Preparation Notice

This tutorial is a summary of the ABC threat modeling paradigm.

This notice is not given to the participants in the user study to avoid disclosing the name of the threat modeling framework.

Threat Modeling Framework B - Tutorial

Consists of three steps:

1. System Model Characterization.
2. Threat Identification.
3. Threat Scenario Enumeration and Reduction.

1. System Model Characterization.

Before we begin, we need to understand the system.

- List the activities in the system, i.e. all of the actions performed by all parties.
- Make a list of the participants based on their roles, i.e. clients, servers, etc. Add a participant "external" that represents all actors who are not part of the system.
- List the assets (items of value) in the system. Generally framework "B" defines the following assets in resource-backed cryptocurrencies:
    - the service,
    - the currency (payments),
    - and the currency exchange medium (blockchain, transactions, and the communication network).
- List any external dependencies on other systems or technologies, and all assumptions made. Draw a network diagram of the system activities.

Example Scenario: *Suppose that there is a vending machine that works as follows. Customers purchase goods from the vending machine. Re-suppliers visit the vending machine and re-supply goods in low supply, but can not access the cash box. The owner of the machine is allowed to withdraw money from the cash box. The owner compensates re-suppliers for the resupplying service. An attacker may attack the system only if it benefits from the attack.*

Example Characterization:

List of activities: purchase goods, resupply goods, withdraw money, compensate re-supplier

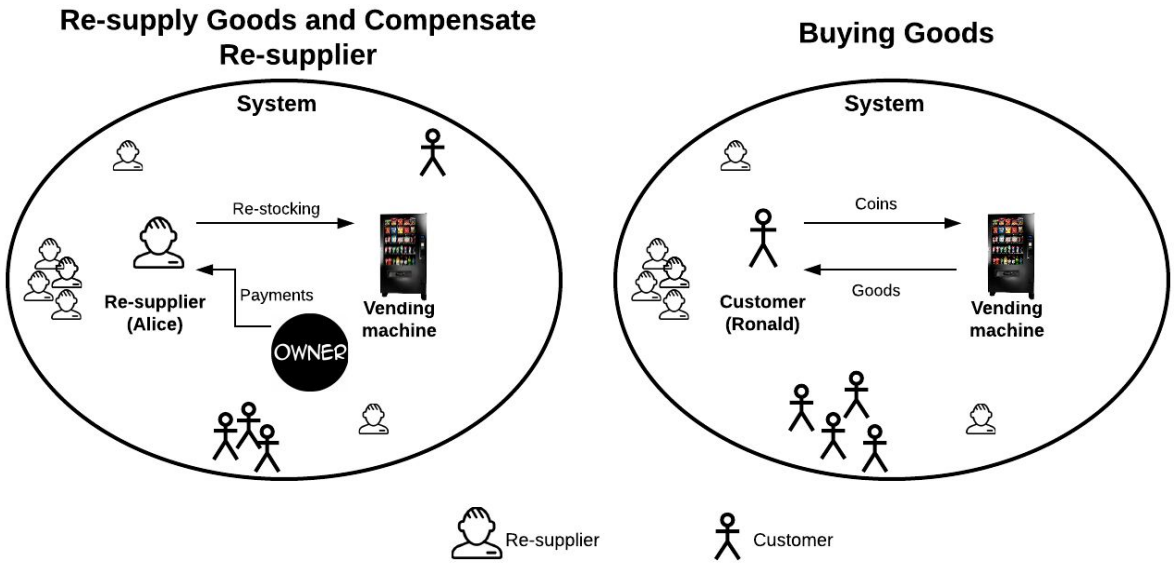
List of participants: customers, re-suppliers, owner, external

List the assets of value: currency, service (re-supplying service, goods selling service)

List assumptions and external dependencies:

- *re-suppliers cannot access the cash box,*
- *one owner of the vending machine, while we have several re-suppliers and customers.*
- *attackers work for their interest only.*

Network Model:



2. Threat Identification

In this step we identify the threats to the systems. You may find Table 1 useful in identifying the threat categories. These threats are classified based on the assets in the system, we consider only the service and currency assets in this study.

Table 1: Threat categories.

Asset	Security Threat
Service	Service corruption (serve a corrupted or invalid service).
	Denial of service (interrupt the legitimate operation of the parties in the system to make the service unavailable).
	Information disclosure (The content of the service and the service requests are public).
	Repudiation (the server is not bound to the service it provides).
Currency	Service slacking (A server tries to collect payments without performing all the promised work).
	Service theft (A client tries to obtain service for payments lower than the agreed upon amount. Hence, a client saves currency when obtaining a cheaper service in a malicious way).

Vending Machine Example:

Threats:

- *Re-supplying service theft (obtain re-supplying service without compensating the re-supplier)*
- *Goods selling service theft (take supplies without payments),*
- *Re-supplying Service slacking (re-supplier slacking off from resupplying),*
- *Service corruption (hand expired goods to customers),*
- *etc.*

Due to time constraints, you will ***work on only one threat*** *in this study*. **STOP AT THIS POINT AND ASK THE MONITOR TO HAND YOU THE REST OF THE STUDY THAT DETERMINES WHICH THREAT TO WORK ON.**

3. Threat Scenario Enumeration and Reduction

The next step is to enumerate how the participants could potentially perform a specific threat. This is done as follows:

a. Construct a collusion matrix for each threat.
b. Enumerate all scenarios of each threat inside the cells of the matrix.
c. Reduce these scenarios if applicable.

A. Collusion Matrix

Two dimensional matrix of attackers and targets as follows:

- **Attackers:** Along the side, list all participants as well as the “external”, and add all combinations of different groups of parties to cover all collusion cases.
- **Targets:** Along the top, list all participants in the system (not including the external party). Also add all combinations of different groups of parties.

Each cell in the matrix represents a threat scenario to investigate.

Vending Machine Example:

A collusion matrix of the slacking off from re-supplying service threat is shown in Figure 2.

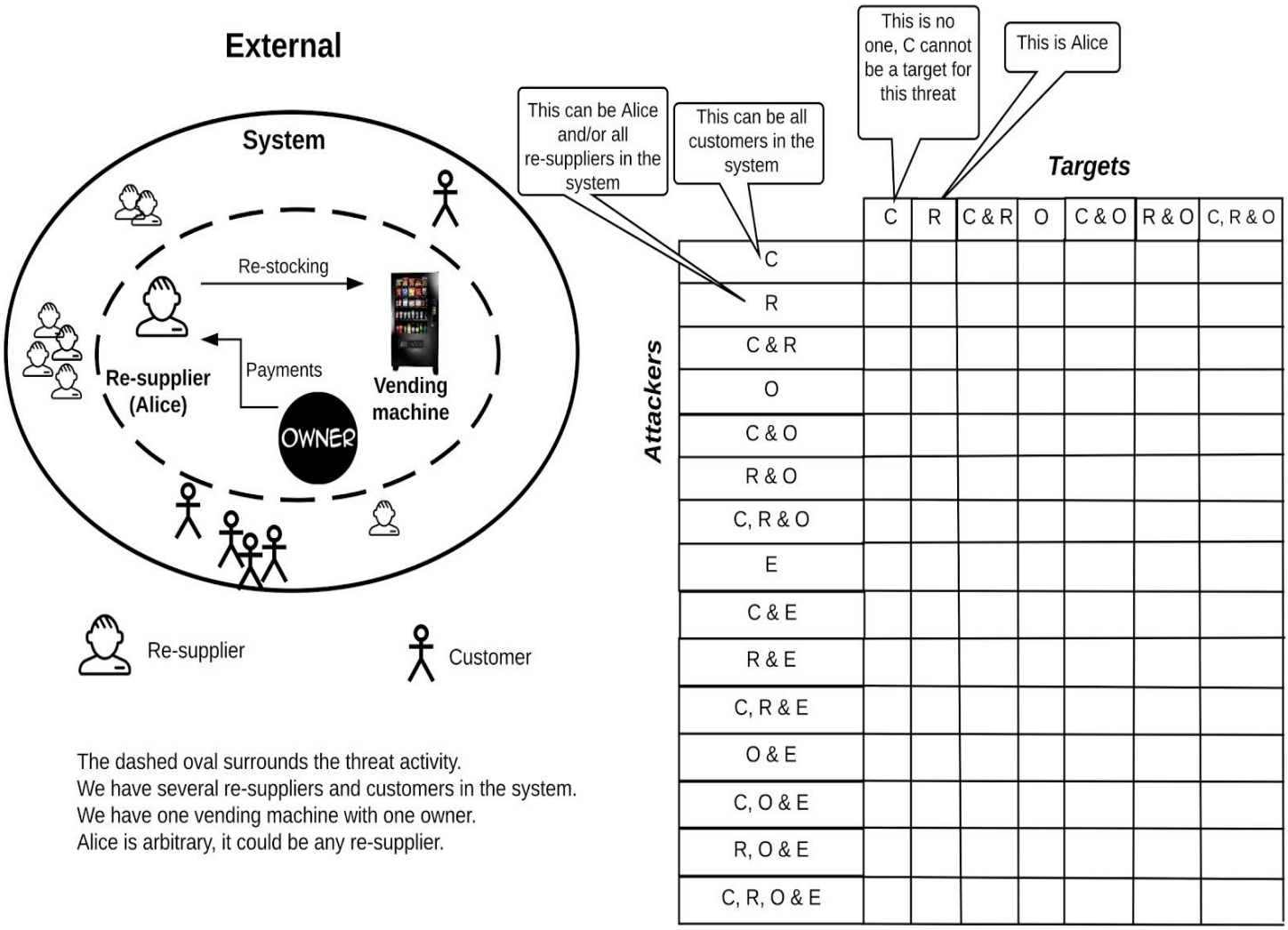


Figure 2: Slacking off from re-supplying threat collusion matrix
Participant short names: C:Customer, R: Re-supplier, O: Owner, E:External

B. Enumerate Attacker(s) Strategies

Then, inside each cell list all the strategies attackers may follow to attack the target parties. You may find the following broad strategies useful in figuring out these scenarios:

- **Spoofing** — an attacker imitates other parties or components in the system.
- **Tampering** — an attacker alters data such as messages exchanged, payments transactions, etc., to fool the honest parties.
- **Repudiation** — attackers perform actions that cannot be traced back to them.
- **Information disclosure** — an attacker steals or exposes others' data.
- **Denial of service** — interrupt the legitimate operation of the parties in the system.
- **Elevation of privilege** — an attacker gains higher privileges than what it is entitled for.

C. Threat Scenario Reduction

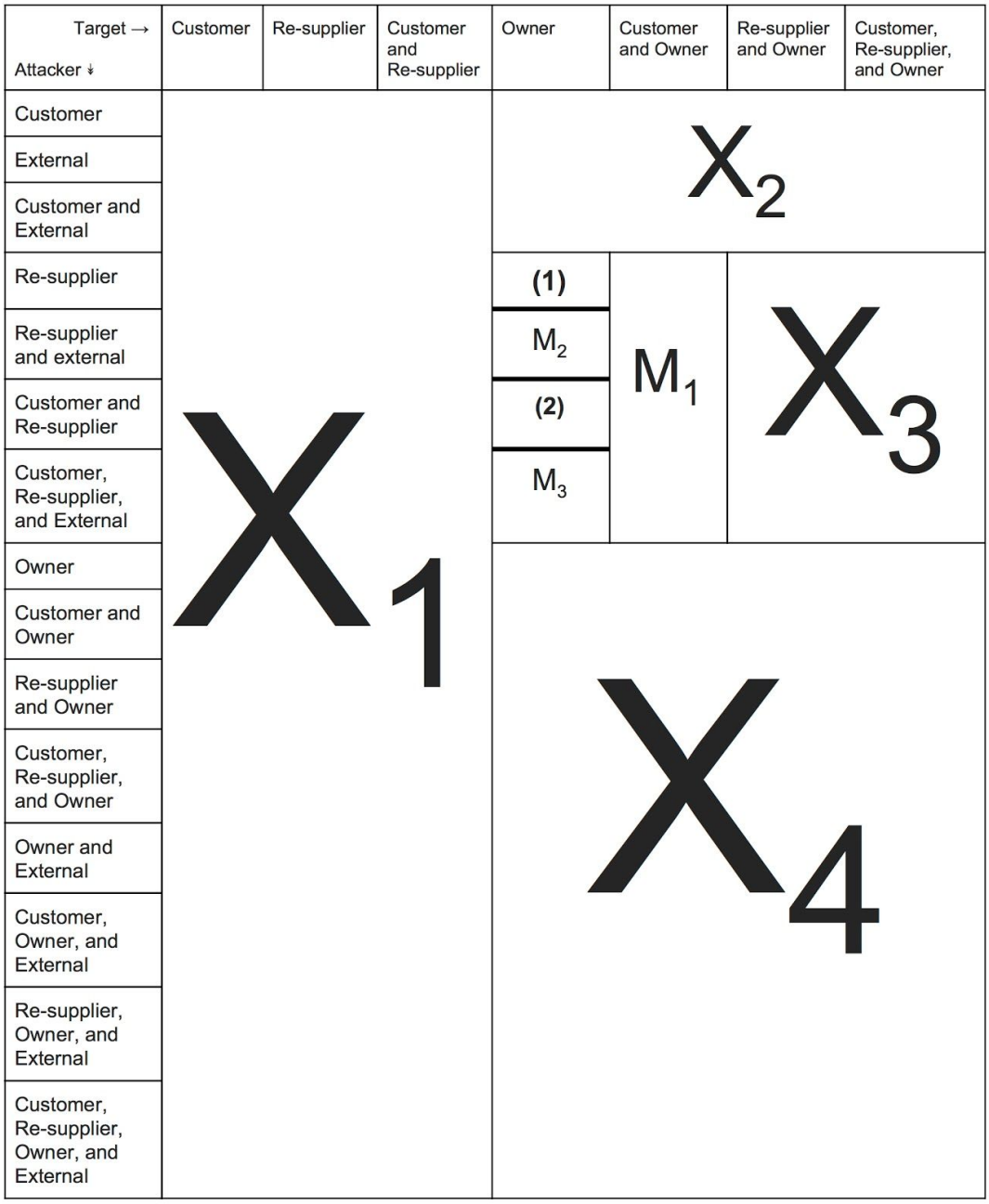
Explore each cell in the matrix and reduce the threat scenarios as follows:

- **Cross out all unlikely to happen threats.** Some threats are unlikely to happen due to system assumptions, the target cannot be attacked, etc.
- **Merge threats that have the same effect together.** For example, some threats will not become stronger with collusion. The effect is the same as an attacker is attacking the system on its own.

Lastly, list a brief description of the distilled threats resulted from reduction. These are the threats that must be addressed by the system design.

Vending Machine Example:

Threat: ***Slacking off from resupplying****. (Label descriptions are on the next page.)*



Rationale behind threat crossing out (labeled with X):

- X_1: Cannot be targets, only the owner can be a target in this threat.
- X_2: Customer/external does not benefit from the attack, will not attack.
- X_3: The attacker re-suppliers are outside the activity since the re-supplier inside is a target now (i.e. other than Alice in Figure 2). They will not attack since they do not benefit from the attack.
- X_4: The owner will not attack itself , we have a single owner of the vender machine.

Rationale behind threat merging (labeled with M):

- M_1: Just like attacking the owner alone, customers cannot be targets. Merge with Owner column.
- M_2: a re-supplier colludes with an external is the same as re-supplier is attacking on his own. This is because the external does not play a role in the re-stocking or payments. Merge with threat (1) below.
- M_3: a re-supplier and customer collude with an external is the same as re-supplier colluding with a customer. This is because the external does not play a role in the re-stocking or payments. Merge with threat (2) below.

Distilled Threats Description:

(1) A re-supplier does not do all the work he was contracted to do by the owner, but still obtains full payments.

(2) A re-supplier and a customer(s) work together to deceive the owner into paying the re-supplier for work that was not performed. Perhaps the customer pretends to have paid for goods that the re-supplier added.