{ct}_A = \operatorname{Enc}_{\operatorname{pk}_A}(m_A)$ and $\operatorname{ct}_B =$
\Box ct _{res} such that $\operatorname{dec}_{sk_A}(ct_{res}) = m_A \times m_B$. \Box ct _{res} such that $\operatorname{dec}_{sk_A}(ct_{res}) = m_A + m_B$.	ct_{res} such that $dec_{sk_A}(ct_{res}) = m_B.$ None of these choices.
Question 4 Recall that adversarial examples are i attacker has designed to cause the model to make a nabout adversarial examples?	nputs to a machine learning model that an nistake. Which one of the following is <i>true</i>
 In high-dimensional spaces, it is possible to defend against all possible adversarial examples by detecting suspicious queries. An attacker may use the transferability property of adversarial examples to attack different machine learning models with the same adversarial example. 	 In all cases, adversarial examples have to be imperceptible by humans. It is possible to defend against all possible adversarial examples via adversarial training.

Question 5 The GA4GH Beacon Project gathers be queried by researchers. To limit privacy concerns, We assume here that the attacker is a honest-but-curr queries to the database through the correct interface	ious adversary and acts as a researcher sending
The probability of success for a reidentification attack consisting of j queries can be lowered by only answering "yes" to queries for which there are more than k patients satisfying the query	Limiting the number of queries that an attacker can send is enough to make reidentification and membership inference attacks impossible. It is possible to protect the database
terms. An attacker having no other side information about a subject except than his name can still re-identify or infer (with 100% certainty) the presence of this subject in the Beacon Project database.	against re-identification attacks without altering its utility.
-	le. validate_password is a function that is
vulnerable to a timing attack; an adversary can re remote procedure call) and analyze the timings to re	
The operator ^ denotes the bitwise exclusive OR a	<u>-</u>
converts a char to a number, and zip(a,b) loops ov	ver the two sequences simultaneously.
1. pwd="password123"	
<pre>2. def validate_password(user_input):</pre>	
3. return user_input == pwd	<pre># timing attack!</pre>
4. def fn1(a,b):	
5. a_original = a	
6. while len(a) < len(b):	
7. a += " "	
8. result = 0	
9. for x , y in $zip(a, b)$:	
10. result = result $(ord(x) ^ ord(x))$	
11. return (len(a_original) == len(b)) a	and (result == 0)
12. def fn2(a,b):	
13. import time, random	
14. time.sleep(random.randint(1,100) / :	10000)
15. return (a == b)	
16. def fn3(a,b):	
17. result = 0	
18. for c in a:	
19. result = result ^ ord(c)	
20. for c in b:	
21. result = result ^ ord(c) 22. return (len(a) == len(b)) && (resulting to the content of the c	t == 0)
To remove the timing attack in validate_password() keep the intended functionality, the most secure opt	
Replace line 3 by	Replace line 3 by
return fn3(user_input, pwd)	return fn1(user_input, pwd)
Replace line 3 by return user_input==sha256(pwd)	Replace line 3 by return fn2(user_input, pwd)

Question 7 The <i>Trojan</i> problem in access control uses the access rights of a user to access protected everybody. Which form of access control is designed	
 Discretionary access control Mandatory Access Control with a no write-up rule 	■ Mandatory Access Control with a no write-down rule □ Role based access control
Question 8 Which of the following choices correct The completeness, soundness and zero-knowledge probe guaranteed in settings where	ctly completes the following statement? roperties of zero-knowledge-proof systems can
a potentially dishonest prover wants to prove a statement to an honest verifier. an honest prover wants to prove a statement to a potentially dishonest verifier.	 a potentially dishonest prover wants to prove a statement to a potentially dishonest verifier. None of these choices.
Question 9 A Web Application Firewall (WAF block attacks to a web server by looking for pattern attack can not be detected by such a WAF?) is a reverse proxy that tries to detect and as in the requests it receives. Which type of
☐ SQL injection attacks ☐ Buffer overflow attacks	☐ LDAP injection attacks ☐ Insecure Direct Object References
Question 10 Which one of the following statement	ents is false?
In Bitcoin, stealing a specific private key allows to rewrite the transaction history for that key.	In permission-less blockchains the number of participants does not need to be predefined.
Bitcoin's security uses digital signatures.	Permission-less and open blockchain refer respectively to who can write and read the chain.
Question 11 Which of the following is <i>not</i> a prin	mitive of asymmetric cryptography.
Message authentication codes	Digital signature
Public and private keys	Interactive key exchange (e.g. Diffie-Hellman)
Question 12 Consider a machine M using a Truelarge, secret list of pseudonyms L_1 , sealed by the TP which software is running on M ; in this process, a TP private list of pseudonyms L_2 over the confidential chand returns the results over the TLS connection. When	LS connection is established. Then, I sends a nannel. M , using the TPM, computes $L_1 \cap L_2$
 On the machine M side, the TLS connection is terminated by (that is, decrypted by) the Operating System, which forwards the data to and from the TPM. Changes to the OS (for instance, installing software updates) will alter the attestation process, but will not require 	 Any change to the OS of M (for instance, installing software updates) requires re-sealing the list L₁. On the machine M side, the TLS connection is terminated by (that is, decrypted by) the TPM, which forwards L₁ to the OS to compute L₁ ∩ L₂. The TPM encrypts and returns the answer
re-sealing the list L_1 .	to the initiator.

Question 13 W	hat is a	zero	day	exploit?						
An exploit for no patch exists An exploit tha vulnerability it	s yet it was p	ublis	hed	after the		A	_	t that	exist	ery simple to exploit s in the original ver-
Question 14 W	hich is t	he b	est v	vay to pro	otect	against :	SQL inj	ection	s?	
reject any input words (e.g. und escape all occur ble quotes (' -	ion, sele	\cot) of \sin	ngle			use prepared statements use only indirect object references				
Question 15 Co of attesting which O M receives a networ request is answered to the initiator of the with the TPM for other controls.	Derating rk reque to by the ne reque	g Systest from the THest.	om a PM, After	n (OS) is an extern which est rwards, th	runni al pa ablisl he ini	ng. Firsty to proper a TL tiator of	et, M is rove whas change the rec	turne ich O nel and quest	ed on S has d send may o	been loaded. This ds back information continue interacting
cess, that is, lo Master Boot	☐ The very first steps of the booting process, that is, loading the BIOS and the Master Boot Record (MBR), may be safely omitted in the attestation process. ☐ The establishment of the TLS channel is primarily for confidentiality purposes (for instance, so that the OS does not observe the subsequent communication).									
	The Endorsement Key (EK) is used in A challenge (or nonce) is not required to									
Question 16 In accessible by any ent										public, i.e., is fully queries of the form:
SELECT COUNT(*	() FROM	dat	abas	se 1 WHE	RE D	isease=	arg1 AN	D Age	e in	[arg2,arg2+6]
A researcher chooses from the protocol. We and that a research following is <i>true</i> ?	Ve assun	ne th	at I	Database 1	is co	rrectly p	rotecte	d agai	nst aı	my type of injections
	Database					Database				
	Zipcode	Age	Sex	Disease		Name	Zipcode	Age	Sex	
	1183 1456	29 21	M F	COVID-19 Diabetes		Alban Michelle	1183 1456	29 21	M F	
	1183	25	M	COVID-19		Louis	1183	25	M	
	1018	30	М	Flu		Joseph	1018	30	М	
If an attacker process SELECT COUNT WHERE Disease Age in [23,2] on Database 1 only 50% process COVID-19.	(*) FRO e=COVII 9] 4, he/sh)M Da D-19 e wi	atab AND ll kr	pase 1		m fie A qu di ☐ H	ake re-icult for research reries to isease of	dentifa mal her ne Data each re-ide	ications icious eeds to base indiventification icious icio	m Database 1 would on attacks more dif- s researcher. o perform at least 3 1 in order to find the idual in Database 2.

Question 17 In e-voting, when using a mixnet to shur all the $N \geq 2$ votes and assuming honest voters, which	ffle the votes, assuming each server shuffles of the following statement is <i>correct</i> ?
 □ To prevent linking the ballots to the voters, a threshold T > 1 (T defined as a cryptographic threshold used in secret-sharing) of honest mixnet servers is needed. □ A global network adversary observing both the inputs and the outputs of an honest mixnet server can correlate which input correspond to which output. 	If all mixnet servers are malicious and under the control of the adversary A , then A is still unable to link a ballot in the output to a particular voter. To prevent linking the ballots to the voters, a single honest mixnet server is needed.

ASLR and buffer overflows

Question 18 Explain how Address Space Layout Randomization (ASLR) can prevent the exploitation of a stack-based buffer overflow.

0 0 5 1

0 0 5 1

ASLR randomizes the address of the stack (among others). The attackers don't know the address of the code they are writing in the stack and thus can't make a return address point to it.
,

Certificate pinning

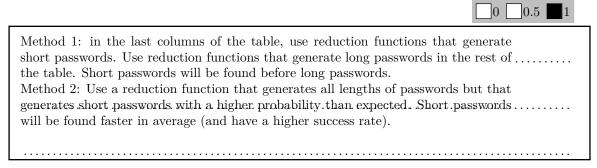
Question 19 Many mobile applications use certificate pinning. This protects against a certain type of attacks. Describe this attack in following terms:

- Who can do the attack,
- what type of attack is it,
- and how they can achieve it.

Trusted CAs can make a (TLS) man-in-the-middle attack by creating a trusted) certificate for the attacked web server.	fake (but

Rainbow tables

Question 20 Describe a way to construct a rainbow table that can crack passwords of different length, but that finds the short passwords faster that the long passwords.



TZ		1			
ĸ	\mathbf{er}	h	e_1	\mathbf{r}	2

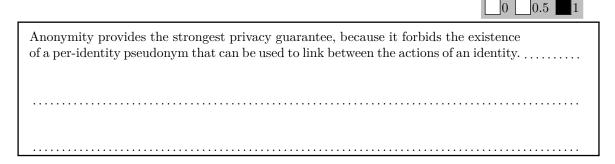
Question 21 Describe the operations that a server must carry out to verify that a Kerberos ticket it received together with an authenticator is a valid ticket.

0 0 5

0 0.0
Decrypt the ticket with its own key. Retrieve session key from the ticket to decrypt the authenticator. Verify that the id in the authenticator and ticket are the same

Privacy Preserving Techniques

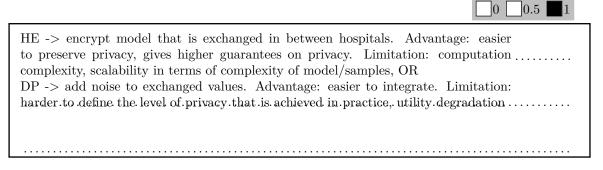
Question 22 In privacy evaluation of systems, which of anonymity and pseudonymity corresponds to the strongest privacy guarantee? Explain why.



Federated Learning

Question 23 Consider a federated learning setting with 4 hospitals where the data of the hospitals remain in their own trusted servers, but a global logistic regression model is trained collaboratively. Assume that this is achieved by averaging the local models from hospitals after each iteration of the learning process to obtain the global model.

State one possible protection mechanism to protect hospitals' input data *during* training, explain how to use it and state its one advantage and one limitation.



				•
к	\mathbf{loc}	kc.	กล	ın
_			ш	

Question 24 Can somebody who lost their bitcoin-wallet secret-key realistically recover their bitcoins? If yes, explain how, if no explain why.
No. The coins are lost as, under today's standard cryptographic assumptions, one cannot realistically break the bitcoin underlying PKI to recover the key or transfer
Question 25 Propose the types of blockchains required [open/closed, Permissionless (public)/Permissioned (private)] by the following two use cases and explain why: 1. Medical records among hospitals 2. Personal fitness data in crowdsourcing
1. Closed + Private: very sensitive and long term data + could implicate more than the owner. 2. Open + Public/Private: depends on the motivation but crowdsourcing makes it open.
Question 26 In blockchains, is there a best performing consensus algorithm? If yes, which one? If not, explain why.
No there is not. Different need for scalability, energy consumption, use-case/business requirements, security and privacy, and throughput

Privacy and health

Question 27 An imaginary government decided that a citizen should be able to know a little bit more about its fellow citizens overall health status. It therefore decided to build a central database containing the name, age and disease of each citizen. For security, all elements are encrypted under a combination of the keys of the government and the hospitals by using a probabilistic homomorphic encryption scheme. The query:

SELECT COUNT(*) FROM db WHERE Disease=arg1 AND age=number,

can be executed by any citizen. It is performed by relying on deterministic tagging, which enables re-encryption from probabilistic encryptions to deterministic encryptions. Explain (1) why the selection cannot be done directly on HE encrypted data, (2) which information can still be deduced from the deterministic tags by an entity that has access to the query and the deterministic ciphertexts and (3) which privacy risk (provide one example), even without deterministic tagging, is still present even if the data are encrypted and why? One line per answer.

 (1) the HE scheme is probabilistic, two encryptions of the same value are different; (2) such an entity can observe the frequency or distribution of the selection criteria in the database; (3) re-identification attacks, centralization of the data.