**1) Give examples of the following information security concepts at a university:**

(a) No-write-down policy: A professor when writing final exam contents, should not write it down to any users or groups of below level (teacher assistants, students, etc) so as the exam details are kept confidential

(b) Sanitizing data before downgrading: When scores of a final exam is released, the names and information of the grader is deleted (sanitized) so that there would not be biases for some students nor doubt against the grader.

(c) Covert channel: During exams, the supervisors and some students try to communicate with each other other than speech, which goes unrecognized

(d) Separation-of-duty policy: Lecturers issue grades to students, but only admin staff can enter them into the study register

(e) Pseudonym: A student, staff or personnel uses a name that cannot be used to verify their true identity in their records

(f) Data deanonymization: In the student grades records, an attacker or just a friend or professor can guess which student the record belongs to based on the grades and the taken courses

(g) Consent (as in GDPR) (The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy): Students have total rights to determine how their personal data is used and handled by the university

(h) Defense in depth: To prevent unwanted cyber attack on student records, universities implement many layers of protection, such as **DNS protection, intrusion detection and endpoint detection**

(i) Isolation: Website that contains student grades should be in isolation from the normal course website as to prevent unwanted attack from modifying the grades in the system

(j) Minimizing attack surface: The software engineers of the university website and course registration pages must investigate the number of attacking points (xxs, sql injection, etc) and try to fix them, thus minimizing the attack surface

**2) Define or explain concepts**a) Privacy  
**Privacy** is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

When something is private to a person, it usually means that something is inherently special or sensitive to them  
b) Identity provider

An **identity provider** (abbreviated **IdP** or **IDP**) is a system entity that creates, maintains, and manages identity information for [principals](https://en.wikipedia.org/wiki/Security_principal) and also provides authentication services to relying applications within a federation or distributed network  
c) Identity proofing

Identity proofing is the process of verifying a user's identity: confirming that they are who they say they are

**3) Give an example of the following with one sentence**

1. Key distribution: Transport Layer Security (TSL) holds public key distribution, which the browser relies on to verify certificate chains in PKI. In public key cryptography, the key distribution of public keys is done through public key servers. When a person creates a key-pair, they keep one key private and the other, known as the public-key, is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message…

For example, Diffie-Hellman key distribution where each party has a key pair: private keys and public keys, where public keys are distributed by public key distributer like transport layer security, while the private key is used to verify the integrity of the sent data

1. Input sanitization:

Input sanitization is a cybersecurity measure of checking, cleaning, and filtering data inputs from users, APIs, and web services of any unwanted characters and strings to prevent the injection of harmful codes into the system.

This can be done in three ways:

Whitelist sanitizing allows only valid characters and code strings.

Blacklist sanitizing cleans the input by removing unwelcomed characters such as line breaks, extra white spaces, tabs, &, and tags.

Escape sanitizing rejects invalid data requests and strips inputs in order not to be seen as codes.

1. Non-repudiation:

In digital security, non-repudiation means:

A service that provides proof of the integrity and origin of data.

An authentication that can be said to be genuine with high confidence.

Non-repudiation refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract.[1] The term is often seen in a legal setting when the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated".[citation needed]

For example, Mallory buys a cell phone for $100 and writes a paper cheque as payment, and signs the cheque with a pen. Later, she finds that she can't afford it, and claims that the cheque is a forgery. The signature guarantees that only Mallory could have signed the cheque, and so Mallory's bank must pay the cheque. This is non-repudiation; Mallory cannot repudiate the cheque.

**4) Give example in computer software or operating system in one sentence**

1. No write up policy
2. Data sanitization during downgrading
3. Stateful security policy: Stateful applications and processes, however, are those that can be returned to again and again, like online banking or email. They’re performed with the context of previous transactions and the current transaction may be affected by what happened during previous transactions. For these reasons, stateful apps use the same servers each time they process a request from a user.

**5) Give an example of each of the following concepts:**

1. trusted path
2. low water mark policy
3. separation of duty
4. covert channel
5. parameterized role
6. principle of least privilege: **an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions**

**6) Give example for non military info system**

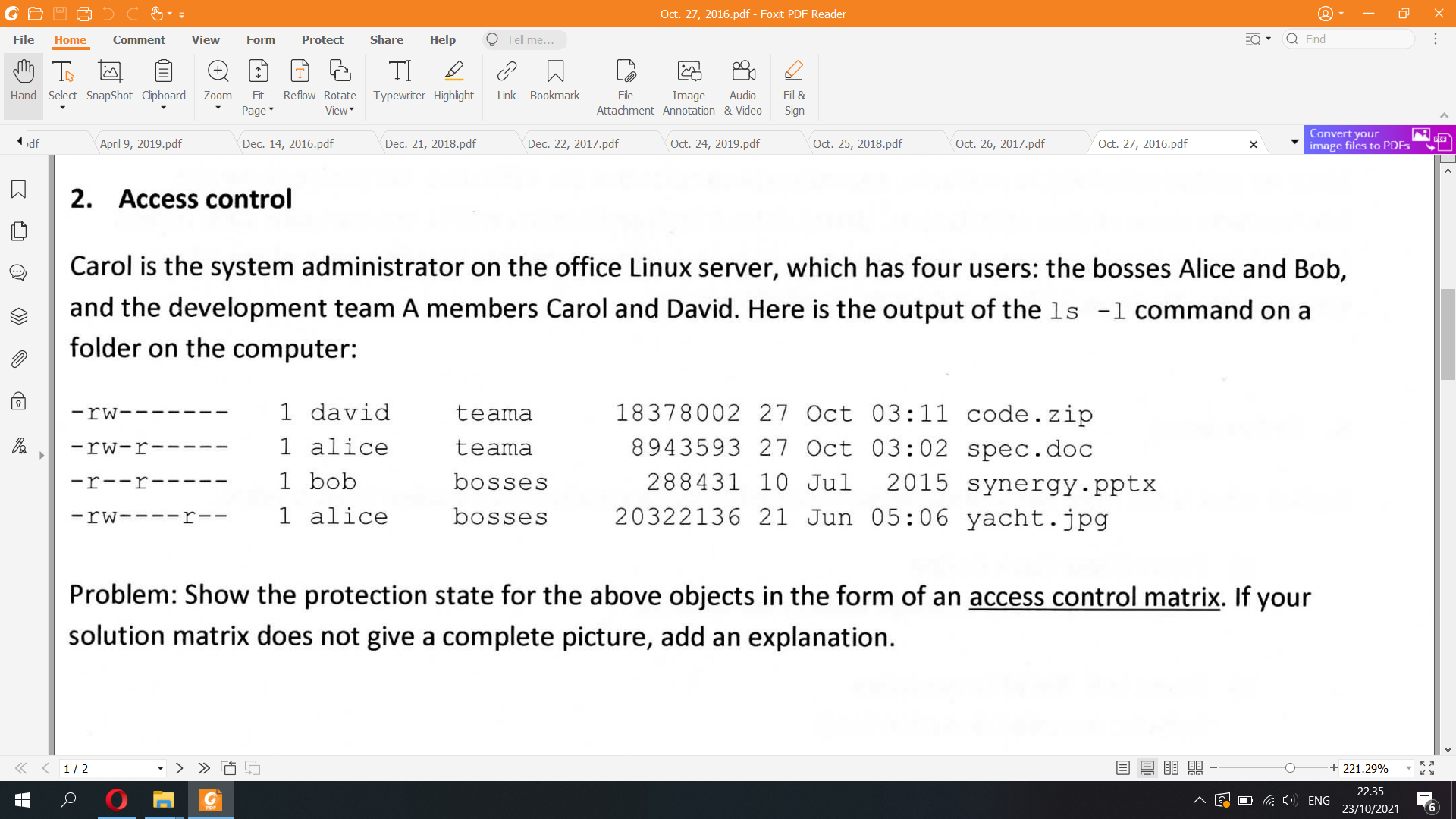
1. Principle of minimum privilege
2. covert channel
3. role inheritance

**7) The answer should be an example; no points will be given for a definition.**

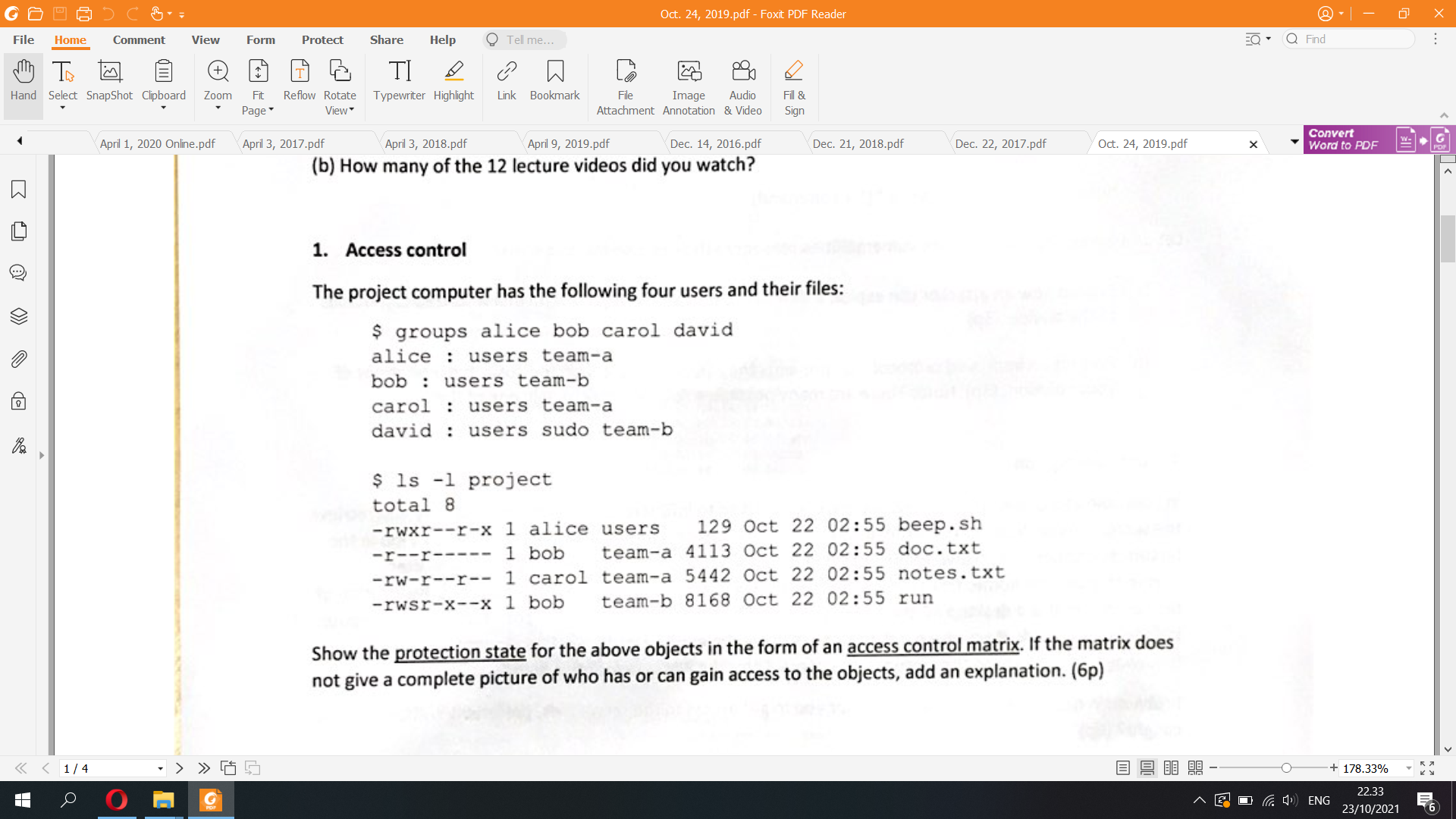
1. no-write-up policy

2. de-anonymization

3. risk-based authentication



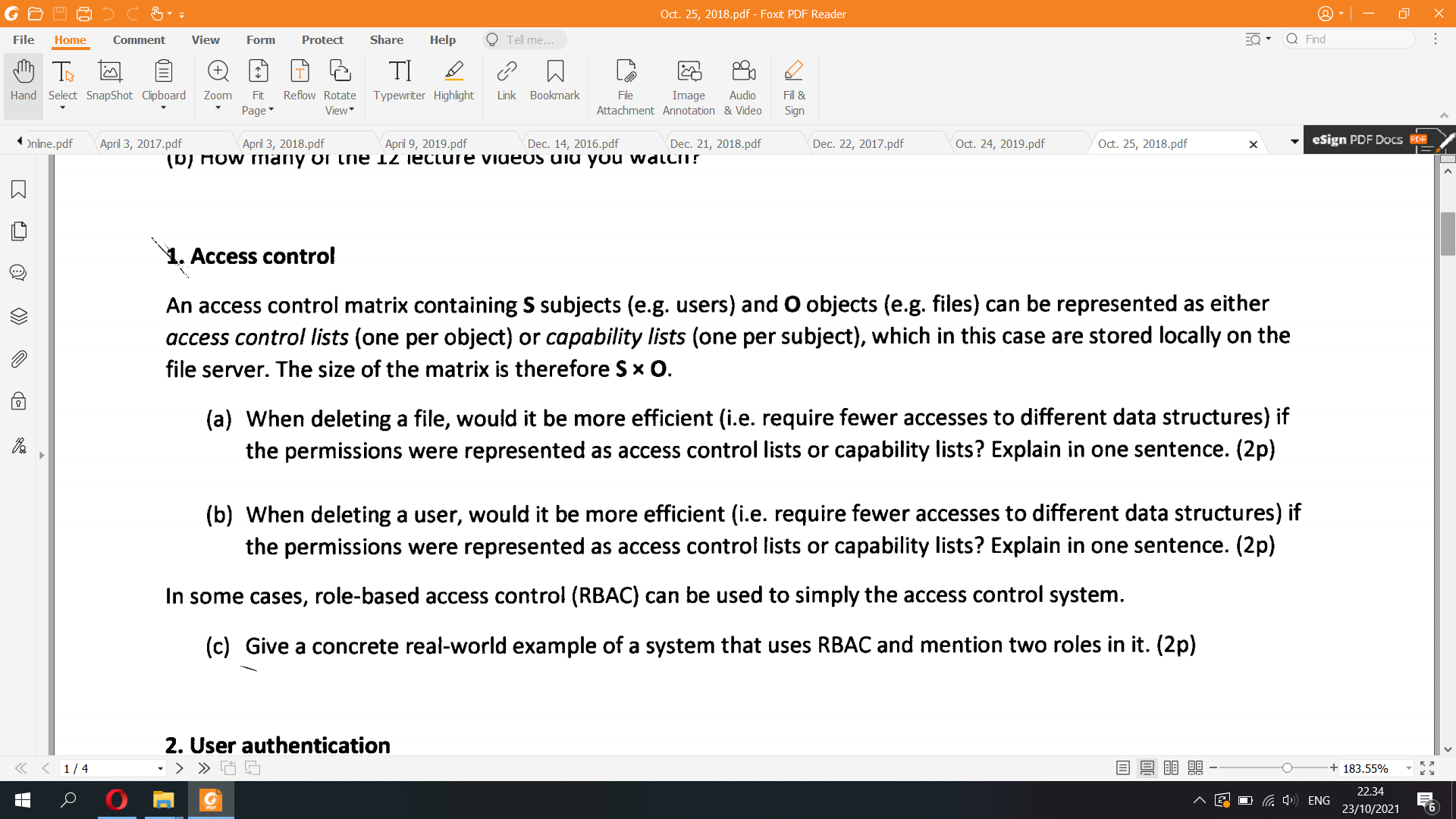
|  | alice | bob | david | teama | bosses | others |
| --- | --- | --- | --- | --- | --- | --- |
| code.zip |  |  |  |  |  | xxx |
| spec.doc |  |  |  |  |  | xxx |
| synergy.pptx |  |  |  |  |  | xxx |
| yacht.jpg |  |  |  |  |  | xxx |



Alice belongs to both groups users and team-a  
David belongs to 3 groups: users, sudo, team-b

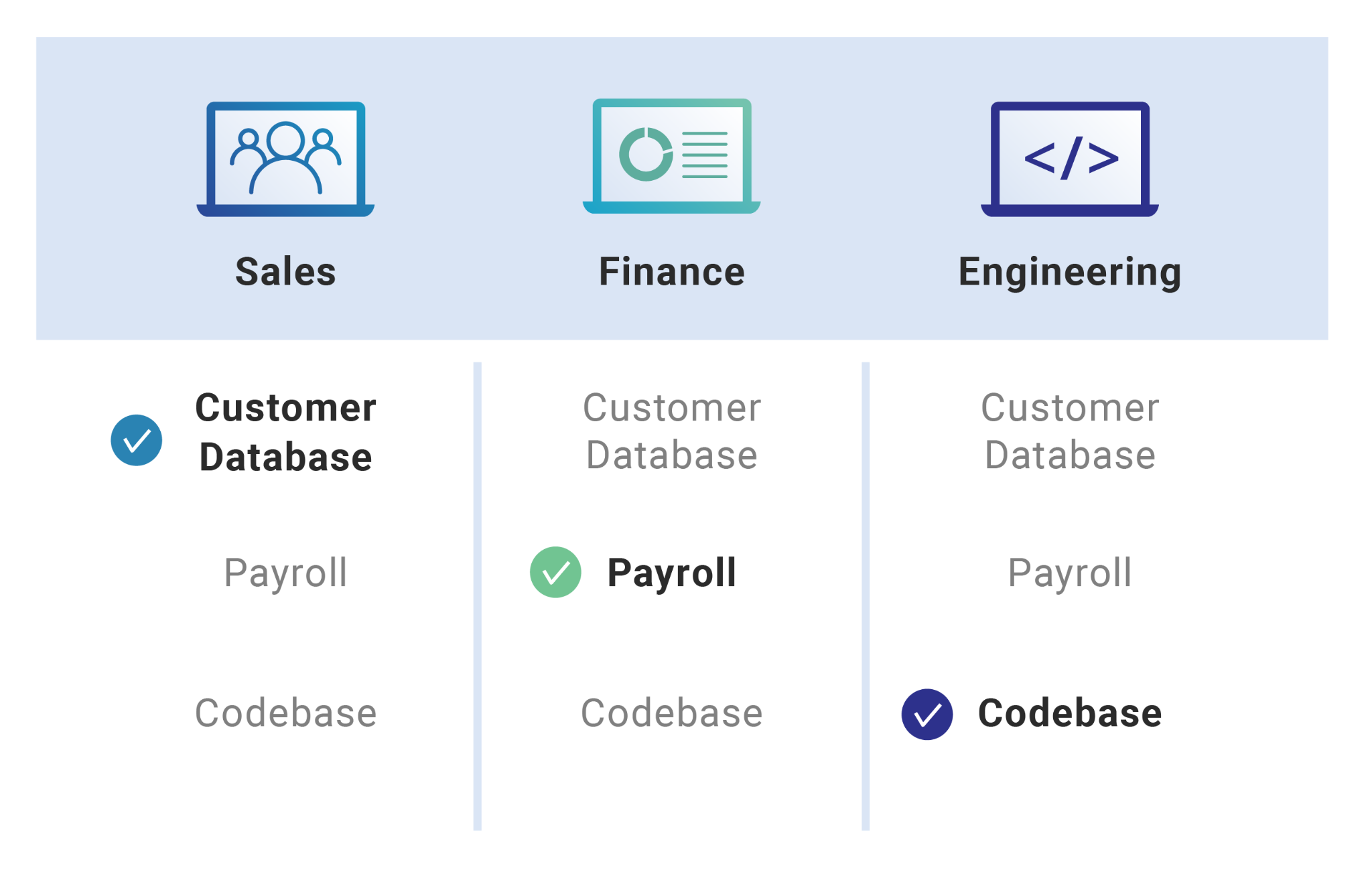
rws, s means the setguid bit is set, so te executed object will run with the effective rights of the group owner (instead of that of the user who executed it)

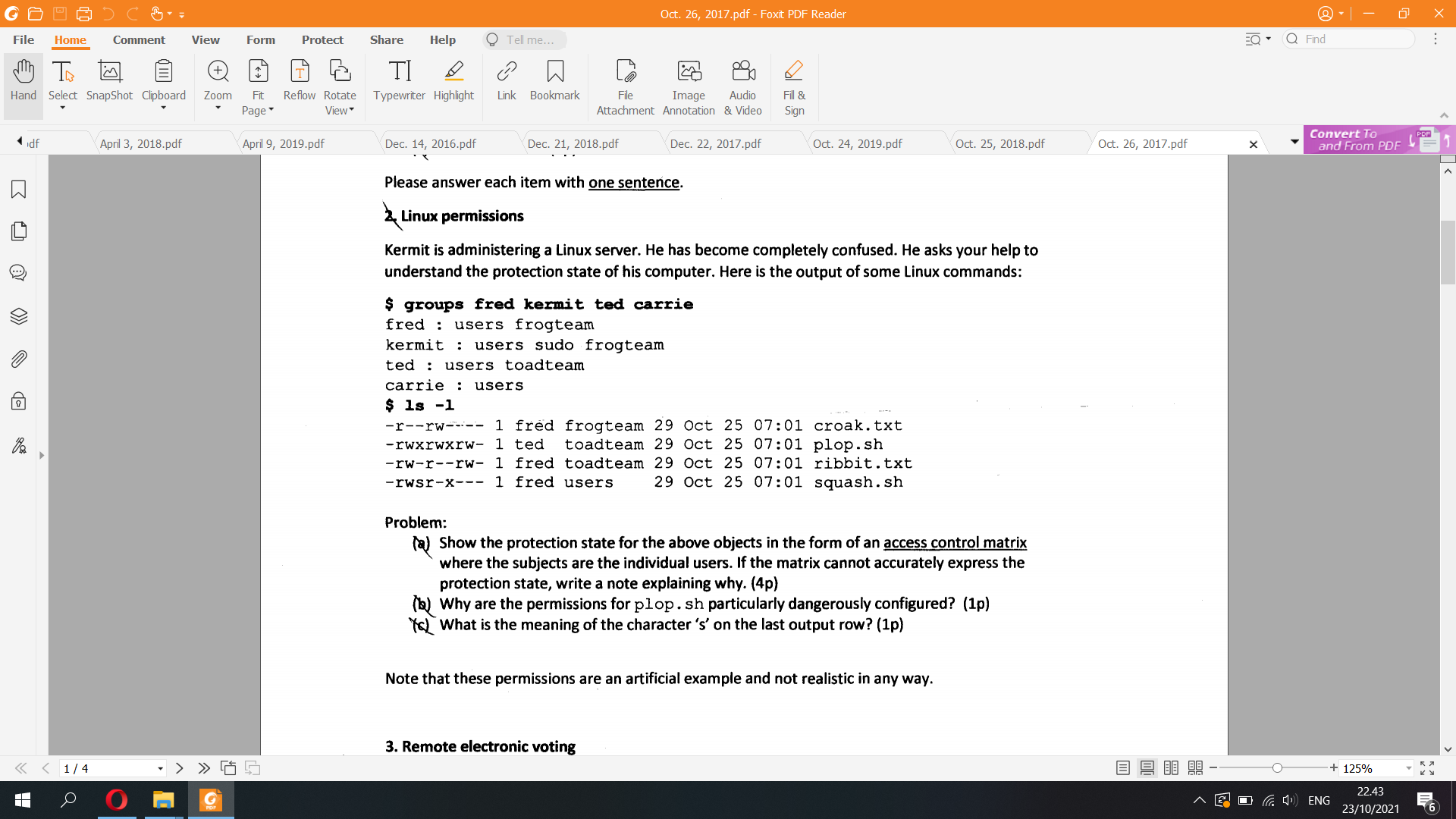
|  | alice | bob | carol | david | users | team-a | team-b | others |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| beep.sh | rwx | r-- | r-- | r-- | r-- | r-x | r-x | r-x |
| doc.txt | r-- | r-- | r-- | --- | --- | r-- | --- | --- |
| notes.txt | r-- | r-- | rw- | r-- | r-- | r-- | r-- | r-- |
| run | --x | rws | --x | r-x | --x | --x | r-x | --x |



a) ACL is better since we need to find only the row of that file and see who can delete that file or can update permissions on that file

b) Capability lists is better since we need to find only the row of that user and see who can delete that user  
c) For example, in social platform companies such as Facebook and Twitter, RBAC

* **Software engineering role:** Has access to GCP, AWS, and GitHub
* **Marketing role:** Has access to HubSpot, Google Analytics, [Facebook Ads](https://visme.co/blog/email-images/), and Google Ads
* **Finance role:** Has access to Xero and ADP
* **Human resources role:** Has access to Lever and BambooHR   
  



a) Like above

b) A file with . sh extension is a scripting language commands file that contains computer program to be run by Unix shell. It can contain a series of commands that run sequentially to carry out operations such as files processing, execution of programs and other such tasks. In plop.sh, the permission of others is set as rw-, which means they can read and write commands into the shell to change AC configurations of owner and group, which is inherently dangerous.

c) What is RWS permission Unix?

The s in rws stands for setuid meaning set user ID. This is a special permission bit that allows the program, when run by any user, to be run with the effective UID of the owner, in this case, root. So when you as a normal user run the sudo executable, you effectively do so as root.