
A thief having the motive to earn money, intercepts active session between Foodify and back-end system, gains access to the systems existing session, assumes the role of the user and copies customer personal data, due to a lack of session handling, causing a negation of confidentiality of the customer's personal data.

2.1. Context and Asset Model

Fig. 1. Context and Asset Model in Security Risk-Oriented BPMN
2.2. Security Risk Model

Fig. 2. Security Risk Model in Security Risk-Oriented BPMN
2.3. Security Countermeasure Model

Fig. 3. Security Countermeasure Model in Security Risk-Oriented BPMN

2.4. Limitations

With PBMN we couldn't explicitly express risk treatment decision and security control.
A thief (Cyber Criminal) with an intention to steal credit card information from the users in order to sell the credit card numbers on the dark web launches brute force attacks to user accounts and hacks the users who have simple passwords and usernames. Then steals the payment data from the system and sells the credit card information on the dark web.

**Threat Context and Asset Model**

![Diagram](image-url)

- **Users**
  - **Login Credentials**
  - **Credit Card Info**
- **Foodly App**
- **Orders**
- **Application Server**

**Fig. 4. Context and Asset Model in Security Risk-Aware Secure Tropos**
3.2. Security Risk Model

Fig. 5. Security Risk Model in Security Risk Aware Secure Tropos
3.3. Security Countermeasure Model

Fig. 6. Security Countermeasure Model in Security Risk-Aware Secure Tropos

3.4. Limitations

Business Asset and System stayed a bit unrelated. We could not show how attack affects those. Attack method was able to shown on integral part of the System Asset but not on business assets.
Vandal communicates with the component from outside the local domain in order to send an error message to the Foodify customer and interrupt the order input, which leads to the order to be uncompleted and reputational risk.

4.1. Context and Asset Model

Fig. 7: Context and Asset Model in Security Risk-Oriented Misuse Cases

- Customer
- Foodify worker
- Foodify
- Make order
- Submit order
- Transfer customer order
- Register order
- 'security criterion'
- Integrity of order
- Check customer's login and password
- "Confidentiality of submitted order"
A thief intercepts the communication between the customer and Foodify, reads the customer data submitted in the Food Order Frame and sends it to own server in order to earn money, while selling private personal data to third parties. This leads to customer personal data leakage and reputational risk.

### 5.1. Context and Asset Model

Fig. 10. Context and Asset Model in Mal-activities for Security Risk Management

### 5.2. Security Risk Model

Fig. 11. Security Risk Model in Mal-activities for Security Risk Management
5.3. Security Countermeasure Model

Fig. 12. Security Countermeasure Model in Mal-activities for Security Risk Management

5.4. Limitations

We couldn’t show risk treatment decision and business assets directly.