TMoC : Threat Modeling on Chain

ICSP(Institute of Cyber Security & Privacy)
School of Cybersecurity, 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

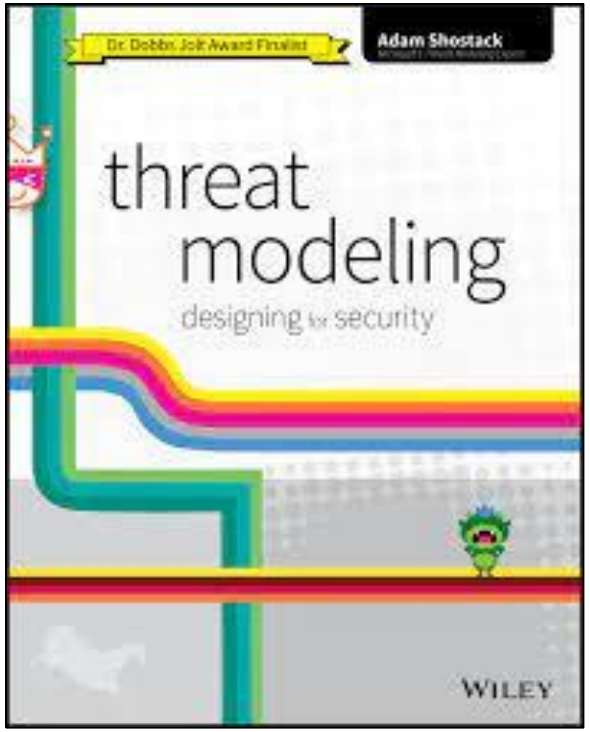
0x02 Threat Modeling on Chain

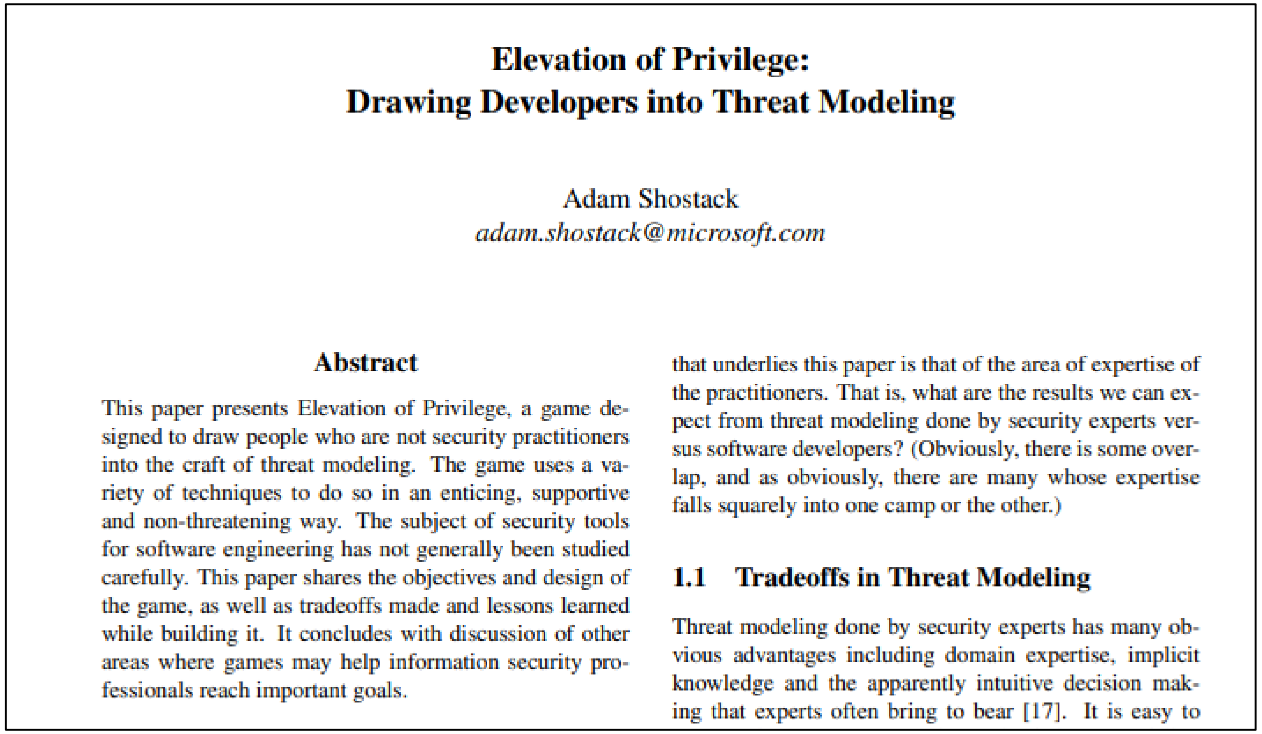
0x01

Introduction

0x01 Introduction

- Threat Modeling is a Team Sport Method
  - Threat modeling is a systematic way to identify threats that might compromise security which has been a well-accepted practice by the industry
  - Threat modeling helps various participants derive threats to the target of analysis, such as team sports





Elevation of Privilege: Drawing Developers into Threat Modeling

Adam Shostack
adam.shostack@microsoft.com

Abstract

This paper presents Elevation of Privilege, a game designed to draw people who are not security practitioners into the craft of threat modeling. The game uses a variety of techniques to do so in an enticing, supportive and non-threatening way. The subject of security tools for software engineering has not generally been studied carefully. This paper shares the objectives and design of the game, as well as tradeoffs made and lessons learned while building it. It concludes with discussion of other areas where games may help information security professionals reach important goals.

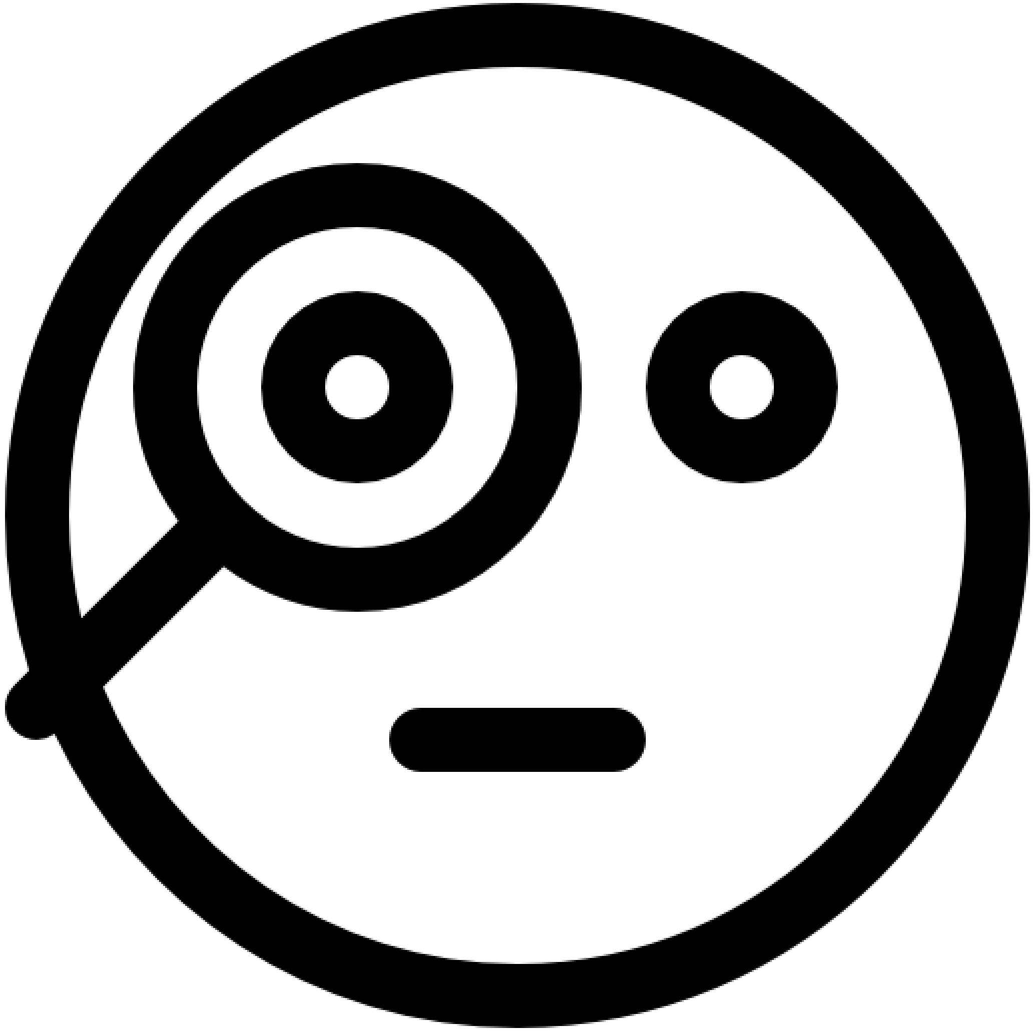
that underlies this paper is that of the area of expertise of the practitioners. That is, what are the results we can expect from threat modeling done by security experts versus software developers? (Obviously, there is some overlap, and as obviously, there are many whose expertise falls squarely into one camp or the other.)

1.1 Tradeoffs in Threat Modeling

Threat modeling done by security experts has many obvious advantages including domain expertise, implicit knowledge and the apparently intuitive decision making that experts often bring to bear [17]. It is easy to

0x01 Introduction

- What is TMoC?
  - TMoC is a blockchain-based threat modeling tool in the form of a decentralized web developed as an open source



0x01 Introduction

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

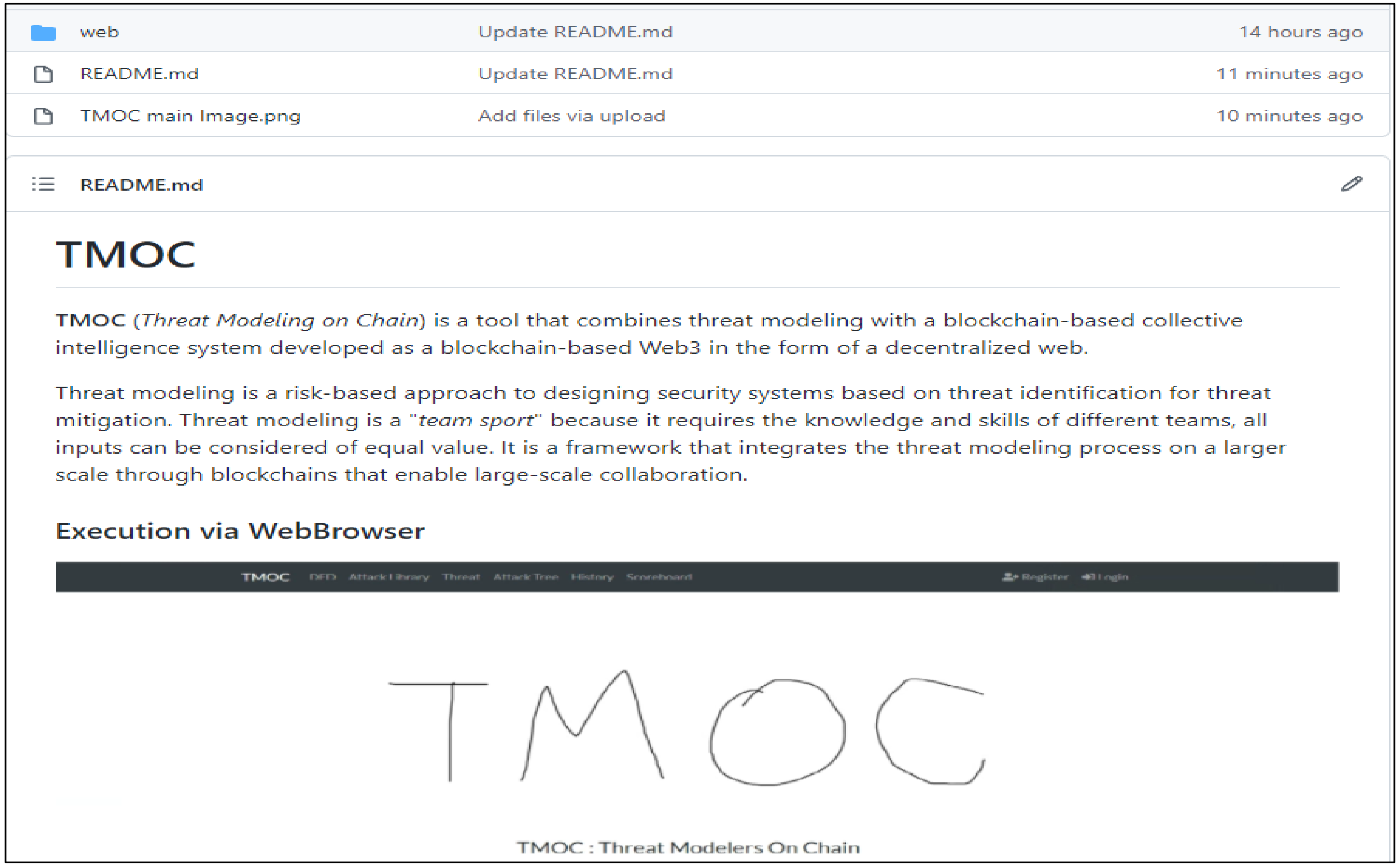
#01	#02	#03	#04	#05	#06	#07
Register user	Perform task	Submit task	Program update	Evaluate task	Arbitration	Receive reward
Users register themselves on the blockchain network	*Threat modeling performers* perform task	Submit the task completed by the *Threat modeling performer*	Blockchain Update	Evaluator performs an evaluation of the tasks performed	If there is a problem, the *Arbiter* arbitrates.	*Threat modeling performers* receive rewards

0x02

Threat Modeling on Chain

0x02 Threat Modeling on Chain

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



web	Update README.md	14 hours ago
README.md	Update README.md	11 minutes ago
TMOC main Image.png	Add files via upload	10 minutes ago

README.md

TMOC

TMOC (*Threat Modeling 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.

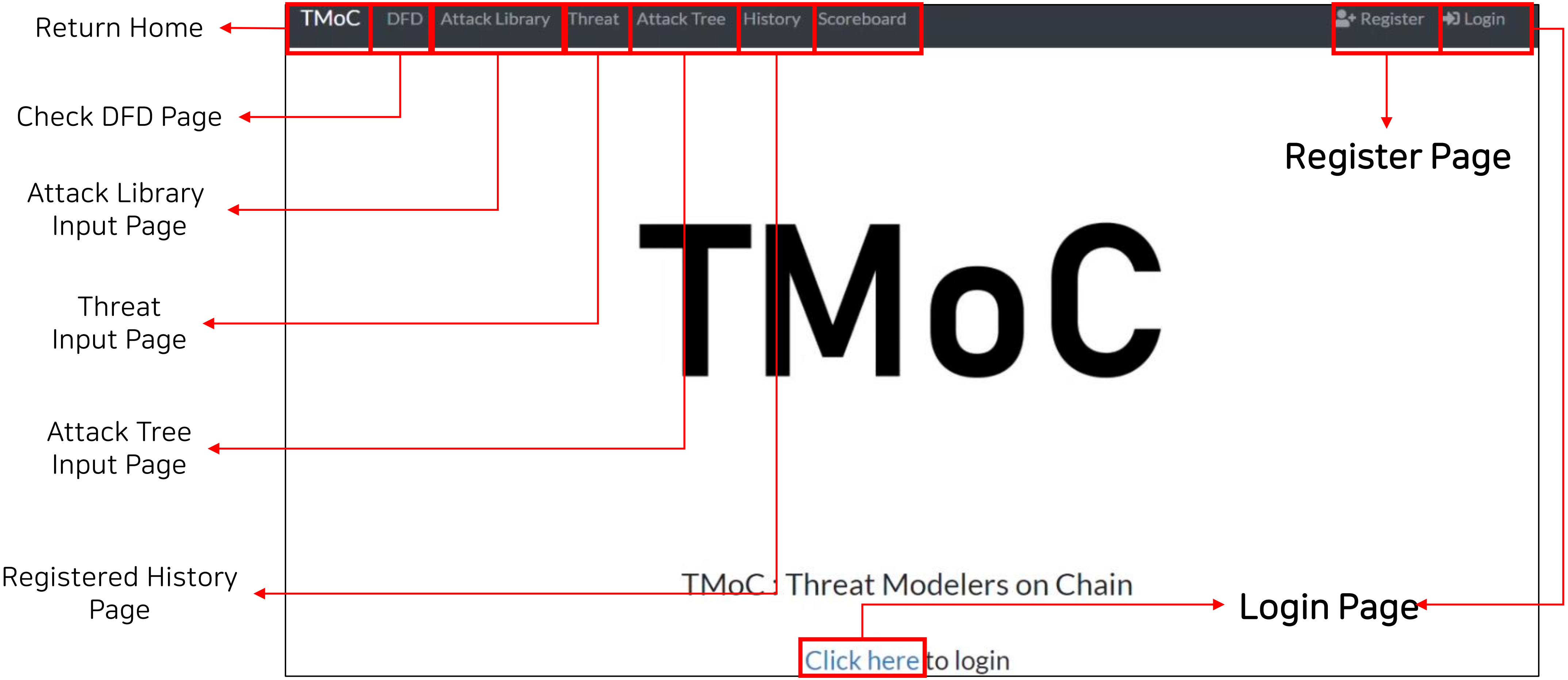
Execution via WebBrowser

TMOC : Threat Modelers On Chain

Link : https://github.com/SANELab/TMOC/tree/master

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



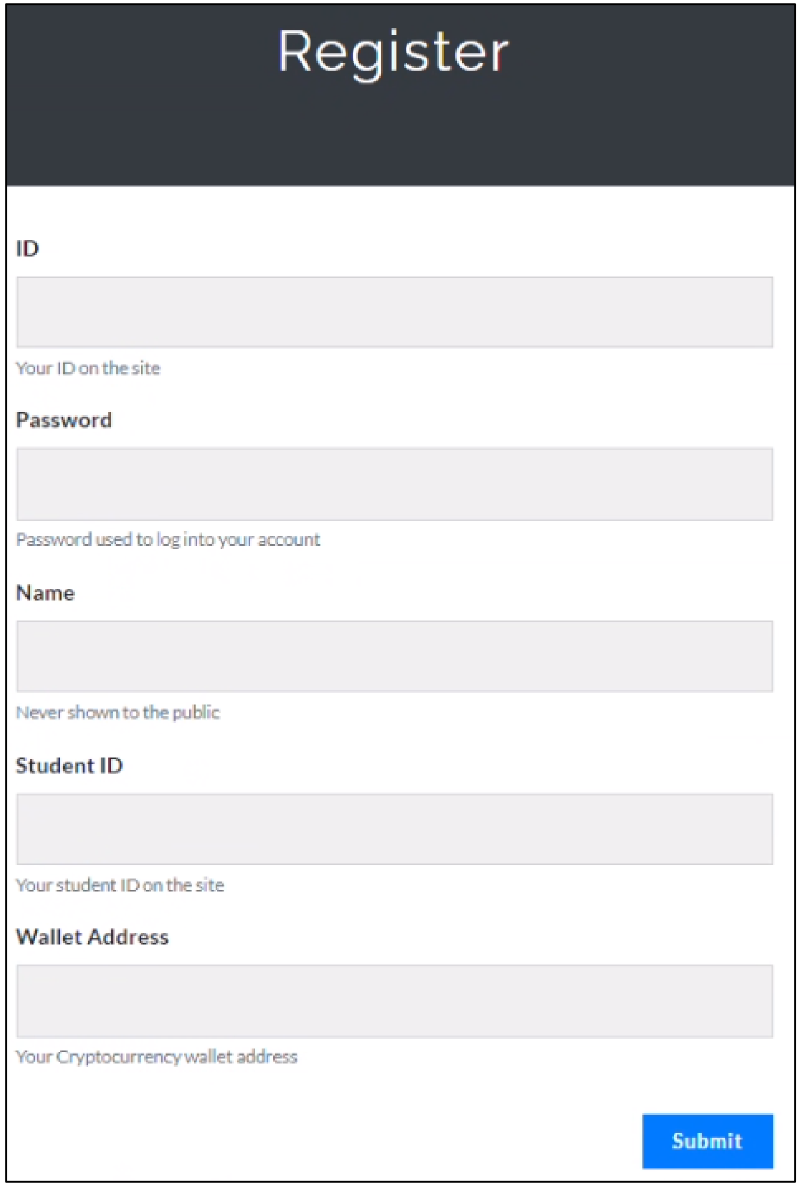
TMoC

TMoC : Threat Modelers on Chain

Click here to login

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



Register

ID

Your ID on the site

Password

Password used to log into your account

Name

Never shown to the public

Student ID

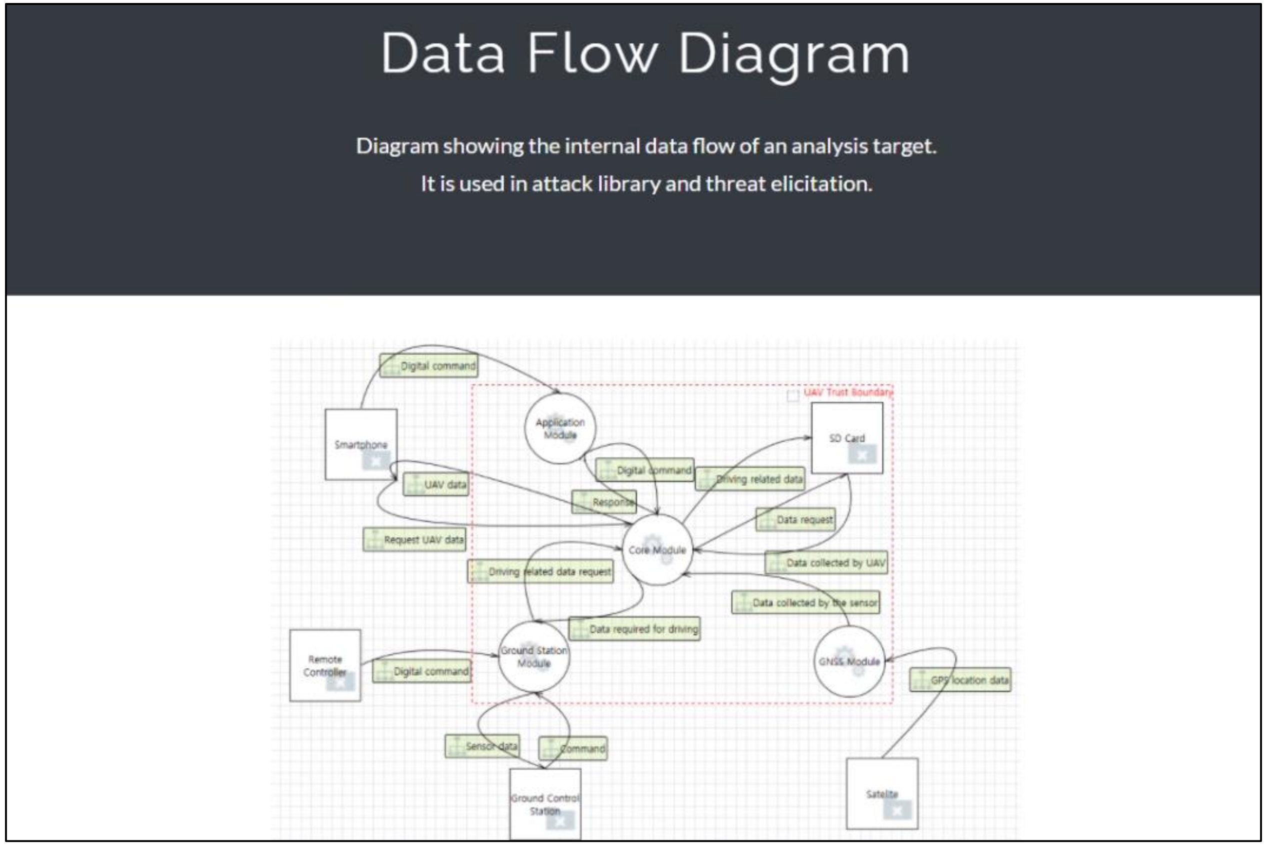
Your student ID on the site

Wallet Address

Your Cryptocurrency wallet address

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

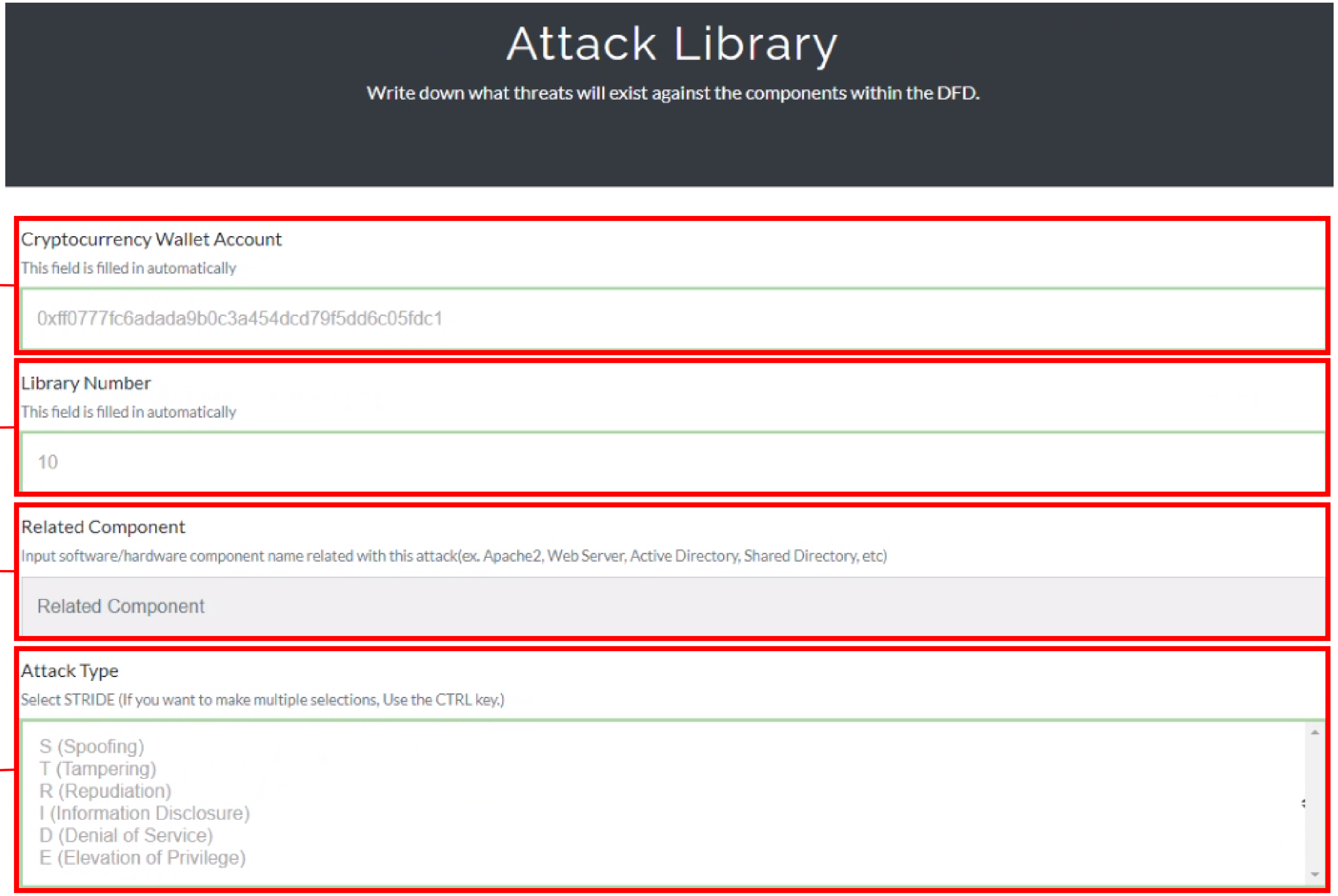


Data Flow Diagram

Diagram showing the internal data flow of an analysis target.
It is used in attack library and threat elicitation.

0x02 Threat Modeling on Chain

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



Attack Library

Write down what threats will exist against the components within the DFD.

Cryptocurrency Wallet Account

This field is filled in automatically

0xff0777fc6adada9b0c3a454dcd79f5dd6c05fdc1

Library Number

This field is filled in automatically

10

Related Component

Input software/hardware component name related with this attack(ex. Apache2, Web Server, Active Directory, Shared Directory, etc)

Related Component

Attack Type

Select STRIDE (If you want to make multiple selections, Use the CTRL key.)

S (Spoofing)
T (Tampering)
R (Repudiation)
I (Information Disclosure)
D (Denial of Service)
E (Elevation of Privilege)

Wallet address entered
when registering as a member

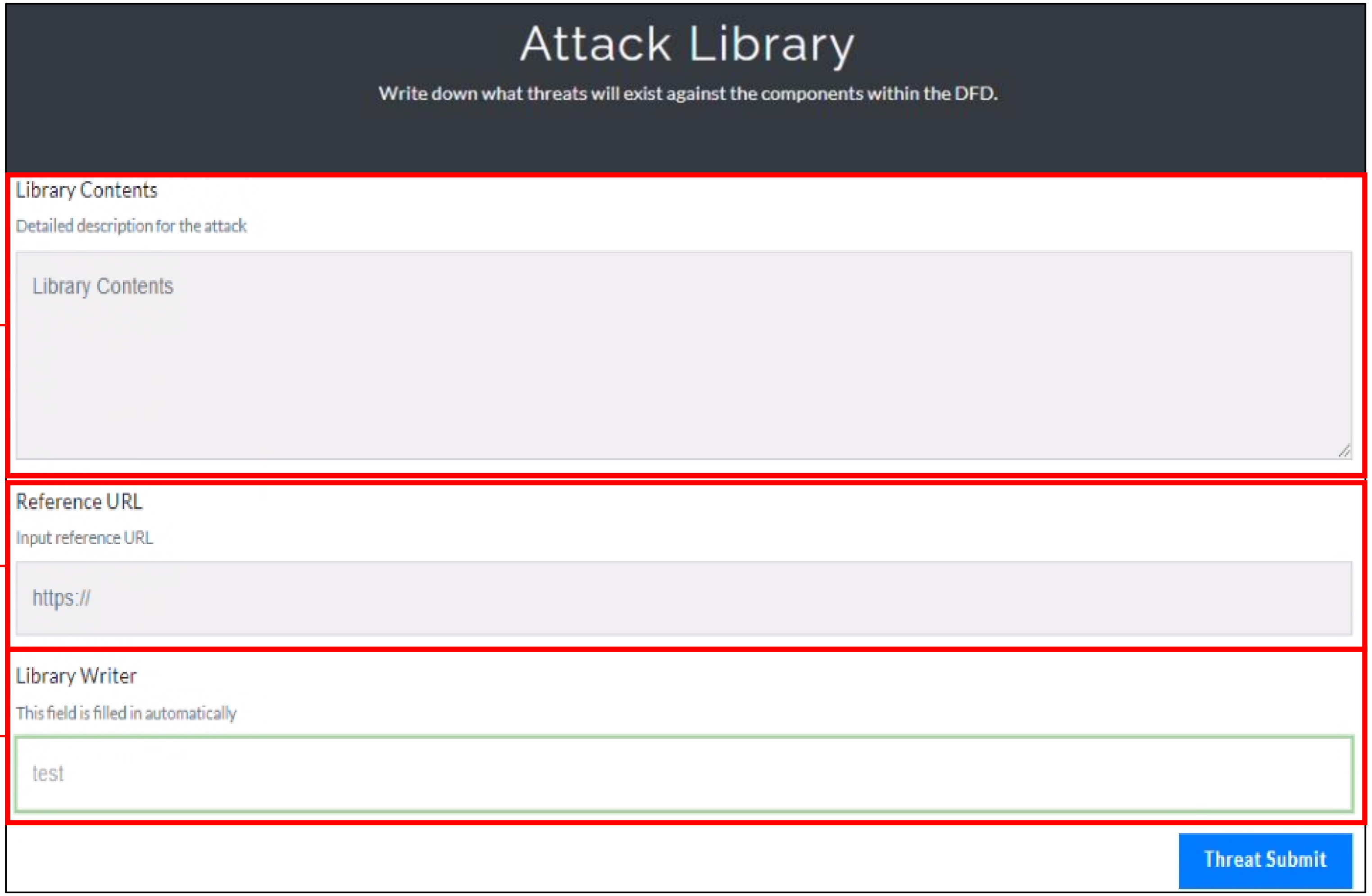
Number in the Attack Library field

Attack targets that map to what you add

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



Attack Library

Write down what threats will exist against the components within the DFD.

Library Contents

Detailed description for the attack

Library Contents

Reference URL

Input reference URL

https://

Library Writer

This field is filled in automatically

test

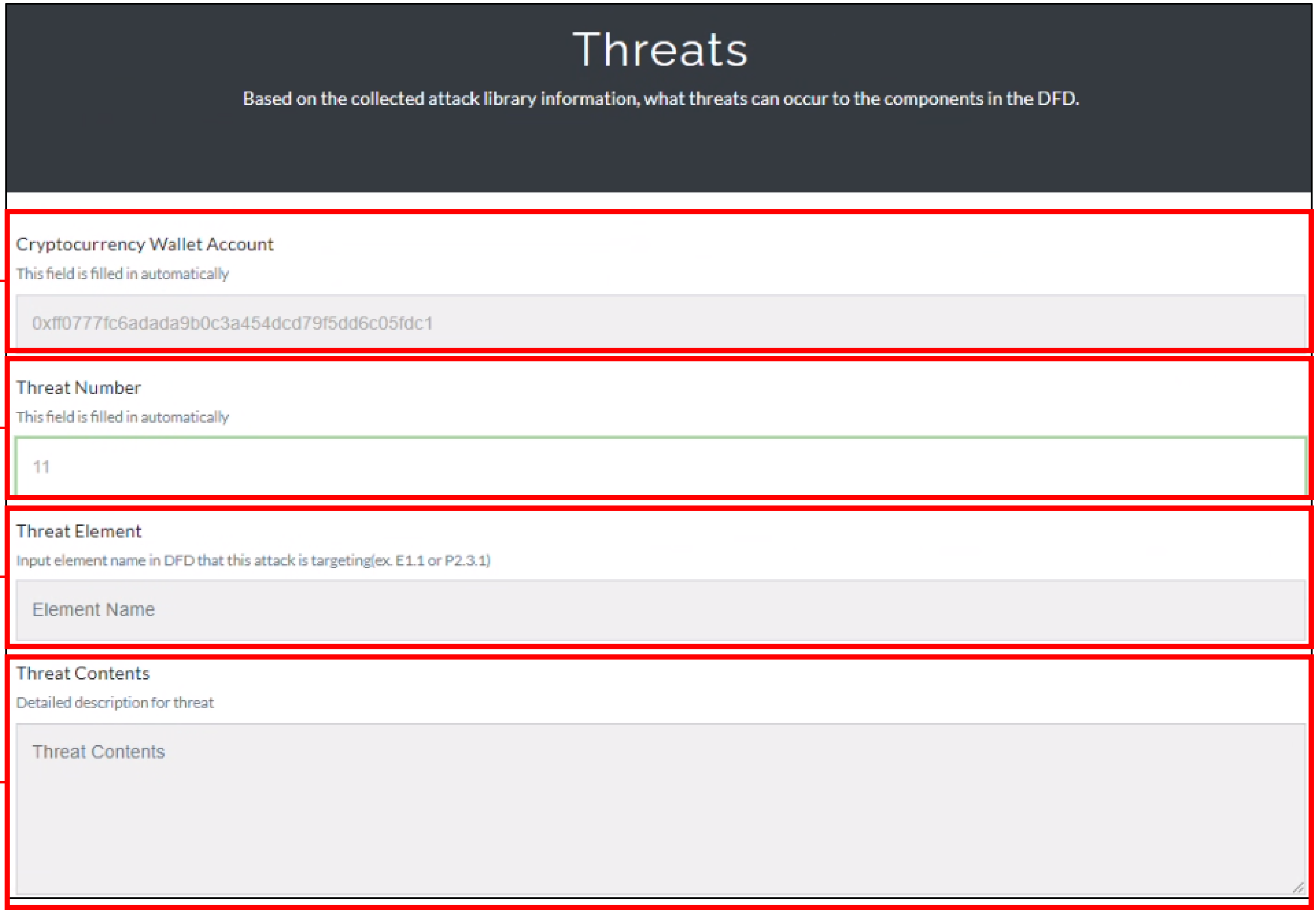
Description of the attack library to be mapped and the reason for the mapping

Evidence link to the mapped attack library

Author's nickname

0x02 Threat Modeling on Chain

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



Threats

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

Cryptocurrency Wallet Account

This field is filled in automatically

0xff0777fc6adada9b0c3a454dcd79f5dd6c05fdc1

Threat Number

This field is filled in automatically

11

Threat Element

Input element name in DFD that this attack is targeting(ex. E1.1 or P2.3.1)

Element Name

Threat Contents

Detailed description for threat

Threat Contents

Wallet address entered when registering as a member

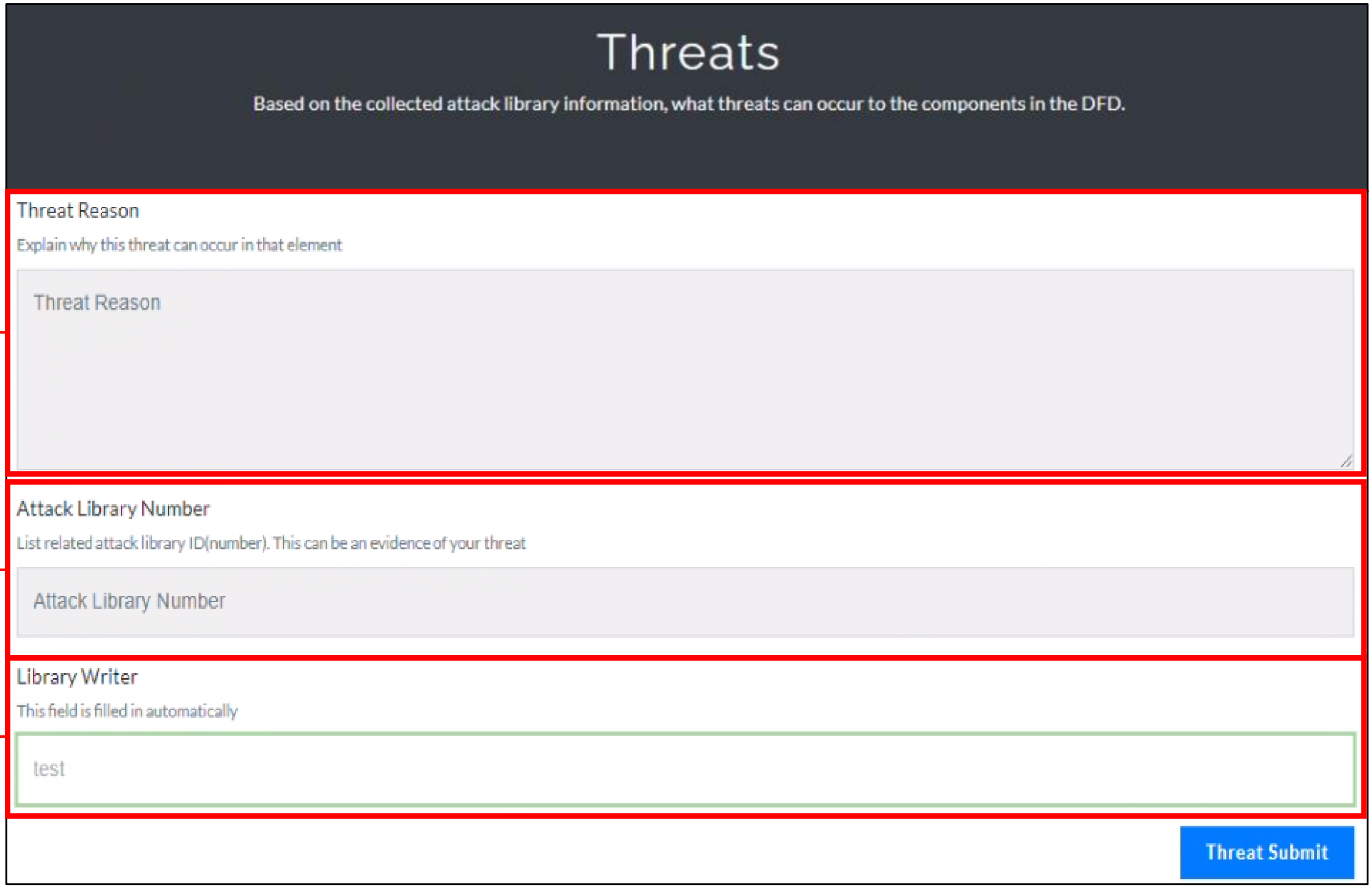
Number in the Threat field

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



Threats

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

Threat Reason

Explain why this threat can occur in that element

Threat Reason

Attack Library Number

List related attack library ID(number). This can be an evidence of your threat

Attack Library Number

Library Writer

This field is filled in automatically

test

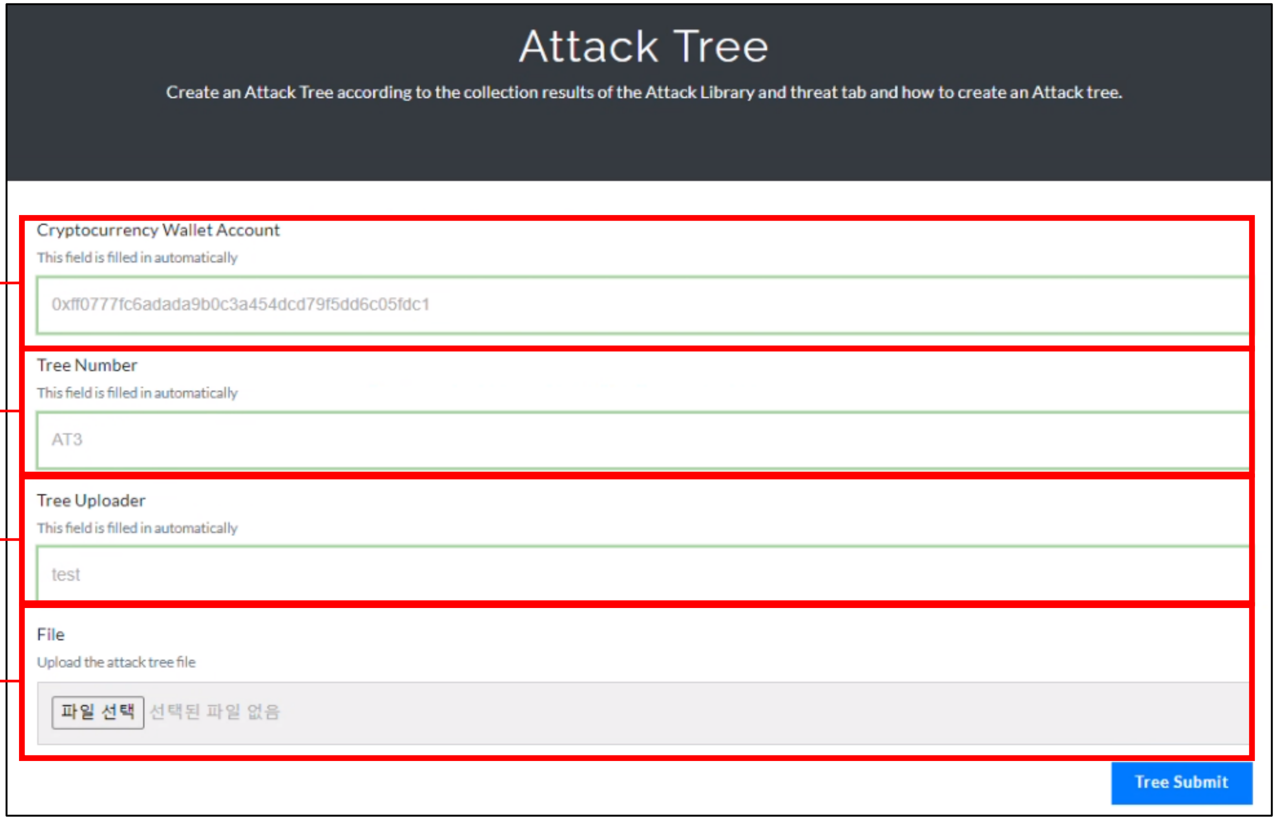
Description of the Threat to be reason for the mapping

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



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.

Cryptocurrency Wallet Account
This field is filled in automatically
0xff0777fc6adada9b0c3a454dcd79f5dd6c05fdc1

Tree Number
This field is filled in automatically
AT3

Tree Uploader
This field is filled in automatically
test

File
Upload the attack tree file
파일 선택 선택된 파일 없음

Wallet address entered
when registering as a member
(auto)

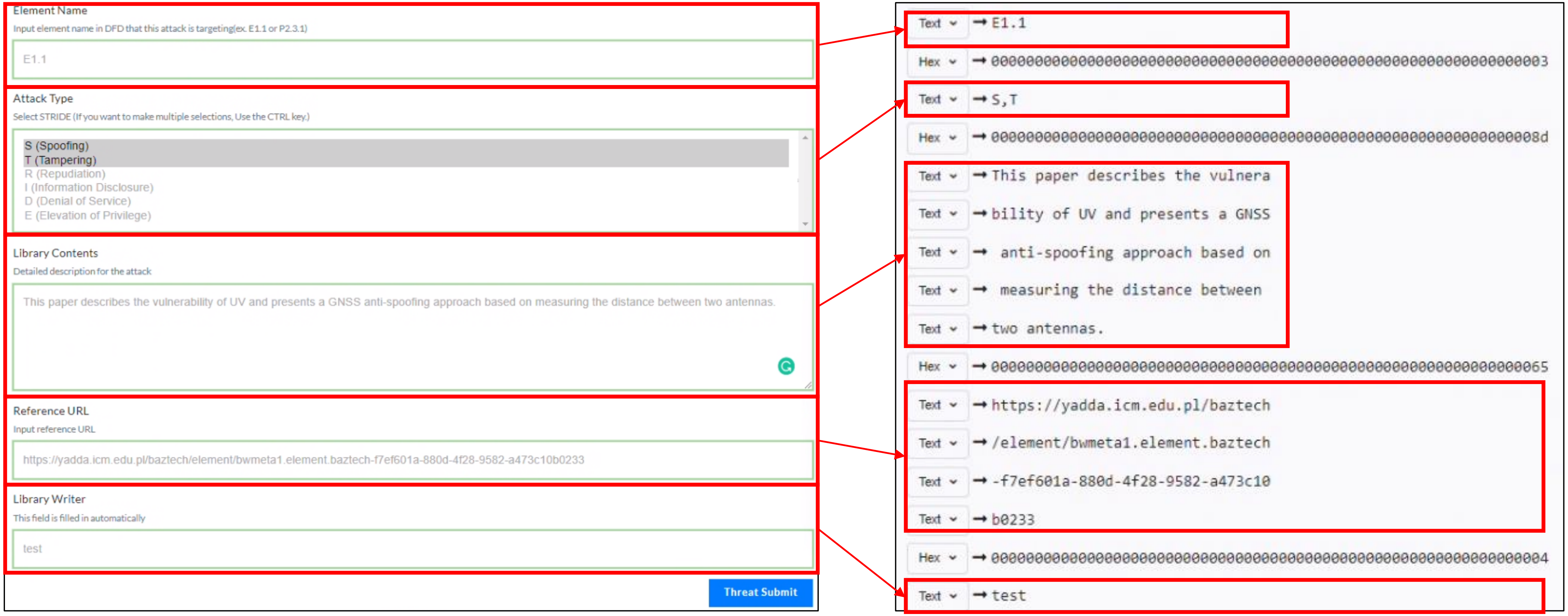
Number in the Attack Tree field
(auto)

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)



Element Name

Input element name in DFD that this attack is targeting(ex. E1.1 or P2.3.1)

E1.1

Attack Type

Select STRIDE (If you want to make multiple selections, Use the CTRL key.)

S (Spoofing)
T (Tampering)
R (Repudiation)
I (Information Disclosure)
D (Denial of Service)
E (Elevation of Privilege)

Library Contents

Detailed description for the attack

This paper describes the vulnerability of UV and presents a GNSS anti-spoofing approach based on measuring the distance between two antennas.

Reference URL

Input reference URL

https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-f7ef601a-880d-4f28-9582-a473c10b0233

Library Writer

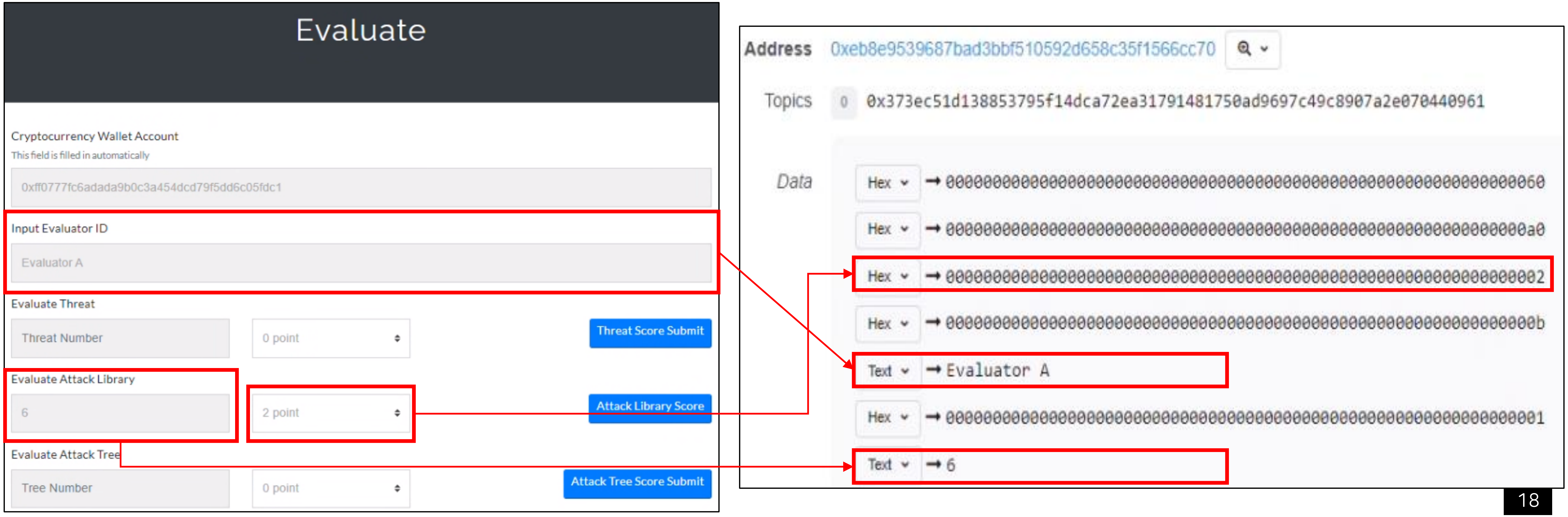
This field is filled in automatically

test

```
Text → E1.1
Hex  → 0000000000000000000000000000000000000000000000000000000000000003
Text → S,T
Hex  → 000000000000000000000000000000000000000000000000000000000000008d
Text → This paper describes the vulnera
Text → bility of UV and presents a GNSS
Text →  anti-spoofing approach based on
Text →  measuring the distance between
Text → two antennas.
Hex  → 0000000000000000000000000000000000000000000000000000000000000065
Text → https://yadda.icm.edu.pl/baztech
Text → /element/bwmeta1.element.baztech
Text → -f7ef601a-880d-4f28-9582-a473c10
Text → b0233
Hex  → 0000000000000000000000000000000000000000000000000000000000000004
Text → test
```

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



Evaluate

Cryptocurrency Wallet Account

This field is filled in automatically

0xff0777fc6adada9b0c3a454dcd79f5dd6c05fdc1

Input Evaluator ID

Evaluator A

Evaluate Threat

Threat Number | 0 point | Threat Score Submit

Evaluate Attack Library

6 | 2 point | Attack Library Score

Evaluate Attack Tree

Tree Number | 0 point | Attack Tree Score Submit

```
Address  0xeb8e9539687bad3bbf510592d658c35f1566cc70

Topics   0  0x373ec51d138853795f14dca72ea31791481750ad9697c49c8907a2e070440961

Data     Hex  → 0000000000000000000000000000000000000000000000000000000000000060
         Hex  → 00000000000000000000000000000000000000000000000000000000000000a0
         Hex  → 0000000000000000000000000000000000000000000000000000000000000002
         Hex  → 000000000000000000000000000000000000000000000000000000000000000b
         Text → Evaluator A
         Hex  → 0000000000000000000000000000000000000000000000000000000000000001
         Text → 6
```

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)