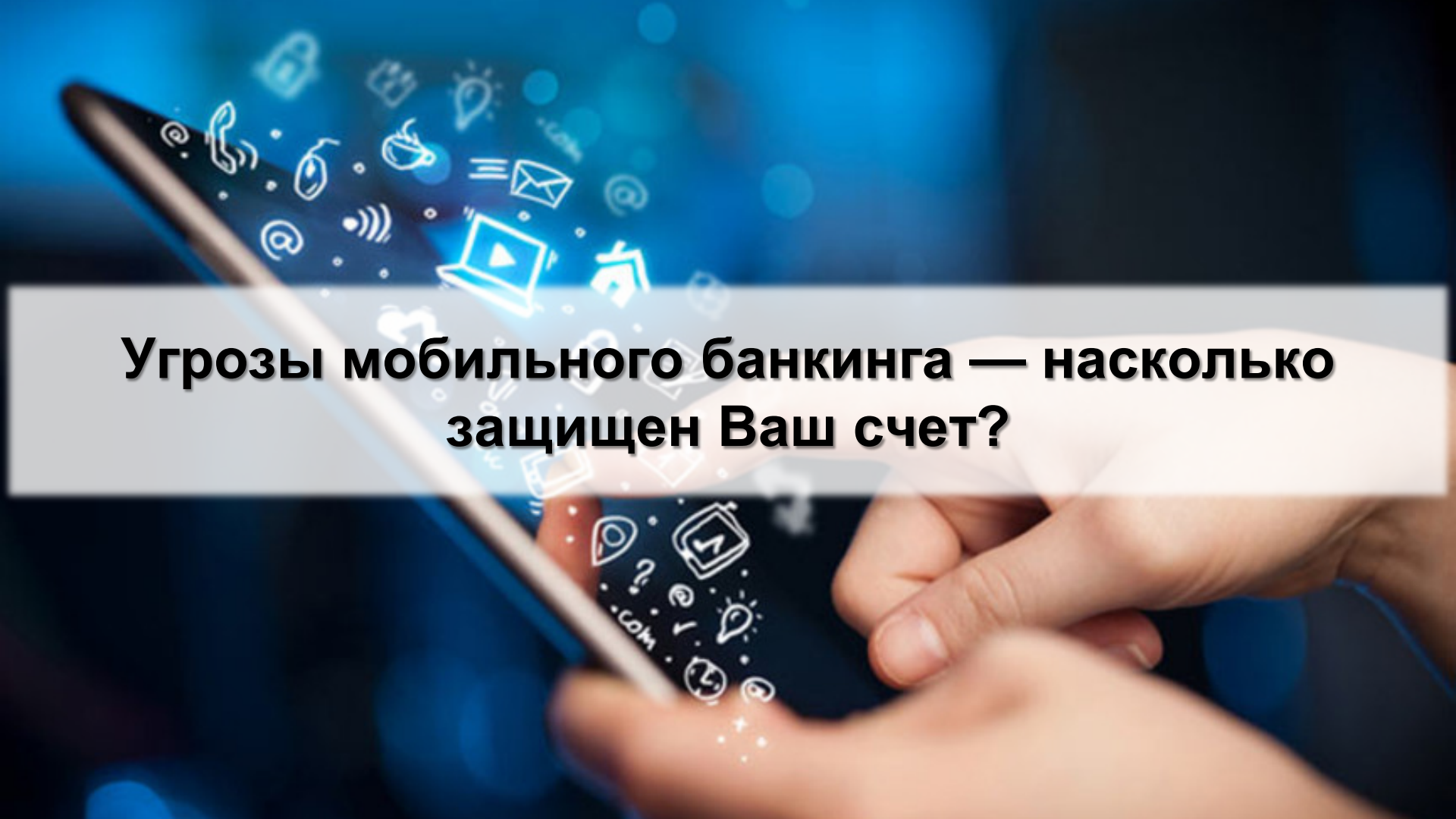


Угрозы мобильного банкинга — насколько защищен Ваш счет?

Мобильные банковские приложения

- Все крупные банки имеют свое мобильное приложение
- Полный доступ к счетам и картам
- 70% интернет-аудитории пользуется этими приложениями
- Почти половина мобильных вредоносных программ нацелена на банковские приложения, количество активных банковских троянов удвоилось за 2018й год

Основные угрозы

- Социальная инженерия
- Кража данных карты с PoS или банкомата
- Мобильные банковские трояны
- Перехват звонков и SMS
- Перехват сетевого трафика
- Физический доступ к мобильному устройству

Исследование мобильных приложений

- 5 приложений из топ 10 самых популярных мобильных банковских приложений

Направления исследования

- Защищенность протокола связи от перехвата, подмены и повтора
- Безопасность процедур авторизации и продолжения существующей сессии
- Корректность работы с резервным копированием
- Сторонние компоненты и их взаимодействие с облаком
- Защита конфиденциальных сведений и персональных данных
- Защита от манипуляций с приложением

Защищенность подключения

- Проверка валидности сертификата сервера
- Проверка отпечатка сертификата сервера при подключении к нему
- Безопасный механизм обновления отпечатков

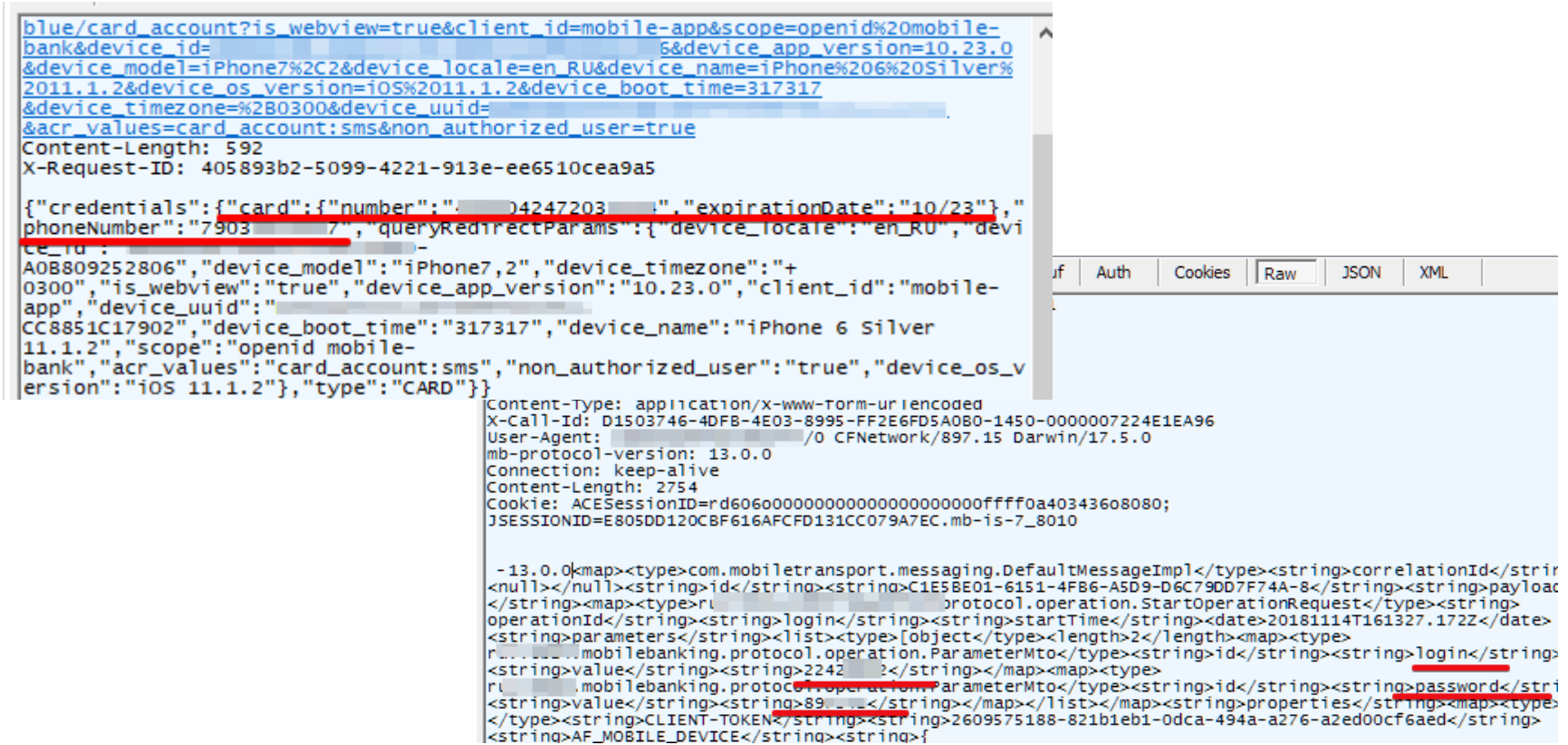
Оценка:

Безопасность авторизации

- Используемый протокол авторизации
- Шифрование или хэширование паролей и пин-кодов
- Уведомление о подключении новых устройств
- Новые сессии подключенных устройств

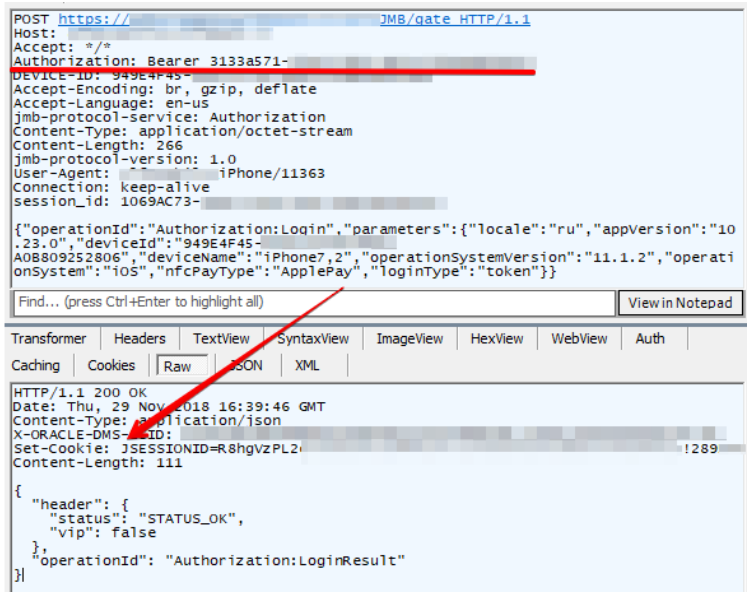
Оценка:

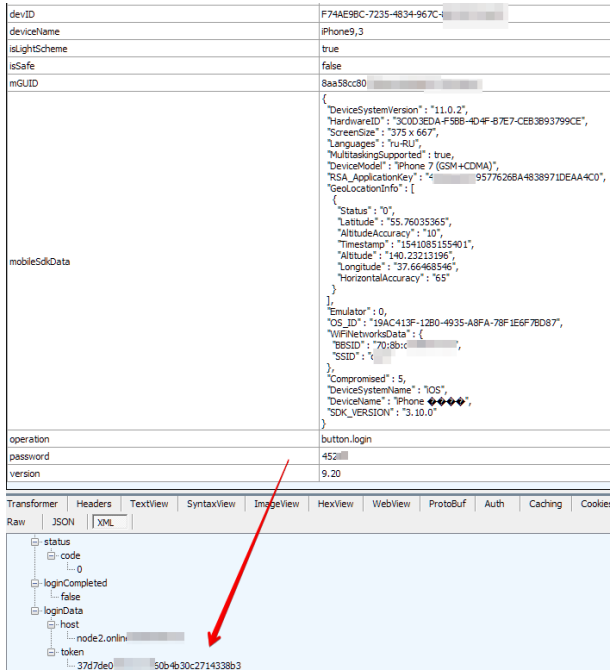
Учетные данные в открытом виде



Новые сессии

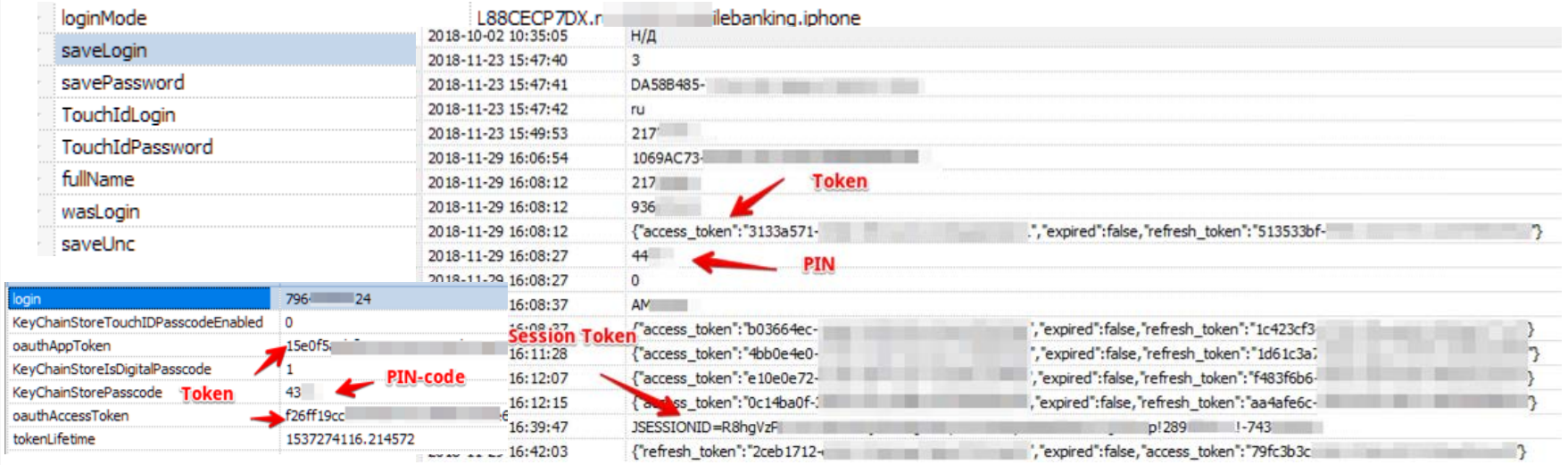
- Для открытия новой сессии достаточно неизменяемого токена или короткого цифрового пин-кода





Резервные копии

- Хранение критически важной информации в открытом виде в резервных копиях



Оценка:

Сторонние компоненты

- Безопасная передача данных
- Фильтрация передаваемых данных
- Фильтрация сохраняемых на устройство данных
- Безопасная обработка ответов сервера

Оценка:

Запросы к облаку

- Дополнительная защита персональных данных и банковской тайны
- Запрос подтверждения на совершение значимых операций
- Верификация источника запроса

Оценка:

Запросы к облаку: проблемы

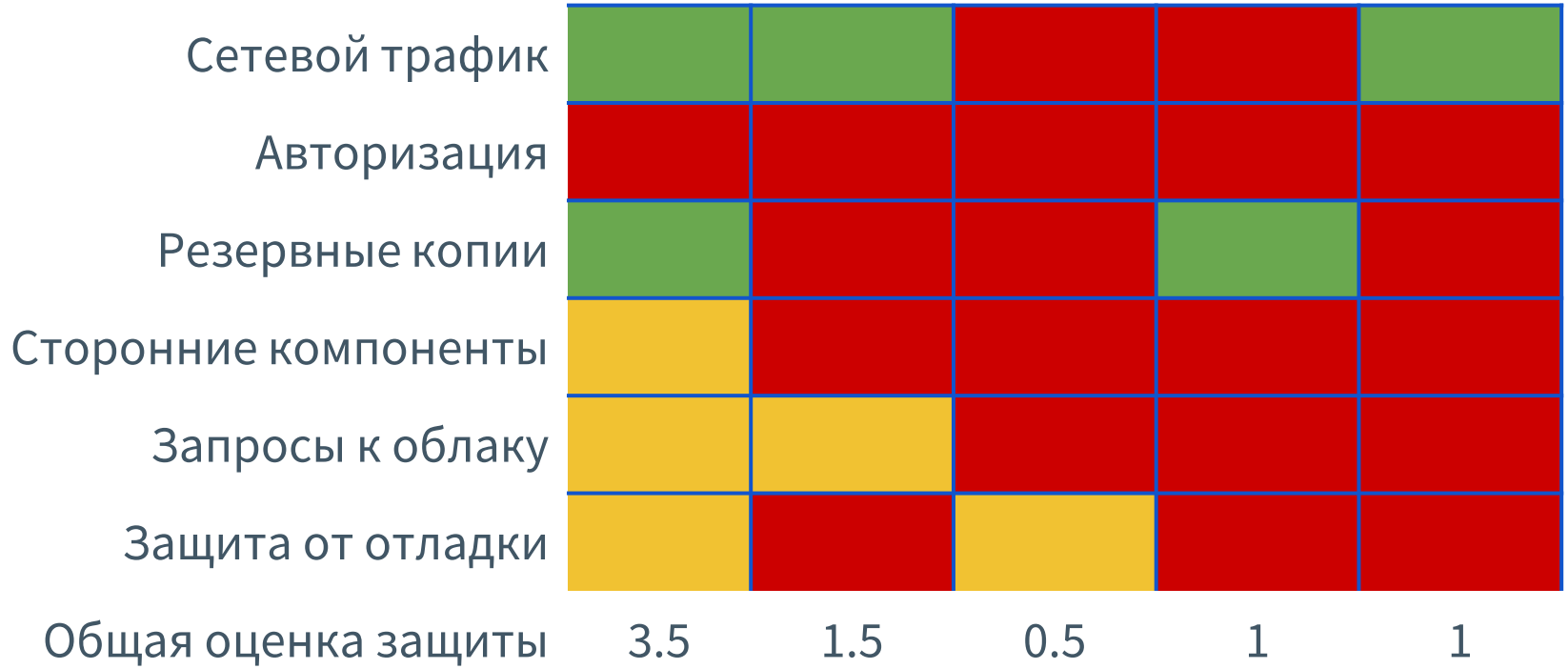
- Отсутствие механизмов подписи запросов
- Персональные данные клиента в открытом виде
- Список контактов без разрешения пользователя
- Получение персональных данных других клиентов банка по номеру телефона
- Выполнение операций без подтверждения
- Переписка с сотрудниками банка

Защита памяти и файлов приложения

- Проверка цифровых подписей
- Обнаружение рута/джейлбрейка
- Защита от отладки
- Раскрытие данных в системных журналах

Оценка:

Итоги


Сетевой трафик
Авторизация
Резервные копии
Сторонние компоненты
Запросы к облаку
Защита от отладки
Общая оценка защиты
3.5
1.5
0.5
1
1

Противодействие угрозам

- Регулярный аудит силами независимого от разработчиков подразделения или сторонней организацией
- Использование всего спектра возможностей, предоставляемых каждой конкретной платформой
- Мониторинг тенденций в области атак на мобильные банковские приложения и принятие превентивных мер

Современные технологии и возможности платформ

- Несколько примеров:
- Шифрование при помощи аппаратно-защищенных ключей: Android Keystore, iOS Secure Enclave
- Валидация сетевых соединений на стороне сервера при помощи одноразовых токенов
- Второй фактор через встроенные TOTP генераторы или аппаратные токены

Спасибо за внимание!