ФК 78-НС1-033
05.03.2019

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ
НАУЧНО ЖУРИ
СОФИЯ

СТАНОВИЩЕ

относно дисертационен труд за придобиване на образователна и научна степен „**доктор**"

Автор на дисертационния труд: **инж. Шайк Джейвид Рашийд**

Тема на дисертационния труд: "**СИГУРНИ И ЕФЕКТИВНИ МЕТОДИ БАЗИРАНИ НА КРИПТОГРАФИЯТА С ЕЛИПТИЧНИ КРИВИ ЗА ЗАЩИТА НА ТРАНЗАКЦИИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ**"

Член на научното жури: **проф. д-р Георги Илиев**

1. Научна новост и актуалност на разработвания в дисертационния труд проблем.

Актуалността в тази дисертация е свързана с предлагането на нови протоколи и техники за подобряване на сигурността на приложенията за електронна търговия чрез осигуряване на механизми за автентикация и оторизация. Анализът на различни елиптични криви се извършва, за да се установи подходящата крива за реализация на ECC в приложенията за електронна търговия с ограничени ресурси. Трудът също така предлага усъвършенстван протокол за автентикация на потребител на базата на смарт карта, който може да осигури сигурен достъп до отдалечен сървър. Надеждната и усъвършенствана техника за откриване на DoS атаки е разработена и изследвана в мрежа за електронна търговия. Техниката е разработена за откриване на DoS атаки в транзакциите за електронна търговия, като се използва предложения GSO-SVNN класификатор. Предложеният класификатор е проектиран чрез модифициране на SVNN чрез алгоритъм GSO и дава най-добри резултати в сравнение с други подобни техники.

2. Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд

Основната цел на дисертационния труд е да се разработи и развие сигурен и надежден механизъм за автентикация, който да се използва в приложенията за електронна търговия с ограничени ресурси и да се проектира сигурна и надеждна техника за оторизация за защита на транзакциите при електронна търговия от атаки DoS.

Методологията на изследване в дисертацията включва използването на цифрови и симулационни подходи. Предложеният нов модел за сигурност използва ECC като криптографски алгоритъм. Анализът на ефективността на стандартните елиптични криви е полезен, за да се определи подходящата крива за използването на ECC в приложенията за електронна търговия с ограничени ресурси.

3. Приноси в дисертационния труд.

По мое мнение основните приноси са:

1. Създаден е нов модел за защита на системата за електронна търговия, използващ ECC, който има по-голямо бързодействие, изисква по-малко памет и има по-малък размер на ключа в сравнение със съществуващите модели за сигурност, които използват алгоритъма RSA.

2. Извършен е анализ на различни налични елиптични криви, за да се установи коя крива е подходяща за приложения за електронна търговия с ограничени ресурси.

3. Предложен е усъвършенстван и ефективен потребителски протокол за автентикация, използващ ECC. Протоколът се използва за валидиране на легитимен потребител.

4. Разработена е процедура за регистрация и автентикация между потребителя и сървъра, при която са развити четири различни нива на проверка.

5. Разработен е мощен механизъм за откриване на DoS атаки, който използва GSO-SVNN за защита на електронните търговски транзакции.

4. Преценка на публикациите по дисертационния труд.

По темата на дисертационния труд са направени 7 публикации, от които 5 доклада на международни научни конференции и 2 статии в научни списания. Една от публикациите са самостоятелни. Публикациите отразяват съществени моменти от дисертационния труд.

5. Препоръки и критични бележки.

Бих препоръчал на дисертанта да продължи работата си в избраната научна област, като положи усилия за още по-широкото разпространение и приложение на резултатите от дисертационния труд в практиката.

6. Заключение

Въз основа на изложеното считам, че дисертационният труд отговаря на изискванията на Закона за развитие на академичния състав в Република България и Правилника за неговото приложение и има необходимите качества, за да се присъди на неговия автор, маг. инж. Шайк Джейвид Рашийд, научната и образователна степен „доктор".

05.03.2019 г. Член на научното жури:

София (проф. д-р Георги Илиев)