Руководство
для разработчиков

Проверка безопасности мобильных приложений

Общие требования

Область проверки	Пункты проверки	✓
Обнаружение использования Jailbreak и Root на устройстве	Приложение проверяет использование Jailbreak и Root на устройстве и в случае их наличия предупреждает пользователя о возможных рисках (потеря доступа к учетной записи, финансовых средств и пр.)	
Атаки на канал связи типа MITM	Внедрен и корректно настроен SSL	
	Внедрен и корректно настроен SSL-pinning	

Android

Область проверки	Пункты проверки	✓
API	В настройках резервного копирования указано, какая именно информация должна попадать в Google Cloud	
	Наличие двухфакторной аутентификации	
	Длина кода второго фактора (SMS, OTP) составляет 6 и более символов	
	Используется актуальная Android SDK версия	
	Запрещена отладка приложения	
	Важные компоненты приложения (активити экраны, контент-провайдеры и т.д.) **не** являются экспортируемыми и общедоступными	

Android

Область проверки	Пункты проверки	✓
API	Применяемые криптографические алгоритмы (шифрование, хэширование) актуальны	
	Для выполнения важных действий **не** используется проверка на стороне клиента (client-side)	
	Приложение **не** запрашивает «dangerous» разрешения, не соответствующие характеру приложения	
	Все входящие данные обрабатываются и фильтруются должным образом	
Хранение критичной информации	Чувствительные данные **не** попадают в логи приложения	
	Приложение скрывает чувствительные данные с экрана, когда находится в фоновом режиме	
	В приложении предусмотрена аутентификация с помощью PIN/отпечатка пальца	
	Освобождена память, выделенная под хранение критичных данных (логин, пароль)	
	Важные пользовательские данные хранятся вне общедоступной памяти (sdcard)	
	Предусмотрено полное завершение сессии приложения	
	После завершения сессии вся клиентская информация с устройства должна быть удалена (Cookie, KeyStore и пр.)	
	При использовании сторонних сервисов (например, аналитики) чувствительные пользовательские данные маскируются при отправке	
	Проведена проверка пакетов приложений, подтверждено отсутствие отладочной информации, файлов с информацией для внутреннего использования, приватных ключей, информации о реализации новой функциональности и т.п.	
	Данные пользователя, расположенные в Shared Preferences, SQLite БД (логин/пароль, PIN, сессионные токены, данные кредитных карт) и прочих хранилищах, содержатся в зашифрованном виде. Ключи шифрования — в KeyStore	

iOS

Область проверки	Пункты проверки	✓
Возможные недостатки безопасности в архитектуре приложения	Используются последние версии SDK (9.0) с улучшенными механизмами защиты, новыми API и поддержкой новых устройств	
	Используются AppTransportSecurity (ATS)	
API	Проверка SSL-сертификатов на наличие критичной информации (внутренние адреса, домены сервисов, тестовые стенды и т.д.)	
	Внедрены механизмы шифрования трафика HTTP-соединения на основании протокола TLS	
	Наличие двухфакторной аутентификации	
	Длина кода второго фактора (SMS/OTP) - 6 и более символов	
	Биометрическая аутентификация **не** является event-bound (использует только API, которое возвращает «true» или «false»). Вместо этого она основана на разблокировке keychain/keystore	
	Все случайные значения генерируются с использованием безопасного генератора случайных чисел	
	Приложение **не** экспортирует чувствительные данные через кастомные URL-схемы, если эти механизмы не защищены должным образом	
	Применяемые криптографические алгоритмы (шифрование, хэширование) актуальны	
	Для выполнения важных действий **не** используется проверка на стороне клиента (client-side)	
	Приложение запрашивает минимально необходимый набор разрешений	
	Все входящие данные обрабатываются и фильтруются должным образом	
	JavaScript отключен в компонентах WebView, если в нем нет необходимости	
	Десериализация объектов, если она есть, реализована с использованием безопасного API	

iOS

Область проверки	Пункты проверки	✓
Хранение критичной информации	Чувствительные данные **не** попадают в логи приложения	
	Приложение скрывает чувствительные данные с экрана, когда находится в фоновом режиме	
	В приложении предусмотрена аутентификация с помощью PIN/отпечатка пальца	
	При использовании сторонних сервисов (например, аналитики) чувствительные пользовательские данные маскируются при отправке	
	В NSUserDefaults размещены только неключевые настройки приложения (настройка языка, часового пояса, раскладка клавиатуры и пр.)	
	Данные пользователя, расположенные в Shared Preferences, SQLite БД (логин/пароль, PIN, сессионные токены, данные кредитных карт и т.д.) и прочих хранилищах, содержатся в зашифрованном виде. Ключи шифрования — в KeyChain	
	Освобождена память, выделенная под хранение критичных данных (логин, пароль)	
	Приложение **не** хранит чувствительные данные в памяти дольше, чем необходимо, и полностью удаляет их из памяти после работы с ними	
	Предусмотрено полное завершение сессии приложения	
	После завершения сессии вся клиентская информация с устройства должна быть удалена (Cookie, KeyChain и пр.)	
	Кэш (clipboard copy) клавиатуры выключен для полей ввода чувствительных данных.	
	Чувствительные данные, такие как пароли или пин-коды, скрыты в пользовательском интерфейсе	
Качество кода и настройки	Приложение подписано валидным сертификатом. Реализована проверка валидности подписи	
	Все сторонние компоненты, используемые мобильным приложением (библиотеки и фреймворки), идентифицированы и проверены на наличие известных уязвимостей	
	Отладочные символы удалены из нативных бинарных файлов	

Область проверки	Пункты проверки	✓
Качество кода и настройки	Активированы все стандартные функции безопасности, предусмотренные инструментами разработчика (такие как минификация байт-кода, защита стека, поддержка PIE и ARC)	
	Код отладки и вспомогательный для разработки код (например, тестовый код, бэкдоры, скрытые настройки) удалены. Приложение **не** логирует подробные ошибки и отладочные сообщения	

Взаимодействие банков с операторами сотовой связи

Область проверки	Пункты проверки	✓
Подмена Caller ID через SIP-сервисы	Банк запрашивает дополнительные сведения, подтверждающие личность абонента, во время звонка (секретное слово, часть паспортных данных)	
Перевыпуск SIM-карты злоумышленником	При заключении контракта на банковское обслуживание банк совершает первичный HRL запрос и сохраняет IMSI клиента, после чего с определенной частотой совершает HLR запросы для сверки данных; в случае их изменения предпринимает меры	

Эти проверки входят в состав работ по нашей услуге «Анализ защищенности мобильного приложения».

С удовольствием расскажем больше о нашей методике и обсудим сотрудничество

Свяжитесь с нами

inbox@dsec.ru 7 (495) 223-07-86