EECS 565 Introduction to Computer and Information Security

Exam 2

Name: Jay Offerdahl

KUID: 2760730

Due: Tuesday May 10, end of day. No Extension!

Please upload to Blackboard. No email submission!

Do it by yourself. No discussion!

1. True or False with justification. For each of the following statements, identify whether it is true or false (write "true" for "false" on the line), and then briefly justify your verdict for the "false" statements. (20 points)

1.1 With digital forensics technology, any recently deleted file could be fully recovered.
T or F: ___False___
Short justification for False statements:

- While it's true that many files can be fully recovered, it really depends on the type of filesystem implemented. For example, in linux, if ext2 file deletion is used, the previous directory's entry length is adjusted to obscure the deleted record. However, if ext3 was used, inode is wiped upon file deletion, which means the block numbers associated with the content are lost. It's also worth mentioning that even though a file may have been recently deleted, if the media was destroyed (like with a drill, for example) or securely overwritten with software/other memory, it becomes very difficult/impossible to recover the data.

1.2 Firewalls block traffic based on source IP, source port, destination IP and destination port.
T or F: ___False___
Short justification for False statements:

- This is false because firewalls can block traffic based on these attributes by themselves or in some cases in unison. We don't always have to have all of the information to setup a rule. This simply means we can block traffic on a source IP or port or destination IP or port. It's also worth mentioning that it's really not worth anything for a firewall to block traffic based on source port because attackers could simply change the port they attack over.

1.3 With application-layer end-to-end encryption, eavesdroppers cannot identify the sender and the receiver.
T or F: ___False___
Short justification for False statements:

- Application-layer end-to-end encryption means data/messages are encrypted all the way from the application on the sender's side to the application on the receiver's side. This means the message still has to travel from the sender to the receiver. With that said, it's clear that an eavesdropper could still easily identify the sender and receiver, but they would be unable identify the contents of the message. They would be able to grab the IP headers to find out this information as well as potentially setup a man in the middle attack.

1.4 To use link encryption, sender and receiver must negotiate a pair of key for every connection.
T or F: ___False___
Short justification for False statements:

- While this is mostly true, for systems with multiple intermediate stages, each intermediate stage has the ability to use a different key/algorithm for the data encryption, as long as the other side of the link knows how to decrypt it. For general cases where the setup is point to point, this statement would be true because the sender/receiver would decide on the key for every (1) connection.

1.5 Firewalls can never prevent a compromised internal computer from sending data to an external server.
T or F: ___False___
Short justification for False statements:

- Firewalls allow/block traffic in or out of the network they are protecting. This means a rule could be set up to block traffic on a certain port from an IP. While this will not ALWAYS prevent compromised internal computers from sending data to external servers, it could block some cases, which may come in handy when trying to protect your network. For example, if a computer is infected by a Trojan horse and the firewall has been setup to only allow incoming/outgoing traffic over HTTP, FTP, and maybe a few others like SSH, depending on the Trojan horse, this attack could be blocked on ports that have been closed by the firewall.

1.6 In order to execute a file, Alice must have both read and write rights to the file.
T or F: ___False___
Short justification for False statements:

- If Alice has executable permissions, she can execute the file. She does not need to be able to read or write to the file. However, if Alice does not have executable permissions, she could get away with executing the file if she had the ability to read the file, and therefore the ability to copy the file. Assuming her user group has access to executable permissions at all, she could then execute this new file.

1.7 Compared with access control lists, the access control matrix always requires less memory space for the same set of users and access rights.
T or F: ___False___
Short justification for False statements:

- The access control matrix requires more memory space for the same set of users and access rights. This is the case because access controls lists can omit users with no permissions. There is the case where the access control matrix could use equivalent memory space as access control lists. However, in a general conclusion, the access control matrix will, for the most part, require more memory space than access control lists.

2**. Network security (10 points)**

2.1 Mallory successfully launched DNS spoofing attack on a small network. All traffic to www.xyzbank.com is now re-directed to a server controlled by Mallory. Alice visits www.xyzbank.com using HTTPS (HTTP over SSL/TLS), what could Alice discover?

- Alice will discover that the certificate returned to her is either self-signed, which will normally show an alert message of "Deceptive site ahead..", depending on the browser. If this is not the case, Alice would receive the legitimate certificate, however, because Mallory doesn't have the private key, she'll be unable decrypt the master secret, so the connection will fail.

2.2 A global company has two data centers in Antarctica and Arctic, respectively. They rent submarine communication cables to share data between two data centers. The traffic is routed through Easter Island. The CEO claims: "The communication between Antarctica and Easter Island is encrypted at link layer, and communication between Easter Island and Arctic is also encrypted at link layer. Therefore, we do not need to encrypt the data by ourselves, to save computing power". Is he right? Please explain.

- He is right that the data is encrypted at link layer between Antarctica and Easter Island and between Easter Island and Arctic. However, his statement becomes wrong when he says that they do not need to encrypt the data ourselves. He is assuming that the data is secure 100% of the way. However, when using link encryption, the data is decrypted at Easter Island. This means an attacker could access the data at Easter Island when it's decrypted above the physical layer. So, in the end, the CEO is wrong about not needing to encrypt the data themselves, and he probably needs to consult his CTO.

3. Firewalls (20 points)

A small company has one firewall that is deployed between the company's internal network and the Internet.

3.1 The CISO (Chief Information Security Officer) discusses the company's firewall rules with the CEO. The CEO made the following statements. Are they valid (from technical point of view)? Why?

A) As long as we keep our firewall effective and up-to-date, it is less important to patch our web, FTP, database, and email servers behind the firewall, since they are protected by the firewall.

- This statement is blatantly invalid. All of these services would (most likely) need to communicate with the Internet, so traffic to them will be open to some extent. Whether this is port 80 for web/ftp or 110 (pop3) or 143 (imap), these services will have a link to the internet. It is absolutely necessary to patch these servers because if malicious traffic enters on these ports, it could still infect the machines. The firewall might be good enough to block all traffic on ports other than these mentioned here, but the firewall isn't the only line of defense in a properly configured network.

B) Since HTTPS connections are encrypted and secure, we should allow all HTTPS connections.

- This statement is also invalid, but not as much as the first question. While HTTPS connections are encrypted and secure, a website could still contain malicious content that could potentially harm the company's network. HTTPS does a great job of preventing man in the middle attacks and tapping, but does absolutely nothing against the web server being hacked or exploited. In the end, allowing all HTTPS connections is a step in the right direction, but some level of care should still be put on this rule.

3.2 The CISO plans to deploy an intrusion detection system (IDS) along with the firewall. He has two options: deploying it behind the firewall, or deploying it in front of the firewall. “Behind the firewall” means the internal (i.e. LAN) side of the firewall, while “in front of the firewall” means the Internet (i.e. WAN) side of the firewall. Please discuss the effectiveness of each IDS in defending against the following attacks,

A) Port scanning from external adversaries.

- An intrusion detection system in front of the firewall would be most effective in this case. The IDS would see the traffic before the firewall, and would be able to alert the sys admin about the potentially malicious traffic. If we were to put the IDS behind the firewall, our external adversaries would have free reign to run port scans on our firewall. The IDS would only be able to pick up on these port scans if the firewall went down or allowed traffic through.

B) Worm spreading in the local area network (LAN).

- An IDS in front of the firewall would be completely useless here, unless our services were spreading the worm to the internet (WAN). In this case, placing the IDS behind the firewall would be the surefire solution to detecting this type of attack because the IDS would have direct access to check for intrusion signatures or attack signatures from known attacks. In a more extreme case, the worm may try to spread to the IDS itself.

4. Multi-level security (15 points)

Multi-level security is employed in a database system. Access control is enforced at record level. The following table contains records about employees' information:

ID	ID_C	title	title_c	task	task_c	report	report_c	TC
7256	S	manager	S	K2398	S	09/20/2010	S	S
3592	C	special agent	C	D9372	C	08/28/2010	C	C
5697	UC	special agent	UC	K8364	UC	09/05/2010	UC	UC
0036	TS	director	TS	K2398	TS	09/27/2010	TS	TS
6585	S	assistant	S	K2934	S	09/20/2010	S	S

4.1 a user at security level 'C' browses the database, what could he/she see from the table?

ID	ID_C	title	title_c	task	task_c	report	report_c	TC
3592	C	special agent	C	D9372	C	08/28/2010	C	C
5697	UC	special agent	UC	K8364	UC	09/05/2010	UC	UC

- A user at level 'C' would be able to see all records at classification 'C' and below, which includes one 'UC' record.

4.2 a user at security level 'TS' wants to change the *task num* attribute of ID 6585 from "K2934" to a new task "K9998". How will the request be processed? What is the rationale behind the procedure?

ID	ID_C	title	title_c	task	task_c	report	report_c	TC
7256	S	manager	S	K2398	S	09/20/2010	S	S
3592	C	special agent	C	D9372	C	08/28/2010	C	C
5697	UC	special agent	UC	K8364	UC	09/05/2010	UC	UC
0036	TS	director	TS	K2398	TS	09/27/2010	TS	TS
6585	S	assistant	S	K2934	S	09/20/2010	S	S
6585	S	assistant	S	K9998	TS	09/20/2010	S	TS

- The updated database is shown above. The request will of course be successful because the 'TS' user has access to perform this action. The request will first replicate the tuple and will change the task to "K9998", while at the same time updating the task_c variable and tuple classification. The rationale behind this procedure is that users at higher security levels can't expose information to lower security levels.

5. We recently discovered that a corporate data center was compromised. Through intensive investigation, we found that the attacker performed the following operations. For each step described below, please identify one defense mechanism that you think is the most effective. (20 points)

A) The attacker obtained the login credentials of data center user *User1* through spear phishing.

- To protect against spear phishing attacks, **all** users should be trained to identify and verify these suspicious emails, as well as social engineering attacks. The security team at this company could also make it harder to obtain personal information.

B) The attacker discovered that remote desktop connection (RDC) was enabled on a desktop computer *Desktop1*, which was inside the corporate network. The attacker used *User1*'s credentials obtained from Step (A) to login to *Desktop1* during late night hours.

- In this situation, I would think that the company could implement an access control mechanism that would restrict access on user accounts at least for remote desktop protocol (and maybe some other services) when it's not working hours. This would have ensured the attacker wouldn't have been able to access this desktop in a lower security setting.

C) The attacker scanned the internal network from *Desktop1*, and found the database server *DB1*. *User1* is authorized to query *DB1*.

- An intrusion detection system (IDS) would come in handy here because it would be able to recognize the network scan from desktop1. This would alert security staff and the attacker would be unable to proceed (so long as other damage hadn't been dealt).

D) Every night between 3am and 4am, the attacker connected to *Desktop1* to issue queries to *DB1*, and stored the answers to the corporate's shared data storage, which was only accessible to the internal network. The attacker used a script to do this every day for almost three months.

- To reiterate from part B, an access control mechanism could be put in place to refuse connections during non-working hours. However, another solution would be to remove executable permissions for this user on this machine except for the absolutely necessary programs.
- Also, an IDS could prove handy here as it may be able to detect this recurring activity late at night which would tip off the security team that something regular is happening.

E) Finally, the attacker moved all the data files to the corporates Web server, and downloaded the file from the Internet.

- There are several solutions to this problem. To begin, the company could have modified their database DB1 by randomly modifying data, swapping values, etc. (data obfuscation). Other than this, they could have made records k-anonymous with each other in order to protect individual records, assuming the data being stored was individual records.
- Also, the company could have restricted access control to not allow this user access to the web server. In addition to this, they could set a limit on how much data could be uploaded/downloaded at a time, making the process of transferring the company's shared data storage much more time consuming, allowing for more time to catch the attacker.

6**. Privacy (15 points)**

The following table was obtained from electrical-medical-records:

First	Last	Age	State	Income	bloodtype	lab-1	lab-2	lab-3
Frank	Davis	23	PA	55K	O	2.5	-	79
Isabella	Brown	45	NY	63K	AB	3.2	+	75
William	Wilson	37	PA	70K	A	3.1	-	66
Alice	Moore	45	NJ	110K	O	2.6	+	68
Ethan	Harris	53	OH	45K	O	2.1	+	58
Michael	Martin	26	NJ	62K	B	2.6	-	77
William	Clark	28	NY	73K	O	3.0	-	54
Daniel	Lee	32	VA	83K	A	3.0	-	62
Alexander	Hall	40	MA	98K	AB	2.8	+	80
Emily	Johnson	36	CT	100K	O	2.5	-	73
Emma	Hill	43	MA	80K	A	3.1	+	68

6.1 Please point out: identifiers, quasi-identifiers, sensitive attributes.

- Identifiers:
  - `First, Last`
- Quasi-identifiers:
  - `Age, State, Income, Bloodtype`
- Sensitive attributes:
  - `lab-1, lab-2, lab-3`

6.2 For a medical research, we need to publish Age, State, Income, lab-1 and lab-2. Please modify the data so that the Age attribute is protected under 3-anonymity.

Age	State	Income	lab-1	lab-2
< 30	PA	55K	2.5	-
>= 40	NY	63K	3.2	+
>= 30, < 40	PA	70K	3.1	-
>= 40	NJ	110K	2.6	+
>= 40	OH	45K	2.1	+
< 30	NJ	62K	2.6	-
< 30	NY	73K	3.0	-
>= 30, < 40	VA	83K	3.0	-
>= 40	MA	98K	2.8	+
>= 30, < 40	CT	100K	2.5	-
>= 40	MA	80K	3.1	+

- Age is now protected under 3-anonymity. I setup age brackets for less than 30, between 30 and 40, and greater than or equal to 40.

6.3 When an attacker obtains the table you created in 6.2, could he/she discover the true identity of the owners of the records? (Assume that the attacker knows all the personal information about the patients) why?

Age	State	Income	lab-1	lab-2
< 30	PA	55K	2.5	-
>= 40	NY	63K	3.2	+
>= 30, < 40	PA	70K	3.1	-
>= 40	NJ	110K	2.6	+
>= 40	OH	45K	2.1	+
< 30	NJ	62K	2.6	-
< 30	NY	73K	3.0	-
>= 30, < 40	VA	83K	3.0	-
>= 40	MA	98K	2.8	+
>= 30, < 40	CT	100K	2.5	-
>= 40	MA	80K	3.1	+

- Yes, an attacker could discover the true identities of the records by using a basic background information attack. For example, if I see a record that shows the state as MA and their income as 98K, I know the lab results belong to Alexander Hall.

6.4 Further modify the data so that (Age, State, Income) are protected by 3-anonimity.

Age	State	Income	lab-1	lab-2
< 30	*	*	2.5	-
>= 40	*	*	3.2	+
>= 30, < 40	*	*	3.1	-
>= 40	*	*	2.6	+
>= 40	*	*	2.1	+
< 30	*	*	2.6	-
< 30	*	*	3.0	-
>= 30, < 40	*	*	3.0	-
>= 40	*	*	2.8	+
>= 30, < 40	*	*	2.5	-
>= 40	*	*	3.1	+

- I have modified my data to basically show the age as I had it from 6.2. Also, the states/incomes have been omitted because our dataset included a wide range of states. This, combined with the small size of the dataset meant there was no way to 3-anonimize the states. (There are four N* states, but this is the only case). Next, the income had to be omitted because any division of income resulted in at least one set of data that was still identifiable. (<70K and >= 70K would be identifiable with age, etc.)
- It's worth mentioning that I tried to anonymize age even more to be able to retain some information in state/income, but the above condition was present.
- Even if you broke down age into two categories, anonymizing another category would require 4 breakdowns (for example, age < 35, age >= 35 and income split requires 2 income breakdowns, so 4 equivalence classes) – not possible with 11 entries.