Universitatea Tehnică a Moldovei

ELABORAREA INSTRUMENTELOR UTILIZATE LA MODELAREA PROTOCOALELOR CRIPTOGRAFICE PE BAZA PETRI NET

РАЗРАБОТКА СРЕДСТВ МОДЕЛИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Student:

Hîrbu Rima

Conducător:

conf.univ.dr. Pușneac Iurie

Chişinău - 2019

Ministerul Educației, Culturii si Cercetarii al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat „Securitatea informației în sisteme și rețele de comunicații”

Admis la susținere

Șef departament: dr. P. Nicolaev

„ _ ” _____ 2020

ELABORAREA INSTRUMENTELOR UTILIZATE LA MODELAREA PROTOCOALELOR CRIPTOGRAFICE PE BAZA PETRI NET

РАЗРАБОТКА СРЕДСТВ МОДЕЛИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Teză de master

Masterand: Hîrbu (Hîrbu Rima)

Conducător: (Pușneac Iurie)

Chișinău – 2019

REZUMAT

Lucrarea este dedicată elaborarii instrumentelor utilizate la modelarea protocoalelor criptografice pe baza rețelelor Petri.

A fost realizata analiza rețelelor Petri ca instrument de modelare și sa evaluat adecvarea utilizării lor pentru modelarea protocoalelor criptografice. S-a constatat că rețeaua Petri ca model permite reflectarea adecvată a logicii protocolului, luând în considerare parametrii legați de timp, identificând blocaje, demonstrând clar vulnerabilitățile și reconstruind rapid toate opțiunile posibile de executare a protocolului.

A fost elaborat un tip special de rețea Petri, care corespunde specificului protocoalelor criptografice. Sa propus o structură de fișiere de configurare care permite descrierea oricărei retele Petri de tipul respectiv și componentele sale individuale: poziții, tranziții, arcuri și greutăți ale acestora, reguli de tranziție, precum și marcarea inițială și curentă a rețelei. A fost dezvoltată o metodă pentru introducerea comenzilor de protocol criptografic în structura Petri net. A fost elaborat un program universal în Python 3.0 care modelează funcționarea oricărei rețele Petri de tipul respectiv.

Ca exemplu, a fost creată o rețea Petri, care modelează comportamentul renumitului protocol Diffie-Hellman. Rețeaua nu numai că imită funcționarea protocolului, dar creează și obiectele corespunzătoare într-un mediu criptografic real. Rezultatul executării sale sunt aceleași chei secrete pentru ambele părți implicate în protocol.

SUMMARY

The work is devoted to the development of cryptographic protocol modeling tools based on Petri nets.

The analysis of Petri nets as a modeling tool is carried out and the appropriateness of their use for modeling cryptographic protocols is evaluated. It was found that the Petri net as a model allows adequately reflecting the protocol logic, taking into account time-related parameters, identifying deadlocks, clearly demonstrating vulnerabilities, and quickly reconstructing all possible protocol execution options.

A special type of Petri net was developed, corresponding to the specifics of cryptographic protocols. A structure of configuration files was proposed, that allows describing any Petri network of the type in question and its individual components: positions, transitions, arcs and their weights, transition rules, as well as the initial and current marking of the network. Also has been developed a method for introducing cryptographic protocol commands into the Petri net structure. A universal program in Python 3.0 has been developed. It simulates the operation of any Petri nets of the type in question.

As an example, a Petri net was created for simulating the behavior of the well-known Diffie-Hellman protocol. The network not only imitates the operation of the protocol, but also creates the corresponding objects in a real cryptographic environment. The result of its execution are the same secret keys for both sides involved in the protocol.

РЕЗЮМЕ

Работа посвящена разработке средств моделирования криптографических протоколов на основе сетей Петри.

Проведен анализ сетей Петри как инструмента моделирования и оценена целесообразность их использования для моделирования криптографических протоколов. Установлено, что сеть Петри как модель позволяет адекватно отражать логику протокола, учитывать параметры, связанные со временем, выявлять тупиковые ситуации, наглядно демонстрировать уязвимости, а также оперативно воссоздавать все возможные варианты исполнения протокола.

Разработана сеть Петри специального типа, соответствующая специфике криптографических протоколов. Предложена структура конфигурационных файлов, позволяющих описывать любую сеть Петри рассматриваемого типа и ее отдельные компоненты: позиции, переходы, дуги и их веса, правила переходов, а также начальную и текущую маркировку сети. Разработан способ внедрения команд криптографического протокола в структуру сети Петри. Разработана универсальная программа на языке Python 3.0, моделирующая работу любых сетей Петри рассматриваемого типа.

В качестве примера создана сеть Петри, моделирующая поведение известного протокола Диффи-Хеллмана. Сеть не просто имитирует работу протокола, но и создает соответствующие объекты в реальной криптографической среде. Результатом ее выполнения являются одинаковые секретные ключи у обеих сторон, участвующих в протоколе.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Криптографические протоколы составляют основу информационной безопасности любых современных коммуникаций. Они обеспечивают аутентификацию сторон, передачу секретного ключа, целостность и достоверность передаваемых сообщений, неотрекаемость, анонимность, одновременность и многие другие составляющие информационной безопасности.

Важнейшие требования к криптографическому протоколу – это отсутствие в нем потенциальных уязвимостей и высокая криптографическая стойкость. Поиск и выявление потенциальных уязвимостей протокола является очень сложной проблемой. Известны случаи, когда протоколы, находившиеся много лет в эксплуатации и казавшиеся надежными, оказывались в конце концов взломанными – например, протокол передачи ключа Нидхема -Шрёдера.

Существуют методы анализа протоколов, позволяющие выявлять потенциальные уязвимости. К их числу относятся эвристические методы (метод проб и ошибок), формальные методы (BAN-логика), методы доказательства безопасности и другие. К сожалению, ни один из указанных методов не является универсальным.

Именно поэтому разработка новых методов поиска уязвимостей протоколов по-прежнему остается актуальной проблемой. Одно из перспективных и малоисследованных направлений в этой области – это имитационное моделирования криптографических протоколов с целью поиска уязвимостей с помощью так называемых сетей Петри.

Целью данной работы является разработка средств имитационного моделирования криптографических протоколов на основе сети Петри специального типа.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ сетей Петри с целью оценки их моделирующих возможностей и определения преимуществ перед другими методами анализа протоколов.

2. Разработать сеть Петри специального типа, соответствующую специфике большинства криптографических протоколов.

3. Разработать структуру конфигурационных файлов, позволяющих описывать любую сеть Петри рассматриваемого типа.

4. Разработать способ внедрения команд криптографического протокола в структуру сети Петри, чтобы обеспечить связь средств моделирования с реальной предметной областью.

5. Разработать универсальную программу на языке Python 3.0, способную исполнять любую сеть Петри рассматриваемого типа.

6. Для одного из известных криптографических протоколов построить сеть Петри, моделирующую его выполнение.

7. Выполнить моделирование работы протокола при различных внешних условиях, например, с разным составом участников.

Теоретическую основу дипломной работы составили:

(a) Криптография, раздел “Криптографические протоколы”

(b) Теория сетей Петри

Для решения поставленных практических задач в дипломной работе были использованы следующие инструменты:

(a) Язык программирования Python 3.0

(b) Библиотека криптографических функций OpenSSL

(c) Механизм исполняемых файлов (file.bat) операционной системы Windows.

БИБЛИОГРАФИЯ

1. Питерсон Дж. Теория сетей Петри и моделирования систем. – 1984 - 265 с.
2. https://itmodeling.fandom.com/ru/wiki/Сети_Петри._Структура_и_правила_выполнения_сетей_Петри. – *Структура и правила выполнения сетей Петри.*
3. https://studfile.net/preview/5332439/ - *Моделирование систем и процессов.*
4. http://bourabai.kz/cm/petri_nets.htm - *Сети Петри - математический аппарат для моделирования.*
5. https://cyberleninka.ru/article/v/seti-petri-i-modelirovanie - *Сети Петри и моделирование.*
6. https://cyberleninka.ru/article/n/verifikatsiya-kriptograficheskih-protokolov-raspredeleniya-klyuchey-s-ispolzovaniem-raskrashennyh-setey-petri - *Верификация криптографических протоколов распределения ключей с использованием раскрашенных сетей Петри.*
7. http://facweb.cs.depaul.edu/research/techreports/tr04-003.pdf - *Protocol Verification And Analysis Using Colored Petri Net.*
8. Шнайер Брюс. Прикладная криптография, 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – 2002- 610 с. - *2.Элементы протоколов.*
9. https://cyberleninka.ru/article/n/modelirovanie-protokola-vzaimodeystviya-tls-na-osnove-seti-petri-pri-realizatsii-zaschischennyh-soedineniy - *Моделирование протокола взаимодействия tls на основе сети Петри при реализации защищенных соединений*
10. http://repo.ssau.ru/bitstream/Perspektivnye-informacionnye-tehnologii/Modelirovanie-protokola-SSL-na-osnove-seti-Petri-61961/1/pit_14_1_5_74.pdf - *Моделирование протокола ssl на основе сети Петри.*
11. https://cyberleninka.ru/article/n/kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti - *Криптографические протоколы: основные свойства и уязвимости.*
12. http://www.williamspublishing.com/PDF/5-8459-0847-7/part.pdf - *Шифрование-ассиметричные методы.*
13. https://tproger.ru/translations/diffie-hellman-key-exchange-explained/ - *Как работает обмен ключами в протоколе Диффи-Хеллмана.*

14. https://habr.com/ru/company/yandex/blog/327636/ - *Введение в криптографию и шифрование.*
15. https://www.openssl.org/ - *Библиотека OpenSSL*
16. Саммерфилд Марк. Программирование на Python 3.0 - 2009 - 609 с.
17. https://studbooks.net/2004644/informatika/yazyk_programmirovaniya_python#44 - *Язык программирования Python.*
18. https://studbooks.net/2004645/informatika/osobennosti#19 – *Синтаксис языка Python.*
19. https://studbooks.net/2004646/informatika/opisanie_programmy#87
20. https://studbooks.net/2004647/informatika/zaklyuchenie#238
21. https://younglinux.info/python/task - *Решение задач на Python.*
22. https://www.python.org/download/releases/3.0/ - *Python 3.0 Release.*
23. https://sourceforge.net/projects/pyscripter/ - *PyScripter- Python IDE.*