Список литературы:

1. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер – 2020 – 448 с.
2. Документация по использованию OWASP ZAP [Электронный ресурс] – Режим доступа: URL: https://www.zaproxy.org/docs
3. Знакомство с OWASP ZAP [Электронный ресурс] – Режим доступа: URL: https://devopedia.org/owasp-zap

УДК 004.056.53

Яковлева Дарья Алексеевна, Савилова Ульяна Андреевна,
Шибков Денис Александрович, Машкова Оксана Сергеевна,
Тамбовский государственный технический университет, г. Тамбов
Yakovleva Darya Alekseevna, Savilova Ulyana Andreevna,
Shibkov Denis Aleksandrovich, Mashkova Oksana Sergeevna
Tambov State Technical University, Tambov

МОДЕЛИРОВАНИЕ ПРОТОКОЛА ANDOS НА ОСНОВЕ СЕТЕЙ ПЕТРИ
SIMULATION OF THE ANDOS PROTOCOL BASED ON PETRI NETS

Аннотация: в данной работе рассматривается процесс построения сети Петри, представляющей собой динамическую модель криптографического протокола ANDOS, который обеспечивает надежную защиту процедуры аутентификации.

Abstract: this article deals with the process of the construction a Petri net, which is a dynamic model of the ANDOS, a cryptographic protocol. It provides reliable protection for the authentication procedure.

Ключевые слова: информационная безопасность, аутентификация, криптографический протокол ANDOS, бескомпромиссное раскрытие тайн, динамическая модель, сети Петри.

Keywords: information security, authentication, ANDOS cryptographic protocol, uncompromising disclosure of secrets, dynamic model, Petri net.

Повсеместное применение информационных технологий все чаще требует повышенного внимания к вопросам информационной безопасности. Одним из важнейших механизмов защиты информации считается процедура аутентификации.

Зачастую в процессе аутентификации секретная информация может быть перехвачена злоумышленником и в дальнейшем использована для осуществления несанкционированного доступа под видом законного пользователя.

Для предотвращения подобных угроз может быть применен криптографический протокол ANDOS (All-or-Nothing Disclosure Of Secrets – бескомпромиссное раскрытие тайн). Данный протокол способен обеспечить более высокий уровень защищенности процедуры аутентификации, так как секретная информация, участвующая в процессе аутентификации, не раскрывается. Иными

словами, лицо, продающее «секрет» (формирующее аутентификационную информацию), никогда не узнает какой именно «секрет» приобрел покупатель (выбрал аутентификационную информацию) [1-2].

Моделирование данного протокола выполним на основе сетей Петри. Для этого выполним процедуру спецификации сети.

Определим сеть Петри как

$$C = \{P, T, I, O, \mu\}, \quad (1)$$

где P – конечное множество позиций; T – конечное множество переходов; I – множество входных функций; O – множество выходных функций; μ_0 – начальная маркировка сети.

Обозначение элементов сети:

1) конечное множество позиций имеет вид:

$$P=\{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}\};$$

2) конечное множество переходов имеет вид:

$$T=\{t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{11}\};$$

3) множество входных позиций перехода имеет вид:

$$I=\{I(t_0), I(t_1), I(t_2), I(t_3), I(t_4), I(t_5), I(t_6), I(t_7), I(t_8), I(t_9), I(t_{10}), I(t_{11})\}.$$

$$I(t_0)=\{p_0, p_1\}, I(t_1)= \{p_0, p_1\}, I(t_2)= \{p_0, p_2\}, I(t_3)= \{p_0, p_3\}, I(t_4)= \{p_0, p_4\},$$
$$I(t_5)=\{p_{11}, p_6\}, I(t_6)= \{p_{11}, p_7\}, I(t_7)=\{p_{11}, p_8\}, I(t_8)=\{p_{11}, p_9\}, I(t_9)=\{p_{11}, p_{10}\},$$
$$I(t_{10})=\{p_{12}, p_{13}\}, I(t_{11})=\{ p_{14}, p_{16}\};$$

4) множество выходных позиций перехода имеет вид:

$$O = \{O(t_0), O(t_1), O(t_2), O(t_3), O(t_4), O(t_5), O(t_6), O(t_7), O(t_8), O(t_9), O(t_{10}), O(t_{11}),$$
$$O(t_{12}), O(t_{13}), O(t_{14}), O(t_{15}), O(t_{16})\}.$$

$$O(t_0)=\{p_6\}, O(t_1)=\{p_7\}, O(t_2)=\{p_8\}, O(t_3)=\{p_9\}, O(t_4)=\{p_{10}\}, O(t_5)=\{p_{12}\},$$
$$O(t_6)=\{p_{12}\}, O(t_7)=\{p_{12}\}, O(t_8)=\{p_{12}\}, O(t_9)=\{p_{12}\}, O(t_{10})=\{p_{14}\}, O(t_{11})=\{p_{15}\};$$

5) начальная маркировка имеет вид:

$$\mu_0 = \{5, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1\}$$ [3].

Схема разработанной динамической модели протокола ANDOS представлена на рисунке 1.

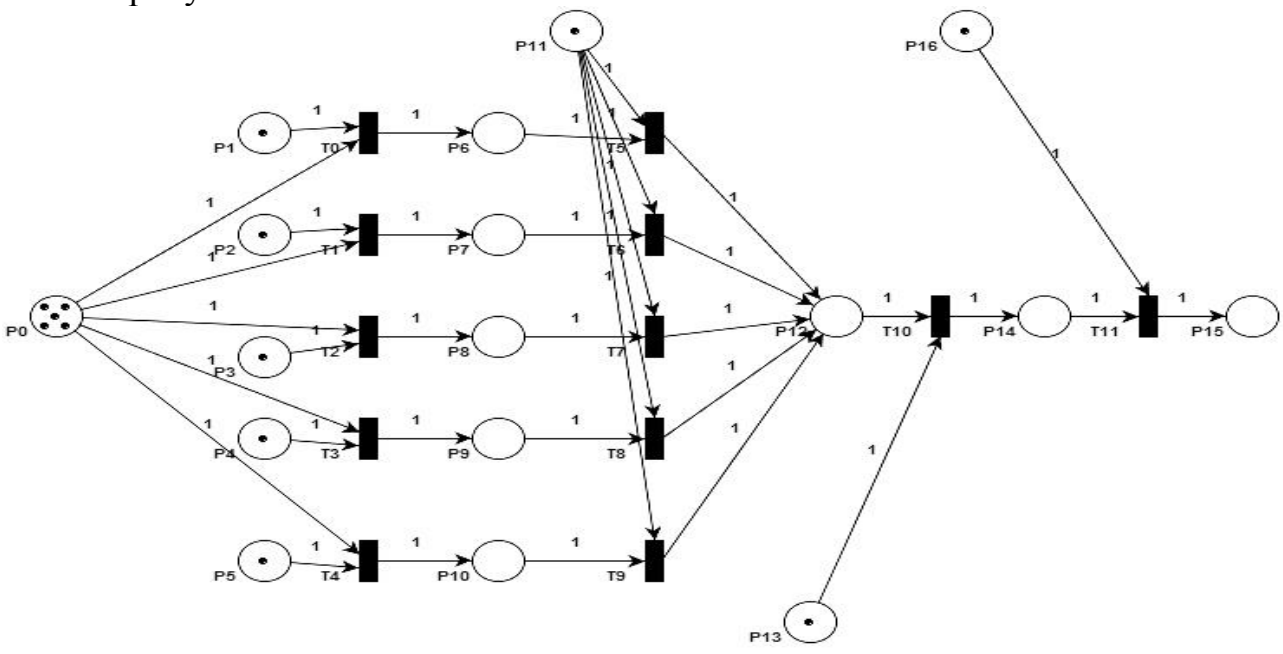

Рисунок 1 – Модель протокола ANDOS на основе сети Петри

Описание элементов модели протокола ANDOS представлено в таблице 1.

Таблица 1

Спецификация элементов динамической модели

Обозначение элемента	Описание
t_0, t_1, t_2, t_3, t_4	Установить маскирующую последовательность продавца на секреты
t_5, t_6, t_7, t_8, t_9	Разрешить покупателю выбрать один (несколько) секретов
t_{10}	Обработать продавцом транзакцию продажи
t_{11}	Снять с приобретенного секрета маскирующую последовательность покупателя
p_0	Установка маскирующей последовательности продавца
p_1, p_2, p_3, p_4, p_5	Исходное состояние секретов
p_6, p_7, p_8, p_9, p_{10}	Выставленные на продажу секреты
p_{11}	Покупатель, который готов приобрести секрет (установка маскирующей последовательности покупателя)
p_{12}	Отобранный для покупки секрет с наложенной на него маскирующей последовательностью покупателя
p_{13}	Обработка транзакции покупки секрета продавцом (снятие маскирующей последовательности)
p_{14}	Снятие маскирующей последовательности продавца
p_{16}	Обработка приобретенного секрета покупателем (снятие маскирующей последовательности покупателя)
p_{15}	Конечное состояние приобретенного секрета

Этапы функционирования динамической модели протокола ANDOS:

1) подготовка «секретов» *S* для продажи. Алиса своим «ключом» маскирует секреты перед продажей;

2) выбор одного «секрета» (нескольких «секретов») *S* для покупки. Боб своим «ключом» маскирует выбранный секрет перед покупкой;

3) снятие с приобретенного «секрета» *S* Алисой своего маскирующего «ключа»;

4) снятие с приобретенного «секрета» *S* Бобом своего маскирующего «ключа».

Таким образом, разработанная модель криптографического протокола ANDOS обладает строгим математическим описанием, на основе которого возможно провести анализ взаимодействия двух субъектов отношений: продавца и покупателя. Подобный анализ позволяет получить сведения для дальнейшего усовершенствования протокола в целях повышения уровня защищенности процедуры аутентификации.

Список литературы:

1. Покатаева Е. Прозрачный черный ящик // Итоги. – 2012. – № 9. – URL: http://www.itogi.ru/hitech-business/2012/9/175252.html (дата обращения: 27.07.2020).

2. Brassard G., Crepeau C., Robert JM. All-or-Nothing Disclosure of Secrets. // Advances in Cryptology – CRYPTO’ 86. – 1987. – vol. 263. – pp. 234-238.

3. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 264 с.