Mini-Exam 5, Most Repeated Errors

September 15, 2021

Question: BigCorp Photos

Error 1: The manager is thinking only in terms of social privacy. Such a response was never penalized in grade. However, as a clarification: The manager could be considering either institutional or social privacy, or both. This is because these two adversarial models treat the service provider as *trusted*, and BigCorp Photos is arguably satisfying requirements of both social and institutional privacy (see more on this in the next bullet).

Error 2: The fact that BigCorp employees have access to the photos is a concern in terms of institutional privacy. Such a justification did not receive the full grade. Within the adversarial model of institutional privacy, a user would consider the provider *trusted*. Among everything else, this means that any internal accesses of employees to private data are assumed to be done for operational purposes. A concern within the framework of institutional privacy should refer to a breach of one or more principles of data protection, e.g., the photos are uploaded without the user's consent. If such additional assumptions were explicitly stated and were reasonable, we did give the full grade for the argument that the user is concerned about institutional privacy.

Error 3: End-to-end encryption (E2E) is a technology that addresses social-privacy concerns. The goal of E2E encryption between users is to prevent an intermediary (the service provider) from seeing the encrypted content. However, in the social-privacy model the service provider is trusted, thus E2E encryption is not relevant. The notion of social privacy is concerned with the privacy on a higher level of abstraction, considering the low-level infrastructural issues out of scope.

Error 4: Saying "E2E encryption with ends being the user and the service provider." If the encryption is between a user and the service provider, it is not E2E encryption. The communication can be E2E-encrypted either between users or between the provider's servers.

Error 5: Anonymization is applicable to BigCorp Photos. As the content of the photos itself can easily identify the owner and it is accessible to BigCorp em-

ployees, no anonymization/pseudonymization technique (e.g. hiding the email of the uploader of a photo) is sufficient to preserve the privacy of photos.

Question: Low-latency vs. High-latency

Error 1: The user only communicates in LAN. The problem states that the adversary is limited to observing the LAN (like your roommate or another student in library). This does not mean that users are limited to only having connections to nodes inside the LAN. Only that adversaries have limited visibility. The user may visit any site on the Internet.

Question: Botnets

Error 1: The anti-virus would not prevent the botnet attack because it is signature-based. Some answers stated that the reason for the anti-virus being ineffective was because it was signature-based and would not be able to detect new viruses. We did not accepted this as correct. The question asked about preventing the botnet attack. The virus is a consequence of the botnet attack, not the attack itself. So, using an anti-virus (either kind) will not protect the company's network from the botnet.

Question: Wormtail

Error 1: Signature-based IDS is useless. The question states that there is a part of the worm's code that stays invariant regardless of the mutation: the part of the code that exploits the buffer overflow. This is suitable as a signature for an IDS. That the rest of the code mutates does not invalidate the signature-based IDS approach.

Error 2: The buffer overflow itself is an anomaly detectable by an IDS. Buffer overflows are not an anomaly, but as bad memory use. IDS does not check for overflows. A more fitting anomaly would be the deletion of all files of a program.

Question: USB

Error 1: The name says anti-virus, so it should be good against viruses. This is not an acceptable justification. We expect you to consider the scenario in the question and provide details. In fact, anti-viruses cannot solve all virus problems. In here, an anti-virus is useful if it scans the USB immediately and prevents the infection. On the other, if the virus is already on the computer, then an anti-virus cannot detect and delete viruses on the booting process.

Error 2: not considering the problem scenario. The question presents a specific scenario where the virus is new, is in a USB, and the virus targets the booting process. These details impact the decision on whether you should an anti-virus or what type of anti-virus you should use.

Question: Tor vs TLS

Error 1: Because Tor packets between the exit node and the destination are in

clear, they leak information about the client. In the LAN of the server, the source IP of these packets appears as the exit node's IP. Moreover, as in the question the packets are TLS, their contents are encrypted. Thus, in this scenario the adversary cannot learn much about the client's identity.

Error 2: After the TLS handshake, the TLS packets do not reveal the source or destination IP adresses. All TLS packets reveal both the source and destination IP addresses, not only the handshake.

Question: GreedyCorp

Error 1: Attack requires to know sensitive information upfront. If Daria already knows Alice's full purchase history, including the *exact items* she bought over a longer period, Daria would not learn any new sensitive information and this would not be a very useful privacy attack. To argue that an inference attack leads to a privacy leakage there needs to be a clear separation between background knowledge and sensitive information leaked.
We gave points for attacks that use some partial knowledge about particular items Alice bought, but only when it was clearly specified how much of Alice's purchase history is considered background knowledge and how much Daria will uncover only through the attack.

Error 2: Not specifying the conditions under which Alice can be singled out. As we explicitly asked to detail a full attack it was not enough to state that Daria would link some background knowledge to the database containing Alice's records. We only gave full points if the answer specifies under which conditions Daria would be able to uniquely identify, i.e., single out, Alice's records.

Question: Taylor Swift

Error 1: List Tor as the most relevant privacy mechanism under all three privacy threat models. The Tor browser is an anti-surveillance tool with a specific privacy threat model in mind. To evaluate the privacy of the shy TA with respect to other users of the platform, i.e., the other TAs, it is, however, not the most relevant privacy mechanism. In a privacy evaluation, you need to first argue the privacy adversary, for instance, other users who might or might not be friends of the TA, and then argue which mechanisms might or might not protect against this adversary, for instance, the access control mechanisms implemented by the platform. Matching the mechanism to the privacy model was a key part of this question and simply evaluating with respect to Tor did not give full points.

Question: Login over Tor

Error 1: The adversary can see the password if no TLS is used. The traffic between the client and the entry node is encrypted (with as many keys as nodes in the path) *even* if TLS is not in use. TLS does not add protection to the client-guard connection.

Error 2: BGP hijacking can be used to take control of the user Tor circuit. Tor is an overlay network (works at the application layer). BGP hijacking operates at the network layer. It cannot change the Onion routers that are chosen by the user.

Error 3: It is possible to MITM the connection to the guard node. The key agreement protocol in Tor is authenticated. The client can check the authenticity of the Onion router they are connecting to. It is not possible to impersonate these nodes.