МОДЕЛ ПРЕТЊИ

Моделовање претњи служи као основа за анализу и спецификацију безбедносних захтева. Оно подразумева разумевање комплексности система и идентификацију могућих претњи за систем. Идентификоване претње се даље анализирају на основу нивоа утицаја на систем и могућности појављивања и одлучује се да ли се предузимају контрамере за ту претњу или се прихвата ризик који она носи по систем.

Како би се обавио процес моделовања претњи система за плаћање, углавном су се пратили следећи кораци:

1. идентификовани су ресурси од значаја у систему,
2. идентификовани су нивои поверења у систему,
3. идентификоване су улазне тачке у систем,
4. креирани су дијаграми тока података,
5. идентификоване су потенцијалне претње,
6. одређен је ризик који свака претња носи,
7. наведене су контрамере.

1. Идентификација ресурса од значаја и приступних тачака

У овом кораку идентификују се ресурси од значаја и приступне тачке система. Идентификација ресурса од значаја је веома битан део моделовања претњи, јер ресурси есенцијално представљају мете одређених претњи. Приступна тачка (енгл. *access/entry point*) је интерфејс преко којег потенцијални нападач може да ступи у интеракцију са системом и добије приступ ресурсима од значаја. Поред тога, битно је дефинисати границе поверења (енгл. *trust boundaries*). Граница поверења је граница изван које постоје разни нивои поверења. Нивои поверења описују колико поверења је потребно како би се приступило компоненти система. У табели 4.1. приказани су ресурси од значаја за систем, а у табели 4.2. дефинисани су нивои поверења.

Ресурси од значаја		
ID	Назив	Опис
A1	Креденцијали корисника	Креденцијали за пријаву на систем које користи корисник када се пријављује.
A2	Персонални подаци везани за корисника	Апликација чува неке податке о корисницима. Ти подаци укључују име корисника, идентификатор корисника, адреса, итд.
A3	Подаци о платним трансакцијама	Апликација чува податке о трансакцијама за различите врсте плаћања. Ти подаци укључују токен корисника за плаћање путем *Bitcoin*, информације о клијенту за плаћање путем *PayPal*, информације о платној картици итд.
A4	База података	База података која садржи све податке које систем користи.
A5	Могућност читања базе података	Могућност повезивања са базом података, слања упита и читања података.
A6	Бизнис логика система за плаћање	Све функционалности које главна апликација (*Payment Concentrator*) омогућава.
A7	Складишни простор датотека	Сви документи генерисани од стране система.
A8	Репозиторијуми за складиштење сертификата (енгл. *keystore*, *truststore*)	Садрже сертификате одговарајућих сервиса и сертификате других сервиса којима се верује.
A9	Конфигурационе датотеке	Датотеке са информацијама о конфигурацији компонената система.

Табела 4.1. *Идентификовани ресурси од значаја*

Следећи корак је идентификовати нивое поверења корисника система. Нивои поверења представљају права приступа додељена корисницима.

Нивои поверења корисника система		
ID	Назив	Опис
TA1	Нерегистровани корисник	Корисник који нема могућност пријаве на систем, ни регистрације. Он има могућност одабира начина плаћања.
TA2	Регистровани корисник - Продавац	Крајњи корисник који је познат систему, има креденцијале за логовање и има приступ одређеним клијентским акцијама, као што су одабир начина плаћања, креирање плана за плаћање (енгл. *Billing Plan*).
TA3	Администратор	Корисник који има право да додаје нову апликацију и за њу бира начине плаћања.

Табела 4.2. *Нивои поверења*

Генерално, претње могу да потекну од два примарна извора: интерног чиниоца (корисник који има ауторизован приступ) и екстерног чиниоца (неко ко нема ауторизован приступ). Заштита од интерних чинилаца је много изазовнија него заштита од екстерних чинилаца, јер интерни чиниоци имају легитиман приступ ресурсима од значаја.

Затим се идентификују улазне тачке за систем. Оне су приказане у табели 4.3.

Улазне тачке система			
ID	Назив	Опис	Нивои поверења
EP1	Страница за пријаву на систем	Страница преко које се регистровани корисници пријављују на систем.	TA2, TA3
EP2	Форме за унос параметара за плаћање	Форме приказане само пријављеним корисницима апликације које имају поља за унос одговарајућих параметара за плаћање.	TA2

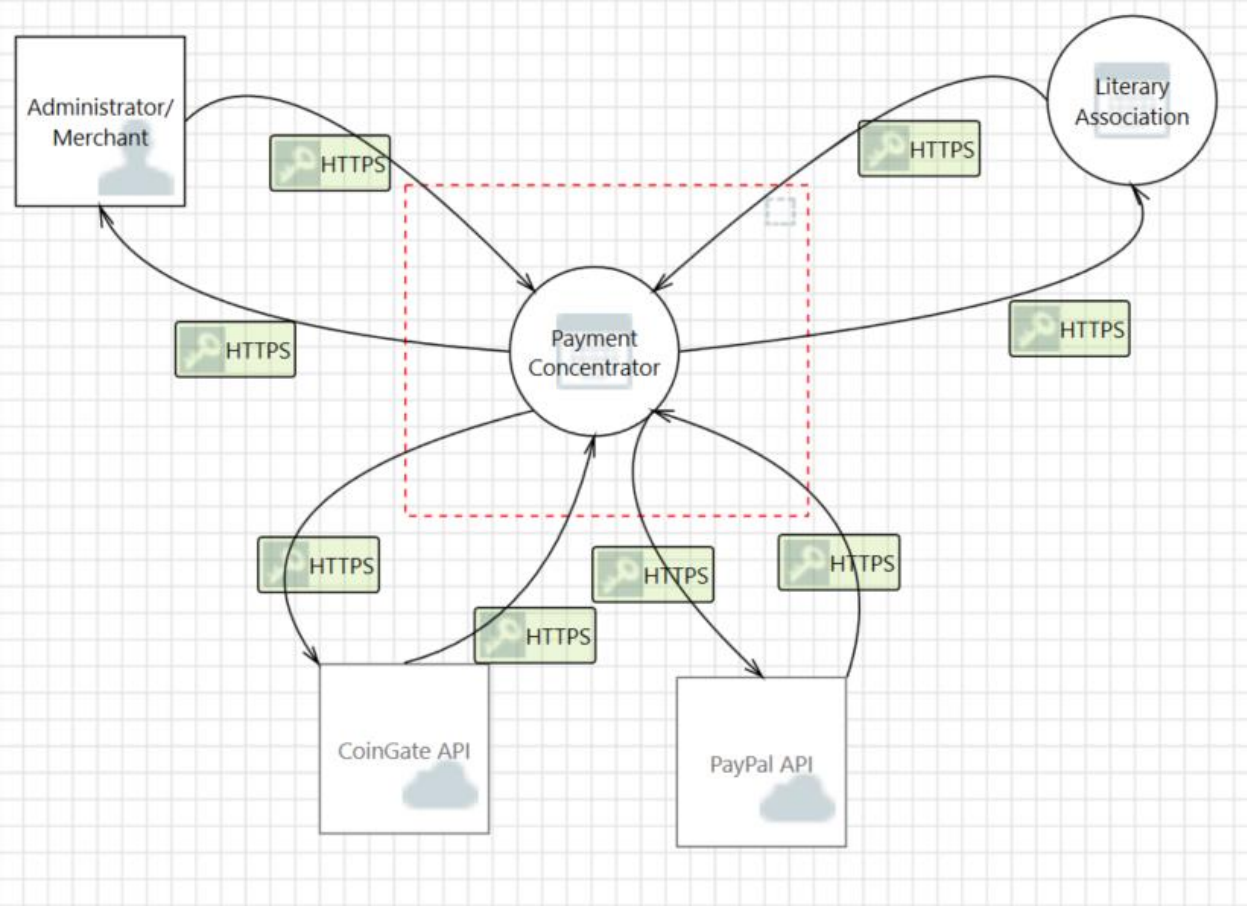
EP3	*HTTP* порт	Комуникациони канал коришћен од стране свих типова корисника	TA1, TA2, TA3
EP4	Фајл систем	Систем за плаћање је веб апликација која се ослања на фајл систем када је у питању чување одређених фајлова у фајл систему, као што су *log* фајлови.	/

Табела 4.3. *Улази у систем*

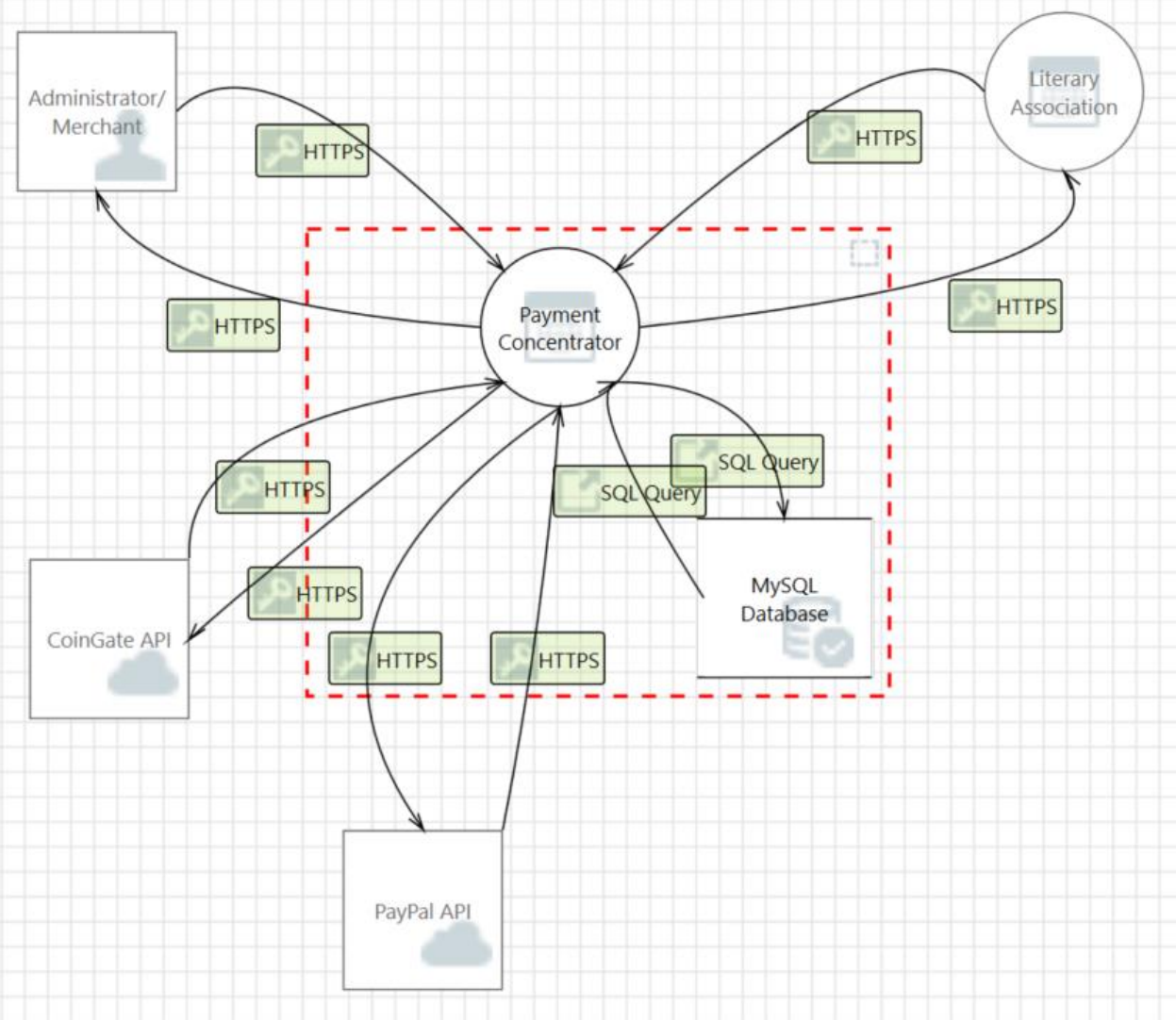
2. Дијаграм тока података

Дијаграм тока података (енгл. *Data Flow Diagram*, скр. *DFD*) представља начин декомпоновања система на високом нивоу и анализира ток података кроз компоненте у систему. Олакшава идентификовање претњи, олакшава праћење и анализу података нападача и команди кроз систем и олакшава идентификацију који ресурси од значаја су у интеракцији са њим.

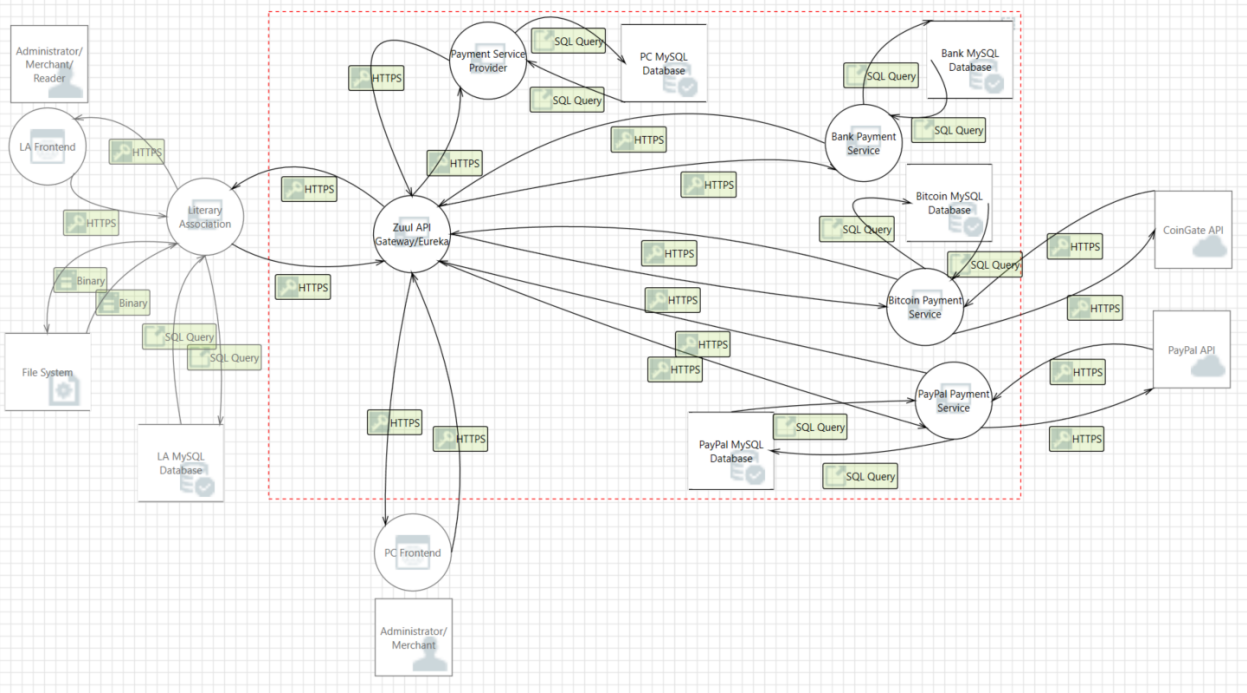
Како би *DFD* био транспарентнији, могуће је креирати више нивоа *DFD* дијаграма. *DFD*-ови на високим нивоима су мање детаљни (више детаља се агрегира у нижим нивоима). Контекстуални *DFD* је највиши у хијерархији, па затим иде *DFD* нултог нивоа и садржи најважније (агрегиране) функције система, па *DFD* првог нивоа итд. Број нивоа зависи од величине модела система. У тексту ће бити приказани концептуални дијаграм тока података, *DFD* нултог нивоа и *DFD* вишег нивоа за систем за плаћање. Они су креирани користећи *Microsoft Threat Modeling Tool 2016* и приказани су на сликама 4.1, 4.2 и 4.3. Овај алат је такође изгенерисао извештај који ће бити посебно приложен, а који је помогао при идентификацији претњи.



Слика 4.1. *Концептуални DFD система за плаћање*



Слика 4.2. *DFD нултог нивоа система за плаћање*



Слика 4.3. *DFD вишег нивоа за систем плаћања*

3. Идентификација претњи и анализа ризика

У овом делу потребно је идентификовати и документовати претње које би могле да утичу на систем и компромитују ресурсе од значаја. Да би се претње описале, узели су се у обзир не само ресурси од значаја него и потенцијални циљеви нападача. За процес идентификације претњи користила се *STRIDE* метода, због тога је издвојена посебна колона у табели 4.3. која даје информацију о томе на коју од познатих *STRIDE* претњи се издвојена претња односи.

STRIDE процењује дизајн детаља система. Моделује систем у контексту употребе. Користи се изградњом дијаграма тока података (енгл. *data-flow diagrams*, скр. DFDs) како би идентификовао ентитете, догађаје и границе у систему. *STRIDE* примењује колекцију познатих претњи, чија почетна слова формирају име ове методе:

- **S**poofing – претварање нападача да је неко други или нешто друго што није,
- **T**ampering – измена података на диску, мрежи, у меморији или било где другде,
- **R**epudiation – нападач тврди да није урадио нешто или да није одговоран за нешто, што може бити истина или не,
- **I**nformation disclosure – пружити информације некоме ко није ауторизован да им приступи,
- **D**enial of service – укидање приступа сервису или подацима,
- **E**levation of privilege – дозвола да неко изврши операцију за коју није ауторизован.

Такође, поред описа и идентификатора претње наведено је какав утицај та претња има на систем. Утицај се мери коришћењем три вредности: *High (H* –велики утицај на систем*), Medium (M* - мањи утицај на систем*), Low (L* – јако мали утицај на систем*).* Претње су у табели описане тако да наглашени део описује претњу, а након тога следи опис напада на систем. Последња колона у табели представља вероватноћу појављивања одговарајуће претње и такође има вредности: *High (H* – велика вероватноћа да ће се претња појавити*), Medium (M* - мања вероватноћа да ће се претња појавити*), Low (L* – јако мала вероватноћа да ће се претња појавити*).* У табели 4.4. приказане су идентификоване претње системаза плаћање.

Претње				
ID	Опис	*STRIDE*	Утицај на систем	Вероватноћа појављивања
T1	**Губитак идентитета:** Корисник остави своје креденцијале на јавном месту или их подели са неким	S	L	H
T2	**Крађа или злоупотреба идентитета:** Администратор злоупотребљава идентитет осталих корисника у сврху обављања малициозних радњи	S	M	M
T3	**Компромитовање личних података корисника:** Екстерни чинилац долази до свих корисничких података – креденцијали, лични подаци	S	H	H
T4	**Лажно представљање:** Нападач краде *JWT* и лажно се представља као пријављени корисник.	S	H	L
T5	**Лажно представљање:** Нападач зна *email* регистрованог корисника и врши *brute force* напад како би дошао до лозинке тог корисника	S	H	H
T6	**Компромитовање личних података корисника:** *SQL Injection*	S	H	H

T7	**Компромитовање личних података корисника:** Нападач открива лозинку жртве прочитану из базе података	S	H	L
T8	**Компромитовање личних података корисника:** Вршење CSRF (енгл.. *Cross-Site Request Forgery)* напада	S	M	M
T9	**Неауторизовано откривање података:** Преко мреже, користећи портове, нападач приступа машини корисника на којој је покренута апликација	T	M	M
T10	**Неауторизовано откривање података:** Корисник ненамерно приступа поверљивим подацима преко малвера који је инсталиран на његовој машини (T6)	I	L	M
T11	**Неауторизован приступ:** Нападач приступа функционалностима за чије коришћење није ауторизован	I	M	M
T12	**Неауторизован приступ:** Преко *injection* напада, нападач заобилази ауторизацију	I	M	L
T13	**Неауторизован приступ:** Корисник са мање привилегија намерно или случајно приступа функционалностима изван својих привилегија	E	L	L
T14	**Нарушавање доступности сервиса:** Вршење DOS (енгл. Denial of Service) напада	D	M	M
T15	**Напад на непорецивост:** Нападач приступа *log* фајловима и мења их у своју корист	R	L	L
T16	**Напад на поверљивост и интегритет:** Вршење *Replay* напада	I	H	M
T17	**Компромитовање података платних трансакција:** Екстерни чинилац долази до свих	S	H	M

	корисничких података – креденцијали, лични подаци			
T18	**Неауторизовано откривање података платних трансакција:** Преко мреже, користећи портове, нападач приступа машини корисника на којој је покренута апликација и открива информације попут *PAN* броја	I	H	M

Табела 4.4. *Претње система за плаћање*

Након идентификације претњи, следећи корак је одређивање ризика који та претња носи. Рачунање ризика, као што је поменуто у поглављу 2, се врши на начин приказан изразом:

Ризик = Вероватноћа појављивања * Утицај на систем

Матрични приказ ове формуле као и резултати множења свих комбинација дати су на слици 4.3. и ова матрица се користила како би се израчунао ризик сваке од претњи. Вредности за утицај на систем и вероватноћу појављивања за сваку претњу читају се из табеле 4.3.

У табели 4.5. наведене су претње путем идентификатора из табеле 4.4. и ризици које те претње носе. Највећи ризик је *High, Medium* је мањи ризик, а *Low* најмањи. Приликом отклањања рањивости и имплементације безбедносних механизама прво се обратила пажња на оне претње које носе највећи ризик, затим мањи, и на крају најмањи.

Uticaj / Ver.	L	M	H
L	Low	Low	Medium
M	Low	Medium	High
H	Medium	High	High

Слика 4.3. *Рачунање ризика претњи*

ID претње	Ризик
T1	Medium
T2	Medium
T3	High
T4	Medium
T5	High
T6	High
T7	Medium
T8	Medium
T9	Medium
T10	Low
T11	Medium
T12	Low
T13	Low
T14	Medium

T15	Low
T16	High
T17	High
T18	High

Табела 4.5. *Израчунат ризик за сваку претњу*

4. Идентификација контрамера

- ***HTTS*** – обезбеђена је сигурна комуникација између апликација, којом се шаљу шифровани подаци.
- ***Logging*** – имплементиран механизам за праћење свих догађаја у систему. За сваки догађај се чувај информације о типу и времену, као и порука која је битна за праћење активности на систему.
- **Аутентификација и ауторизација** – имплементиран је механизам за контролу приступа заснован на корисничким улогама и дозволама везаним за сваку улогу - *RBAC*.
- **Енкриптовање података** – осетљиви подаци (кориснички креденцијали, *Card Holder Data*) у бази се чувају у људски нечитљивом облику.
- **Валидација података** – заштита од нежељених ризика попут *XSS*.
- **Параметризовани *query***- заштита од нежељених ризика попут *SQL injection*.