Виктор С. Горбатов[1], Игорь Ю. Жуков[2], Олег Н. Мурашов[3]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, г. Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[3]Акционерное общество «РАМЭК-ВС»,
Волгоградский пр., 2, г. Москва, 109316, Россия
e-mail: olegxozbox@yandex.ru, https://orcid.org/0000-0002-4467-2170

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА

DOI: http://dx.doi.org/10.26583/bit.2019.1.08

Аннотация. В соответствии с законодательством по обеспечению транспортной безопасности ряд транспортных средств должны быть оснащены бортовыми контрольными устройствами, содержащими криптографическое средство аутентификации, регистрации и хранения контрольных данных, в том числе ключевой информации электронной подписи. Целью настоящей работы является представление решения задачи обоснования достаточности мер противодействия известным атакам и методам компрометации предполагаемых криптографических механизмов и соответствующего протокола, оформленного в виде проекта национального стандарта и представленного в предыдущей работе авторов по исследованию его свойств безопасности. Представленное решение ограничено только рассмотрением атак, разделенных на два больших класса: пассивные и активные атаки, включая временные атаки, основанные на изучении времени отклика одного или нескольких участников протокола. Выводы. Анализ модели угроз безопасности протокола выработки общего ключа с аутентификацией абонентов, предназначенного для использования в тахографах, устанавливаемых на транспортные средства, показывает, что исследуемый протокол обеспечивает достаточность мер противодействия известным атакам. Найденные возможные атаки носят формальный характер, не позволяя нарушителю получить какую-либо дополнительную информацию для конструктивной компрометации протокола.

Ключевые слова: безопасность транспорта, контрольное устройство, криптографический протокол, механизмы аутентификации, угрозы безопасности.
Для цитирования: ГОРБАТОВ, Виктор С.; ЖУКОВ, Игорь Ю.; МУРАШОВ, Олег Н. ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА. Безопасность информационных технологий, [S.l.], p. 77-86, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1183>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.08.

Victor S. Gorbatov[1], Igor Y. Zhukov[2], Oleg N. Murashov[3]
[1]National Research Nuclear University MEPhI,
Kashirskoe shosse 31 Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]Ltd «The National Mobile Portal»,
Volgogradskiy pr., 2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[3]Joint-stock company «Ramec-VS»,
Volgogradskiy pr., 2, Moscow, 109316, Russia
e-mail: olegxozbox@yandex.ru, https://orcid.org/0000-0002-4467-2170

Assessment of threats to the security of the cryptographic authentication mechanisms of the monitor devices of vehicles

DOI: http://dx.doi.org/10.26583/bit.2019.1.08

Abstract. According to the legislation on transport security a number of vehicles must be equipped with on-Board control devices containing a cryptographic means of authentication, registration and storage of control data, including key information of the electronic signature.

This paper presents a solution to the problem of justification of the adequacy of measures to counter known attacks and methods of discrediting the suggested cryptographic mechanisms and the corresponding protocol drawn up in the form of a draft national standard and presented in the previous work of the authors devoted to study of its security properties. The solution presented is limited to the consideration of attacks subdivided into two classes: passive and active attacks, including temporary attacks based on the study of the response time of one or more participants of the protocol. The analysis of the security threat model of the Protocol generating a common key with the authentication of subscribers intended for use in tachographs installed on vehicles shows that the protocol provides sufficient measures to counter known attacks. The found possible attacks are of a formal nature, not allowing the offender to obtain any additional information in order to discredit the protocol.
Keywords: transport security, control device, cryptographic protocol, authentication mechanisms, security threats.
For citation: GORBATOV, Victor S.; ZHUKOV, Igor Y.; MURASHOV, Oleg N.. Assessment of threats to the security of the cryptographic authentication mechanisms of the monitor devices of vehicles. IT Security (Russia), [S.l.], p. 77-86, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1183>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.08.

Введение

В соответствии с действующими нормами обеспечения транспортной безопасности [1, 2] определенная категория автомобилей должна быть оснащена бортовыми контрольными устройствами, содержащими криптографическое средство аутентификации, регистрации и хранения контрольных данных, в том числе ключевой информации электронной подписи. Криптографические механизмы и соответствующий протокол, разработанный в соответствии с рекомендациями [3] и оформленный в виде проекта национального стандарта [4], а также его свойства безопасности представлены в работе [5]. Там же поставлена задача обоснования достаточности мер противодействия известным атакам и методам компрометации указанного протокола с целью разработки рекомендаций для его практического применения. Решению указанной задачи и посвящена настоящая работа.

Очевидным этапом достижения положительного решения задачи является разработка модели угроз (возможных видов атак) и анализ мер соответствующего противодействия этим угрозам.

Так как в настоящей работе рассматривается только модель криптографического протокола, а не его программно-аппаратная реализация для конкретного технического средства криптографической защиты, то целесообразно ограничиться рассмотрением только атак, разделенных на два больших класса: пассивные и активные атаки, включая временные атаки, основанные на изучении времени отклика одного или нескольких участников протокола.

1. Пассивные атаки

Пассивные атаки основаны на перлюстрации и последующем криптографическом анализе передаваемых в ходе выполнения протокола сообщений. Поэтому предположим, что перед началом выполнения протокола нарушитель обладает определенной информацией о некотором количестве бортовых устройств $VU_1, \dots, VU_\nu$ и карт тахографа $TC_1, \dots, TC_t$, где *t,* ν — натуральные числа и $\upsilon \geq 1, t \geq 1$, для которых известны:

1. Идентификаторы участников протокола, соответственно:
   $VU_1.CHR, \dots, VU_\nu.CHR$ и $TC_1.CHR, \dots, TC_t.CHR$;
2. Ключи проверки электронной подписи, соответственно:
   $VU_1.P, \dots, VU_\nu.P$ и $TC_1.P, \dots, TC_t.P$;
3. Сертификаты ключей проверки электронной подписи, подписанные электронной подписью Удостоверяющего центра и содержащие в себе как значения ключей проверки электронной подписи, так и значения идентификаторов, соответственно, *VU.CHR* и *TC.CHR*.

Кроме того, нарушителю известны согласованные заранее параметры a, b, p эллиптической кривой Ea,b и точка P ∈ E_(a,b), порождающая подгруппу простого порядка q. Далее мы полагаем, что данные параметры являются одинаковыми для всех возможных сессий протокола. Кроме того, нарушителю известны все криптографические алгоритмы: выработки и проверки подписи, алгоритмы шифрования информации, а также используемая функция вычисления производного ключа.

Таким образом, в соответствии со схемой исследуемого протокола [4] в ходе выполнения одной сессии протокола нарушителю становятся известными следующие значения.

1. Точки эллиптической кривой TC.P, VU.P, используемые для выработки общего сессионного ключа.
2. Случайная последовательность Nonce1, передаваемая от карты тахографа в бортовое устройство.
3. Шифртекст E1, являющийся результатом применения алгоритма шифрования ГОСТ Р 34.12-2015 «Магма» в режиме гаммирования к неизвестному блоку Nonce2 длины 64 бит при неизвестном нарушителю ключе K и неизвестном нарушителю инициализационном векторе (синхропосылке I).
4. Значения электронных подписей S1, S2, вычисленные для неизвестных нарушителю сообщений T1, T3 при помощи неизвестных нарушителю секретных долговременных ключей (ключей электронной подписи TC.SK, VU.SK).

Используя перечисленные выше величины, нарушитель может реализовать следующие угрозы, направленные на компрометацию протокола.

1.1. Атака на долговременные ключи

Поскольку нарушителю известны согласованные заранее параметры a, b, p эллиптической кривой Ea,b и точка P ∈ E_(a,b), порождающая подгруппу простого порядка q, то задача определения долговременного ключа VU.SK бортового устройства сводится к решению задачи дискретного логарифмирования VU.PK = [VU.SK]P в группе точек эллиптической кривой Ea,b. Решение аналогичной задачи TC.PK = [TC.SK]P позволит нарушителю найти долговременный ключ карты тахографа.

Известно, что в настоящее время наилучшим методом решения задачи дискретного логарифмирования в группе точек эллиптической кривой является метод параллельного поиска коллизий Ооршота-Винера [6]. Трудоемкость данного метода оценивается величиной порядка $\frac{\sqrt{\pi q}}{2}$.

Здесь и далее трудоемкость измеряется в операциях сложения различных точек эллиптической кривой Ea,b, где q порядок подгруппы, порожденной точкой P, множитель 2 в знаменателе приведенной дроби означает число эффективно вычислимых автоморфизмов эллиптической кривой. Учитывая, что согласно ГОСТ Р 34.10-2012 для q выполнены неравенства $2^{254} < q < 2^{256}$, можно считать, что трудоемкость решения задачи дискретного логарифмирования оценивается величиной порядка 2^{128}.

1.2. Атака путем решения задачи Диффи-Хеллмана

Пусть $G = \langle P \rangle$, подгруппа точек эллиптической кривой Ea,b, простого порядка q, порожденная точкой P. Пусть в этой подгруппе заданы два элемента $R_a = [k_a]P$ и $R_b = [k_b]P$. Мы будем называть задачей Диффи-Хеллмана задачу определения элемента Q, удовлетворяющего равенству $Q = [k_a k_b]P$. В случае рассматриваемого нами протокола в качестве точки R_a выступает передаваемая в ходе выполнения протокола точка $VU.P$, а в качестве точки R_b – точка $TC.P$. Тогда решение задачи Диффи-Хеллмана будет являться точкой $VU.Q$, вычисляемой бортовым устройством на третьем шаге (п. 4) и точкой $TC.Q$, вычисляемой картой тахографа на четвертом шаге

(п. 1.2) исследуемого протокола. Легко видеть, что решение нарушителем задачи Диффи-Хеллмана приводит к определению неизвестного общего сеансового ключа *K*.

В настоящее время известен только один эффективный метод решения задачи Диффи-Хеллмана, отличный от тотального перебора неизвестных значений, основанный на решении задачи дискретного логарифмирования в группе точек эллиптической кривой Ea,b, рассмотренный ранее.

Таким образом, можно считать, что трудоемкость решения задачи Диффи-Хеллмана совпадает с трудоемкостью решения задачи дискретного логарифмирования и также оценивается величиной порядка 2^{128}.

1.3. Нахождение общего ключа K по шифртексту E_1

Задача нахождения общего сеансового ключа K по заданному шифротексту E1 заключается в определении величины K, удовлетворяющей системе нелинейных уравнений:

$$\begin{cases} E_1 = Nonce_2 \oplus E(K, I) \\ K||I = \left[KDF\left(\pi(VU.Q)\middle||VU.CHR\middle||TC.CHR\right)\right]_{0,\dots,319}, \end{cases}$$

при неизвестных значениях $Nonce_2 \in V^{64}$ и $\pi(VU.Q) = \pi(TC.Q) \in V^{256}$.

Методы решений указанной системы уравнений, отличные от тотального опробования значений $\pi(VU.Q)$, неизвестны. Трудоемкость опробования значений $\pi(VU.Q)$ может быть оценена величиной $O(2^{256})$ математических операций.

1.4. Атака на разовый ключ алгоритма выработки электронной подписи

Под разовым ключом алгоритма выработки электронной подписи подразумевается случайное число *k*, вырабатываемое в процессе вычисления электронной подписи и используемое в уравнении выработки подписи:

$$rx + ke \equiv s(mod\ q).$$

При анализе схемы электронной подписи ГОСТ Р 34.10-2012 считается, что величины *r, s, e* известны нарушителю (пара $r \mid\mid s$ является значением электронной подписи, а величина *e* является значением функции хэширования от подписываемого сообщения).

В случае исследуемого протокола неизвестная величина *x* может принимать значения *VU.SK* или *TC.SK*, то есть является долговременным ключом, который недоступен нарушителю. Величина *e* также не является нарушителю известной, поскольку само подписываемое сообщение T_1 или T_3 ему полностью неизвестно. Таким образом, если нарушителю известно значение разового ключа *k*, то ему необходимо опробовать 2^{64} неизвестных значений $Nonce_1$ или $Nonce_2$, для каждого из таких значений вычислить значение *e* и решить указанное линейное сравнение.

1.5. Атака на разовые случайные значения

В ходе выполнения протокола бортовым устройством и картой тахографа вычисляются случайные целые числа k_t, k_b, удовлетворяющие неравенству:

$$1 \le k_t k_b \le q - 1$$

Легко видеть, что если нарушителю известно хотя бы одно из этих значений, то он может определить общий сеансовый ключ.

Действительно, если нарушителю известно значение k_t, выработанное картой тахографа, то, перехватывая точку *VU.P,* нарушитель может вычислить точку Q - общий секретный ключ из равенства:

$$I = \left[KDF\left(\pi(VU.Q)||VU.CHR||TC.CHR\right)\right]_{0,\ldots,319},$$

где $Q = [K_t]VU.P$.

1.6. Атака на датчик псевдослучайных чисел

Еще одной возможностью скомпрометировать протокол является попытка предсказания результата действия датчика псевдослучайных чисел, используемого бортовым устройством или картой тахографа для генерации случайных значений, вырабатываемых в ходе выполнения протокола.

В ходе одного сеанса протокола нарушитель имеет возможность наблюдать выработанную датчиком карты тахографа последовательность $Nonce_1$ фиксированной длины 64 бита. При этом нарушитель может наблюдать эту последовательность для достаточно большого числа сеансов выполнения протокола и накапливать наблюдаемые данные.

Будем считать, что используемые датчики случайных чисел вырабатывают последовательности равномерно распределенных 64-битных целых чисел со свойством непредсказуемости. В этом случае по заданному множеству элементов последовательности нельзя в масштабе реального времени определить элементы последовательности, выработанные ранее, или элементы, которые будут выработаны впоследствии. Общие требования к таким датчикам могут быть найдены в рекомендациях по стандартизации криптографических протоколов [3].

1.7. KCI и UKS – атаки

Подробный анализ этих видов угроз и рекомендации по противодействию им приведен в работе [5].

2. Формальный анализ активных атак

Одним из возможных способов исследования протоколов относительно возможности проведения активных атак является математическое моделирование действий нарушителя с помощью широкого спектра средств автоматической верификации криптографических протоколов. В работе использованы доступные и хорошо изученные средства автоматической верификации криптографических протоколов *AVISPA – SPAN* [5, 9] и *Scyther* [7].

2.1. Анализ с помощью средства AVISPA-SPAN

Моделирование работы исследуемого протокола проводилось согласно представленной спецификации [3].

Анализ при помощи средства автоматической верификации *AVISPA – SPAN* [8] проводился с использованием модулей *OFMC* и *CL – AtSe*, осуществляющих верификацию методом проверки на модели. Описание используемых модулей приведено в [10]. Исследование свойств безопасности проводилось при помощи встроенных в средство *AVISPA – SPAN* функций: *Secret*, *Witness* и *Request*. Функция *Secret* проверяет выполнения свойства и применима к любым данным, участвующим в процессе выполнения протокола. В частности, она может быть применена к исследованию свойства конфиденциальности вырабатываемого общего ключа, то есть к проверке первого свойства безопасности [5]. При исследовании функция Secret применялась также к разовым секретным ключам k_t, k_b – секретным случайным значениям, вырабатываемым в ходе выполнения протокола. Функции *Witness* и *Request* позволяют проверять

возможность проведения безопасной аутентификации на определенном (конкретном) шаге выполнения протокола. Тем самым применение функций *Witness* и *Request* позволяет провести проверку шестого свойства безопасности [5].

Результаты анализа исследуемого протокола [4] при помощи средства *AVISPA – SPAN* показали, что рассматриваемый криптографический механизм позволяет безопасно проводить аутентификацию и вырабатывать общий секретный ключ. Результаты анализа приведены в следующей таблице.

Таблица 1. Результаты анализа исследуемого протокола при помощи средства AVISPA – SPAN

Модуль	**Детали**	**Свойство**	**Результат**
OFMC	*BOUNDED_NUMBER_OF_SESSIONS*	аутентификация	*SAFE*
OFMC	*BOUNDED_NUMBER_OF_SESSIONS*	секретность	*SAFE*
CL-ATSE	*BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL*	аутентификация	*SAFE*
CL-ATSE	*BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL*	секретность	*SAFE*

Схема выполнения модели исследуемого криптографического механизма в *AVISPA – SPAN* приведена на рис. 1.

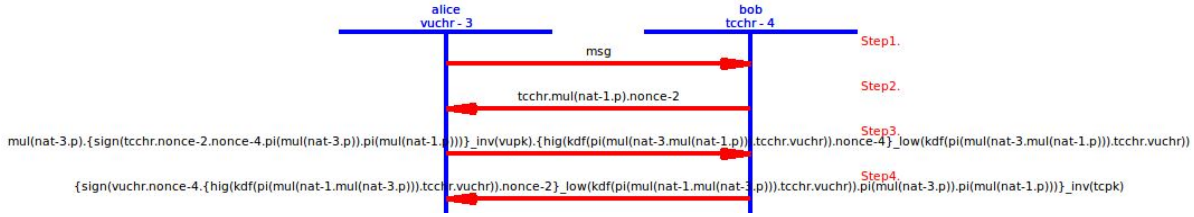

Рис. 1. Оценка протокола в AVISPA–SPAN
(Fig. 1. Protocol evaluation with AVISPA–SPAN)

2.2. Анализ с помощью средства Scyther

Средство *Scyther* использует язык спецификации *SPDL*, который позволяет определить множество состояний и систему переходов между состояниями. При исследовании протокола применяется символический анализ в сочетании с двунаправленным поиском, основанным на частично упорядоченных шаблонах [10, 11]. Формальная модель протокола, используемая в *Scyther*, описывает множество состояний и систему переходов из одного состояния в другое. Состояния, достижимые из заданного начального состояния, проверяются на удовлетворение некоторым свойствам безопасности. Протокол определяется как последовательность событий, причем к событиям относится передача сообщений, которыми обмениваются участники протокола, и сообщений, которые может отправлять злоумышленник. *Scyther* верифицирует ограниченное и неограниченное число сеансов протокола. Используется нотация, позволяющая различать отдельные исполнения того или иного события. *Scyther* не требует задания сценария атаки. Необходимо только задать параметры, ограничивающие либо максимальное число запусков, либо пространство перебираемых траекторий. При верификации протокола *Scyther* рассматривает ряд свойств безопасности, впервые предложенных в работе [12] и выбранных разработчиком *Scyther* для обоснования безопасности исследуемых моделей криптографических протоколов.

При анализе исследуемого протокола использовались следующие свойства безопасности: *Secret*, *Alive*, *Weakagree*, *Niagree* и *Nisynch*.

Свойство *Secret* позволяет проверить выполнение свойства секретности, аналогичного свойству, используемому средством *AVISPA – SPAN*. Определения остальных свойств могут быть найдены в работах [12, 13].

Данные свойства безопасности не имеют точного соответствия свойствам, введенным в работе [5], и имеют собственную трактовку. В связи с этим приведем определения этих свойств в интерпретации, наиболее близкой к рассмотренным в [5] свойствам безопасности.

1. При выполнении свойства *Alive* протокол гарантирует участнику дееспособность (англ. aliveness) другого участника, если участник, действующий как инициатор протокола, после завершения протокола, как он полагает, с участником получает подтверждение того, что действительно являлся участником этого протокола. Отметим, что при этом необязательно, чтобы участник считал, что он взаимодействует с участником, а также что запуск протокола участником был выполнен непосредственно перед завершением запуска протокола участником. Если для свойства *Alive* потребовать, чтобы участник считал, что он взаимодействует с участником, то получаем определение свойства *Weakagree*.

2. При выполнении свойства *Weakagree* протокол гарантирует участнику A слабую согласованность (англ. *weak agreement*) с другим участником B, если участник, действующий как инициатор протокола, после завершения протокола, как он полагает, с участником:

- получает подтверждение того, что действительно являлся участником этого протокола;
- участник A полагает, что взаимодействует с участником B.

3. При выполнении свойства *Niagree* протокол гарантирует участнику одностороннюю аутентификацию с согласованием данных (дословно неинъективную согласованность, от англ. *non-injective agreement*) с другим участником на некотором наборе данных, если, когда бы ни был завершен запуск протокола участником, как он полагает, с участником в роли ответчика:

- участник получает подтверждение того, что действительно был участником данного протокола;
- участник выступал в нем в роли ответчика;
- оба участника согласны с тем, какие данные из набора они использовали при обмене.

4. Свойство *Niagree* означает, что если протокол обеспечивает одностороннюю аутентификацию с согласованием данных на всех шагах выполнения протокола, то можно говорить о выполнении полной согласованности.

5. Свойство синхронности *Nisynch* говорит о наличии общей согласованности, но дополнительно требует, чтобы событию получения каждого сообщения предшествовало событие отправления этого сообщения.

6. Данные определения позволяют разбить процесс проверки выполнимости свойства взаимной аутентификации из [5] на последовательные проверки перечисленных выше свойств безопасности. При этом взаимная аутентификация выполняется в случае выполнения свойства *Nisynch* для обоих участников протокола.

Результаты анализа приведены на рис. 2.

Результаты анализа исследуемой модели протокола, приведенные на рис. 2, показали формальное нарушение свойств *Alive*, *Weakagree* и *Nisynch*. При этом свойство *Niagree* – выполнено.

Формальное нарушение свойств безопасности *Alive* и *Weakagree* связано с тем, что нарушитель может инициировать начало работы протокола, отправляя сообщение *GET_CHALLENGE*. Протокол не дает участникам взаимодействия (*TC* и *VU*) подтверждения того, что участник инициировавший начало работы протокола действительно является легальным участником протокола, тем самым задавая формальное нарушение указанных свойств.

Аналогично свойство *Nisynch* может быть формально нарушено за счет инициирования на первом шаге протокола нарушителем сообщения *GET_CHALLANGE*. При этом дальнейший обмен данными будет проводиться между легальными участниками (*TC* и *VU*). В данном случае формально нарушается предположение о взаимодействии с легальным участником.

Claim				Status		Comments	Patterns
VUTC	VU	VUTC,VU1	Secret kt	Ok		No attacks within bounds.	
		VUTC,VU2	Secret LOW(KDF(PI(ECP(kb,ECP(kt,P))),TC,VU))	Ok		No attacks within bounds.	
		VUTC,VU3	Alive	Fail	Falsified	At least 3 attacks.	3 attacks
		VUTC,VU4	Weakagree	Fail	Falsified	At least 3 attacks.	3 attacks
		VUTC,VU5	Nisynch	Fail	Falsified	At least 2 attacks.	2 attacks
		VUTC,VU6	Niagree	Ok		No attacks within bounds.	
	TC	VUTC,TC1	Secret kb	Ok		No attacks within bounds.	
		VUTC,TC2	Secret LOW(KDF(PI(ECP(kt,ECP(kb,P))),TC,VU))	Ok		No attacks within bounds.	
		VUTC,TC3	Alive	Fail	Falsified	At least 3 attacks.	3 attacks
		VUTC,TC4	Nisynch	Fail	Falsified	At least 2 attacks.	2 attacks
		VUTC,TC5	Niagree	Ok		No attacks within bounds.	
		VUTC,TC6	Weakagree	Fail	Falsified	At least 3 attacks.	3 attacks

Рис. 2. Результаты анализа при помощи Scyther
(Fig. 2. The results of the analysis using Scyther)

Из графического изображения некоторых найденных средством *Scyther* формальных нарушений свойств безопасности видно, что они происходят из-за того, что бортовое устройство направляет карте тахографа запрос *GET_CHALLANGE*. При этом направляемый запрос не содержит каких-либо данных, используемых в протоколе в дальнейшем, а наличие данного запроса обусловлено конструктивными особенностями обмена информацией между бортовым устройством и картой тахографа.

Найденные средством *Scyther* нарушения свойств безопасности действительно носят формальный характер: данные нарушения не позволяют нарушителю получить какую-либо дополнительную информацию и не оказывают какого-либо влияния на дальнейшее выполнение протокола. В связи с этим можно считать, что, несмотря на формальное нарушение ряда свойств безопасности, исследование протокола при помощи средства *Scyther* также не выявило угрозы выработать общий с легальным участником ключ или выдать себя за легального участника протокола.

Заключение

Анализ модели угроз безопасности протокола выработки общего ключа с аутентификацией абонентов, предназначенного для использования в тахографах, устанавливаемых на транспортные средства [3], показывает, что исследуемый протокол обеспечивает достаточность мер противодействия известным атакам. Найденные возможные атаки носят формальный характер, не позволяя нарушителю получить какую-либо дополнительную информацию для конструктивной компрометации протокола.

СПИСОК ЛИТЕРАТУРЫ:

1. Европейское соглашение по работе экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР). Европейская экономическая комиссия. Комитет по внутреннему транспорту. Записка секретариата. Добавление 1В к приложению ЕСТР, содержащее требования к конструкции, испытаниям, установке и инспекции цифрового контрольного устройства, используемого на автомобильном транспорте. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
2. Приказ Минтранса России от 13 февраля 2013 г. № 36. URL: http://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf.
3. Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. – 2016. – 36 с.
4. Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Криптографические механизмы аутентификации для применения в контрольных устройствах, обеспечивающих работу автотранспорта (Проект второй редакции). – 2017. – 21 с.
5. Горбатов, Виктор С; Жуков, Игорь Ю; Мурашов, Олег Н. Криптографический протокол аутентификации и выработки общего ключа контрольных устройств автотранспорта. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/274>. Дата доступа: 09 dec. 2018. doi:http://dx.doi.org/10.26583/bit.2017.4.03.
6. van Oorschot P.C., Wiener M.J., Parallel Collision Search with Cryptanalytic Applications// Journal of Cryptology – Vol. 12 – 1999. – 1-28 P.
7. Blanchet B., An Efficient Cryptographic Protocol Verifier Based on Prolog Rules, Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW), Cape Breton, IEEE Computer Society, 2009. P. 82 – 96.
8. Armando A. et al., The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. Proceedings of Computer Aided Verification'05 (CAV), Vol. 3576 of Lecture Notes in Computer Science, Springer, 2005, P. 281 – 285.
9. AVISPA stands for Automated Validation of Internet Security Protocols and Applications. URL: http://www.avispa-project.org/. (Дата обращения: 09.12.2018).
10. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия. – 2009. – 272 с.
11. Cremers C. J. F. Scyther - Semantics and Verification of Security Protocols// Ph. D. dissertation. Eindhoven University of Technology, 2006.
12. Lowe G. A hierarchy of authentication specifications. In Proc. 10th IEEE Computer Security Foundations Workshop (CSFW). P. 31 – 44. IEEE, 1997.
13. Blanchet B., An Efficient Cryptographic Protocol Verifier Based on Prolog Rules, Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW), Cape Breton, IEEE Computer Society, 2009, P. 82 – 96.

REFERENCES:

[1] European Agreement concerning the Work of Crews of Vehicles engaged in International Road Transport (AETR). economic commission. Inland transport Committee. Note by the Secretariat. Appendix 1B to Annex AETR, which contains requirements for the design, testing, installation and inspection of a digital control device used in road transport. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
[2] Order of the Ministry of transport of Russia of February 13, 2013 № 36. URL: http://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf. (in Russian).
[3] Rosstandart. Information technology. Cryptographic protection of information. Recommendations for standardization. Principles of development and modernization of encryption (cryptographic) means of information security. – 2016. – 36 p. (in Russian).
[4] Rosstandart. Information technology. Cryptographic protection of information. Recommendations for standardization. Cryptographic authentication mechanisms for use in control devices that ensure the operation of vehicles (draft second edition). – 2017. – 21 p. (in Russian).
[5] Gorbatov, Victor S.; Zhukov, Igor Y.; Murashov, Oleg N. Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security (Russia), [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/274>. Date accessed: 09 dec. 2018. doi:http://dx.doi.org/10.26583/bit.2017.4.03. (in Russian).
[6] van Oorschot P.C., Wiener M.J., Parallel Collision Search with Cryptanalytic Applications. Journal of Cryptology – Vol. 12 – 1999. – 1 – 28 p.
[7] Blanchet B., An Efficient Cryptographic Protocol Verifier Based on Prolog Rules, Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW), Cape Breton, IEEE Computer Society, 2009. P. 82 – 96.
[8] Armando A. et al., The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. Proceedings of Computer Aided Verification'05 (CAV), Vol. 3576 of Lecture Notes in Computer Science, Springer, 2005. P. 281 – 285.

[9] AVISPA stands for Automated Validation of Internet Security Protocols and Applications. URL: http://www.avispa-project.org/. (accessed: 09.12.2018).
[10] Cheremushkin A.V. Kriptograficheskie protokoly: osnovnye svoystva i uyazvimosti [Cryptographic Protocols: Basic Properties and Vulnerability]. Moscow, Akademiya, 2009. (in Russian).
[11] Cremers C. J. F. Scyther - Semantics and Verification of Security Protocols. Ph. D. dissertation. Eindhoven University of Technology, 2006.
[12] Lowe G. A hierarchy of authentication specifications. In Proc. 10th IEEE Computer Security Foundations Workshop (CSFW). P. 31 – 44. IEEE, 1997.
[13] Blanchet B., An Efficient Cryptographic Protocol Verifier Based on Prolog Rules, Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW), Cape Breton, IEEE Computer Society, 2009. P. 82 – 96.

Поступила в редакцию – 16 декабря 2018 г. Окончательный вариант – 4 февраля 2019 г.
Received – December 16, 2018. The final version – February 22, 2019.