УДК 004.056

ПРИМЕНЕНИЕ ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА SCYTHER ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ПРОТОКОЛА SKID3[1]

М. И. Цой

Применение стойких криптографических алгоритмов в коммуникационных протоколах еще не гарантирует выполнения свойств, характеризующих безопасность (конфиденциальность, целостность, доступность и др.) передаваемой информации, если их не обеспечивает спецификация протокола. Поэтому актуальной является задача разработки формальных методов анализа безопасности протоколов и их автоматизации [1]. При построении математических моделей протоколов не учитывают особенности реализации используемых в них криптографических примитивов, а также возможные действия, выходящие за рамки данного протокола. Это позволяет сосредоточиться на нахождении слабостей самого протокола [2]. Одной из последних разработок в данном направлении является автоматизированное средство Scyther, предложенное впервые в 2006 г. в рамках диссертации К. Кремерса [3].

Целью данной работы является изучение математического аппарата средства Scyther и его применение для анализа безопасности протокола двусторонней аутентификации SKID3 [4].

Scyther относится к средствам, основанным на методе проверки на модели (model checking [5]). Формальная модель протокола описывает множество состояний и систему переходов из одного состояния в другое. Состояния, достижимые из заданного начального, проверяются на удовлетворение некоторым свойствам безопасности.

Язык, на котором формулируется спецификация анализируемого протокола, достаточно прост и интуитивен, однако недостаточно выразителен, что ограничивает применимость данного средства. В частности, существенным ограничением является отсутствие каких-либо средств описания ветвлений, что не позволяет описать многие из существующих протоколов. Тем не менее есть большое количество протоколов без ветвлений, которые могут быть проанализированы, в частности протоколы аутентификации. Кроме того, математическая модель Scyther не позволяет анализировать протоколы, в которых фигурирует понятие времени (например, в сообщения добавляются временные метки). Вводится только отношение порядка на множестве событий.

Спецификация протокола представляет собой описание ролей и действий, которые выполняют агенты, ассоциированные с этими ролями. Требования к безопасности являются частью спецификации протокола в виде особого класса ролевых действий. Теоретическая модель предполагает возможность проверки секретности некоторого терма (Secrecy), а также четыре вида аутентификации (Injective Synchronisation, Injective Agreement, Non-Injective Synchronisation, Non-Injective Agreement).

Протокол SKID3 — это протокол взаимной аутентификации двух участников. О существующих попытках анализа безопасности данного протокола автору неизвестно. В [4] указано, что SKID3 уязвим к атаке «человек посередине», однако не удалось найти сведений о конкретной ее реализации, а в результате собственных теоретических исследований не получилось установить возможность реализации такой атаки. Вместо этого протокол SKID3 промоделирован средством Scyther с целью проверки выполнения свойств NISynch — существования коммуникационного партнера для

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

каждого экземпляра события-требования и NIAgree — согласованности всех переменных в процессе исполнения протокола [3]. В результате моделирования установлено, что в этом протоколе ни для одной роли свойства NIAgree и NISynch не нарушаются в условиях компрометации одного из агентов и секретных ключей между ним и доверенными участниками протокола, что можно трактовать как то, что протокол SKID3, скорее всего, неуязвим к атаке «человек посередине».

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Автоматизированные средства анализа протоколов // Прикладная дискретная математика. Приложение. 2009. № 1. С. 34—36.
2. *Dolev D., Yao A. C.* On the security of public key protocols // IEEE Trans. Inform. Theory. 1983. No. 29(12). P. 198–208.
3. *Cremers C. J. F.* Scyther — Semantics and Verification of Security Protocols // Ph. D. dissertation. Eindhoven University of Technology, 2006.
4. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). Wiley, 1995.
5. *Кларк Э. М., Грамберг О., Пелед Д.* Верификация моделей программ: Model Checking: пер. с англ. / под ред. Р. Смелянского. М.: МЦНМО, 2002. 416 с.