Рецензия

Върху дисертационен труд за придобиване на образователната и научна степен "доктор ".
Автор на дисертационния труд: маг. Ивелина Миткова Вардева
Тема на дисертационния труд: Модели на процеси в мрежова сигурност чрез обобщени мрежи
Рецензент: Людмил Георгиев Даковски, проф., д.т.н., Европейски политехничеки университет

Представеният ми за рецензиране дисертационен труд съдържа около 111 страници текст, 6 страници с 107 заглавия цитирана литература, списък с фигури и съкращения.

Дисертационният труд е посветен на твърде съществената особено в приложно отношение проблематика за сигурността на интернет пространството.

Авторката познава много добре съвременните публикации по изследваната проблематика (особено в областта на обобщените мрежи), правилно ползува резултатите на другите автори при постановката и анализа на проблемите, които си поставя за решаване, но не винаги съпоставя своите постижения с постигнатите от други автори решения.

Основната решавана в дисертацията задача е да се изследват протичащите в компютърните мрежи информационни процеси и мрежовата сигурност. Идеята е да се проследят и анализират тези процеси, както и изграждането на мрежови връзки между различни организации, от гледна точка на възможните атаки и от там целта да се повиши сигурността в мрежата. Донякъде задачата е ограничена до обмен на медицинска информация между болнични заведения. Като основен апарат за моделиране и анализ са използувани Обобщените мрежи.

Основната задача е декомпозирана правилно на следните подзадачи (донякъде цитирам):

Разработване на обобщено-мрежови модели за видовете атаки в компютърната мрежа.

Детайлизиране на моделите.

Разработване на обобщено-мрежови модели на изграждане на сигурни връзки при предаване на медицинска информация.

Построяване на симулационен модел, който оценява степента на атакуваните съобщения в мрежата.

Накратко подбраната методиката се състои в формулиране на задачата, създаването на подходящ ОМ-модел, детайлизиране на възможни оразмерявания на модела, реализация на решението и негови варианти чрез подходящи средства и тестване с подходящи примери. На редица места авторката коректно е изследвала създадените модели и е откроила препоръки за практиката. Методиката е коректна, има завършен вид и е предпоставка за валидността на получените резултати.

След една разходка из мрежовите модели в 16-те страници на първа глава авторката във втора глава описва варианти на мрежови атаки свързани с подслушване, прекъсване, промяна на информацията, както и скала за оценяване на мрежовата сигурност. Акцентът е върху основните методи за атакуване, за откриване на съответните атаки и методите за оценяването на вредите от тях.

В глава 3 са разработени пет обобщено мрежови модела: първият е основан върху концепцията за конвенционално криптиране чрез симетричен ключ; вторият - на SSL протокола; третият, при който към SSL се добавя изчисляване на интуиционистки размити оценки; четвъртият е изграден на базата на протоколи PPP и SSH; петият работи със сигурна „безпаролна връзка”.

В четвъртата глава са разработени два варианта на ОМ-модел за защита на е-данни на пациенти предавани между информационни болнични системи в обществената мрежа. Те могат да бъдат полезни при създаването и внедряването на специфични за здравеопазването софтуерни и хардуерни продукти, съобразени с интернационалните стандарти за обмен и защита на медицинските данни.

Последната глава естествено е посветена на тестване на модел на скала за оценяване на атакувани съобщения чрез интуиционистки размити вярностни стойности.

Приносите в дисертацията с научен характер се свеждат до обогатяване на теорията с разработените ОМ-модели, а приносите с научно-приложен характер представляват резултати от проведени експерименти с модели и получаването на потвърдителни факти за тяхното успешно функциониране.

Приносите в дисертацията синтезирано могат да се формулират по следния начин:

Разработени са обобщено мрежови модели на:

- мрежови атаки за подслушване и прекъсване на криптирани съобщения;
- мрежови атаки за модифициране и изфабрикуване на криптирани съобщения;
- скала за оценяване степента на атакуваните съобщения предавани по обществената мрежа;
- криптографска система с използване на симетричен ключ;
- затворен съединителен слой (secure socket layer) и на вариант с интуиционистки размити оценки;
- виртуална частна мрежа (virtual private network) от типа point-to-point върху secure shell и вариант за secure shell2 за изграждане на безпаролна vpn връзка;
- защита на е-данни на болнични пациенти.

Може да се приеме, че тези приноси поради новостта си имат научен характер. Проведеният тест на обобщено мрежови модел на скала за оценяване степента на атакуване на съобщения в обществената мрежа и получените реултати имат научно-приложен характер

Приносите са намерили разгласа сред научната общественост в 9 труда. Трудовете са публикувани както следва: 2 в списание Issue on Intuitionistic Fuzzy Sets and Generalized nets (Полша), 1 в „Доклади на БАН" (с импакт-фактор), 2 в тематични издания на Полската академия на науките, 2 в списания в България и 2 в сборници на научни конференции.

В 6 труда докторантката е самостоятелен автор, а останалите три имат още по 1 автор, от което следва значителна степен на самостоятелност на получените в дисертационния труд приноси.

Постиженията в дисертацията са отразени достатъчно пълно и точно в публикуваните трудове.

Има данни за 8 цитирания на 4 статии.

Авторефератът достатъчно пълно отразява направените в дисертацията приноси и е изготвен в съответствие с изискванията.

Направените забележки в предварителната рецензия са отразени достатъчно пълно (с изключение на някои прекалено дълги заглавия), а за някои редакционни и правописни пропуски не считам за необходимо да споменавам.

Заключение. Като вземам предвид направените в дисертационния труд безспорни научни и научно-приложни приноси, разгласата им сред научната общественост, както и практическата им полезност, считам, че дисертацията напълно покрива изискванията на закона за придобиване на образователната и научна степен "доктор" и подкрепям присъждането на тази степен на маг. **Ивелина Миткова Вардева**.

27.03.2012 г.
Рецензент: .....
(проф. Л.Даковски, д.т.н.)