Payment Concentrator System Threat Model

Threat modeling serves as a basis for analysis and specification of security requirements. It implies understanding of system complexity and identification of potential threats. Identified threats are further analyzed according to their impact on system and manifestation probability. Then it is determined if mitigation actions are to be conducted.

Identification of resources of importance and access points

In this stage, resources of importance and system access points are identified. Access point is an interface which could be used to gain access to resources of importance by a potential attacker. Aside from these, it is important to define trust boundaries. Trust boundary describes the level of trust required to access certain system component. Resources of importance are shown in ***Table 1 Resources of importance***, trust boundaries in ***Table 2 User trust levels*** and system access points in ***Table 3 System access points***.

Resources of importance	
ID	**Name**
A1	User credentials
A2	Personal user info
A3	Database
A4	Database read access
A5	Payment Concentrator business logic
A6	Configuration files
A7	Retailer credentials

Table 1 Resources of importance

User trust levels	
ID	**Name**
TA1	Administrator
TA2	Application

Table 2 User trust levels

System access points		
ID	**Name**	**Trust levels**
EP1	Retailer registration page	TA1, TA2
EP2	HTTP port	TA1, TA2

Table 3 System access points

Data Flow Diagram

Data Flow Diagram is a way of decoupling system on a high level of abstraction. It is used for analyzing data flow through system components, which makes threat identification easier. Data Flow Diagram is given on ***Image 1 Data Flow Diagram of Payment Concentrator System***.

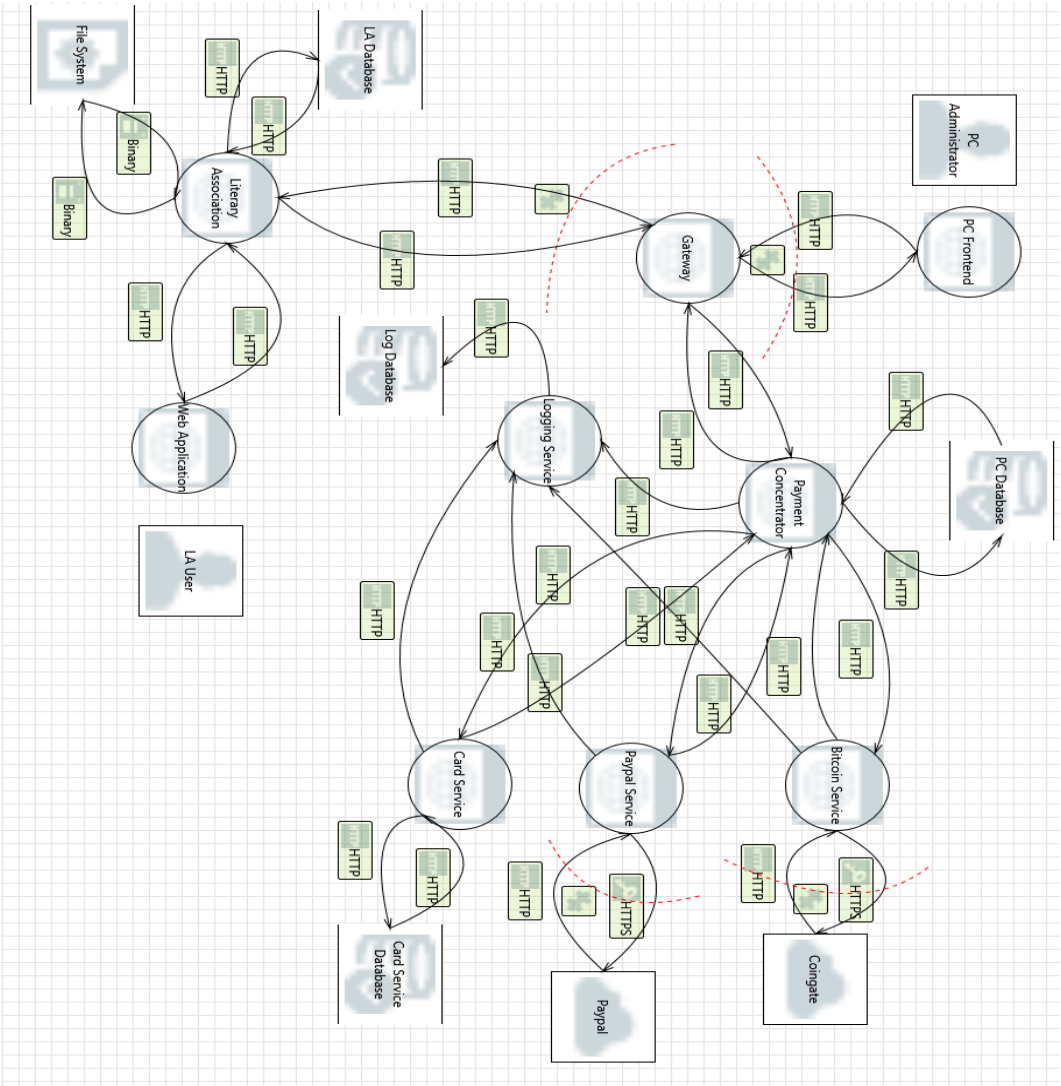

Image 1 Data Flow Diagram of Payment Concentrator System

Threat identification and risk assessment

For threat analysis STRIDE method is used. For every threat, apart from threat identifier and description, STRIDE threat type, impacts on system and occurrence probability are specified, as show in ***Table 4 Identified threats***. Next step is risk assessment for every identified threat. Risk is calculated by formula:

$$Risk = Probability\ of\ occurence * System\ impact$$

Risk categorization can be achieved through following matrix view of this formula, shown on ***Image 2 Risk matrix***. Risk categories are shown in ***Table 5 Assessed risks***.

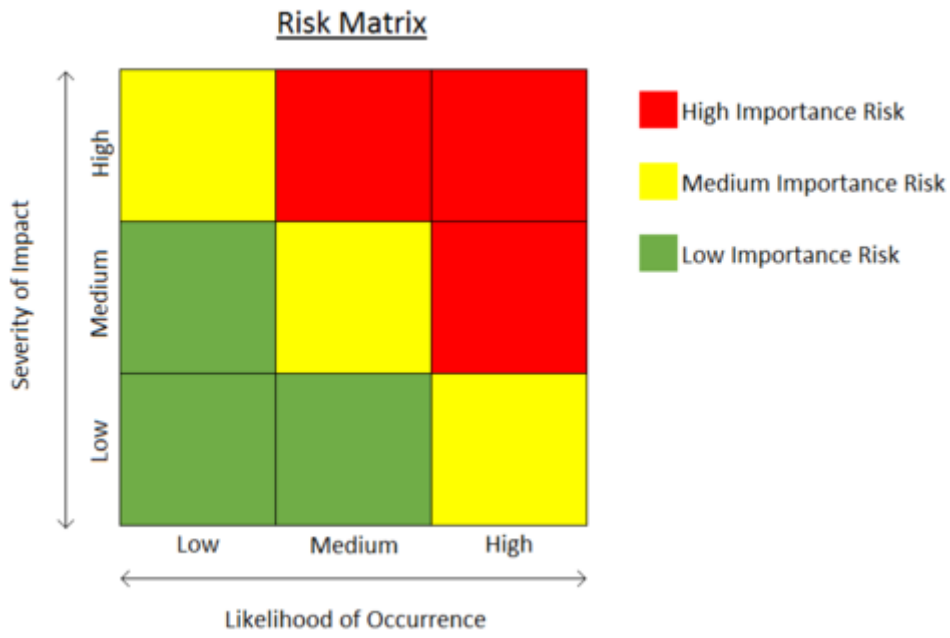

Image 2 Risk matrix

	Threats			
ID	**Description**	**STRIDE**	**System impact**	**Probability**
T1	Identity loss	S	L	H
T2	Identity theft	S	H	M
T3	Compromising user data	S	H	L
T4	Impersonation	S	H	M
T5	Unauthorized data access	T	H	L
T6	Replay attack	I	M	M
T7	Log forging	R	L	L
T8	DOS	D	M	L

Table 4 Identified threats

Risk assessment	
Threat ID	**Risk**
T1	Medium
T2	High
T3	Medium
T4	High
T5	Medium
T6	Medium
T7	Low
T8	Medium

Table 5 Assessed risks