User Study B - Key

Part I. Build the threat model of the above system using framework B. Fill in the result of applying each step of framework B in the appropriate spaces below.

Step 1: **Start time:** **Finish time:**

List the activities in the system:

- Store a file.
- Pay servers for storage periodically.
- Retrieve a file and pay for the service.

List participants:

- Clients.
- Servers.
- external.

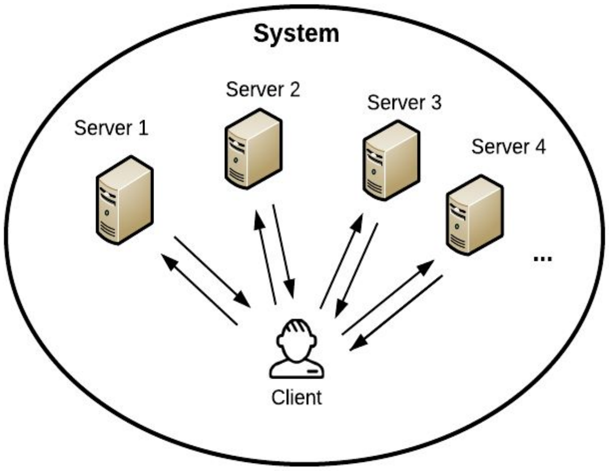
List assets of value:

- *Service (both file storage and retrieval).*
- *Payments or currency.*

Assumptions and external dependencies:

(no need to rewrite them, just read them again)

Network model of the system:



The three activities in the system have the same network model, the difference is in the eschanged messages as follows:
- **Store a file:** client and servers exchange file storage requests and file fragments.
- **Rewarding storage:** client and servers exchange proofs of storage and payments periodically.
- **File retrieval:** client sends a retrieval rqeuests, receive file fragments from servers and then sends them payments.

Step 2: **Start time:** **Finish time:**

Possible threats:

- Service corruption: invalid files are stored at the server, or server discards clients files, receive corrupted files.
- Denial of service.
- Information disclosure: someone track the requests issued by a client and read the content of its files, etc.
- Service slacking/File storage and file retrieval.
- Service theft/File storage and retrieval.

Step 3: **Start time:** **Finish time:**

Fill the following collusion matrix:

Threat: ***service theft / file retrieval (client retrieves file without paying)***

Target → Attacker ↡	Client	Server	Client and Server
Client	**X1**	(1)	**M1**
Server		**X2**	
Client and Server		(2)	
External		**X3**	
Client and External		**M2**	
Server and External		**X4**	
Client, Server, and External		**M3**	

Rationale behind threat omission/merging:

X1: client cannot be a target, it does not provide a service.

X2/3/4: cannot be attacker, they do not pay for the service. (splitted just to make grading easier)

M1: client cannot be a target, this reduces to the case of attacking a server only.

M2: a client colluding with an external will not become stronger, it is just like a client is attacking on its own, merge with (1)

M3: a client/server colluding with an external will not become stronger, it is just like a client/server are attacking on their own, merge with (2)

Distilled Threats Description:

(1) A client receives correct file fragments but does not pay or send invalid payments.

(2) A client colludes with a server to send a corrupted fragment to avoid paying the servers (or even set his own server and store a corrupted file fragment there).