**Анотация**

**Тема: Предсказване на заплахи за сигурността на софтуерни системи**

**Име на дипломанта: Димитър Петров Джонджоров**

**Научен ръководител: доц. д-р Александър Димов, Катедра Софтуерни технологии**

**Дата на защита: 30.05.2015 г.**

Софтуерна сигурност представлява част от изискванията към дадено приложение, която отговаря за запазването на целостта и поверителността на информацията с която то работи, както и на неговите модули. Темата за софтуерната сигурност е все по актуална в наши дни, особено с нарастващият брой атаки (или още – нападения) към различни онлайн системи в последните години.

Макар и нападенията над онлайн системите да стават все по-разнообразни и сложни, се забелязва тенденция няколко типа да преобладават като най-голям брой успешни атаки. За последните 5 години първото място сред атаките е заето от тези от тип инжекция и в частност SQL инжекция. При нея наблюдаваме изменяне на данните, изпратени до сървърната част чрез заявка, така че при динамичното създаване на SQL заявка на сървъра те да станат част от нея. След това заявката се изпълнява и ако дадената система не е защитена атакуващият може да достигне до поверителна информация, да открадне самоличността на потребител на системата, а понякога дори и да и навреди. Възможно е да се стигне дори до изтриване на цели бази данни. Има много архитектурни и реални подходи за предотвратяването на тези атаки от тип SQL инжекция, но те не разграничават различните типове. Затова една стъпка по-напред би било разпознаване на слепите атаки от тип SQL инжекция. По този начин ще можем да определим дали даден потребител има голяма вероятност да извърши подобна атака и евентуално да му се ограничи достъпа до информацията.

В рамките на тази дипломна работа е направен анализ на областта на софтуерната сигурност и по-конкретно различните видове атаки към нея. Разгледани и класифицирани са видовете нападения от тип SQL инжекция. Една от очевидните аномалии в потребителското поведение е сляпата SQL инжекция, защото именно нея използва даден атакуващ за да установи вида на базата данни спрямо която ще извърши нападения. Затова ние ще се фокусираме върху откриването на този тип аномалии, за да предскажем атаки от тип SQL инжекция. В дипломната работа още са представени съществуващите архитектурни подходи за предотвратяване на атаките от този тип, разгледани са два от съществуващите алгоритми за превенция на атаките от тип SQL инжекция и е направен сравнителен анализ и откриване на силните и слабите страни на описаните алгоритми.

На базата на единия алгоритъм и на резултатите от анализа е създаден друг такъв, чиито основни качества са сравнително бързо изпълнение и разграничаване на атаките от тип сляпа SQL инжекция. Направен е и сравнителен анализ на вече трите разгледани алгоритъма. Чрез реализацията на специализиран тестов инструмент, се демонстрира работата на създадения в дипломната работа алгоритъм и е показано, че той изпълнява условията за бързина и разпознаване на съответните аномалии. Накрая е реализиран и изпълнен тестов сценарий, който се състои и от реализирания в дипломната работа инструмент и клиентско приложение, което да симулира заявки от различни потребители и IP адреси към него.

Като предстояща работа по темата бихме посочили анализ и на други типове аномалии в потребителското поведение. Също така бъдещо развитие на дипломната работа е и предсказването и на други типове атаки, като например междусайтово скриптиране, несигурна директна референция и атаки за отказване на достъп, които заемат следващите места по брой атаки, извършени успешно през последните години.