

A hand is shown holding a smartphone. The background is a dark blue with bokeh light effects. Numerous white, glowing digital icons are scattered around the phone, including a padlock, a lightbulb, a mail envelope, a play button, a house, a location pin, a question mark, a person icon, a Wi-Fi symbol, and a speech bubble. A semi-transparent white banner is overlaid across the middle of the image, containing the text.

**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:



Новые сессии

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

```

POST https://[redacted] JMB/gate HTTP/1.1
Host: [redacted]
Accept: */*
Authorization: Bearer 3133a571-[redacted]
DEVICE-ID: 949E4F45-[redacted]
Accept-Encoding: br, gzip, deflate
Accept-Language: en-us
jmb-protocol-service: Authorization
Content-Type: application/octet-stream
Content-Length: 266
jmb-protocol-version: 1.0
User-Agent: iPhone/11363
Connection: keep-alive
session_id: 1069AC73-[redacted]

{"operationId": "Authorization:Login", "parameters": {"locale": "ru", "appversion": "10.23.0", "deviceId": "949E4F45-[redacted]", "A0B809252806", "modelName": "iPhone7,2", "operationSystemVersion": "11.1.2", "operationSystem": "iOS", "nfcPayType": "ApplePay", "loginType": "token"}}

Find... (press Ctrl+Enter to highlight all) View in Notepad

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth
Caching Cookies Raw JSON XML

HTTP/1.1 200 OK
Date: Thu, 29 Nov 2018 16:39:46 GMT
Content-Type: application/json
X-ORACLE-DMS-SESSION-ID: [redacted]
Set-Cookie: JSESSIONID=R8hgvpzPL2-[redacted]; Path=/; HttpOnly
Content-Length: 111

{"header": {"status": "STATUS_OK", "vip": false}, "operationId": "Authorization:LoginResult"}
  
```

devID	F74AE9BC-7235-4834-967C-[redacted]
deviceName	iPhone9,3
isLightScheme	true
isSafe	false
mGUID	8aa58cc80-[redacted]
mobileSdkData	{ "DeviceSystemVersion": "11.0.2", "HardwareID": "3C0D3EDA-F98B-4D4F-87E7-CEB393799CE", "ScreenSize": "375 x 667", "Languages": "ru-RU", "MultitaskingSupported": true, "DeviceModel": "iPhone7 (GSM+CDMA)", "RSA_ApplicationKey": "[redacted] 95776268A4838971DEAA4C0", "GeoLocationInfo": { "Status": "0", "Latitude": "55.76025365", "AltitudeAccuracy": "10", "Timestamp": "1541085155401", "Altitude": "140.23213196", "Longitude": "137.66468596", "HorizontalAccuracy": "65" } }, "Emulator": 0, "Os_ID": "19AC413F-12B0-4935-ABFA-78F1E6F7B087", "WiFiNetworkData": { "BSSID": "70:8b:c-[redacted]", "SSID": "[redacted]" }, "Compromised": 5, "DeviceSystemName": "iOS", "DeviceName": "iPhone [redacted]", "SDK_VERSION": "3.10.0" }
operation	button.login
password	452
version	9.20

Transformer Headers TextView SyntaxView ImageView HexView WebView ProtoBuf Auth Caching Cookie

Raw JSON XML

```

status
├── code
│   └── 0
├── loginCompleted
│   └── false
├── loginData
│   └── host
│       └── node2.onlin-[redacted]
│           └── token
│               └── 37d7de0-[redacted] 50b4b30c2714338b3
  
```

Резервные копии

- ▶ Хранение критически важной информации в открытом виде в резервных копиях

loginMode	L88CECP7DX.r	ilebanking.iphone
saveLogin	2018-10-02 10:35:05	H/Д
savePassword	2018-11-23 15:47:40	3
TouchIdLogin	2018-11-23 15:47:41	DA58B485-
TouchIdPassword	2018-11-23 15:47:42	ru
fullName	2018-11-23 15:49:53	217
wasLogin	2018-11-29 16:06:54	1069AC73-
saveUnc	2018-11-29 16:08:12	217
	2018-11-29 16:08:12	936
	2018-11-29 16:08:12	{ "access_token": "3133a571-", "expired": false, "refresh_token": "513533bf-" }
	2018-11-29 16:08:27	44
	2018-11-29 16:08:27	0
login	796	24
KeyChainStoreTouchIDPasscodeEnabled	0	16:08:37
oauthAppToken	15e0f5-	16:11:28
KeyChainStoreIsDigitalPasscode	1	16:12:07
KeyChainStorePasscode	43	16:12:15
oauthAccessToken	f26ff19cc	16:39:47
tokenLifetime	1537274116.214572	16:42:03

KeyChainStoreTouchIDPasscodeEnabled	0	16:08:37	{ "access_token": "b03664ec-", "expired": false, "refresh_token": "1c423cf3-" }
oauthAppToken	15e0f5-	16:11:28	{ "access_token": "4bb0e4e0-", "expired": false, "refresh_token": "1d61c3a-" }
KeyChainStoreIsDigitalPasscode	1	16:12:07	{ "access_token": "e10e0e72-", "expired": false, "refresh_token": "f483f6b6-" }
KeyChainStorePasscode	43	16:12:15	{ "access_token": "0c14ba0f-", "expired": false, "refresh_token": "aa4afe6c-" }
oauthAccessToken	f26ff19cc	16:39:47	JSESSIONID=R8hgVzFpI-743
tokenLifetime	1537274116.214572	16:42:03	{ "refresh_token": "2ceb1712-", "expired": false, "access_token": "79fc3b3c-" }

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	3.5	1.5	0.5	1	1
Авторизация	3.5	1.5	0.5	1	1
Резервные копии	3.5	1.5	0.5	1	1
Сторонние компоненты	3.5	1.5	0.5	1	1
Запросы к облаку	3.5	1.5	0.5	1	1
Защита от отладки	3.5	1.5	0.5	1	1
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!

