Исследование защищенности мобильных приложений для каршеринга

Июнь 2018

ОФИЦИАЛЬНАЯ ИНФОРМАЦИЯ (DISCLAIMER)

Данный отчет был подготовлен компанией Solar Security с целью исследования программных решений для каршеринга и испытания их функциональности. Отчет может быть использован исключительно в информационных целях.

Информация, полученная в результате проведенного исследования и изложенная в отчете, была получена при использовании технологии автоматического бинарного анализа, без осуществления реверс-инжиниринга (декомпиляции исходного кода).

Иная, содержащаяся в настоящем отчете информация была получена из источников, которые, по мнению Solar Security, являются надежными, однако Solar Security не гарантирует точности и полноты информации для любых целей.

Все упомянутые в отчете товарные знаки являются собственностью их владельцев.

Информация, представленная в этом отчете, не должна быть истолкована, прямо или косвенно, как информация, содержащая рекомендации Solar Security по инвестициям или использованию программных решений. Все мнения и оценки, содержащиеся в настоящем материале, отражают мнение авторов на день публикации и подлежат изменению без предупреждения.

Solar Security не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в данном отчете, включая опубликованные мнения или заключения, а также за последствия, вызванные неполнотой или неточностью представленной информации.

Дополнительная информация предоставляется по запросу.

МЕТОДОЛОГИЯ

Для сравнения уровня защищенности были выбраны популярные мобильные приложения для каршеринга – Делимобиль[1], Карусель[2], Яндекс.Драйв[3], Anytime[4], BelkaCar[5], CAR4YOU[6], CAR5[7], Carenda[8], Carlion[9], Colesa.com[10], EasyRide[11], Lifcar[12], MatreshCar[13], Rent-a-Ride[14], RENTMEE[15], TimCar[16]. Все приложения рассматривались в вариантах для мобильных операционных систем iOS и Android.

Анализ безопасности кода осуществлялся автоматически, с помощью решения Solar inCode – российского программного продукта для проверки безопасности приложений. Решение использует методы статического, динамического и интерактивного анализа. При подготовке исследования модуль декомпиляции и деобфускации был отключен. Статический анализ производился в отношении бинарного кода мобильных приложений в автоматическом режиме.

Проанализировав приложения, Solar inCode сформировал отчеты, в которых была приведена общая оценка защищенности приложения по пятибалльной системе, список обнаруженных закладок, известных уязвимостей и ошибок, ранжированных по уровню критичности. Эти отчеты легли в основу данного исследования.

Оценка защищенности приложения считается автоматически и учитывает такие показатели, как количество различных типов известных уязвимостей критического и среднего уровня и частота их повторяемости (количество вхождений) в коде. Вклад количества критических уязвимостей более высок, при этом он не учитывает объем кода. Количество уязвимостей среднего уровня учитывается с поправкой на объем кода.

Основываясь на выборке из последних 500 сканирований, Solar inCode рассчитывает средний по отрасли уровень защищенности приложений. На момент подготовки отчета он составлял 2,2 балла.

---

[1] Делимобиль for iOS v. 5.0.3; Делимобиль for Android v. 5.0.4.
[2] Карусель for iOS v. 1.04; Карусель for Android v. 1.00.
[3] Яндекс.Драйв for iOS v. 1.2.2; Яндекс.Драйв for Android v. 1.2.0.
[4] Anytime for iOS v. 3.9.6; Anytime for Android v. 3.9.6.
[5] BelkaCar for iOS v. 1.8.1; BelkaCar for Android v. 1.8.0.
[6] CAR4YOU for iOS v. 1.6; CAR4YOU for Android v. 0.8.5.
[7] CAR5 for iOS v. 2.70; CAR5 for Android v. 2.46.
[8] Carenda for iOS v. 1.6; Carenda for Android v. 1.0.7.
[9] Carlion for iOS v. 1.3; Carlion for Android v. 1.1.5.
[10] Colesa.com for iOS v. 1.0.28; Colesa.com for Android v. 2.1.1.
[11] EasyRide for iOS v. 1.7; EasyRide for Android v. 0.8.8.5_m-2-g21ff49b.
[12] Lifcar for iOS v. 1.0.5; Lifcar for Android v. 1.00.
[13] MatreshCar for iOS v. 1.0.2; MatreshCar for Android v. 1.109.
[14] Rent-a-Ride for iOS v. 1.7; Rent-a-Ride for Android v. 1.2.9.
[15] RENTMEE for iOS v. 2.1.15 (1); RENTMEE for Android v. 2.1.20.
[16] TimCar for iOS v. 2.0.0; TimCar for Android v. 1.103.

ВВЕДЕНИЕ

Компания Solar Security, разработчик продуктов и сервисов для целевого мониторинга и оперативного управления информационной безопасностью, представляет сравнение защищенности наиболее популярных мобильных приложений для каршеринга.

Сервисы каршеринга приобретают все большую популярность. По словам главы столичного департамента транспорта, вице-мэра Москвы Максима Ликсутова, число регистраций сервисах краткосрочной аренды автомобиля в Москве к концу 2017 года превысило 1 миллион, а количество поездок за год достигло 5,4 миллиона. В конце 2016 года их было менее 300 тысяч. Таким образом, за год число зарегистрированных пользователей выросло почти в 4 раза.

Основным средством для использования каршеринга являются мобильные приложения, которые, как и все прочие, могут быть содержать различные уязвимости. Для пользователя каршеринга основные риски связаны с возможным похищением аккаунта. В этом случае злоумышленник сможет свободно распоряжаться автомобилем, который в этот момент якобы использует другой человек. Очевидно, что это открывает широкие возможности для различных злоупотреблений и правонарушений.

Это первое исследование, которое рассматривает угрозы безопасности мобильных приложений для каршеринга – от недостаточно надежных методов защиты паролей до уязвимости приложения к различным типам известных атак и эксплойтов.

НАЙДЕННЫЕ ОШИБКИ И ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ

Сканирование показало, что чаще всего в приложениях для каршеринга (как в iOS-, так и в Android-версиях) встречаются такие известные уязвимости, как слабые алгоритмы хеширования, небезопасная реализация SSL, использование незащищенного протокола передачи данных HTTP.

Анализ приложений под Android выявил, что более половины из них уязвимы к атакам типа DoS и DNS spoofing. Примерно в трети случаев наблюдается небезопасное хранение конфиденциальных данных, в том числе паролей. Кроме того, в большинстве рассматриваемых Android-приложений обнаружена такая недекларированная возможность, как специальная учетная запись, прописанная непосредственно в исходном коде.

Для iOS-версий приложений характерны такие уязвимости, как слабый алгоритм шифрования, использование буфера обмена и небезопасная аутентификация. Почти во всех рассматриваемых приложениях под iOS также детектировано использование незащищенного протокола HTTP и небезопасное хранение конфиденциальных данных. В одном случае было обнаружено, что аутентификация по отпечатку пальца в приложении реализована небезопасно.

СЛАБЫЙ АЛГОРИТМ ХЕШИРОВАНИЯ

Хеширование – это криптографическая операция, применяемая в работе большинства современных приложений и ИТ-систем – например, для безопасной передачи и хранения паролей. Одно из важнейших требований к алгоритму хеширования (хеш-функции) состоит в его криптостойкости, то есть способности противостоять взлому и дешифрованию.

На данный момент существует ряд различных алгоритмов хеширования, многие из которых считаются устаревшими и ненадежными ввиду того, что они обладают известными и многократно описанными уязвимостями. Среди них – MD2, MD5 и SHA1. Если эти хеш-функции применяются для хранения ценной информации (например, паролей), ее конфиденциальность потенциально находится под угрозой и может быть нарушена.

За одним исключением, каждое из проанализированных приложений под Android и iOS содержит данную уязвимость.

СЛАБЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Шифрование данных является одним из ключевых условий того, что они не будут скомпрометированы злоумышленником. Однако, как и в случае с хешированием, некоторые алгоритмы шифрования не обеспечивают достаточную криптостойкость, а значит, и достаточную защиту для приложений, работающих с ценными данными.

Например, криптоалгоритм DES из-за небольшой длины ключа (56 бит) может быть взломан методом полного перебора. В случае успеха злоумышленник получает доступ ко всем конфиденциальным данным пользователя.

Данная уязвимость встречается примерно в трети проанализированных приложений под iOS.

НЕБЕЗОПАСНАЯ РЕАЛИЗАЦИЯ SSL

При установлении защищенного (шифрованного) соединения приложение проверяет полученный от сервера сертификат, чтобы убедиться в том, что отправляет данные легитимному получателю, а не злоумышленнику.

В приложениях под Android иногда встречается уязвимость, суть которой состоит в том, что при небезопасной реализации SSL приложение проверяет не все параметры сертификата. Вследствие этого злоумышленник может предоставить самоподписанный сертификат и «выдать» себя за сервер приложения, реализовав таким образом атаку Man-in-the-Middle («человек посередине»). Данная уязвимость может быть легко проэксплуатирована – например, при использовании жертвой публичного Wi-Fi. При этом все данные, передаваемые с помощью приложения, будут похищены, а злоумышленник сможет произвольно менять запросы к серверу и выполнять в приложении любые действия от имени легитимного пользователя. В случае с мобильными приложениями для каршеринга опасность состоит в том, что злоумышленник может похитить данные банковской карты, привязанной к аккаунту, а также сам аккаунт.

Уязвимость обнаружена в трех приложениях под Android.

НДВ: СПЕЦИАЛЬНАЯ УЧЕТНАЯ ЗАПИСЬ

Наличие в исходном коде специальной учетной записи может свидетельствовать о наличии в приложении бэкдора. Есть и другой вариант: разработчики часто используют специальную учётную запись с повышенными привилегиями при отладке приложения, и иногда соответствующие участки кода по ошибке сохраняются в финальной версии. В любом случае, такая уязвимость несет с собой серьезные угрозы.

Если специальная учетная запись оставлена умышленно, это значит, что разработчик может воспользоваться ей в любой момент, и при этом его действия нельзя проконтролировать. В таком случае это либо бэкдор, который планируется использовать в мошеннических целях, либо запись, оставленная «на всякий случай». Очевидно, что в случае конфликта с разработчиком (например, в ходе увольнения) последствия для пользователей приложения могут быть непредсказуемыми.

Если даже специальную учетную запись просто забыли удалить, она продолжает подвергать риску безопасность приложения и пользовательских данных. Злоумышленник может использовать широко доступные сегодня инструменты декомпиляции, извлечь константные строки, задающие параметры специальной учётной записи, и получить доступ к приложению.

Такая уязвимость обнаружена в 14 из 16 проанализированных приложений под Android.

ИСПОЛЬЗОВАНИЕ БУФЕРА ОБМЕНА

Ценные данные, передаваемые через буфер обмена, могут быть доступны приложениям и таким образом скомпрометированы.

Данные, скопированные с использованием функций «вырезать/скопировать» в iOS, поступают в буфер обмена, доступ к которому могут получить сторонние приложения. Таким образом информация может быть скомпрометирована, и, если она была конфиденциальной, последствия могут быть достаточно серьезными.

Уязвимость обнаружена практически в каждом iOS-приложении.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ КАРШЕРИНГА

Оценка защищенности приложения считается автоматически и учитывает такие показатели, как количество различных типов известных уязвимостей критического и среднего уровня и частота их повторяемости (количество вхождений) в коде.

Уровень защищенности Android-версий:

Мессенджер	Критические уязвимости (кол-во уникальных)	Критические уязвимости (кол-во вхождений)	Уязвимости среднего уровня (кол-во уникальных)	Уязвимости среднего уровня (кол-во вхождений)	Общий уровень защищенности
Яндекс.Драйв	0	0	2	16	4.2/5.0
Anytime	1	1	21	211	3.3/5.0
Lifcar	1	1	25	267	3.3/5.0
Карусель	1	1	25	269	3.3/5.0
Carenda	2	3	19	188	2.7/5.0
Carlion	2	5	19	177	2.3/5.0
RENTMEE	2	5	21	212	2.3/5.0
Делимобиль	1	5	20	543	2.1/5.0
EasyRide	2	6	22	200	2.1/5.0
CAR4YOU	2	6	21	222	2.1/5.0
TimCar	1	7	24	273	2.0/5.0
MatreshCar	1	7	25	331	1.9/5.0
Colesa.com	2	8	21	318	1.8/5.0
Rent-a-Ride	3	11	25	315	1.6/5.0
BelkaCar	4	10	29	342	1.6/5.0
CAR5	3	13	25	306	1.4/5.0

Как видно из таблицы, по уровню защищенности «Яндекс.Драйв» лидирует с большим отрывом от конкурентов. Отсутствие известных критических уязвимостей и очень малое количество уязвимостей среднего уровня (на порядок меньше, чем у конкурентов) позволяет говорить о том, что приложение достаточно безопасно как в части защиты данных пользователей, так и в устойчивости к атакам с помощью троянов или известных эксплойтов.

Приложения Anytime, Lifcar и Карусель находятся примерно на одном уровне и, в целом, демонстрируют неплохой результат по отрасли. Каждое из них содержит серьезную уязвимость, но она встречается в исходном коде лишь однажды, поэтому итоговый уровень защищенности остается достаточно высоким – 3,3. На третье место можно поставить приложение Carenda.

Прочих приложения содержат в исходном коде не менее 5 вхождений критических уязвимостей и по несколько сотен уязвимостей среднего уровня, что нельзя назвать удовлетворительным уровнем защищенности.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ КАРШЕРИНГА

Уровень защищенности iOS-версий:

Мессенджер	Критические уязвимости (кол-во уникальных)	Критические уязвимости (кол-во вхождений)	Уязвимости среднего уровня (кол-во уникальных)	Уязвимости среднего уровня (кол-во вхождений)	Общий уровень защищенности
Carenda	1	4	6	281	2.4/5.0
CAR4YOU	1	4	6	284	2.4/5.0
EasyRide	1	4	6	299	2.4/5.0
Карусель	1	4	6	384	2.4/5.0
Lifcar	1	4	6	410	2.4/5.0
Яндекс.Драйв	2	6	7	879	2.0/5.0
Colesa.com	1	8	6	410	1.8/5.0
Делимобиль	1	11	6	411	1.6/5.0
Rent-a-Ride	1	12	6	237	1.5/5.0
TimCar	2	20	6	363	1.1/5.0
Carlion	1	20	8	325	1.1/5.0
CAR5	2	20	6	521	1.0/5.0
MatreshCar	2	20	7	372	1.0/5.0
BelkaCar	2	21	7	709	1.0/5.0
RENTMEE	2	29	6	314	0.8/5.0
Anytime	1	42	6	334	0.5/5.0

Приложения под iOS демонстрируют меньший разброс по уровню защищенности. Carenda, CAR4YOU, EasyRide, Карусель и Lifcar показали практически одинаковые (и не самые лучшие) результаты. За ними следует Яндекс. Драйв, чье iOS-приложение неожиданно уступает версии под Android. То же относится и к Anytime – в версии под Android приложение занимало 2 место в списке, тогда как версия под iOS содержит очень много вхождений критических уязвимостей.

ВЫВОДЫ

Исследование показало, что чаще всего в приложениях для каршеринга (как в iOS-, так и в Android-версиях) встречаются такие известные уязвимости, как слабые алгоритмы хеширования, небезопасная реализация SSL, использование незащищенного протокола передачи данных HTTP.

Анализ приложений под Android выявил, что более половины из них уязвимы к атакам типа DoS и DNS spoofing. Примерно в трети случаев наблюдается небезопасное хранение конфиденциальных данных, в том числе паролей. Кроме того, в большинстве рассматриваемых Android-приложений обнаружена такая недекларированная возможность, как специальная учетная запись, прописанная непосредственно в исходном коде.

Для iOS-версий приложений характерны такие уязвимости, как слабый алгоритм шифрования, использование буфера обмена и небезопасная аутентификация. Почти во всех рассматриваемых приложениях под iOS также детектировано использование незащищенного протокола HTTP и небезопасное хранение конфиденциальных данных. В одном случае было обнаружено, что аутентификация по отпечатку пальца в приложении реализована небезопасно.

В среднем приложения для платформы Android защищены несколько лучше, чем их аналоги под iOS.

Наиболее защищенные Android-приложения для каршеринга – Яндекс.Драйв, Anytime, Lifcar, Карусель и Carenda. Наиболее уязвимые – Rent-a-Ride, BelkaCar и CAR5.

Лидеры по уровню защищенности среди iOS-приложений – это Carenda, CAR4YOU, EasyRide, Карусель и Lifcar. Самые низкие показатели продемонстрировали BelkaCar, RENTMEE и Anytime.

КОНТАКТЫ

Solar Security

127 015 г. Москва, ул. Вятская 35/4,
БЦ «Вятка» 1 подъезд

Телефон офиса: +7 499 755 07 70
Техническая поддержка: +7 499 755 02 20

Email: info@solarsecurity.ru

www.solarsecurity.ru