ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 004.414.023

Верификация криптографических протоколов распределения ключей с использованием раскрашенных сетей Петри

Н. С. Могилевская, С. С. Колчанов
(Донской государственный технический университет)

Рассмотрена и оценена возможность применения раскрашенных сетей Петри для анализа криптографических протоколов распределения ключей на примере симметричного протокола Нидхема — Шрёдера.
Ключевые слова: *верификация протокола, формальный анализ, распределение ключей, протокол Нидхема — Шрёдера, раскрашенные сети Петри, CPN Tools.*

Введение. Одной из наиболее важных задач, которые необходимо решать при организации защиты информационной системы с помощью криптографических алгоритмов, является задача управления ключами. Очевидно, что как бы ни была сложна и разумно устроена криптосистема, некорректное обращение с ключами может значительно понизить уровень её защищённости. Под управлением ключами принято понимать информационный процесс, включающий в себя четыре основных элемента: генерацию ключей, накопление ключей, распределение ключей, процедуру их ввода и синхронизации [1, 2]. Наиболее распространённым решением задачи распределения ключей является использование специализированных криптографических протоколов.

Фактически криптографический протокол — это распределённый алгоритм, определяющий последовательность шагов, точно специфицирующих действия, которые требуются от участников для решения некоторой криптографической задачи, например, обеспечение целостности, секретности, аутентичности информации [2, 3, 4]. При анализе качества протокола необходимо обратить внимание не только на достижение желаемого результата всеми участниками протокола, но и на недопустимость проведения атак на протокол злоумышленниками. Отметим, что при анализе протокола используемые в нём криптографические алгоритмы и примитивы считаются надёжными, а анализу подвергаются сообщения, которыми обмениваются участники протокола, а именно их содержимое и порядок следования. Формальный анализ и выявление недостатков криптографических протоколов на деле оказывается весьма затруднительным. Известны факты, когда протоколы даже с небольшим количеством сообщений долгое время скрывали свои уязвимости [2, 4, 5].

Существует ряд математических аппаратов, используемых для решения задачи формального анализа протокола, например, модальные логики, конечные автоматы, спецификационные языки [2, 4, 6]. Эти подходы достаточно новые, каждый из них имеет как достоинства, так и недостатки. В обзорных работах по формальным методам анализа протоколов часто упоминается возможность верификации протоколов на основе моделирования сетями Петри, однако, исследований, посвящённых именно этому вопросу, достаточно мало, например [4, 6, 7, 8].

Цель работы. Рассмотреть и оценить возможность применения сетей Петри к верификации криптографических протоколов распределения ключей. Для достижения цели в работе с помощью раскрашенных сетей Петри для ряда криптографических протоколов построены модели. По итогам исследования моделей сделаны выводы о возможности верификации криптографических

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè