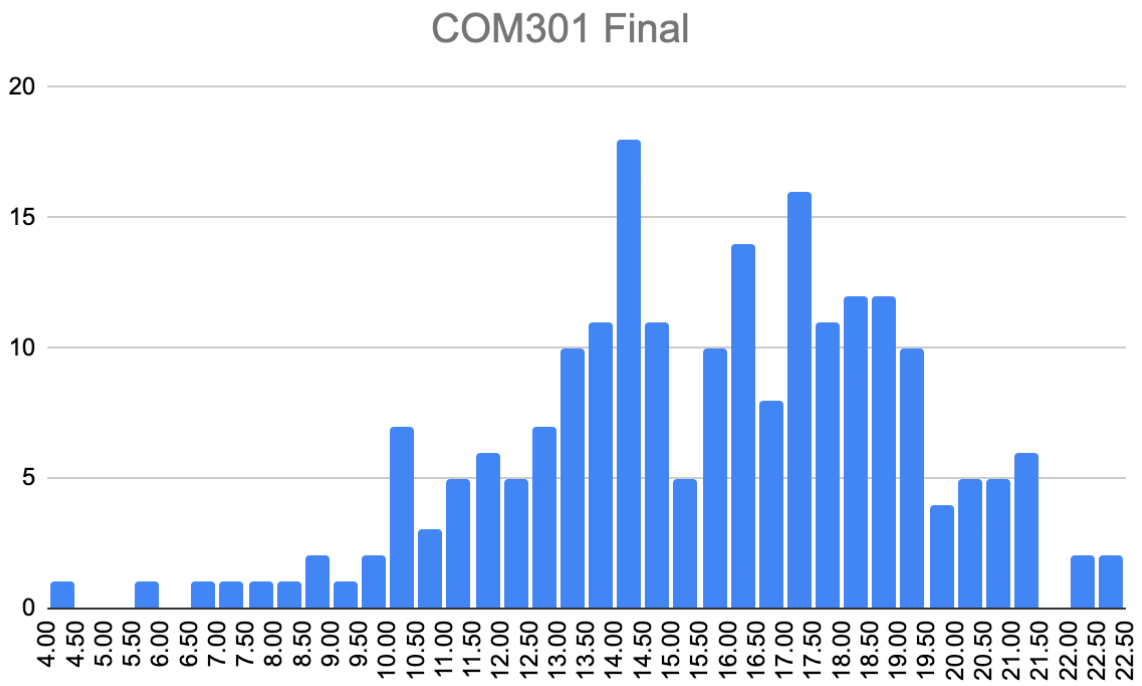
COM301 Final 2022

2023-02-07



General notes about the final results:

- The exam is out of 25 points.
- The average number of points is just above 15; the maximum is 22.5.

Most repeated errors:

MCQ

- Q3: secure hashes can have collisions. Security requires that collisions do not occur above a threshold.
- Q8: many people got confused by the fact that IPSec in transport mode also shows IPs, but this actually does not imply answer A is incorrect. 0.5 was given to correct answers without A (only D ticked). Full points for the correct answer (A+D).
- Q9: anti surveillance privacy cannot be achieved when the communications are not end-to-end. Notice that it is important to understand what “end” actually means. To ensure anti-surveillance privacy, we need “end-user_device-to-end-user_device”. “end-user_device-to-server” is not really “end-to-end”.

Geletram II

- Do not address the problem of Geletram and propose to remove X’ from the database as a fix. Geletram remains broken given an adversary who eavesdrops X’.
- Misinterpretation of forward secrecy: “We stop storing x and y, they will not leak anymore, and forward secrecy is obtained”.

- Not being precise enough. Bad answer: the adversary can compute SK from y and X' and use it to read the messages. Good answer: knowing X' and y, the adversary can compute SK of the christmas session: SK=(X')^y; and use it to recover the messages m from the leaked ciphertexts c: m = Dec(SK, c).

How-To MFA

- "Firewalls" is not a valid answer
- Encryption
    - with student public key: no
    - without mentioning what key nor password
- Delete the code once used, but don't talk about how it's stored

DoReal

- Describing a DoS attack and not DNS hijacking. The whole challenge of the question was to avoid disturbing the lecture. However, from the statement, "the app shows an alert which disturbs the class" in case of DoS.
- Explaining the idea of DNS hijacking but no description of setup/infrastructure.
- Not being precise enough ("setup fake server" or not explaining how DNS requests are intercepted).

- Confusing HTTPS with DoH and DNSSEC.
- Saying there is an issue with encryption (instead of signature).
- Facts without justification (HTTPS hides the fact that students communicate with DoReal, the request will time out) or mismatched justification (Edward cannot replay anymore the "no notification answer" packets from the DoReal server while the attack describes a fake server).

Apple Mail Privacy

- Wrong statements about the setup: "Apple already knows the content of the mail": no. "Apple learns more information by using the proxy": no since the proxy is privacy preserving against Apple.

Thesis Theft

- The adversary showing an encrypted copy, or hash, or signature doesn't prove that it has Ariel's thesis. What should she compare to?

- Many students confused security **properties** with security **principles**. We did not penalize when students provided security principles if justified properly.
    - For example: "least common mechanism is not preserved as the adversary needs to destroy both copies" is not a valid answer.