Автор: Чан Зуи Хань
Год рождения: 1993
Полное название факультет: Факультет безопасности информационных технологий
Направление подготовки: 10.06.01 – Информационная безопасность
Email: viewtheworld93@gmail.com

Соавтор: Ле Зуи Дон
Год рождения: 1995
Полное название факультет: Факультет безопасности информационных технологий
Направление подготовки: 10.06.01 – Информационная безопасность
Email: duydontd1412@gmail.com

Соавтор, научный руководитель: Комаров Игорь Иванович
Год рождения: 1970
Полное название факультет: Факультет безопасности информационных технологий
Степень, звание: кандидат физико – математических наук, доцент
Email: i_krov@mail.ru

УДК 004.056

ВЕРИФИКАЦИЯ БЕЗОПАСНОСТИ ПРОТОКОЛА АУТЕНТИФИКАЦИИ ТИПА «ЗАПРОС – ОТВЕТ» С ПОМОЩЬЮ ИНСТРУМЕНТА AVISPA

Авторы: Чан З. Х., Комаров И. И., Ле З. Д.
ФБИТ, университет ИТМО, Санкт Петербург

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Российская Федерация, 197101, г. Санкт-Петербург, Кронверкский пр., д.49,», E-mail: org@mail.ifmo.ru

Аннотация
Обеспечение информационной безопасности элементов кибер-физических систем является необходимым условием их корректного функционирования. В мобильной распределённой кибер-физической системе эта задача осложняется рядом специфических факторов, связанных, в том числе с неконтролируемым доступом к беспроводной среде передачи данных и ограничениями на применение «тяжёлой» криптографии.
В работе исследуется предложенный автором облегчённый протокол взаимной аутентификации мобильных агентов, а также проводится формализованная проверка выполнения требований по безопасности, предъявляемых к этому протоколу. Результаты исследования подтверждают корректность предлагаемого протокола с учётом ограничений по ресурсоёмкости и целесообразность применения инструментального средства формализованного доказательства корректности параллельных процедур с использованием технологии верификации моделей (Model Checking). Определены ограничения и направления развития технологии верификации протоколов аутентификации с использованием специализированных инструментальных средств.
Ключевые слова
Протокол аутентификации, информационная безопасность, мультиагентная система, верификации моделей, Model Checking, AVISPA.

В кибер-физической системе (КФС) [1] аутентификация объекта (стороны) является необходимым шагом для обеспечения информационной безопасности и корректности функционального взаимодействия. Несмотря на наличие широкого спектра работ в этом направлении, задача разработки оптимального протокола аутентификации для конкретной

реализации КФС остаётся актуальной научно-технической задачей. Причём вопросы доказательства корректности и стойкости протоколов выходят на первый план с увеличением комплексных рисков эксплуатации таких систем.

Цель работы: анализа протокола аутентификации типа «ответ-запрос» на основе ISO/ IEC 9798, а также проведена формальная верификация облегчённого протокол аутентификации, в котором используется односторонняя функция хеширования.

Классический процесс разработки протоколов взаимодействия предполагает: 1) определение требований; 2) собственно разработку протоколов, 3) анализ уязвимостей и 4) их устранение. Такой подход ресурсоёмок, долог и часто вызывает ошибки, однако использование автоматизированных инструментов анализа протоколов, основанных на методе верификации моделей (Model Checking), позволяет сократить срок и повысить доверие к результатам третьей фазы [2, 3]. Краткий сравнительный анализ наиболее известных инструментальных средств (ИСр) верификации процедур взаимодействия компонентов представлен в Таб.1.

Таблица 1: Оценка применимости инструментальных средств верификации протоколов

Инструмент	Гибкость языка	Удобство анализа результатов	Наглядность результатов	Уверенность
ProVerif	-	-	+	+
HERMES	+	-	-	+
AVISPA	**+**	**+**	**+**	**+**
Scyther	-	-	-	+

Свойства безопасности механизма аутентификации включают: предотвращение известных атак: повторения, отражения; взаимная / односторонняя аутентификация; предварительное установление секретов или передача их доверенным третьим лицам.

В работе исследуются свойства безопасности модели аутентификации между двумя агентами КФС [4] с использованием протокола аутентификации типа «запрос-ответ» с помощью ИСр AVISPA.

Стандарты по аутентификации «запрос – ответ»:

- ISO/IEC 9798-1: 2010 – General (дополнения и поправки 2016 гг.);
- ISO/IEC 9798-2: 2008 – Mechanisms using symmetric encipherment algorithms (дополнения и поправки 2010, 2012, 2013 и 2019 гг.);
- ISO/IEC 9798-3: 1998 – Entity authentication using digital signature technique (дополнения и поправки 2009, 2010, 2012, 2019 гг.);
- ISO/IEC 9798-4: 1999 – Mechanisms using a cryptographic check function (дополнения и поправки 2009 и 2012 гг.);
- ISO/IEC 9798-5: 2009 – Mechanisms using zero knowledge techniques (дополнения и поправки 2009 и 2018 гг.);
- ISO/IEC 9798-6: 2010 – Mechanisms using manual data transfer (дополнения и поправки 2010 и 2016 гг.).

Из протоколов, указанных в стандарте ISO/IEC 9798, аутентификация на основе односторонней хеш-функции требует наименьших вычислительных затрат. Ключевая хеш-функция использует общий секретный ключ для вычисления хэш-значения, но необходимо периодически изменять секретный ключ для защиты от некоторых атак. Чтобы решить эту проблему, используется общий секретный ключ в качестве аргумента хэш-функции [5]. Этот метод позволяет хранить общий секретный ключ в течение длительного времени.

Результат: на основании анализа полученных данных формулируется заключение: исследуемый протокол аутентификации безопасен, обеспечивая выполнение требований (целей, свойств) безопасности, установленных на этапе формализации требований к протоколу: безопасность данных, взаимная аутентификация сторон, защита от повторных атак, атак человека посередине.

Подтверждена информационная безопасность предложенного протокола по обеспечению взаимной аутентификации, конфиденциальности данных, предотвращению атаки MITM в рамках заданных ограничений.

Перспективными направлениями исследований являются: разработка методики автоматизированной генерации протоколов аутентификации в группировках агентов - беспилотных транспортных средств в зависимости от условий и требований к функционированию КФС; и, связанное с этим формирование библиотек (шаблонов) примитивов, содержащих верифицированные компоненты протоколов взаимодействия таких агентов.

Литературы:

1. Д A. Humayed, J. Lin, F. Li and B. Luo. Cyber-Physical Systems Security—A Survey // IEEE Internet of Things Journal, Dec. 2017, vol. 4, no. 6, pp. 1802-1831, DOI: 10.1109/JIOT.2017.2703172.
2. Бабенко Л. К., Агустин С. Р. Х. Верификация безопасности протокола электронной цифровой подписи с помощью AVISPA // Вопросы кибербезопасности. – 2017. – №. 2 (20).
3. Кораблин Ю. П., Шипов А. А. Унифицированное представление формул логик LTL и CTL системами рекурсивных уравнений //Программные продукты и системы. – 2019. – Т. 32. – №. 1
4. Чан З. Х. Разработка механизма аутентификации агентов в группировке беспилотных летательных аппаратов //Сборник трудов VIII Конгресса молодых ученых. – 2019. – С. 171-174.
5. В. Н. Никитин, Д. В. Юркин. Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы, № 6, 2010, ст. 42 - 46.