User Study A - Threat Modeling

DIRECTIONS:
Thank you for agreeing to participate in this study. Please read these instructions carefully.

- The goal of this study is to evaluate the effectiveness of two threat modeling frameworks in building threat models for resource-backed cryptocurrency systems. We refer to them as framework A and framework B.
- You will be given the steps of framework A as a separate document to apply it to a simple resource-backed cryptocurrency.
- Lastly, you will fill out a short questionnaire about applying framework A to the system in question.

Please do not discuss the study with other participants until the whole study is over.

If you need a break during the study for any reason please let the monitor know.

Please fill in the start and finish time of each step of the study.

When you stop at step 2 the monitor will take page 5 and hand you the rest of the study that determines which threat you will work on.

ArchiveCoin description:

ArchiveCoin is a monetary-incentivized distributed file storage network. Any party may join the system as a server or as a client. ArchiveCoin provides a paid file storage and retrieval services.

File storage service:

- Clients divide their files into fragments, then they store these fragments at various servers.
- Each server periodically sends the client a proof that certain file fragment is still stored. The client pays the server for the storage service every time a correct proof is received.

File retrieval service:

- A client retrieves a file (it owns) stored in the network by asking the servers to send the fragments they hold.
- The client pays for the retrieval only when it receives correct fragments from all servers.
- Once a file is retrieved it is removed from storage at servers.

Assumptions:

- The machines used by all parties are secure,
- The payments are made using a secure cryptocurrency system (that is once a client issues a payment that reaches this system, it is recorded and credited to the server's account).
- The attackers are malicious (i.e. may perform any attack for the sake of harming the system or the honest parties).
- All messages exchanged are signed but not encrypted, i.e. everyone can read the content of a message but cannot tamper with it.

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

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

List the components in the system:

List participants:

List assets of value:

Assumptions and external dependencies:

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

Draw the DFD (data flow diagram) of the system's components.

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

Possible threats:

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

(The participant is not provided this sheet until later and is asked not to edit earlier pages)

Description of threat scenarios for:

Service theft / file retrieval (client retrieves file without paying)

Part II. Please fill out the following questionnaire:

a. Threat modeling framework A was easy to apply. Please elaborate on your answer below as well as any comments you have about applying framework A to systems similar to ArchiveCoin.	▢ Strongly agree ▢ Agree ▢ Neither agree or disagree ▢ Disagree ▢ Strongly disagree
b. You are confident that the list of threat scenarios you obtained by applying framework A is correct and not missing any threat scenario.	▢ Strongly agree ▢ Agree ▢ Neither agree or disagree ▢ Disagree ▢ Strongly disagree