Катедри за рачунарство и информатику
Математичког факултета
Универзитета у Београду

Извештај о прегледу мастер рада Бранка Поповића

Одлуком Катедре за рачунарство и информатику и Наставно-научног већа Математичког факултета (на Седници ННВ одржаној 18.03.2016.) именовани смо за чланове Комисије за преглед и одбрану мастер рада

Реализација омотача за OpenSSL библиотеку у програмском језику Свифт

кандидата Бранка Поповића, студента мастер академских студија Математичког факултета Универзитета у Београду.

У раду се предлаже креирање омотача око OpenSSL библиотеке у програмском језику Свифт и разматра какву би функционалност требао да има такав омотач. Наиме, коришћењем могућности које пружа скуп алата OpenSSL, могу елегантно да се реше различити проблеми безбедности међуплатформске комуникације који се јављају у реалним ситуацијама. Да би се ово постигло на Apple платформи, потребно је Свифт-програмеру обезбедити једноставан и лак рад са OpenSSL библиотеком.

У оквиру рада на тези дизајнирана је и развијена, као софтвер отвореног кода у програмском језику Свифт, прва итерација омотача за библиотеку OpenSSL. Ова апликација је доступна у репозиторијуму GitHub na адреси https://github.com/thebrankoo/CryptoLab, а такође и на адреси https://github.com/vladofilipovic/MasterMatfBrankoPopovic.

Рад чини осам поглавља (Увод, Програмски језик Свифт, Преглед функционалности CryptoLab омотача, Постојећа решења, Преглед архитектуре, Примери употребе, Систем отвореног кода и његова употреба, Закључак) иза којих следи списак коришћене литературе.

Прво поглавље је уводног типа и у њему се описује тема овог мастер рада, мотивација за избор теме и циљеви који су постављени.

У другом поглављу се даје опис програмског језика Свифт, концепта протокола и реализације тог концепта у програмском језику Свифт.

Поглавље која потом следи садржи преглед функционалности CryptoLab омотача, што обухвата хеш функције, шифровање, аутентификацију порука и размену кључева.

Четврто поглавље садржи опис постојећих решења: омотача за библиотеку OpenSSL, као и њихових карактеристика.

Пето поглаље се односи на архитектуру развијеног омотача. У опису се полази од образаца за пројектоавње до њихове конкретне имплементације, при чему су важнији делови омотача описани са већим степеном детаљности.

Шесто поглавље се односи на примере употребе, где су приказани примери употребе за шифровање и дешифровање (RSA, Blowfish, AES), за рачунање хеш кодова, за аутентификацију порука (RSA, DSA), за HMAC код и за Diffie–Hellman размену кључева.

Седмо поглавље се бави употребом система отвореног кода, а осмо поглавље садржи закључна разматрања.

Литература садржи списак од 17 коришћених референци. Рад садржи укупно 51 страну.

Мастер рад садржи квалитетан приказ релевантних појмова, техника и радова из домена развоја софтвера, који су пажљиво илустровати погодним примерима.

Закључак

Увидом у финални текст мастер рада дошли смо до закључка да је рад квалитетно написан, да је кандидат јасно приказао изложену проблематику од основних појмова, до њихове креативне и технолошке примене. Рад „Реализација омотача за OpenSSL библиотеку у програмском језику Свифт“ у потпуности задовољава захтеве који се постављају у изради мастер рада и предлажемо да се одобри његова јавна одбрана.

др Владимир Филиповић, ванр. проф

др Душан Тошић, ред. проф

др Саша Малков, ванр. проф