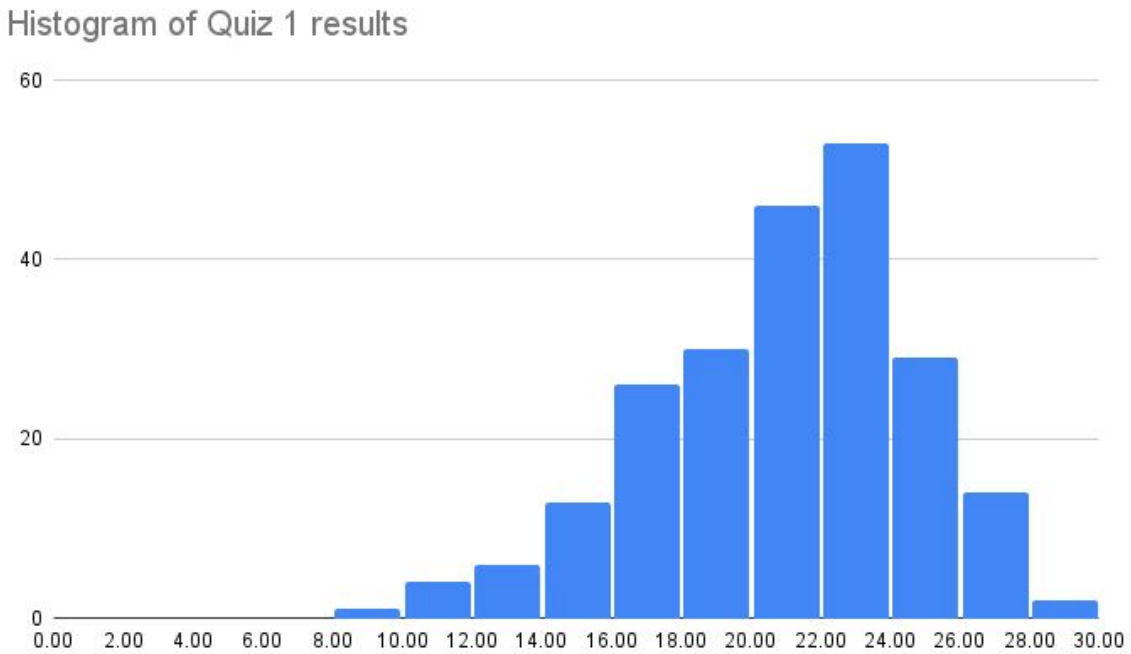
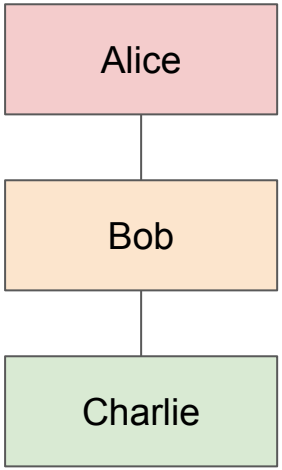
Quiz 01: Statistics



Quiz 01: MAC

Suppose a computer system is setup to use a new hypothetical filesystem, MACfs, which exclusively uses Mandatory Access Control (MAC) to determine which users have what access to which files. There are 3 users in MACfs. They (and their files) are split in 3 corresponding "security" levels (from least to most secret): Alice (unclassified), Bob (classified), and Charlie (secret). Which of the following statements are true?

- **When configured to ensure Confidentiality only, Alice can *modify* the files of Bob**
- **When configured to ensure Integrity only, Charlie can *modify* the files of Alice.**
- **When configured to ensure both Confidentiality and Integrity, Bob can *read* the files of Alice.**



- Confidentiality: no write down!
- Integrity: no write up!
- For both: higher levels can read lower levels

Quiz 01: U2F/2FA

Which of the following are valid authentication factors in a 2FA system?

- **Google Authenticator TOTP**
- **FaceID**
- **Yubikey hardware token**
- **Password**
- **Single-use code via email**

(Note that ALL answers were correct)

Quiz 01: RSA

As discussed in the exercise sessions, which of the following are possible attacks for textbook RSA?

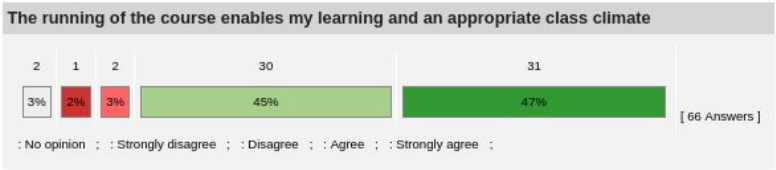
- **When given access to plaintexts of ciphertexts of its choice, the adversary can recover the plaintext of any ciphertext.**
- **When given access to ciphertexts of plaintexts of its choice, the adversary is able to guess which plaintexts out of two was the one that was encrypted.**
- When given two ciphertexts of the same plaintext encrypted via RSA with public keys (n1, e) and (n2, e) respectively, where n1 and n2 are coprime, the adversary can recover the plaintext.

Quiz 01: liblzma

Which of the following statements about the liblzma backdoor are true?

- Some components of the backdoor were deliberately introduced inside the ***OpenSSH source code***
- The backdoor ***did not have any negative performance impact***, making it impossible to detect via performance testing
- **An attacker exploiting the backdoor can get root access to any machine running an OpenSSH server where a vulnerable version of liblzma is present and loaded by OpenSSH**
- Andreas Freund accidentally found the backdoor via ***a fuzzing campaign*** on OpenSSH

Feedback from the feedback



Lecture Style and Content:

Like: passion and engagement

Dislike: jargon, acronyms, fast paste/too many definitions, lack of practice

Quizzes and Assessments: quizzes are too difficult and questions are mean

Exercise Sessions: mixed feedback, some mention that they lack technical skills (e.g., Flask, Docker).

Course Structure and Scheduling: most prefer Monday over Wednesday for class

Overall Course Impression: overall course is OK