MATSUURA LAB.

Cryptography and Information Security

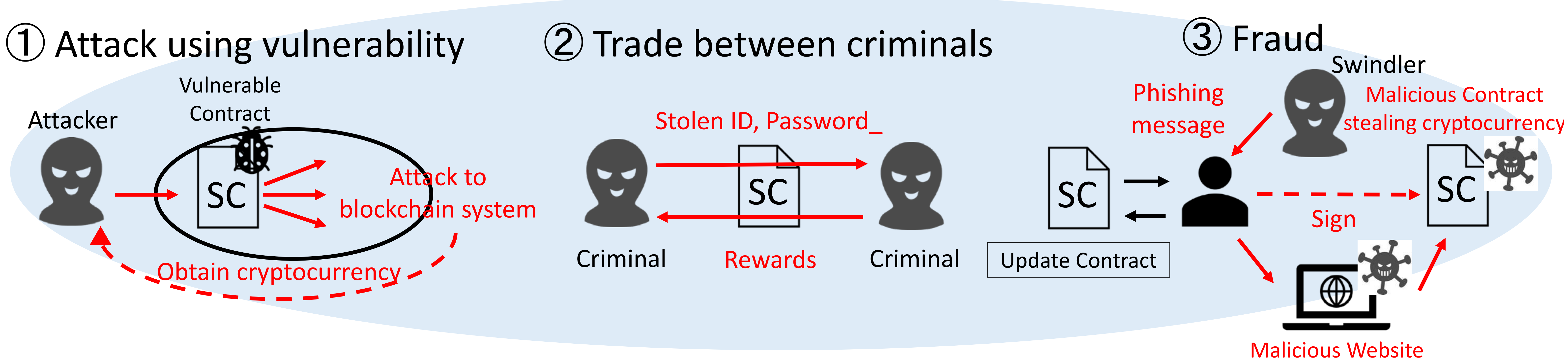
Department of Informatics and Electronics

Information Security
Department of Information and Communication Engineering, GSIST

http://kmlab.iis.u-tokyo.ac.jp/

• Malicious Smart Contract

The number of crimes using smart contracts, which are the computer programs running as application on blockchain systems, **has been increased these days**.



⇒ **To detect malicious smart contracts, which are used in crimes, is an agent need.**

【Existing classification model [1] and its problem】

An existing work proposed a classification model with two types.

① Vulnerable Smart Contract	… has vulnerabilities in their code
② Criminal Smart Contract.	… promotes trade between criminals

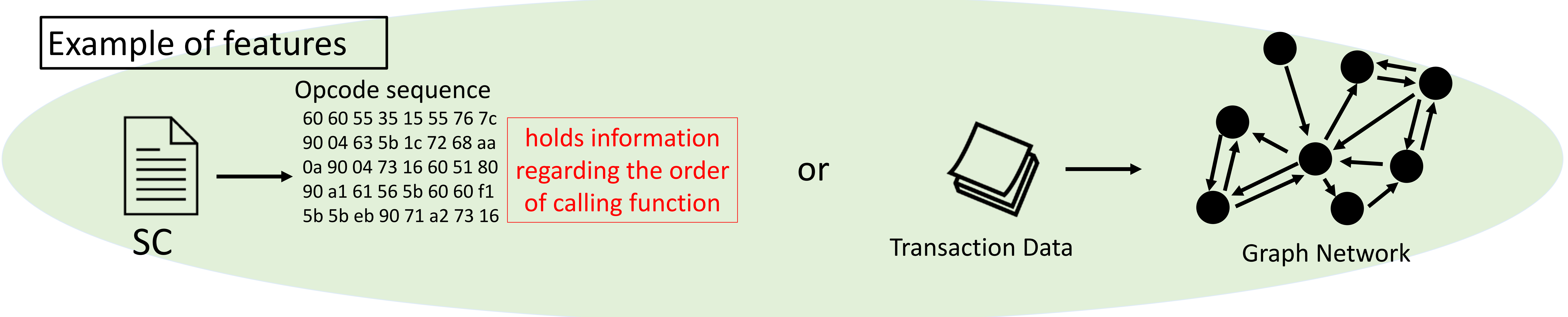
⇒ No existence of the type corresponded to the contract regarding fraud

⇒ Difficulty in comprehensive detection of whole types of malicious smart contracts

We added the contract which promotes fraud (Fraudulent Smart Contract) to the existing model.
⇒ Our goal is to propose a detection system of Fraudulent Smart Contract. [2]

• Prospect of fraudulent smart contract detection

Making features based on code or transaction ⇒ **Machine learning**



```
60 60 55 35 15 55 76 7c
90 04 63 5b 1c 72 68 aa
0a 90 04 73 16 60 51 80
90 a1 61 56 5b 60 60 f1
5b 5b eb 90 71 a2 73 16
```

[1] M.Ndiaye, and P. Konate "Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain." *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2021.pp.1-8

[2] 五十嵐太一ほか. "スマートコントラクトにおけるセキュリティに関する調査". 2023年暗号と情報セキュリティシンポジウム（SCIS2023），3C-1，2023年1月.