User Study Overview

ABC Material
G. Almashaqbeh et al. 2019

Outline

- User study guidelines.
- ArchiveCoin description (the system used in the study).

Guidelines I

- 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/B as a separate document to apply it to a simple resource-backed cryptocurrency (described next).

- Lastly, you will fill out a short questionnaire about applying framework A/B to the system in question.

Guidelines II

- Please do not discuss the study with other participants until the whole study is over.
- 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 give you the rest of the study that determines the threat you will work on.
- If you need a break during the study for any reason please let the monitor know.

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.

ArchiveCoin Description

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.

ArchiveCoin Description

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.