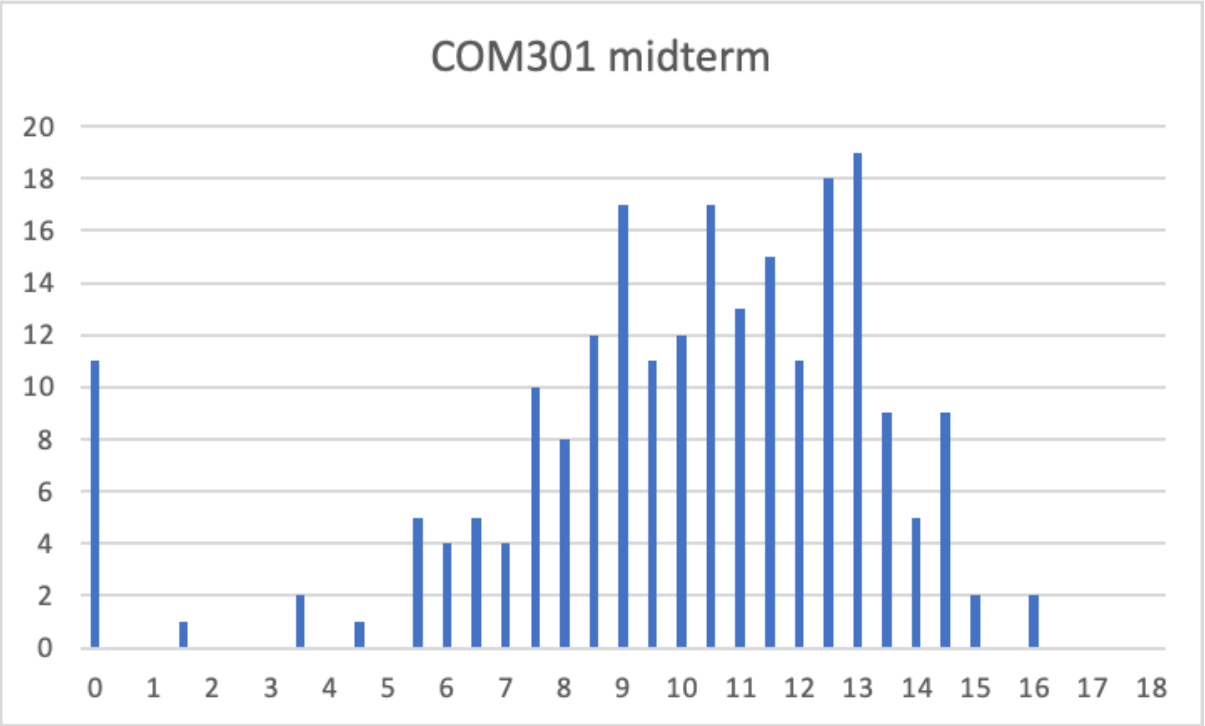
COM301 Midterm 2022

2022-11-17



General notes about the midterm results:

- This is a score out of the maximum total number of points, not a grade on a scale between 1 and 6.
- It will only be reflected in the final grade (30%) if it improves your grade, not if it lowers it.
- The average number of points was 10.5; two students have 16 points, and the maximum is 18.
- 11 students did not participate in the midterm (which is ok since it can only help), are included for transparency in the diagram

The results are in line with the experience from prior years: the midterm serves as a checkpoint and some students realise that attending or watching lectures is not sufficient to solve the questions in the final, and that exercise sessions can really help.

General feedback and advice:

- Read the entire question carefully and answer all of it (ex. In Geletram question, many people did not provide a fix, propose 3 mechanisms instead of 2, etc)
- Use precision in your answers (e.g. “Alice can sign it” → “Alice signs msg using K”)
- Be concise .. the midterm was graded benevolently w.r.t. to the box provided for you answers. The answers alway should be able to comfortably fit in the box

- Provide only one answer … suggesting a correct and an incorrect alternative is not an exam-taking strategy.
- Draft your answers first (pencil, …) you can use the backs of the pages for this.

Some of the most commonly repeated errors are below.

Q1 Security Principles (MCQ)

Answer: (b) Least privilege, if Rob only had access to his files, the damage would have been limited.

Most repeated error: Separation of privilege is not an applicable concept for shared files (a user either can or cannot access a file to read it).

Q3 MAC vs DAC

Answer c is the correct one as covert channels cannot be eliminated in BLP. However, BLP is designed to avoid discretionary declassification, so we also accepted "none" as a valid answer. The other 3 statements are clearly false.

Most repeated error: A system designed using MAC automatically follows the least privilege. This is incorrect, using MAC together with a properly designed DAC can ensure the least privilege principle, but using MAC does not imply that the least privilege is satisfied.

Q7 Hiding the Horcruxes

Most repeated errors:

1. ***Incorrect justification of separation of privilege**: (a) Stating that each follower has their own key and separate responsibilities. (b) Stating that if one follower loses the key/is corrupted, other vaults' keys will still be safe (or need to corrupt all 7 followers). A horcrux can only be accessed with (1) a key (that a follower possesses) and (2) a location (known only by Voldemort) i.e. need to satisfy multiple conditions to access the horcrux, this is why separation of privilege holds.*
2. ***Least privilege:** (a) Confusing it with separation of privilege and stating that followers have the key but don't know the location. (b) Stating the followers only have one key each, so if one follower gets compromised, other horcruxes are safe.*
   Least privilege doesn't hold in this case because once someone gets access to a horcrux, they can do anything with it (steal it, break it, put it back) i.e. there is no privilege-based access control.
3. ***Fail-safe default:** (a) Assuming compromise of key/location. (b) Assuming that the lock is unbreakable/can only be opened with a key i.e. the system doesn't fail.*

The fail-safe default principle is about the security mechanism failing, so if the lock fails, the horcrux is not protected i.e. there is no fail-safe default.

4. ***Open design:*** *The design is not open, the question states that "seven distinct vaults whose security mechanisms are only known to Voldemort."*

Q14+Q15 Life at the Vortex

Most repeated errors:

- *Assuming that downloading the same app can allow you to control the speaker as 'K' will be the same.*
- *Suggesting using hash with salt doesn't solve the problem, this can also be replayed.*
- *Brute forcing of K, or in general determining the key K*
- *Ad-hoc protocol that rotates the shared secret at every transaction (which inevitably will be lost)*
- *Suggesting to use a client-selected nonce or counter, but without a sufficient description of how the server avoids replays (0.5pts)*