Ростелеком
Солар

Исследование защищенности мобильных приложений знакомств.
Сентябрь 2019.

Официальная информация (disclaimer)

Данный отчет был подготовлен компанией «Ростелеком-Солар» с целью исследования и испытания функциональности популярных мобильных приложений знакомств. 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 выполнения реверс-инжиниринга (декомпиляции исходного кода).

Иная содержащаяся в настоящем отчете информация была получена из источников, которые, по мнению «Ростелеком-Солар», являются надежными, однако «Ростелеком-Солар» 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 «Ростелеком-Солар» 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.

«Ростелеком-Солар» 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 знакомств – Tinder[1], Badoo[2], LovePlanet[3], Mamba[4], Фотострана[5], Topface[6], ДругВокруг[7], MyFriends[8], Galaxy[9], Знакомства@mail.ru[10], Teamo[11] и Hitwe[12]. Все приложения рассматривались в вариантах для мобильных операционных систем iOS и Android.

Анализ безопасности кода осуществлялся автоматически с помощью Solar appScreener – российского программного продукта для проверки защищенности 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 appScreener 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 высчитывается 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 appScreener рассчитывает средний по отрасли уровень защищенности приложений. На момент подготовки отчета он составлял 2,2 балла.

---

[1] Tinder for iOS v. 10.16.0; Tinder for Android v. 10.18.0
[2] Badoo for iOS v. 5.121.0; Badoo for Android (версия зависит от устройства)
[3] LovePlanet for iOS v. 2.76; LovePlanet for Android v. 2.94.5
[4] Mamba for iOS v. 3.2.27; Mamba for Android v. 3.100.3
[5] Фотострана for iOS v. 1.3.9; Фотострана for Android v. 2.8.11
[6] Topface for iOS v. 3.14.6; Topface for Android v. 3.4.42
[7] ДругВокруг for iOS v. 3.7.16; ДругВокруг for Android (версия зависит от устройства)
[8] MyFriends for iOS v. 1.8.1; MyFriends for Android v. 1.8.3.808
[9] Galaxy for iOS v. 9.4.3; Galaxy for Android (версия зависит от устройства)
[10] Знакомства@mail.ru for iOS v. 3.2.42; Знакомства@mail.ru for Android v. 3.104.0
[11] Teamo for iOS v 4.1.9., Teamo for Android v. 2.7.12
[12] Hitwe for iOS v. 3.4.6, Hitwe for Android v. 4.3.4

Введение

Компания «Ростелеком-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет сравнение защищенности наиболее популярных мобильных приложений знакомств.

С каждым годом сервисы онлайн-знакомств становятся все более привлекательными как для целевой аудитории, так и для инвесторов. По данным аналитика японского холдинга Nomura Instinet Марка Келли, к 2020 году объём мирового рынка онлайн-знакомств вырастет до $12 млрд. «Примерно половина интернет-пользователей не состоят в браке, и мы предполагаем: к 2020 году 20% из них будут готовы использовать сервисы онлайн-знакомств, а это 310 млн человек во всём мире, исключая Китай», — сообщил Келли.[13]

По данным портала statista.com, объем российского рынка онлайн-знакомств в 2017 году оценивался в $66 млн. При этом актуальным рыночным трендом в 2018-м году был назван переход аудитории на мобильные приложения, доля которых к концу года, по мнению аналитиков, достигла 60%.[14]

В связи с востребованностью данного направления эксперты компании «Ростелеком-Солар» провели исследование уровня защищенности популярных мобильных приложений знакомств с помощью инструмента Solar appScreener.

Сервисы для анализа были отобраны согласно критерию популярности: количеству скачиваний в Google Play и App Store, а также позиции в рейтинге сайтов знакомств RatingDatings.ru[15].

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

---

[13] Markets Insider. Online dating could be worth $12 billion - and it's all thanks to Tinder, analyst says (MTCH)
[14] Forbes.ru. Ты мне друг: как устроен рынок онлайн-знакомств в России
[15] RatingDatings.ru Лучшие приложения для знакомств на iPhone августа 2019 года

Найденные ошибки и потенциальные уязвимости

Проверка исследуемых приложений показала: подавляющее большинство Android-версий содержат ключ шифрования, заданный в исходном коде. Что касается приложений знакомств на iOS, то все без исключения проанализированные программы имеют слабый алгоритм хеширования. А более половины iOS-версий – еще и слабый алгоритм шифрования. Таким образом, в отличие от предшествующих двух исследований, в данном отчете не оказалось ни одного приложения, которое не содержало бы критической уязвимости.

По результатам анализа Android-версий выяснилось, что в 83% приложений знакомств ключ шифрования задан в исходном коде. Эта критичная уязвимость может привести к компрометации всех данных, содержащихся в программе. Кроме того, все исследованные приложения под Android допускают внутреннюю утечку ценной информации и возможность обхода проверок безопасности Security Manager (угроза выполнения злоумышленником произвольного кода).

Что касается iOS-версий приложений, принявших участие в исследовании, – все они содержат слабый алгоритм хеширования (риск утраты конфиденциальности данных). А более чем в половине из них заложены слабые алгоритмы шифрования (потенциально могут быть взломаны методом полного перебора). Наиболее частыми «спутниками» iOS-приложений знакомств являются такие уязвимости среднего уровня критичности, как использование NSLog (возможность осуществить атаку на приложение) и небезопасная рефлексия (возможность выполнения вредоносного кода или использования недокументированных возможностей приложения).

КЛЮЧ ШИФРОВАНИЯ ЗАДАН В ИСХОДНОМ КОДЕ

Этот тип уязвимости может привести к компрометации данных приложения. Устранить угрозы безопасности, связанные с заданными в исходном коде ключами, достаточно сложно. Такие ключи как минимум доступны каждому разработчику приложения. Более того, после установки приложения удалить из его кода ключ можно только через обновление. Константные строки легко извлекаются из скомпилированного приложения декомпиляторами. Поэтому злоумышленнику даже не нужен доступ к исходному коду, чтобы узнать значение используемого ключа.

Эту уязвимость содержат **83% мобильных приложений знакомств на базе Android.**

ВНУТРЕННЯЯ УТЕЧКА ЦЕННОЙ ИНФОРМАЦИИ

В случае утечки подробной информации о конфигурации системы внутренний злоумышленник может воспользоваться этими данными для разработки плана атаки.

В зависимости от настроек приложения техническая информация и сообщения об ошибках в приложении могут логироваться, выводиться в консоль управления или передаваться пользователю. В некоторых случаях внутренний злоумышленник, например, сотрудник компании-разработчика или заказчика системы по сообщению об ошибке может узнать об имеющейся в приложении уязвимости. Например, ошибка базы данных может свидетельствовать об уязвимости к атакам типа SQL injection. Информация о версии операционной системы, сервера приложений или конфигурации системы может стать основой для планирования атаки. Поэтому следует исключить из внутренних сообщений об ошибках слишком подробную техническую информацию о системе и её конфигурации.

Этот вид уязвимости встречается **во всех проанализированных приложениях для ОС Android**.

ОБХОД ПРОВЕРОК БЕЗОПАСНОСТИ SECURITYMANAGER

Приложение допускает небезопасный вызов метода из недоверенного кода. В результате злоумышленник получает доступ к пакету с ограниченным доступом и может выполнять произвольный код.

Небезопасный вызов метода из недоверенного кода позволяет обойти проверки безопасности SecurityManager, контролирующие наличие достаточных привилегий по всей цепочке вызовов. В результате один из элементов цепочки может получить доступ к ресурсу, не обладая достаточными на то правами.

Данная уязвимость содержится **во всех исследованных Android-приложениях**.

СЛАБЫЙ АЛГОРИТМ ХЕШИРОВАНИЯ

Примененная в приложении хеш-функция не является безопасной и может привести к утрате конфиденциальности данных.

Хеш-функции представляют собой инструмент криптографии, используемый для выполнения самых разных задач – аутентификации, проверки целостности данных, защиты файлов и многого другого. Алгоритмы хеширования отличаются криптостойкостью, сложностью и другими параметрами.

Некоторые хеш-функции имеют известные уязвимости, и нахождение коллизий для них не является трудоемкой задачей. Соответственно, если эти функции применяются для хранения ценной информации (например, паролей), её конфиденциальность может быть нарушена. Хеш-функция, используемая для хранения паролей, помимо устойчивости к коллизиям, должна быть не слишком быстрой, чтобы осложнять атаку путём полного перебора.

Приведем пример атаки с использованием данной уязвимости. Пусть пароли пользователей хранятся на сервере в зашифрованном виде с использованием небезопасной хеш-функции. Сначала злоумышленник получает доступ к базе зашифрованных паролей. Затем, используя уязвимость алгоритма хеширования, он вычисляет строку, для которой алгоритм хеширования даёт то же значение, что и для пароля пользователя. Затем злоумышленник проходит аутентификацию, используя вычисленную строку.

Уязвимости типа «слабая криптография» (Insufficient Cryptography) занимают **пятое место в рейтинге уязвимостей приложений «OWASP Top 10 Mobile Risks».**

Данный вид уязвимости содержится **во всех просканированных iOS приложениях**.

СЛАБЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Если в приложении использованы устаревшие алгоритмы шифрования, они создают риски для решений, оперирующих ценными данными. Такие алгоритмы из-за небольшой длины ключа можно взломать методом полного перебора.

Поэтому разработчикам приложений, оперирующих особо ценными данными пользователей (данными банковских счетов, платежных карт и т.п.), необходимо использовать протестированные версии стандартизированных алгоритмов шифрования с достаточной длиной ключа.

«Слабая криптография» (Insufficient Cryptography) является одним из наиболее критичных видов уязвимостей мобильных приложений по версии **«OWASP Top 10 Mobile Risks» (пятое место в рейтинге).**

Эту уязвимость авторам исследования удалось обнаружить **более чем в половине приложений под iOS.**

ИСПОЛЬЗОВАНИЕ NSLOG

Использовать этот метод можно в процессе отладки программного обеспечения, но никак не на стадии коммерческой эксплуатации приложения. Все сообщения, генерируемые с помощью NSLog, можно просмотреть посредством XCode (среды разработки ПО под iOS). В результате

может быть раскрыта информация, которая позволит злоумышленнику реализовать атаку на приложение. Уже не говоря о том, что активное использование NSLog серьезно замедляет работу приложения.

Данным видом уязвимости охвачены **все iOS-версии приложений знакомств.**

НЕБЕЗОПАСНАЯ РЕФЛЕКСИЯ

С помощью небезопасной рефлексии злоумышленник может взять приложение под свой контроль, обойти механизмы аутентификации и ограничения доступа и выполнить произвольный вредоносный код, поскольку этот метод принимает в качестве аргумента данные из недоверенного источника.

Если рефлексия используется для вызова произвольного кода, это может привести к завершению работы приложения или зависанию. Вызвав неправильный код, злоумышленник инициирует ошибку времени выполнения, которая приводит к утечке конфиденциальной информации в сообщении об ошибке.

Уязвимости типа «подделка кода» (Code Tampering) занимают **восьмое место в рейтинге уязвимостей приложений «OWASP Top 10 Mobile Risks».**

Метод, реализующий рефлексию, встречается **во всех iOS-приложениях.**

Сравнительный анализ безопасности мобильных приложений знакомств

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

Уровень защищенности Android-версий:

Приложение	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
Teamo	1	1	30	268	3.2/5.0
Фотострана	1	1	32	387	3.2/5.0
ДругВокруг	1	1	32	526	3.1/5.0
Galaxy	2	2	29	319	2.9/5.0
Badoo	1	2	30	333	2.9/5.0
Hitwe	1	3	27	264	2.6/5.0
Tinder	2	3	29	389	2.6/5.0
Mamba	3	4	31	392	2.4/5.0
Знакомства@mail.ru	3	4	31	406	2.4/5.0
LovePlanet	3	5	34	708	2.1/5.0
Topface	4	7	32	317	2.0/5.0
MyFriends	1	7	32	603	1.9/5.0

Из вышеприведенной сравнительной таблицы видно, что безусловного лидера по уровню защищенности среди Android-версий приложений знакомств нет. Приложения Teamo и Фотострана демонстрируют самый высокий показатель защищенности 3.2 балла. При этом приложение Фотострана содержит чуть больше уязвимостей и вхождений среднего уровня, что, однако, не повлияло на показатель общего уровня его защищенности за счет чуть меньшего количества содержащихся в нем уязвимостей низкого уровня. Немного отстает от лидеров по уровню защищенности приложение ДругВокруг (3.1 балла).

Неожиданно в приложении Знакомства@mail.ru (Mail.ru Group) для ОС Android была обнаружена высококритичная уязвимость, входящая в международный рейтинг наиболее критичных уязвимостей «OWASP Mobile Top 10 2016». В случае ее успешной эксплуатации злоумышленник может получить доступ к учетной записи пользователя приложения и, соответственно, ко всей незашифрованной информации, которое приложение передает на сервер.

Благодаря уязвимости данного класса хакер может стать обладателем логина и пароля пользователя, с их помощью войти в приложение и получить доступ к переписке, видео и аудио-контенту, которым владелец аккаунта обменивался со своими знакомыми в приложении. Этот контент может стать компроматом на любого человека, по той или иной причине заинтересовавшего злоумышленника. Наконец, пользователи часто ленятся запоминать разные логины и пароли и используют одну и ту же связку и для аккаунта в приложении знакомств, и, например, для доступа в онлайн-банк. Что, в свою очередь, создает уже финансовые риски.

В описании к Знакомства@mail.ru в Google Play сказано, что данное приложение является лидером российского рынка сервисов знакомств. При этом по результатам автоматизированного анализа сервис занял предпоследнее место по уровню защищенности среди приложений с количеством установок более 5 млн (8 из 12-ти исследованных приложений).

Самое большое количество уязвимостей среди Android-версий было обнаружено в мобильном приложении MyFriends. Уровень защищенности этого сервиса равен всего 1.9 баллам, поскольку приложение содержит в исходном коде 7 вхождений критических уязвимостей. Такое число вхождений превышает предельно допустимый показатель 5 единиц, необходимый для того, чтобы не опуститься ниже среднего по рыку показателя общего уровня защищенности. При этом MyFriends содержит и наибольшее количество вхождений уязвимостей среднего уровня, поэтому его уровень защищенности нельзя назвать удовлетворительным.

Уровень защищенности iOS-версий:

Приложение	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
Hitwe	1	21	9	476	1.0/5.0
LovePlanet	1	29	8	857	0.7/5.0
Galaxy	1	34	7	653	0.6/5.0
Badoo	2	37	8	761	0.5/5.0
Tinder	2	38	9	758	0.5/5.0
Фотострана	2	39	9	753	0.5/5.0
Мой Мир	2	49	7	1009	0.4/5.0
Teamo	2	56	6	346	0.3/5.0
Mamba	2	56	9	891	0.3/5.0
Знакомства@mail.ru	2	56	9	910	0.3/5.0
ДругВокруг	3	96	9	2079	0.1/5.0
MyFriends	4	98	9	2099	0.1/5.0
Topface	2	168	9	2146	0.0/5.0

Результаты, представленные в таблице, свидетельствуют о крайне низком уровне защищенности мобильные приложений знакомств, разработанных под операционную систему iOS, по сравнению с их Android-аналогами. Столь низкие показатели объясняются на один-два порядка бОльшим количеством вхождений уязвимостей критического уровня в iOS-версиях по сравнению с соответствующими Android-приложениями. Что, однако, в некоторой степени компенсируется более высокой защищенностью самой операционной системы.

Мобильное приложение знакомств Topface для платформы iOS включает множество уязвимостей – его общий уровень был оценен анализатором Solar appScreener в 0.0 балла.

Выводы

Исследование защищенности мобильных приложений знакомств показало, что Android-версии проанализированных мобильных сервисов отличаются более высокой защищенностью, нежели их iOS-аналоги.

По итогам сканирования в приложениях обнаружен ряд критических уязвимостей, потенциально ведущих к компрометации всех обрабатываемых данных, в том числе паролей от учетных записей пользователей, их конфиденциальной переписки, технической информации о конфигурации приложений и проч.

Проверка приложений на базе Android показала, что 83% из них содержат ключ шифрования в исходном коде. Эта уязвимость оценивается международными аналитическими лабораториями как высококритичная, поскольку потенциально ведет к компрометации всех данных, содержащихся в программе. Дело в том, что заданные в исходном коде ключи шифрования свободно доступны каждому разработчику приложения. А после установки приложения удалить из его кода ключ можно только посредством обновления. Соответственно, для технического специалиста получить доступ ко всем данным такого приложения не составит труда.

Кроме того, все исследованные Android-версии мобильных сервисов знакомств допускают внутреннюю утечку информации о конфигурации системы, с помощью которой внутренний злоумышленник может организовать атаку на приложение. Также все они содержат уязвимость, создающую угрозу выполнения злоумышленником произвольного кода в приложении.

Еще печальнее обстоят дела с безопасностью мобильных приложений знакомств на базе iOS: все они содержат уязвимость, создающую риск компрометации конфиденциальных данных пользователей, в силу применения слабого алгоритма шифрования. В целом, iOS-версии мобильных сервисов знакомств содержат гораздо большее количество уязвимостей, чем Android-приложения, что, однако, в некоторой степени компенсируется более высокой защищенностью самой iOS.

Самыми защищенными Android-версиями приложений знакомств оказались приложения Teamo и Фотострана. А наиболее уязвимым – приложение MyFriends. Неожиданно в приложении Знакомства@mail.ru (Mail.ru Group) для ОС Android была обнаружена высококритичная уязвимость, входящая в международный рейтинг наиболее критичных уязвимостей «OWASP Mobile Top 10 2016». По результатам автоматизированного анализа данный сервис занял предпоследнее место по уровню защищенности среди приложений с количеством установок более 5 млн (8 из 12-ти исследованных приложений).

Среди iOS-версий исследованных приложений нет ни одного, удовлетворяющего хотя бы среднему по отрасли уровню защищенности.