Framework “B” Tutorial

ABC Material
G. Almashaqbeh et al. 2019

Outline

- Threat modeling framework “B” steps.
- Example scenario.
- Running example application.

OVERVIEW

- In this tutorial we will explore the steps of a threat modeling framework, we refer to it as framework "B".
- You will use this framework to build a threat model of a simplified resource-backed cryptocurrency system in the study.
- When running the study, this tutorial is given to you as a handout.

Example Scenario

- We will demonstrate the steps of framework "B" by applying them to the following example:

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.*

Framework "B" Steps

- Consists of three steps:
  1. System Model Characterization.
  2. Threat Identification.
  3. Threat Scenario Enumeration and Reduction.

1. System Model Characterization

- List the activities in the system.
  - ***<u>List of activities:</u>*** purchase goods, resupply goods, compensate re-supplier, withdraw money.

- List of the participants based on their roles. Add a participant "external".
  - ***<u>List of participants:</u>*** customers, re-suppliers, owner, external.

1. System Model Characterization

- List the assets in the system.
  - ***List the assets of value:*** currency, service (re-supplying service, goods selling service).
- List any external dependencies on other systems and all assumptions.
  - ***List the assumptions:***
    - 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.

1. System Model Characterization

- Draw a network diagram of the system activities.

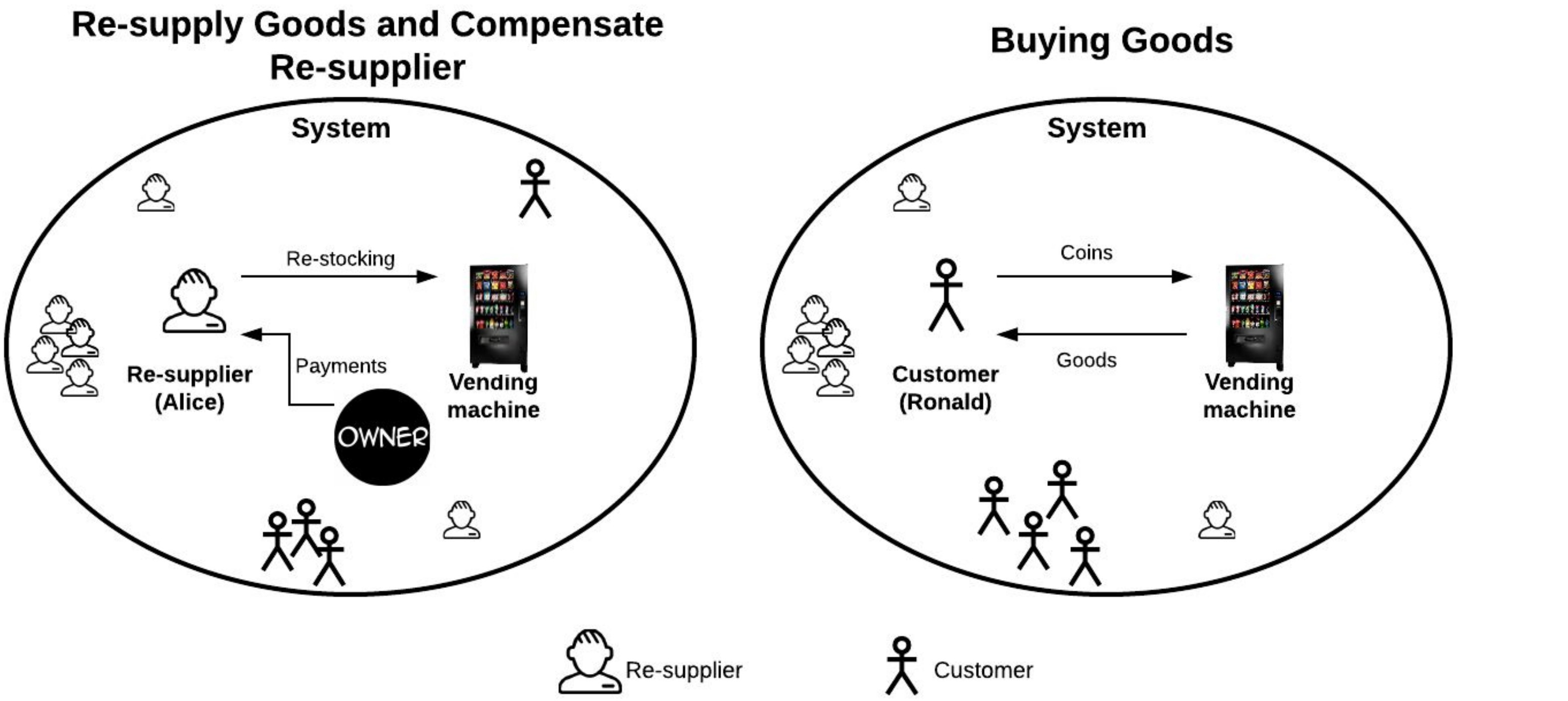


Figure 1: vending machine example network model

2. Threat Identification

- In this step we identify the threats to the systems.
- You may find Table 1 useful in identifying the threat categories.

Table 1: Threat categories.

Asset	**Security Threat**
Service	Service corruption (serve corrupted or invalid service).
	Denial of service (interrupt the legitimate operation of the system to make the service unavailable).
	Information disclosure (the content of the service requests/replies/etc. are public).
	Repudiation (servers actions during serving clients cannot be traced back to them).
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).

Running Example Application

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.

3. Threat Scenario Enumeration and Reduction

- 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.

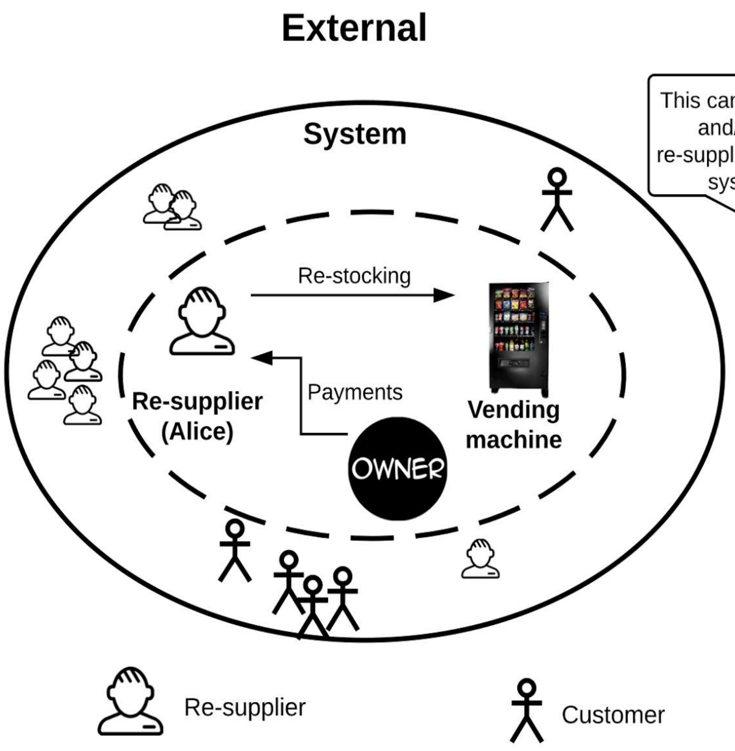
A. Collusion Matrix

- 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.

Running Example Application



The dashed oval surrounds the threat activity.
We have several re-suppliers and customers in the system.
We have one vending machine with one owner.
Alice is arbitrary, it could be any re-supplier.

This can be Alice and/or all re-suppliers in the system

This can be all customers in the system

This is no one, C cannot be a target for this threat

This is Alice

Targets

Attackers

	C	R	C & R	O	C & O	R & O	C, R & O
C							
R							
C & R							
O							
C & O							
R & O							
C, R & O							
E							
C & E							
R & E							
C, R & E							
O & E							
C, O & E							
R, O & E							
C, R, O & E							

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

- Inside each cell list all strategies attackers may follow to attack the target parties.
- You may find the following broad strategies useful while doing that:
  - **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 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.**
  - **Merge threats that have the same effect together.**
- Lastly, list a brief description of the distilled threats resulted from reduction.

Target → Attacker ↡	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer							
External							
Customer and External							
Re-supplier							
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner							
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge
(.): threat

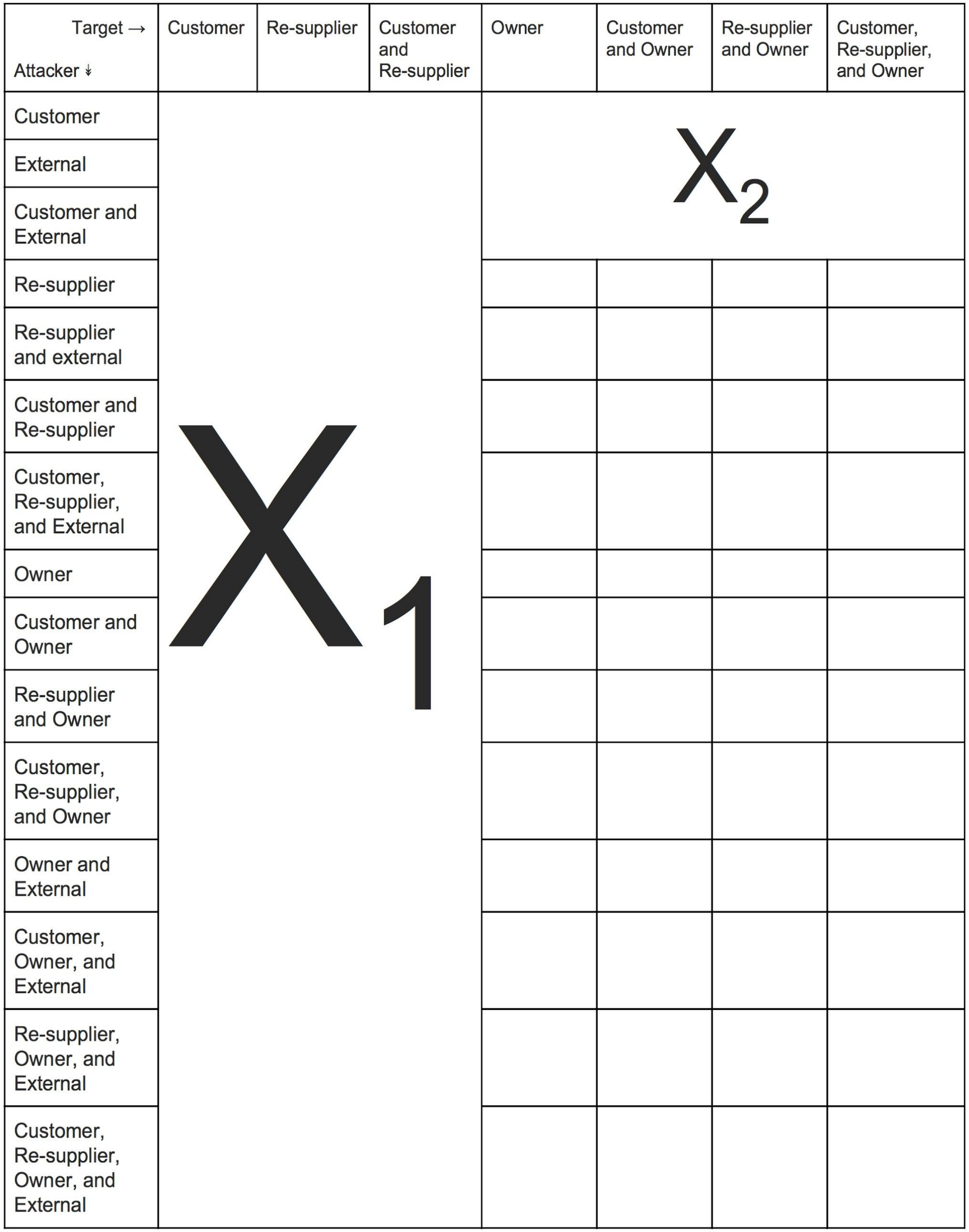
Running Example Application

Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1						
External							
Customer and External							
Re-supplier							
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner							
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Threat: ***Slacking off from re-supplying***.

X: cross out, **M**: merge
(.): threat

X_1: Cannot be targets, only the owner can be a target in this threat.



Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier							
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner							
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge
(.): threat

X_2: Customer/external does not benefit from the attack, will not attack.

Running Example Application

Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier						X_3	
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner							
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Threat: ***Slacking off from re-supplying****.*

X: cross out, **M**: merge

(.): threat

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.

Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier						X_3	
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner				X_4			
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

Threat: ***Slacking off from re-supplying****.*

X: cross out, **M**: merge
(.): threat

X_4: The owner will not attack itself , we have a single owner of the vender machine.

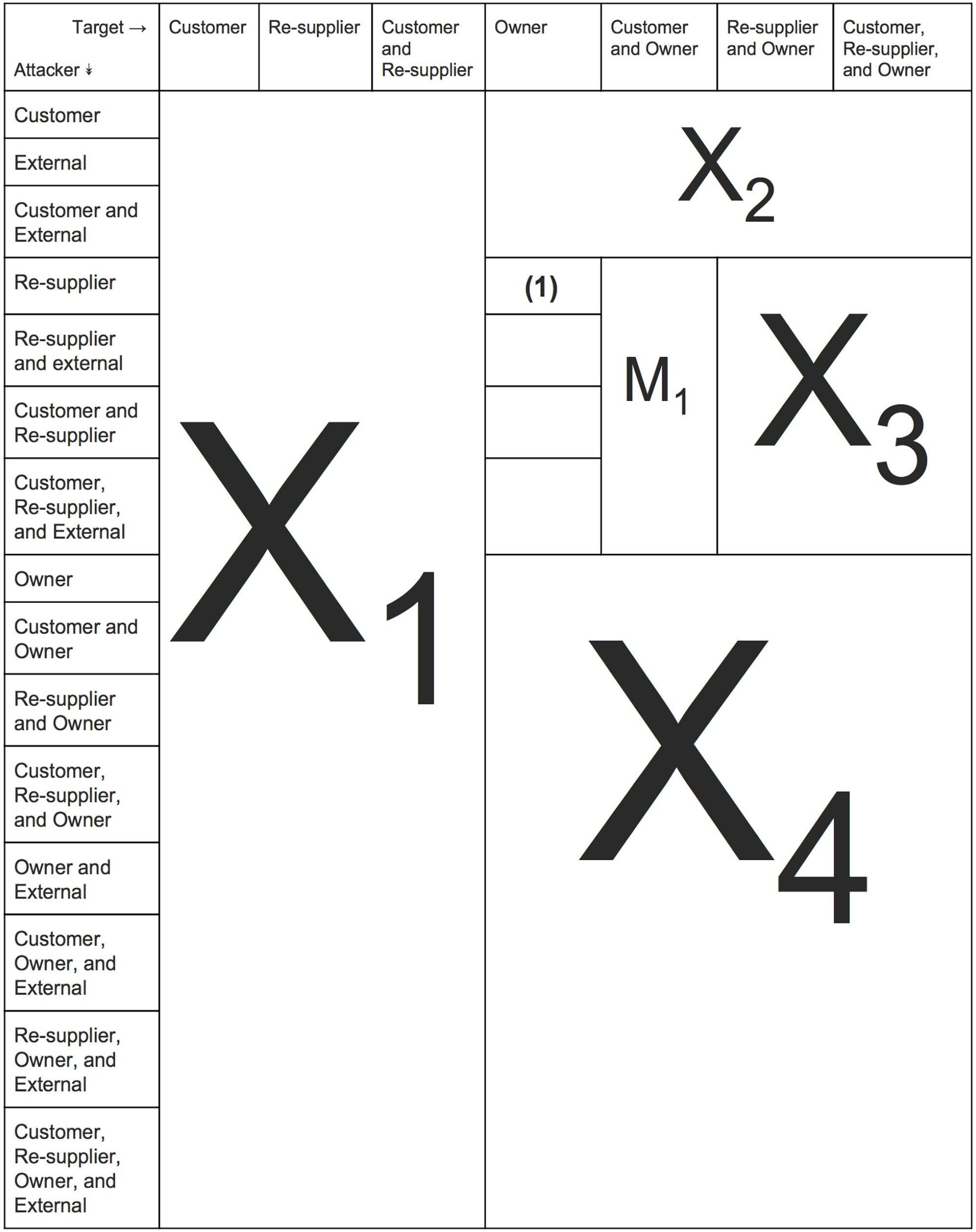
<table>
<tr><th>Target →
Attacker ↓</th><th>Customer</th><th>Re-supplier</th><th>Customer and Re-supplier</th><th>Owner</th><th>Customer and Owner</th><th>Re-supplier and Owner</th><th>Customer, Re-supplier, and Owner</th></tr>
<tr><td>Customer</td><td rowspan="16" colspan="3">X_1</td><td rowspan="3" colspan="4">X_2</td></tr>
<tr><td>External</td></tr>
<tr><td>Customer and External</td></tr>
<tr><td>Re-supplier</td><td></td><td rowspan="4">M_1</td><td rowspan="4" colspan="2">X_3</td></tr>
<tr><td>Re-supplier and external</td><td></td></tr>
<tr><td>Customer and Re-supplier</td><td></td></tr>
<tr><td>Customer, Re-supplier, and External</td><td></td></tr>
<tr><td>Owner</td><td rowspan="9" colspan="4">X_4</td></tr>
<tr><td>Customer and Owner</td></tr>
<tr><td>Re-supplier and Owner</td></tr>
<tr><td>Customer, Re-supplier, and Owner</td></tr>
<tr><td>Owner and External</td></tr>
<tr><td>Customer, Owner, and External</td></tr>
<tr><td>Re-supplier, Owner, and External</td></tr>
<tr><td>Customer, Re-supplier, Owner, and External</td></tr>
</table>

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge
(.): threat

M_1: Just like attacking the owner alone, customers cannot be targets.
Merge with Owner column.



Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier				**(1)**	M_1	X_3	
Re-supplier and external							
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner				X_4			
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge

(.): threat

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

Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier				**(1)**	M_1	X_3	
Re-supplier and external				M_2			
Customer and Re-supplier							
Customer, Re-supplier, and External							
Owner				X_4			
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge

(.): threat

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).**

<table>
<tr><th>Target →
Attacker ↡</th><th>Customer</th><th>Re-supplier</th><th>Customer and Re-supplier</th><th>Owner</th><th>Customer and Owner</th><th>Re-supplier and Owner</th><th>Customer, Re-supplier, and Owner</th></tr>
<tr><td>Customer</td><td colspan="3" rowspan="15">X_1</td><td colspan="4" rowspan="3">X_2</td></tr>
<tr><td>External</td></tr>
<tr><td>Customer and External</td></tr>
<tr><td>Re-supplier</td><td><b>(1)</b></td><td rowspan="4">M_1</td><td colspan="2" rowspan="4">X_3</td></tr>
<tr><td>Re-supplier and external</td><td>M_2</td></tr>
<tr><td>Customer and Re-supplier</td><td><b>(2)</b></td></tr>
<tr><td>Customer, Re-supplier, and External</td><td></td></tr>
<tr><td>Owner</td><td colspan="4" rowspan="8">X_4</td></tr>
<tr><td>Customer and Owner</td></tr>
<tr><td>Re-supplier and Owner</td></tr>
<tr><td>Customer, Re-supplier, and Owner</td></tr>
<tr><td>Owner and External</td></tr>
<tr><td>Customer, Owner, and External</td></tr>
<tr><td>Re-supplier, Owner, and External</td></tr>
<tr><td>Customer, Re-supplier, Owner, and External</td></tr>
</table>

Running Example Application

*Threat: **Slacking off from re-supplying**.*

X: cross out, **M**: merge
(.): threat

(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.

Target → Attacker ↓	Customer	Re-supplier	Customer and Re-supplier	Owner	Customer and Owner	Re-supplier and Owner	Customer, Re-supplier, and Owner
Customer	X_1			X_2			
External							
Customer and External							
Re-supplier				**(1)**	M_1	X_3	
Re-supplier and external				M_2			
Customer and Re-supplier				**(2)**			
Customer, Re-supplier, and External				M_3			
Owner				X_4			
Customer and Owner							
Re-supplier and Owner							
Customer, Re-supplier, and Owner							
Owner and External							
Customer, Owner, and External							
Re-supplier, Owner, and External							
Customer, Re-supplier, Owner, and External							

Running Example Application

Threat: ***Slacking off from re-supplying****.*

X: cross out, **M**: merge
(.): threat

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).

Running Example Application

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.

NOTE

- Due to time constraints, you will be asked to examine only one threat in the study.

STOP AFTER STEP 2 AND ASK THE MONITOR TO HAND YOU THE REST OF THE STUDY THAT DETERMINES WHICH THREAT TO WORK ON.