CS-301 Fall 2020 Mini-Exam 5

September 15, 2021

1 Concert

InYourLivingRoom (IYLR) is a new company that sells tickets to concerts that get live-streamed to people's SmartTVs. Users buy tickets through the IYLR app using their bank card as a payment method. To let people connect to the show, IYLR is considering two different options:

1. When a user buys a ticket, their bank gives them a unique code. When the user enters this code into the IYLR browser on their SmartTV, IYLR asks the bank whether this code is associated with a payment. If the bank confirms the payment, the concert is streamed to the SmartTV.

2. Users use the app to prove that they bought a ticket using an anonymous credential. To stream a concert, they provide the IP address of their SmartTV in the IYLR app and the concert is streamed to their TV.

Compare these two options in terms of privacy of users with respect to IYLR: What does IYLR learn about users' music taste, which concerts they streamed, and their location?
Note: Assume that all internet connections are secured using TLS and that the SmartTV is not behind a NAT.

2 Taylor Swift

One of the COM-301 TAs is a big fan of Taylor Swift and would like to leave an appreciating comment under a video of one of her concerts on a new video platform called OurSpace. However, he is concerned that 1) the other TAs of the class will find out that he likes Taylor Swift's music and that 2) OurSpace collects data about his music taste. To be able to leave a comment on OurSpace, OurSpace requires you to prove that your are older than 18 years old.
Name (1) one privacy technology that OurSpace could implement to provide privacy for the TA's comment with respect to the other TAs (2) one privacy technology that would enable the Taylor fan to provide the comment but have privacy with respect to OurSpace.

3 Botnets

Part 1. Agree or disagree with the following statement:
"Running an antivirus based on signatures on all machines within a company's internal network provides protection against a Botnet that attacks your company's network from the outside"
Justify your decision.
Part 2. If you agree, provide a way for Botnets to bypass the defense. If you disagree, provide an alternative defense mechanism that would provide protection against Botnet attacks.

4 Wormtail

A new worm, Wormtail, has appeared on the Internet that threatens the operation of your company. As a security engineer, you are tasked with finding a suitable protection mechanism. What we know about this worm is that:
- Wormtail exploits a buffer overflow on a piece of networking software used by your company.
- After the buffer overflow, Wormtail deletes all files from a particular program.
- Every two weeks Wormtail mutates its code, targeting a different program, but keeps the same lines of code that exploit the buffer overflow to be able to enter in the companies' systems.
From COM-301 you remember that Intrusion Detection Systems are a defense against worms but there are two types: signature-based and anomaly-based.
Part 1. Which of this types would you recommend to your company? Justify.
Part 2. Explain in one or two sentences what the Intrusion Detection System that wants to detect Wormtail should look at.

5 TorTLS

Agree or disagree with the following statements:
1) "If a user's connection to a server is protected by TLS, using Tor does not increase the user's privacy towards a local adversary that can only observe the LAN of the client"
2) "If a user's connection to a server is protected by TLS, using Tor does not increase the user's privacy towards a local adversary that can only observe the LAN of the server"
Justify your decision.

6 TorLogin

Agree or disagree with the following statements:
1) "If you log into Facebook via Tor, there is no need to use TLS to protect the password from a local adversary that can only see the connection from your

gateway to the entry node". 2) "If you log into Facebook via Tor, there is no need to use TLS to protect the password from an adversary that can see the connection from your gateway to the entry node and has the capability to perform BGP hijacking on traffic towards Facebook".
Justify your decision.

7 TorMix

Agree or disagree with the following statements:
1) "If you only care about an adversary in the LAN, low-latency and high-latency communications provide the same protection".
2) "Low-latency and high-latency communications provide the same protection against a global adversary that can observe the full network".
Justify your decision.

8 Photos

BigCorp Photos is a mobile application from BigCorp corporation that can automatically upload user's photos to the BigCorp's cloud servers. The photos are transmitted securely to the BigCorp servers, and once they get there they are securely stored. BigCorp Photos also enables to share access to photos with other users of the system, and to revoke this access. For operational purposes, BigCorp employees and internal scripts have access to all the photos' content and metadata.
The following is a conversation between a BigCorp employee and a user that happened publicly on the Internet:

@BigManagerAtBigCorp: "Tell us what you want to see next from BigCorp Photos!"
@PrivacyConcernedUser: "How about some privacy?"
@BigManagerAtBigCorp: "What do you mean? BigCorp Photos is extremely private"

Clearly, "privacy" means different things to the manager at BigCorp and the privacy-concerned user.
(1) Map the views on "privacy" of these two people to the social, institutional, or anti-surveillance adversarial models of privacy. Justify.
(2) Name one privacy technology within one of the adversarial models from (1) (specify within which) that is applicable to BigCorp Photos, explain what private information it would protect, and identify whether it is already implemented in BigCorp Photos.

9 Data Anonymisation

GreedyCorp, a popular supermarket chain, has introduced a customer loyalty card that allows customers to get access to discounts and special offers. To

participate in the program, a customer has to scan their loyalty card for every purchase at one of GreedyCorp's shops. The loyalty card is linked to a unique identifier and the customer's name. Every time a customer's card is scanned, GreedyCorp stores a record about this purchase in their database.
For instance, if Alice who regularly shops at GreedyCorp recently bought bread, grapes, and Gruyere, this will be recorded as *(Alice, ID1234, 2020-02-11 18:31, [bread, grapes, Gruyere])*.
After six months of data collection, GreedyCorp asks their data analyst, Daria, "what are the most popular items amongst customers who participate in the loyalty card program?
To prevent Daria from learning which individual customers bought what items, GreedyCorp removes customer names from each record before giving the data to Daria. For instance, Alice's sanitised purchase record would look like *(-, ID1234, 2020-02-11 18:31, [bread, grapes, Gruyere])*.
Daria wants to learn what items her friend Alice bought at GreedyCorp. What would Daria need to know about Alice's purchasing behaviour to be able to identify which of the sanitised records belong to Alice? *Detail an attack* that enables Daria to achieve her goal using this knowledge about Alice's purchasing behaviour.
Assume that Daria has access neither to the table that links a customer's name to their unique ID.

10 Taylor Swift

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.
One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.
Does this setup provide good privacy to the TA if his main privacy concern is that
(1) The other TAs learn that the shy TA is a big fan of Taylor Swift?
(2) OurSpace learns that the TA is a big fan of Taylor Swift?
(3) The TA's Internet Service Provider learns that he is a big fan of Taylor Swift?
Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.