

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 (visitor00@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



How to approach
Threat Modeling

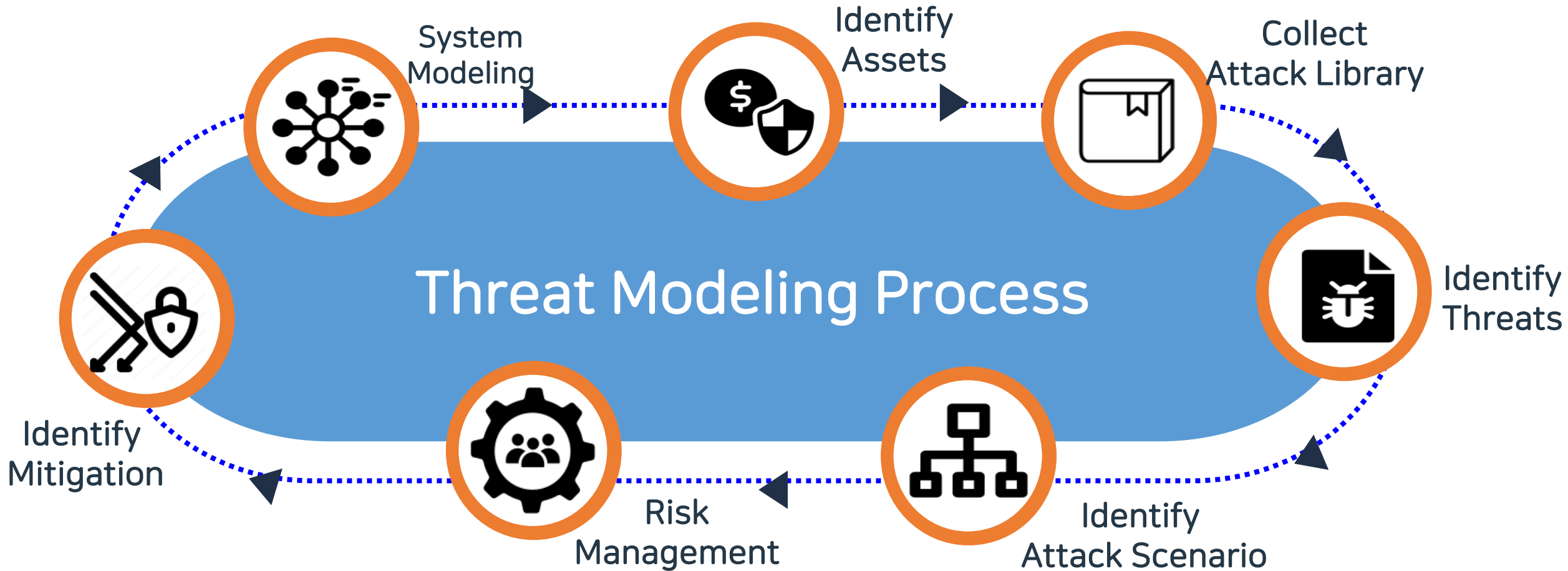


[Amazon AWS(Darran Boyd), How to approach threat modeling]

- 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

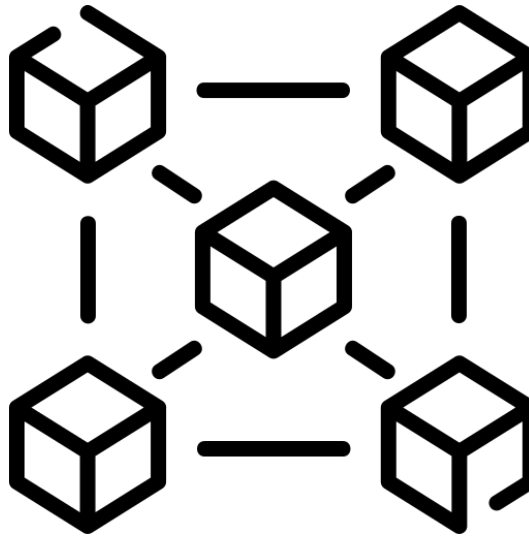


0x01 Introduction

- 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

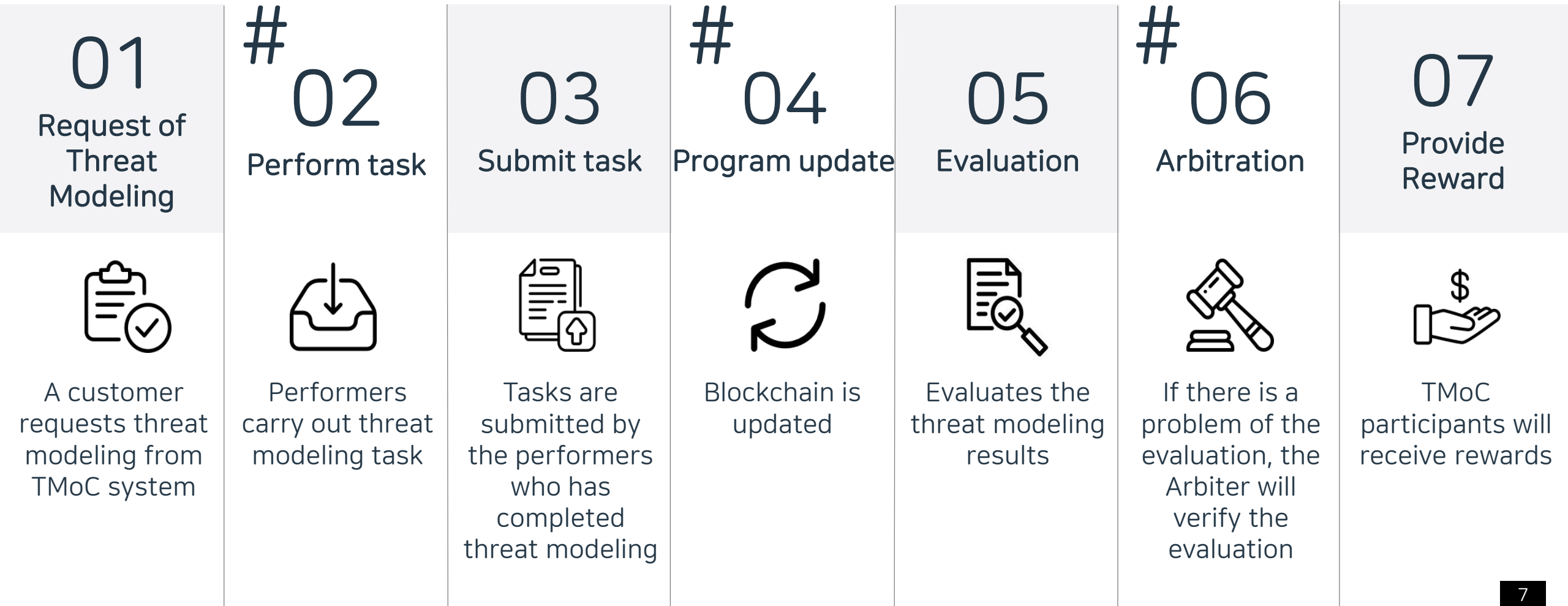


Threat Modeling

0x01 Introduction

- TMoC Basic Process

- The operation sequence of TMoC proceeds as follows

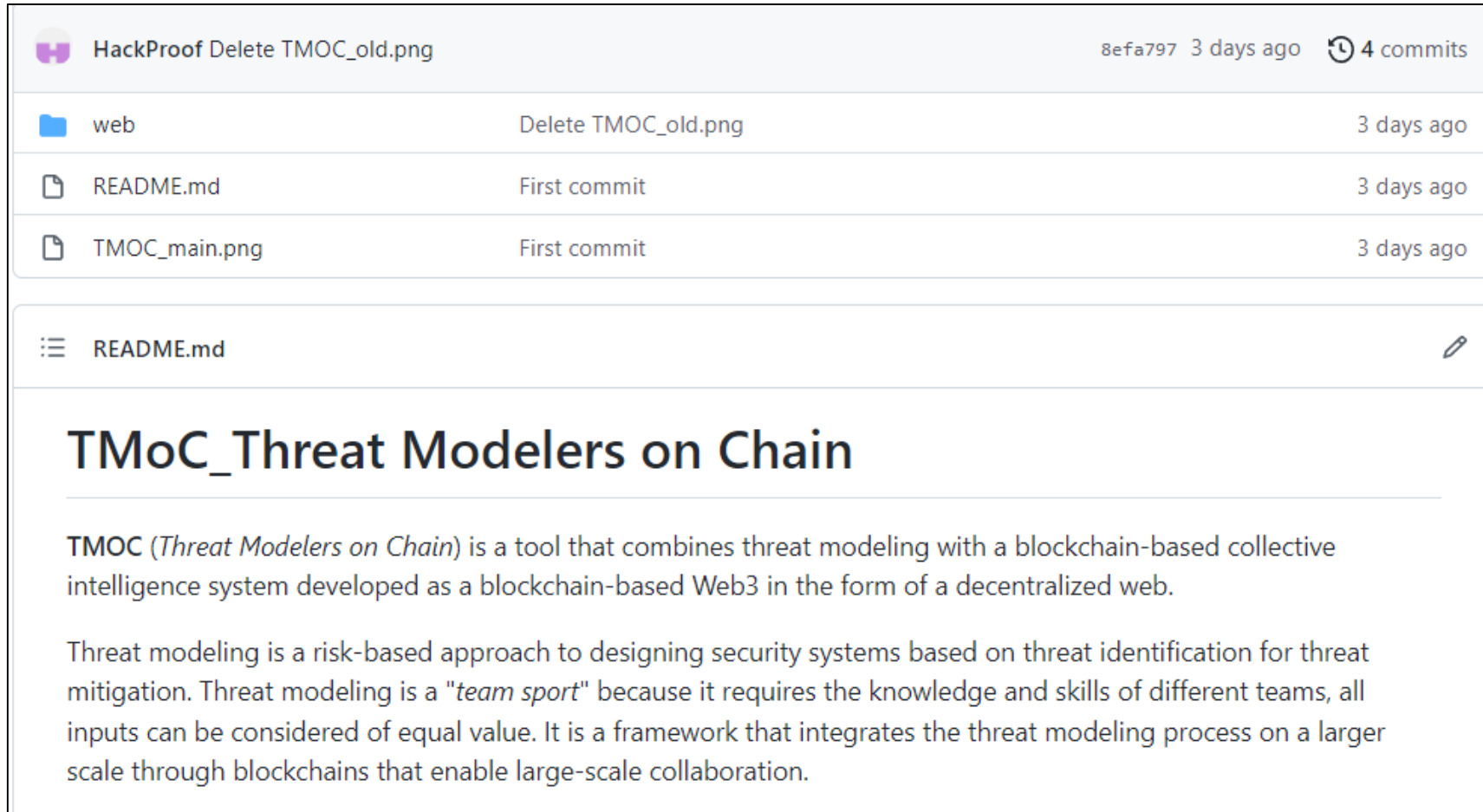


0x02

Threat Modeling on Chain

0x02 Threat Modeling on Chain

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



The screenshot displays a GitHub repository interface for 'HackProof'. At the top, the repository name 'HackProof' is shown with a commit message 'Delete TMOc_old.png', commit hash '8efa797', and a timestamp '3 days ago'. It also indicates '4 commits'. Below this, a table lists the repository's files and folders:

File/Folder	Commit Message	Time
web	Delete TMOc_old.png	3 days ago
README.md	First commit	3 days ago
TMOc_main.png	First commit	3 days ago

Below the file list, the 'README.md' file is selected, showing its content. The title is 'TMoC_Threat Modelers on Chain'. The text describes TMOc as a tool combining threat modeling with a blockchain-based collective intelligence system. It also defines threat modeling as a risk-based approach to designing security systems.

TMoC_Threat Modelers on Chain

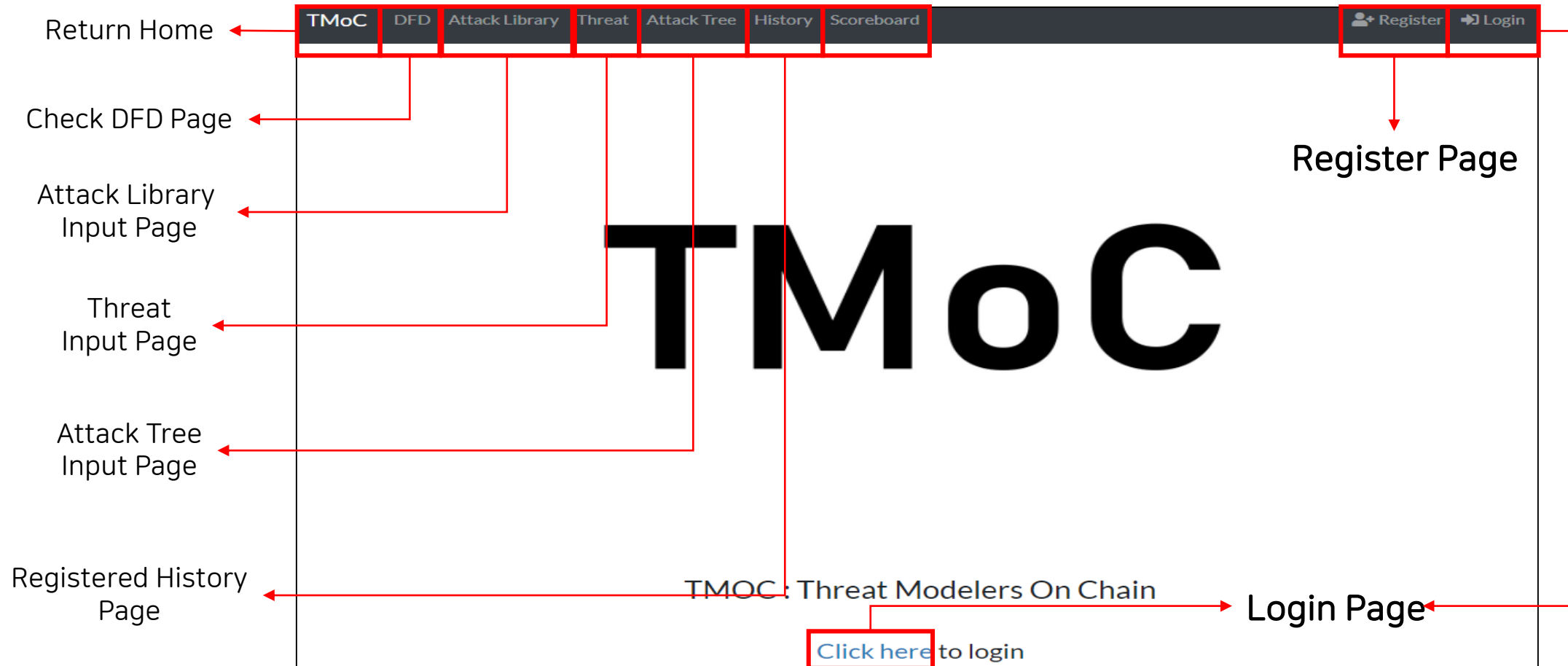
TMOc (*Threat Modelers on Chain*) is a tool that combines threat modeling with a blockchain-based collective intelligence system developed as a blockchain-based Web3 in the form of a decentralized web.

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.

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

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

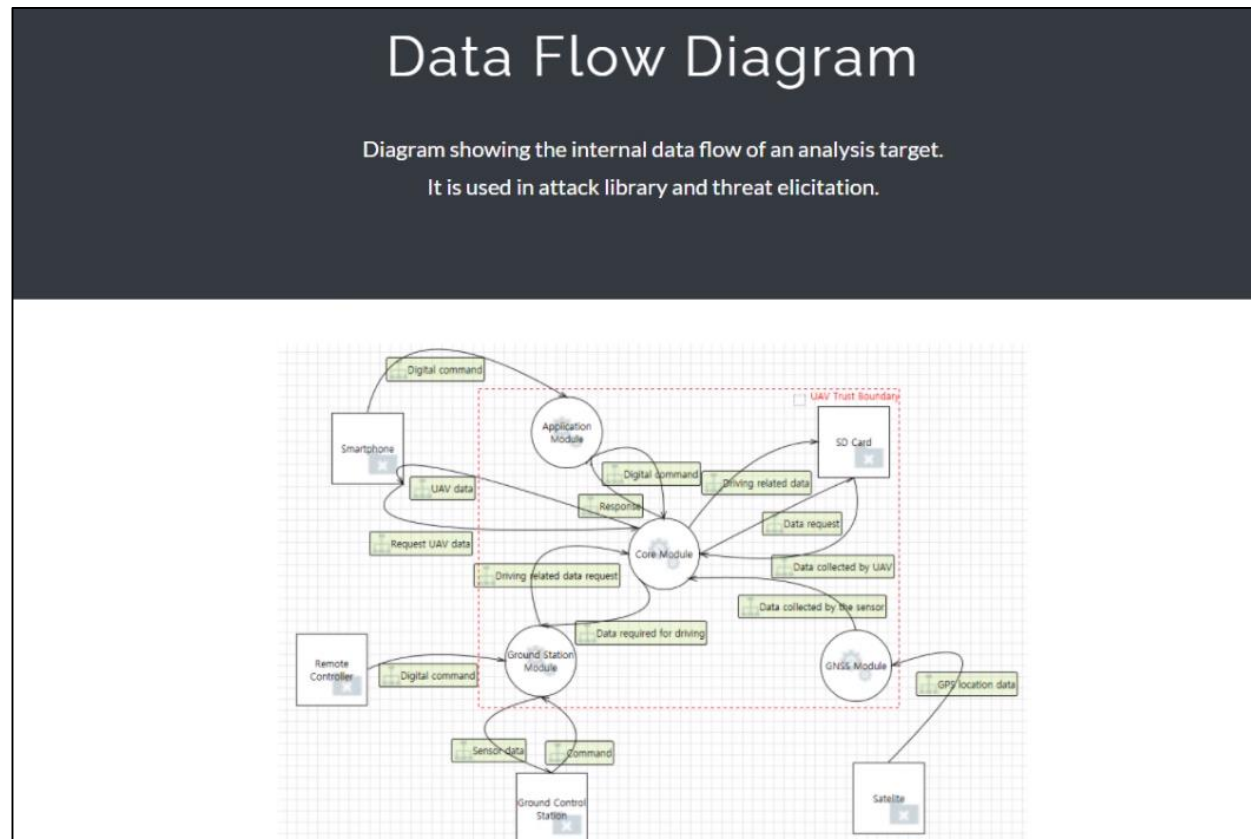
Wallet Address

Your Cryptocurrency wallet address

Submit

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

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

6

Element Name

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

Element Name

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
(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)

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

Threat Submit

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

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

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)

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

Threat Submit

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

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

0x1f0777fc6adada9b0c3a454dcd79f5dd6c05fdc1

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

Tree Submit

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)

[illegible]

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
-------------	---------	--------------------------

Receipt Event Logs

Address 0xeb8e9539687bad3bbf510592d658c35f1566cc70

Topics 0 0x373ec51d138853795f14dca72ea31791481750ad9697c49c8907

Data

Hex	→ 00
Hex	→ 00
Num	→ 2
Hex	→ 00
Hex	→ 00
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)