TMoC : Threat Modeling on Chain

ICSP(Institute of Cyber Security & Privacy)
School of Cybersecuruty, Korea University

Yejun Kim (v3locy@korea.ac.kr)
Kwangsoo Cho (cks4386@korea.ac.kr)
Paul Hong (visitator00@korea.ac.kr)
Seungjoo Kim (skim71@korea.ac.kr)

AGENDA

0x01 Introduction

0x02 Threat Modeling on Chain

0x01

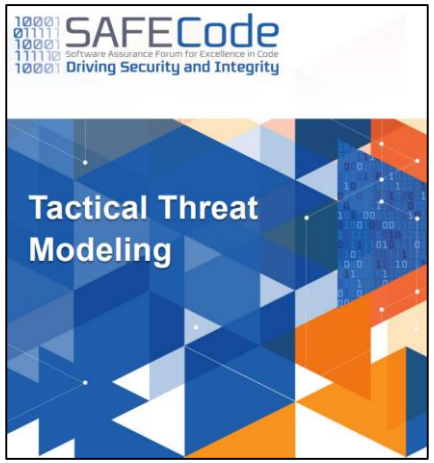
Introduction

0x01 Introduction

- Threat Modeling is a Team Sport Method

[Adam Shostack, Threat Modeling (Elevation of Privilege: the Threat Modeling Game)]

- **To motivate "The Crowd" to participate in Threat Modeling, collective intelligence is required, we propose threat modeling in the form of a game**



[SAFECode, Tactical Threat Modeling]

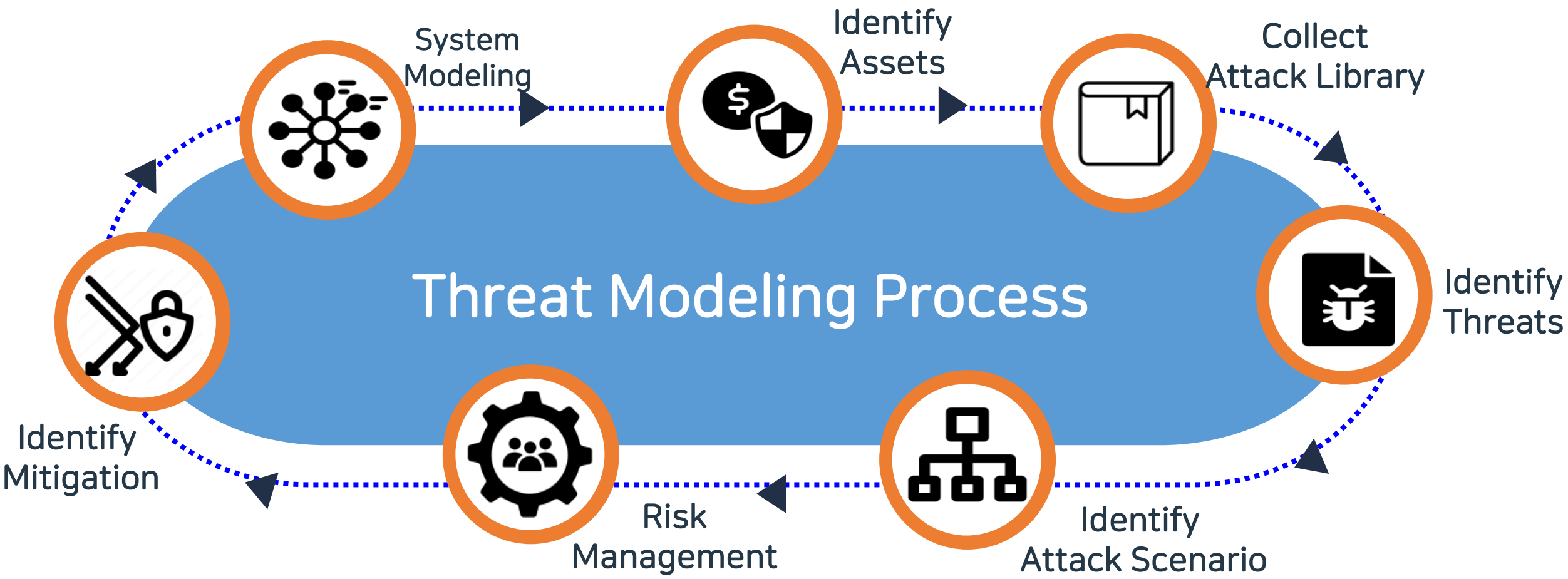
- **Threat modeling is like a "team sport" where that helps different participants to derive threats from analysis target**

[Amazon AWS(Darran Boyd), How to approach threat modeling]

- **Threat modeling is a "team sport" that requires the knowledge and skills of various teams.**
- **All inputs have equal value**

0x01 Introduction

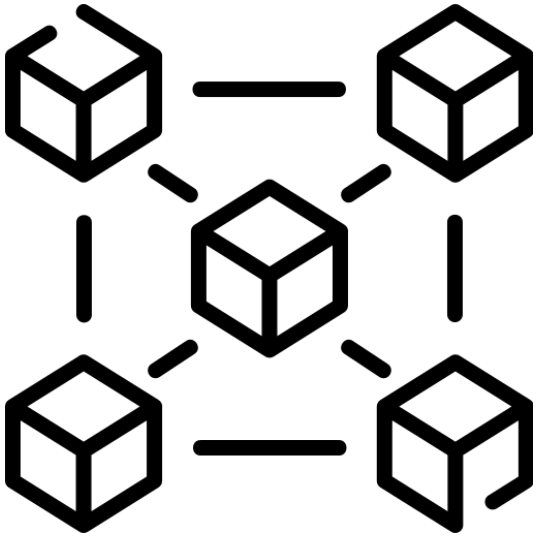
- Threat Modeling Process



0x01 Introduction

- TMoC(Threat Modelers on Chain) is a first block-chain based collective intelligence threat modeling tool
  - TMoC is a follow-up study on “Blockchain as a Threat Modeling Thinking Tools” at DEFCON 29
  - We call this MMOTM(Massive Multiplayer Online Threat Modeling)

MMO



Block-chain

Threat Modeling

0x01 Introduction

- TMoC Basic Process
  - The operation sequence of TMoC proceeds as follows

01	# 02	03	# 04	05	# 06	07
Request of Threat Modeling	Perform task	Submit task	Program update	Evaluation	Arbitration	Provide Reward
A customer requests threat modeling from TMoC system	Performers carry out threat modeling task	Tasks are submitted by the performers who has completed threat modeling	Blockchain is updated	Evaluates the threat modeling results	If there is a problem of the evaluation, the Arbiter will verify the evaluation	TMoC participants will receive rewards

0x02

Threat Modeling on Chain

0x02 Threat Modeling on Chain

- TMoC Source Code
  - TMoC uploaded in our Github repo(open source license)

HackProof Delete TMOC_old.png 8efa797 3 days ago 4 commits

web	Delete TMOC_old.png	3 days ago
README.md	First commit	3 days ago
TMOC_main.png	First commit	3 days ago

README.md

TMoC_Threat Modelers on Chain

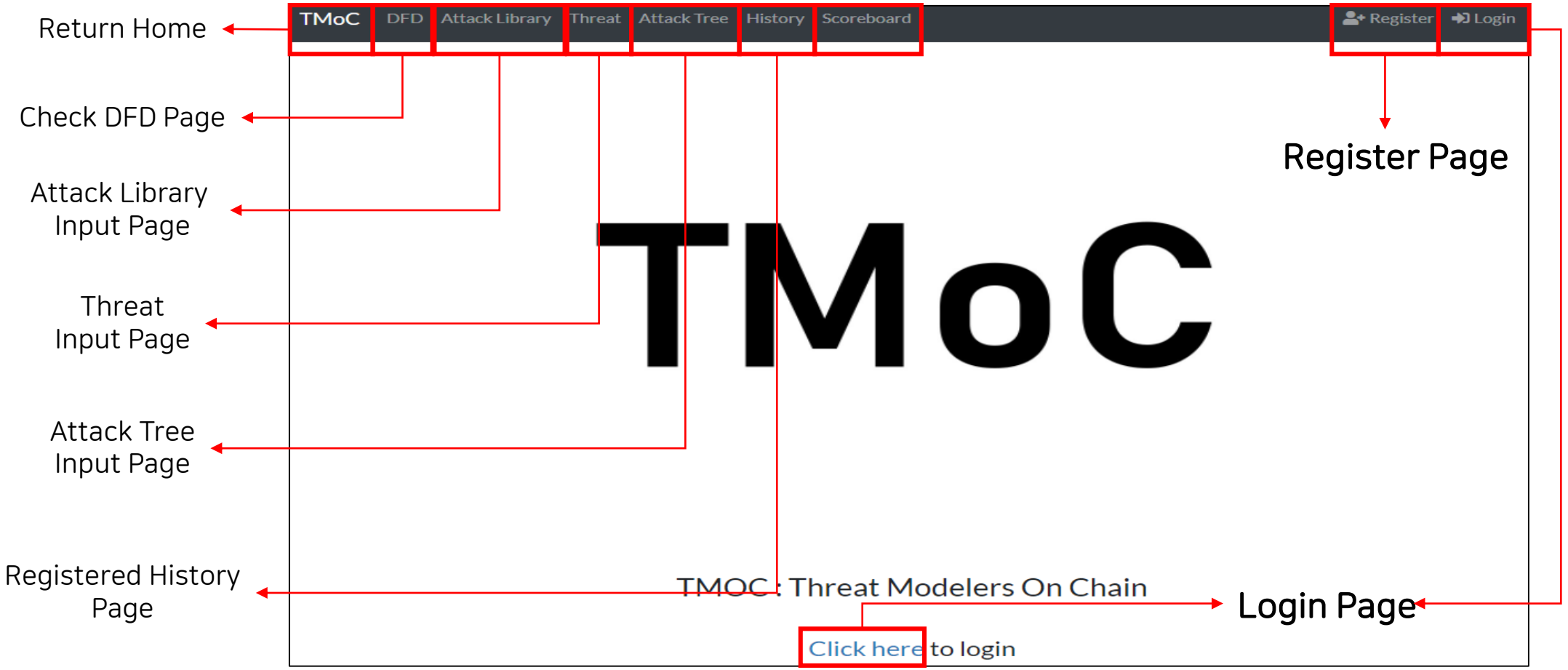
TMOC (*Threat Modelers on Chain*) is a tool that combines threat modeling with a blockchain-based collective intelligence system developed as a blockchain-based Web3 in the form of a decentralized web.

Threat modeling is a risk-based approach to designing security systems based on threat identification for threat mitigation. Threat modeling is a "*team sport*" because it requires the knowledge and skills of different teams, all inputs can be considered of equal value. It is a framework that integrates the threat modeling process on a larger scale through blockchains that enable large-scale collaboration.

Link : https://github.com/HackProof/TMoC

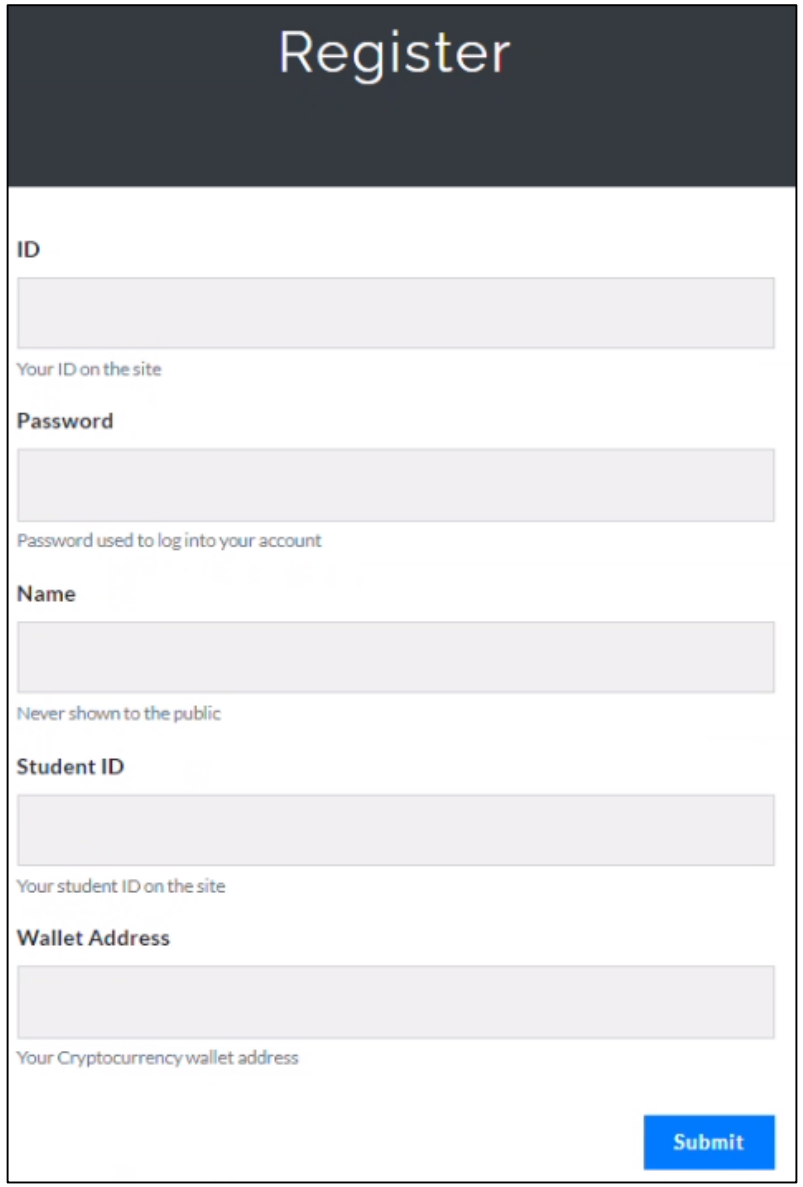
0x02 Threat Modeling on Chain

- Main Pages
  - It is the main page of TMoC, where you can register for membership, log in, and go to each function page



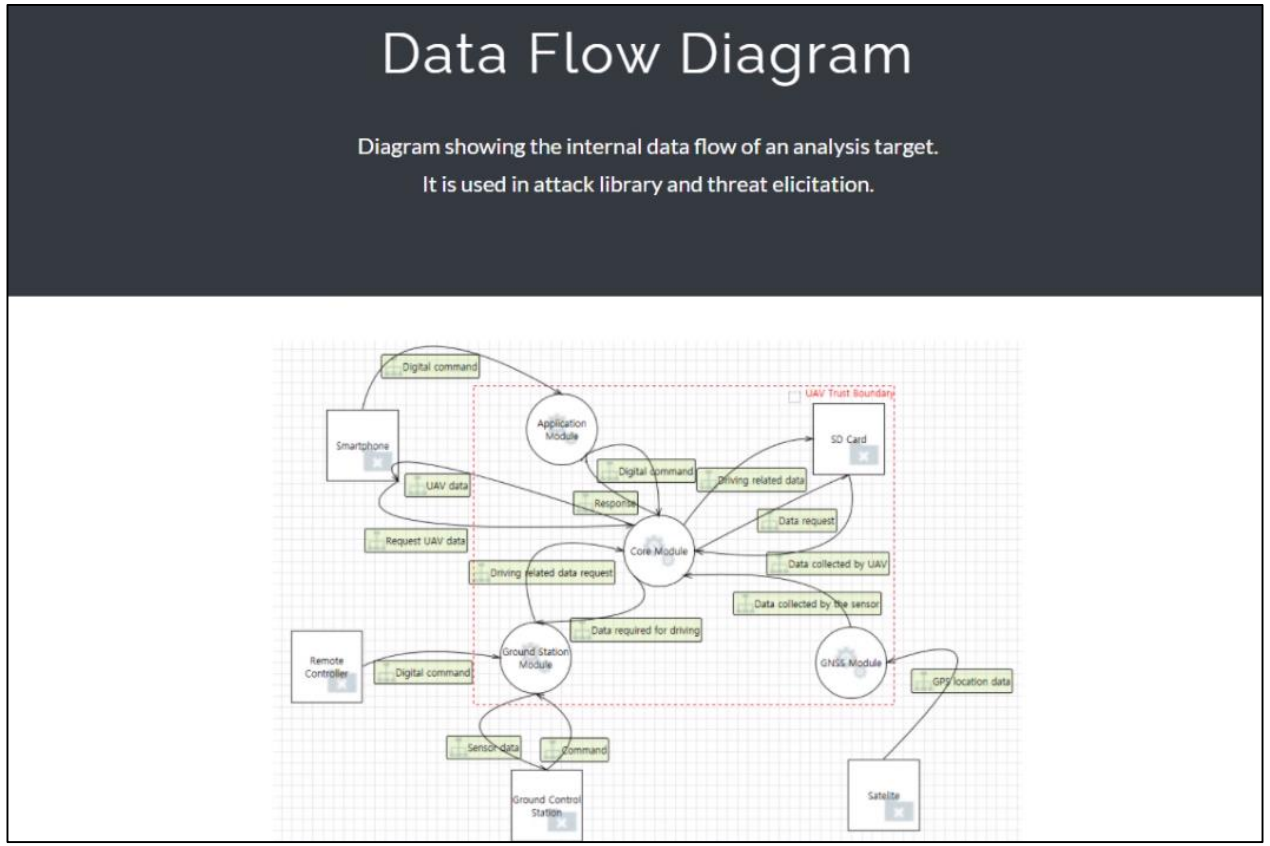
0x02 Threat Modeling on Chain

- Register
  - TMoC registration page, where you enter your ID, PW, Username, and Metamask Wallet Address
  - The information entered when registering as a member can be edited after logging in
  - Gas fee and threat modeling compensation generated during the threat modeling process are paid through the wallet address created when registering as a member



0x02 Threat Modeling on Chain

- DFD (Data Flow Diagram)
  - A diagram showing the internal data flow of an analysis target, which is utilized when deriving an attack library and threats
  - In the case of data flow diagrams, web sources can be transformed and applied to various targets



0x02 Threat Modeling on Chain

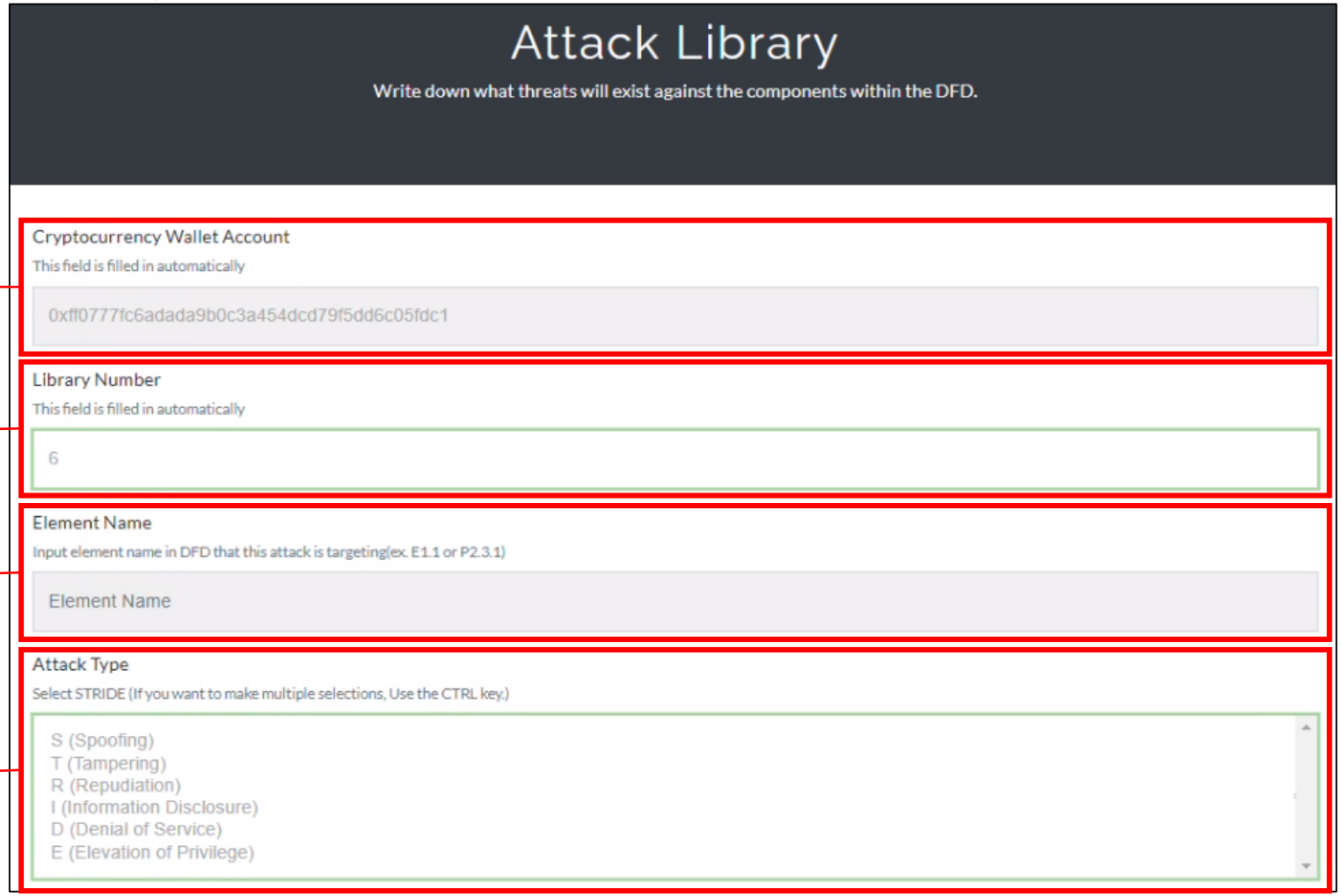
- Attack Library
  - Write down what threats will exist against the components within the DFD

Wallet address entered when registering as a member (auto)

Number in the Attack Library field (auto)

The number of the DFD element to which the attack library is mapped.

Input the attack type of the mapped attack library in the form of STRIDE



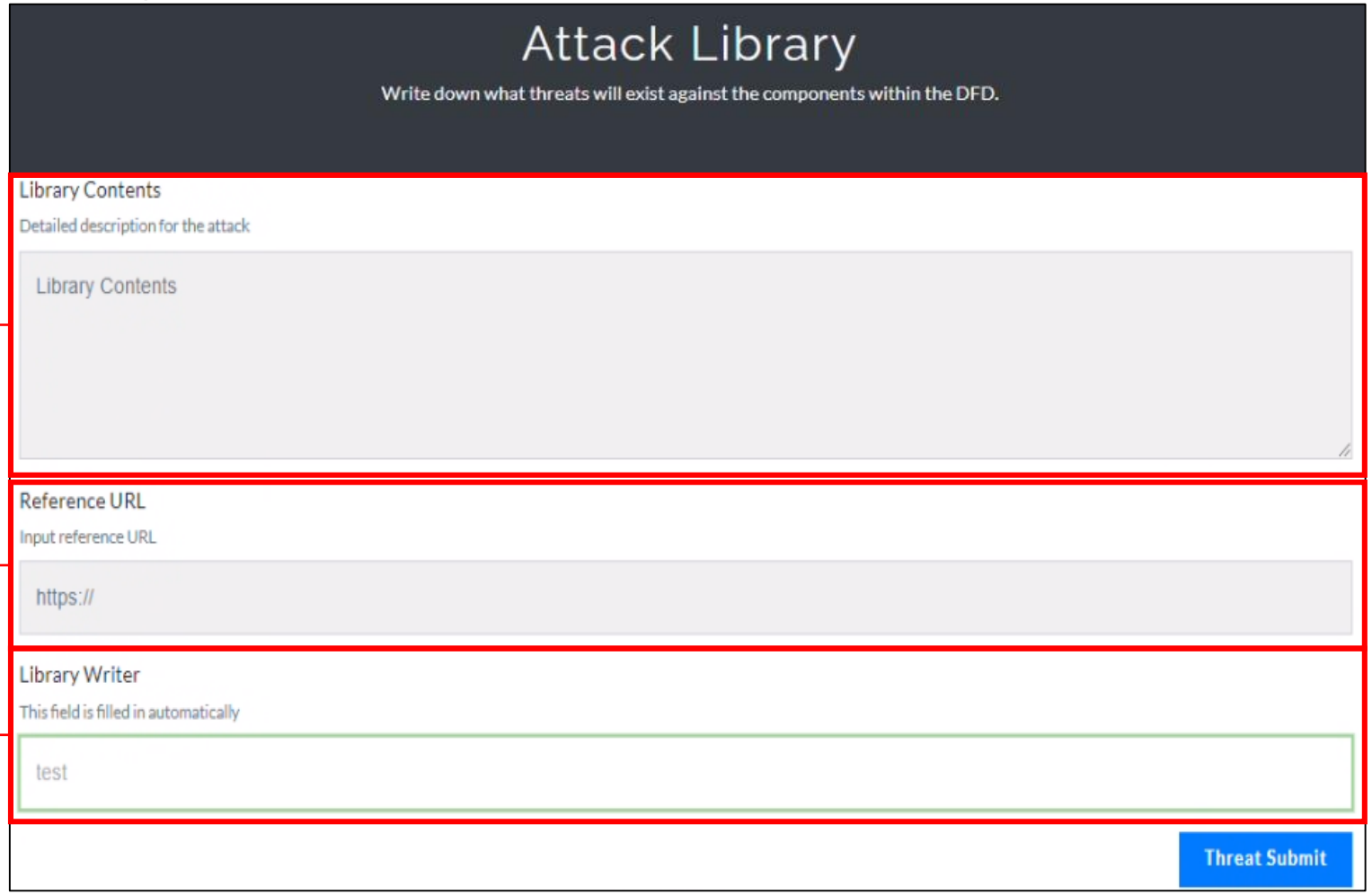
0x02 Threat Modeling on Chain

- Attack Library
  - Write down what threats will exist against the components within the DFD

Description of the attack library to be mapped and the reason for the mapping

Evidence link to the mapped attack library

Author's nickname (auto)



0x02 Threat Modeling on Chain

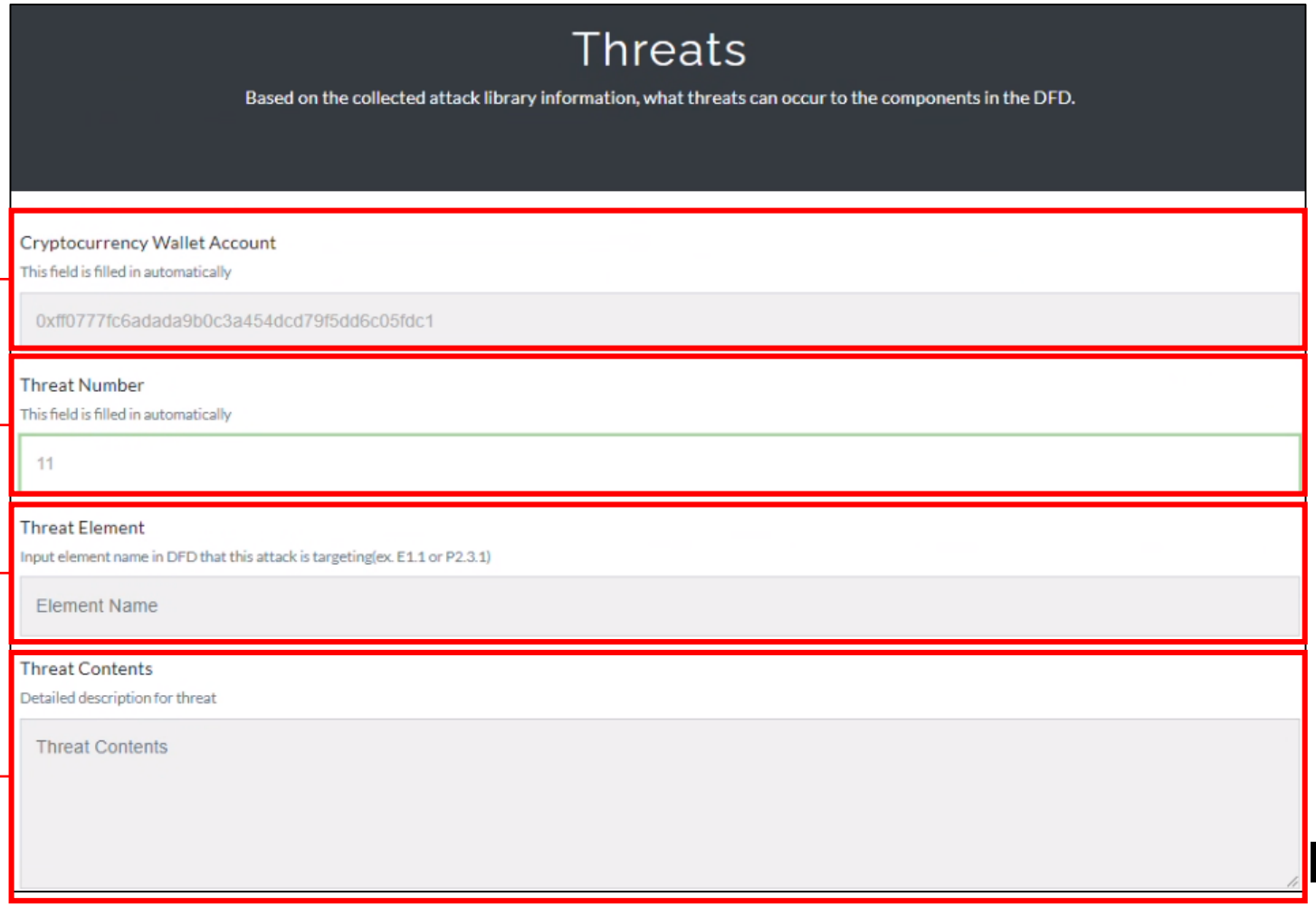
- Threats
  - Based on the collected attack library information, what threats can occur to the components in the DFD

Wallet address entered when registering as a member (auto)

Number in the Threat field (auto)

The number of the DFD element to which the Threat is mapped.

Description of the Threat to be mapped



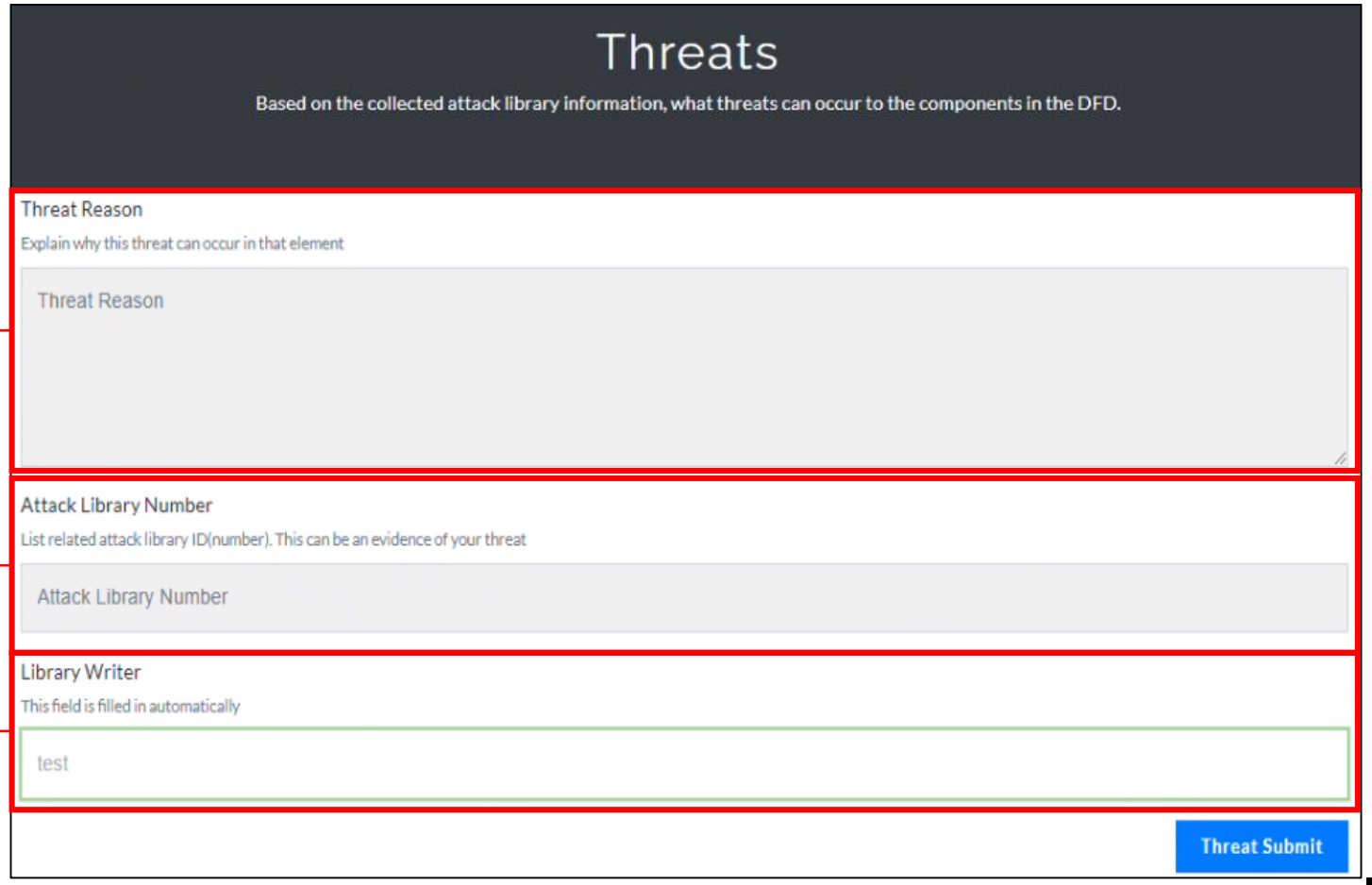
0x02 Threat Modeling on Chain

- Threats
  - Based on the collected attack library information, what threats can occur to the components in the DFD

Description of the Threat to be reason for the mapping

The number of the attack library mapped to the threat

Author's nickname (auto)



0x02 Threat Modeling on Chain

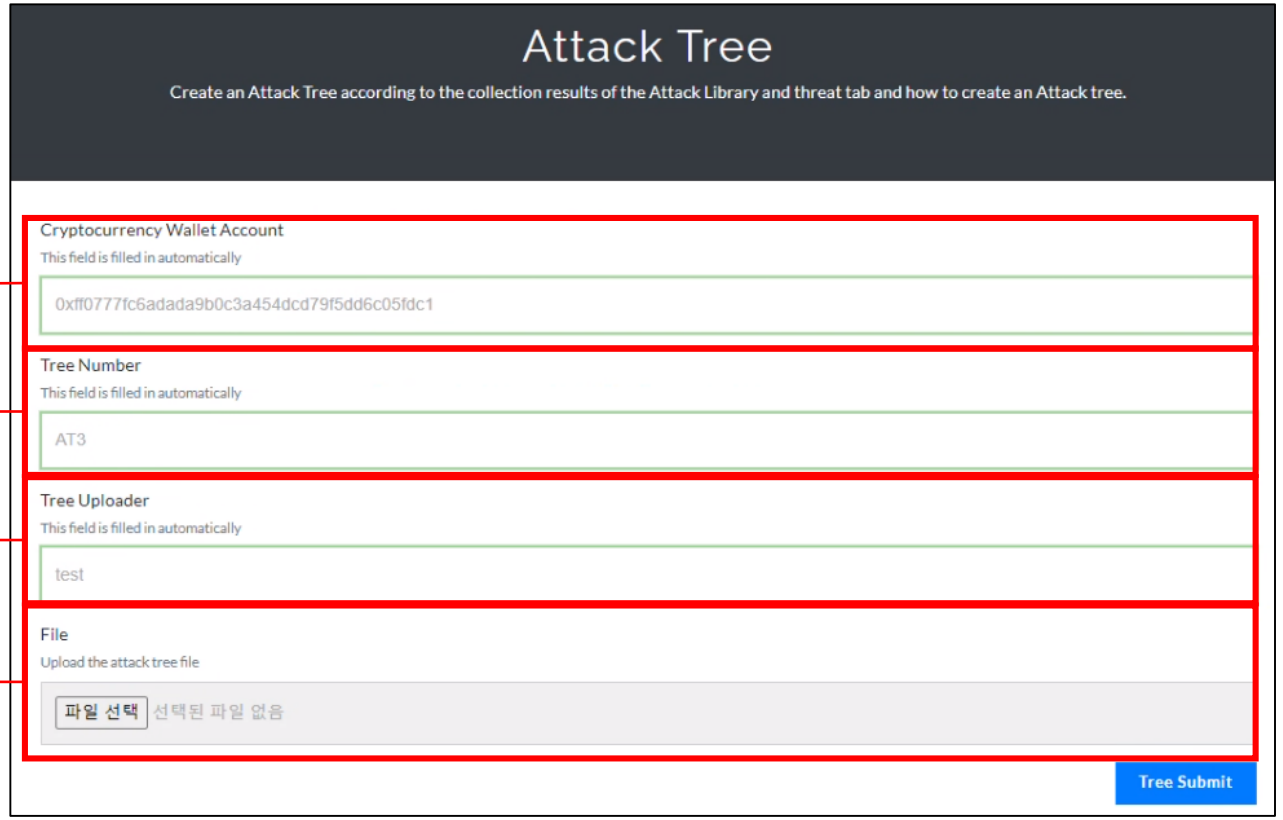
- Attack Tree
  - Create an attack tree according to the collection results of the attack library and threat tab and how to create an attack tree (Attack tree uploads files in image format)
  - Calculate the hash value (sha-256) of the uploaded file and send it as a block

Wallet address entered when registering as a member (auto)

Number in the Attack Tree field (auto)

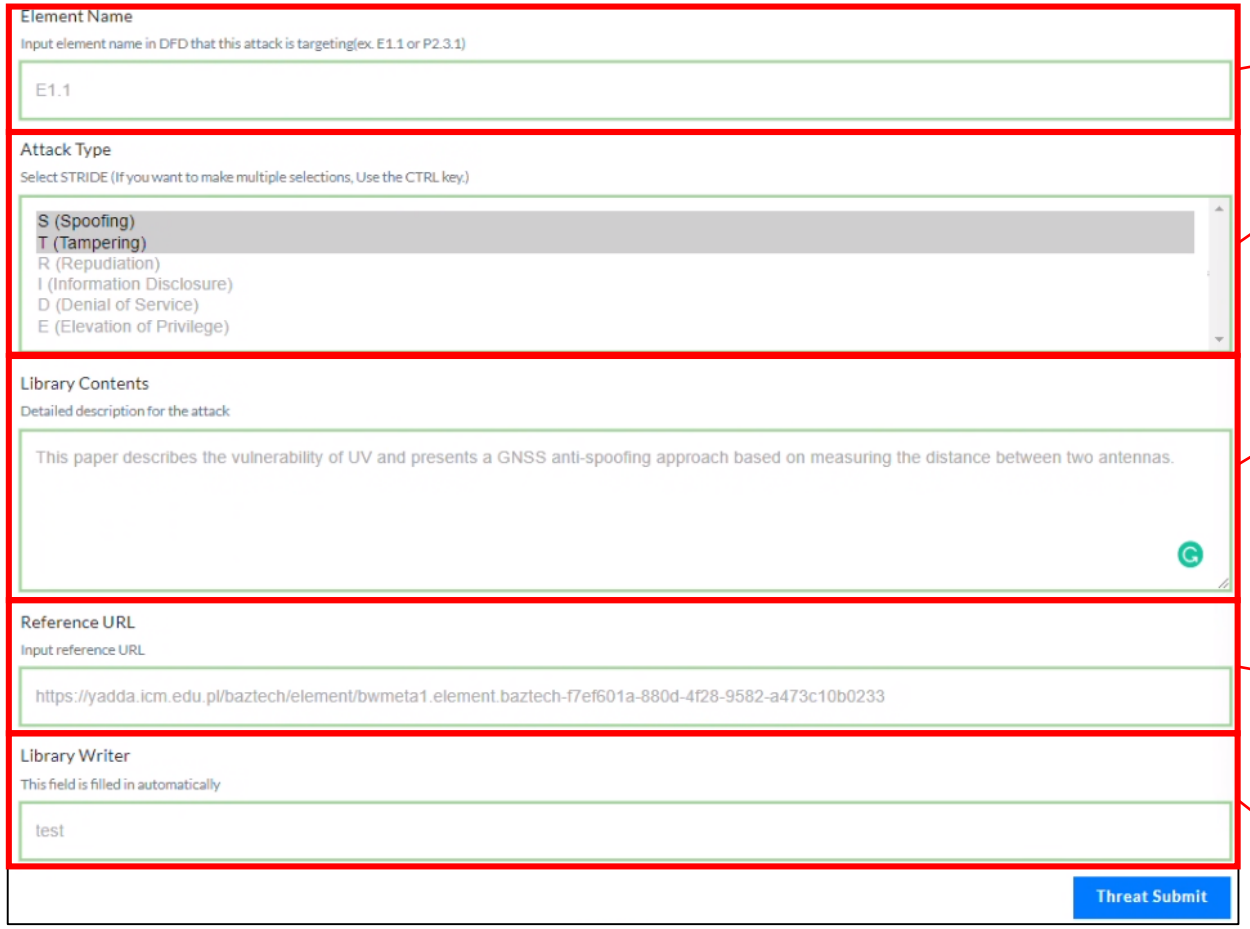
Author's nickname (auto)

Upload Attack Tree images



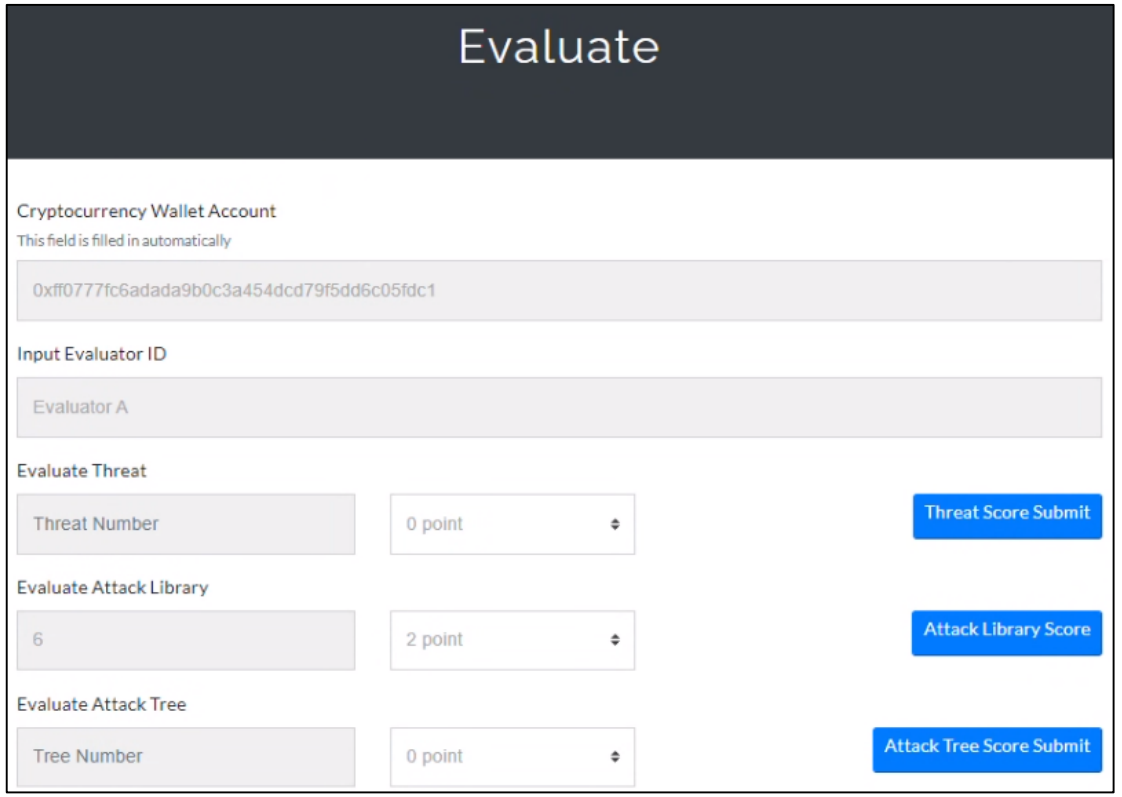
0x02 Threat Modeling on Chain

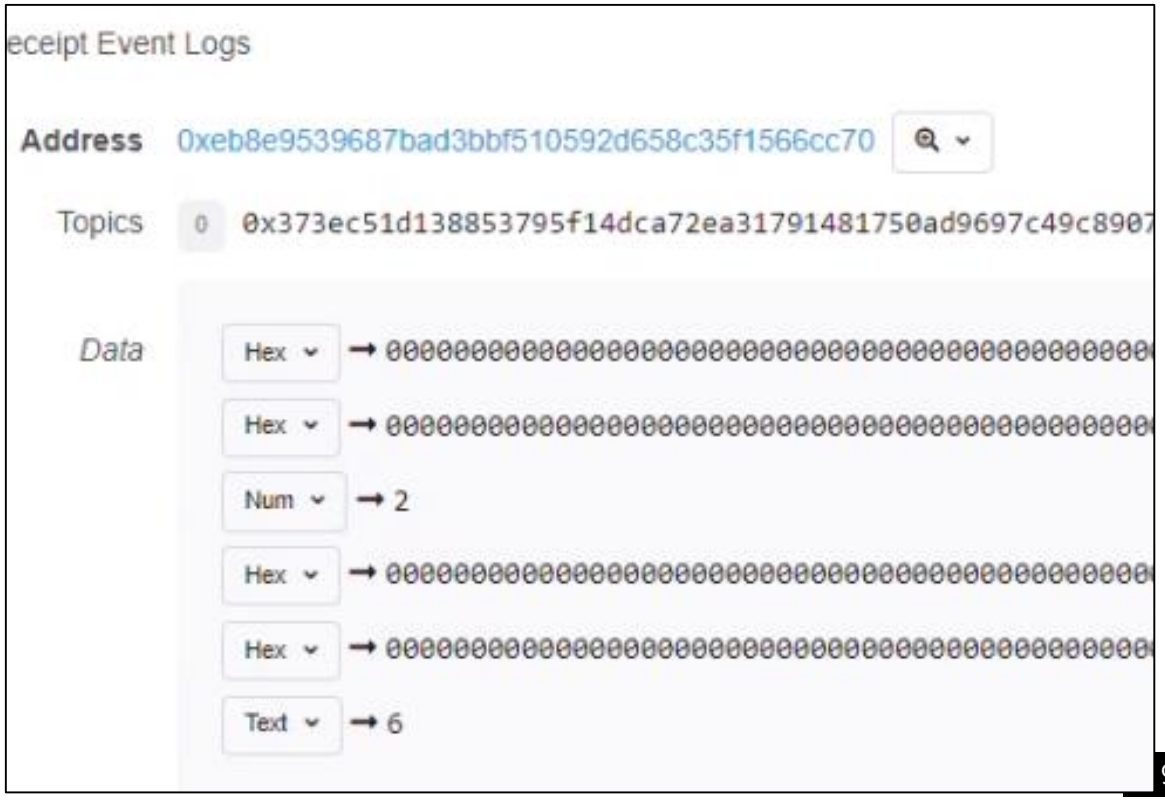
- Register on Ethereum block
  - When a user submits in each phase of TMoC, data can be registered in the block by paying gas fee in Metamask (Users can directly check the block log on the Etherscan Transaction Log)



0x02 Threat Modeling on Chain

- Evaluate
  - Evaluator can evaluate each stored threat, attack library and attack tree through the Evaluate page
  - In addition, the score registered by the Evaluator is also stored in the block so that the user can check it through Etherscan





Thank You

Yejun Kim (v3locy@korea.ac.kr)
Kwangsoo Cho (cks4386@korea.ac.kr)
Paul Hong (visitator00@korea.ac.kr)
Seungjoo Kim (skim71@korea.ac.kr)