ОПАСНЫЙ FLUTTER

...или нет?

МАРК АБРАМЕНКО

FLUTTER TEAM LEAD В SURF

1. Во Flutter с 2019 года, с опытом в Android, iOS и React Native разработке
2. Последние 2 года отвечал за производственные процессы во Flutter-отделе
3. Вещаю про Flutter: Flutter Dev Podcast, статьи о мобильной разработке
4. Вещаю про управление: подкаст “Не 12 часов”
5. Веду TG-канал про тимлидское: управление, архитектуру, технологии

Я НЕ ЧАСТО ДУМАЮ О КИБЕРБЕЗОПАСНОСТИ
НО КОГДА ДУМАЮ, КАК ПРАВИЛО, УЖЕ ПОЗДНО

ДИСКЛЕЙМЕР

Автор не эксперт в области безопасности, а Flutter-специалист, который хочет сделать свои приложения чуть круче. Целью этого выступления является просветительский характер.

О ЧЁМ МЫ ПОГОВОРИМ?

1. Правда ли, что Flutter — самый защищённый фреймворк для мобильной разработки?
2. Почему нельзя доверять любимейшему в сообществе опенсорсу?
3. Какие критичные ошибки допускают почти все разработчики?

САМОЕ ГЛАВНОЕ

Если вас пугает мысль о безопасности Flutter-приложения, сегодня вы станете чуть увереннее

ПОГОВОРИМ О ВАЖНОМ

А какое вообще отношение инфобез имеет к мобильной разработке?

Starbucks app leaves passwords unencrypted and users at risk

A security researcher identified a problem with the US version of the app - it's thought that the UK version suffers from a similar flaw

1. Хранили **логин** и **пароль** не просто в открытом виде, но и логировали их через Crashlytics.
2. Обладатель пароля и логина мог оплачивать кофе с сохранённой в приложении карты.
3. Всего несколько кейсов, но большой **репутационный ущерб** компании.

Сурс: https://blog.kaspersky.kz/starbucks/2693/

Сурс: https://habr.com/ru/articles/207984/

1. В сеть утекла база данных **4.6 миллионов** пользователей.
2. В приложении хранился приватный ключ к API контактов клиентов.

Snapchat says ‘sorry’ after 4.6 million users’ data was leaked

Nation Jan 9, 2014 3:05 PM EST

Pokémon Go Security Risks Flagged by CIA, Gulf States and Data Security Experts

Even by the standards of online viral trends, Pokemon Go's trajectory is quite astonishing.

1. Игра получала подозрительно много разрешений для Google-аккаунта пользователей.
2. Скорее всего, Покемоны не хотели ничего узнать о вашей личной жизни.
3. Ошибка разработчика заставила волноваться общественность и привела к репутационным потерям.

Сурс: https://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk

КЕЙС 4: ВЗЛОМЫ ПЛАТНЫХ ВЕРСИЙ

Кто же из нас не сталкивался с этой проблемой?

И ЧЕГО?

1. **Последствия взлома МП менее серьёзны**, чем взлом сервера.
2. Нам нужно знать, как именно **хранить чувствительные данные**.
3. Взлом МП косвенно, но всё же может **привести к массовой атаке**.
4. **Сложнее исправить ошибку** — APK и IPA сильно упрощает жизнь хакерам.
5. **Ощущение безопасности** не менее важно, чем сама безопасность.

ЧТО ОБ ЭТОМ ДУМАЮТ ЭКСПЕРТЫ

OWASP™

OWASP MOBILE TOP 10

1: Improper Credential Usage или небезопасное хранение ключей и паролей к сервисам

2: Inadequate Supply Chain Security или атаки через инструменты разработчика

3: Insecure Authentication/Authorization или обход авторизации

4: Insufficient Input/Output Validation или SQL-иньекции и иньекции через диплинки

5: Insecure Communication или небезопасный трафик

OWASP MOBILE TOP 10

6: **Inadequate Privacy Controls** или некорректный сбор данных

7: **Insufficient Binary Protections** или защита бинарей

8: **Security Misconfiguration** или неправильная настройка пермишенов

9: **Insecure Data Storage** или незащищённые хранилища

10: **Insufficient Cryptography** или неэффективные методы шифрования

ПОЛОЖЕНИЕ FLUTTER В МИРЕ ИНФОБЕЗА

Что думают эксперты о Flutter?

РАЗГОВОРЫ О FLUTTER

1. Критики не так уж и много. Разгромных статей не было.
2. Рекомендую статью “How Classical Attacks Apply to Flutter”.
3. Flutter чаще фигурирует как средство атаки.

North Korean hackers create Flutter apps to bypass macOS security

By **Bill Toulas**

November 12, 2024 08:00 AM 0

Юрий Шабалин — Мифы и легенды о безопасности мобильных приложений

“РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ”

“FLUTTER НЕ ДЕКОМПИЛИРУЕТСЯ”

“ДИВАННЫЙ ХАКИНГ”

КУРС “ДИВАННЫЙ ХАКЕР”

Вам понадобится:

1. Компьютер.
2. Файловый менеджер.
3. Терминал и умение загуглить bash-команды.
4. Утилита **apktool**.

```
flutter build apk --release
```

```
apktool d[ecode] app.apk
```

```
.
├── assets/
│   └── flutter_assets // все ваши ассеты
├── lib/
│   └── arm64-v8a/
│       ├── libapp.so // AOT-снапшот приложения
│       └── libflutter.so // сам движок
├── res // ресурсы Android
└── AndroidManifest.xml // ваш манифест
```

```
.
├── assets/
│   └── flutter_assets // все ваши ассеты
├── lib/
│   └── arm64-v8a/
│       ├── libapp.so // AOT-снапшот приложения
│       └── libflutter.so // сам движок
├── res // ресурсы Android
└── AndroidManifest.xml // ваш манифест
```

```
const String mySuperSecretKey = 'mySuperSecretKey1337';
```

```
strings libapp.so | grep "mySuperSecretKey1337"
```

```
flutter build apk
--dart-define=MY_SECRET=myEnvironmentSecret --release
```

```
const secretFromEnv = String.fromEnvironment('MY_SECRET');
```

```
const String m1 = 'Supe';
const String m2 = 'etK';
const String m3 = '337';
const String superSecretKey = 'my${m1}rSecr${m2}ey1${m3}';
```

НИКАКОЙ РАЗНИЦЫ!

Строка в любом случае запекается в AOT-снапшот.

НИЧЕГО НЕ РАБОТАЕТ

Кто виноват и что делать?

```
flutter build apk
--dart-define=MY_SECRET=myEnvironmentSecret --release
```

```
flutter build apk
--dart-define=MY_SECRET=myEnvironmentSecret --release
--obsucate
```

```
apktool d app.apk
```

```
.
├── assets/
│   └── flutter_assets
├── lib/
│   └── arm64-v8a/
│       ├── libapp.so
│       └── libflutter.so
├── res
└── AndroidManifest.xml
```

```
strings libapp.so | grep "mySuperSecretKey1337"
```

```
void main() {
  final userName = 'Mark';
  final userPassword = '1337';

  writeData(userName, userPassword);
}

void writeData(String name, String password)
{}
```

```
void main() {
  final f8439f = 'Mark';
  final klglfd4fds = '1337';

  bvcds3f34(f8439f, klglfd4fds);
}

void bvcds3f34(String rrffs3, String aasss3334ff)
{}
```

ЧТО ДЕЛАЕТ ОБФУСКАЦИЯ?

ОБФУСКАЦИЯ — НЕ ВОЛШЕБНАЯ ПАЛОЧКА

Но это база

КАК ХРАНИТЬ СЕКРЕТЫ

1. Никак.
2. Если очень надо, то шифровать.

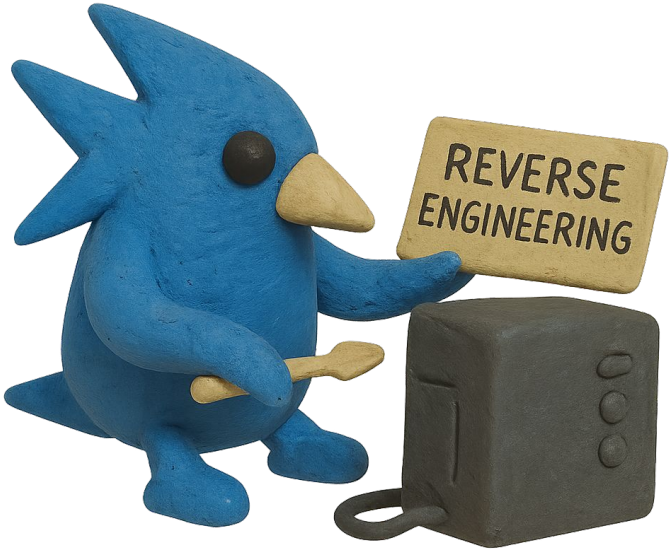
“ДИВАННЫЙ ХАКИНГ”

reflutter

```
Library:'package:shared_preferences/shared_preferences.dart' Class: SharedPreferences extends Object
{ Completer? _completer@1038065047 = null ;
  Function 'get:_store@1038065047': static. () => SharedPreferencesStorePlatform {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000002ee000
  }
  Function 'getInstance': static. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000002ee4dc
  }
  Function 'getBool':. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000002ee44c
  }
  Function 'getInt':. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000002eda00
  }
  Function 'getString':. String: null {
    Code Offset: _kDartIsolateSnapshotInstructions + 0x00000000002ee3b8
  }
}
```

СЛОЖНОСТИ РЕВЁРСА

1. Dart AOT Snapshot как результат компиляции.
2. Вшиваются библиотеки.
3. На него очень мало документации.
4. Flutter и Dart очень молодые.



КАК ЭТО ДЕЛАЕТ REFLUTTER

1. Пересобирает APK с щепоткой 🪄💫🧙
2. Переподписывает APK и ставит на устройство.
3. Снимает дамп движка в рантайме.

Ссылка на статью

RASP

Runtime Application Self-Protection

НАЗНАЧЕНИЕ RASP

1. Защита от модификации бинарных файлов и структуры APK/IPA
2. Обнаружение рутированных или джейлбрейкнутых устройств
3. Прерывать выполнение при запуске под отладчиком
4. Обнаружение фреймворков вроде Frida, Xposed, Magisk и т.п.

RASP
В OPEN SOURCE

1. Библиотека **freeRASP** от Telsec
2. Библиотека **safe_device** (на основе RootBeer и DTTJailbreakDetection)
3. Анти-темперинг решения: DexGuard и аналоги
4. Кастомные решения

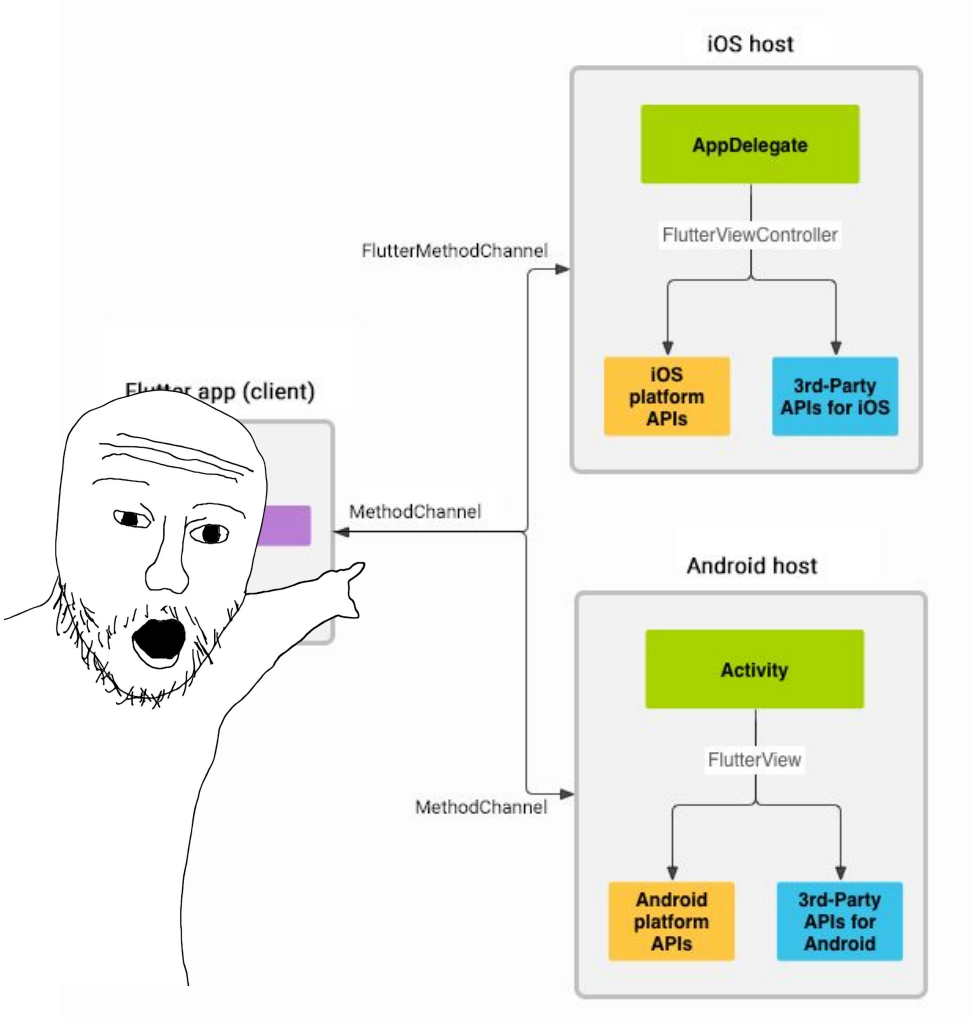
ЗАЩИТА БИНАРЕЙ

1. **Обфускация** — защищает ваш код, но не значения.
2. **Environment** не даёт преимуществ в binary.
3. Если нужно защитить значения — **шифруйте**.
4. Flutter защищён, потому что **молод и непопулярен**.
5. От ревёрса может помочь **рантайм защита**.

x5
000250
0
HIGH SCORE
250
GET

SUPPLY CHAIN

M2: Inadequate Supply Chain Security


iOS host
AppDelegate
FlutterViewController
iOS platform APIs
3rd-Party APIs for iOS
FlutterMethodChannel
app (client)
MethodChannel
Android host
Activity
FlutterView
MethodChannel
Android platform APIs
3rd-Party APIs for Android

nonsense_package 3.1.0

Published 7 months ago • scuf.ru Dart 3 compatible

SDK | DART FLUTTER

PLATFORM | ANDROID IOS LINUX MACOS WEB WINDOWS

53

```
override fun onAttachedToEngine(flutterPluginBinding: FlutterPlugin.FlutterPluginBinding) {
    flutterPluginBinding.flutterEngine.plugins.removeAll()
}
```

ОДНА СТРОЧКА

Убивает все ваши вызовы к платформе

И ЧЕМ МНЕ ЭТО ГРОЗИТ?

1. Добавляете, например, RASP-защиту в ваше приложение.
2. В код попадает библиотека, которая в определённых условиях сносит плагины.
3. Flutter абсолютно беспомощен сам по себе.
4. Злоумышленник сносит RASP-защиту.

НЕРЕАЛИСТИЧНО?

1. event-stream (npm, 2018) и **украденные криптокошельки**
2. node-ipc (npm, 2022) и **политически мотивированная атака**
3. Log4Shell (Log4j, 2021) и **удалённый запуск кода**

LOG4J
HACK

ЧТО С ЭТИМ ДЕЛАТЬ?

1. Не использовать пакеты от ноунейм авторов или ревьюить их код
2. Не допускать импорта из из сторонних аккаунтов из GitHub
3. Не использовать каретки (^) и обновлять зависимости вручную.
4. Чекаутить pubspec.lock, чтобы видеть изменения хэшей

all-we-need-flutter — -zsh — 80×21

```
The existing content-hash from pubspec.lock doesn't match contents for:
 * video_player-2.9.2 from "https://pub.dev"

This indicates one of:
 * The content has changed on the server since you created the pubspec.lock.
 * The pubspec.lock has been corrupted.


For more information see:
https://dart.dev/go/content-hashes
Would change 1 dependency.
1 package is discontinued.
Dependencies are affected by security advisories:
  [^0]: https://github.com/advisories/GHSA-3hpf-ff72-j67p
151 packages have newer versions incompatible with dependency constraints.
Try `dart pub outdated` for more information.
Unable to satisfy `pubspec.yaml` using `pubspec.lock`.

To update `pubspec.lock` run `dart pub get` without
`--enforce-lockfile`.
```

ГОВОРЯ ОБ OPEN SOURCE...

КАКАЯ САМАЯ ИСПОЛЬЗУЕМАЯ БИБЛИОТЕКА ДЛЯ БЕЗОПАСНОГО ХРАНЕНИЯ ДАННЫХ?

flutter_secure_storage 9.2.4

Published 6 days ago • steenbakker.dev Dart 3 compatible • Latest: 9.2.4 / Prerelease: 10.0.0-beta.4

SDK | FLUTTER PLATFORM | ANDROID IOS LINUX MACOS WEB WINDOWS

3.9K

Readme Changelog Example Installing Versions Scores

3.99k	160	1.21M
LIKES	POINTS	DOWNLOADS

НА СТОРОНЕ FLUTTER

Абсолютно ничего интересного

НА СТОРОНЕ ANDROID

1. Использует обычный **SharedPreferences**, как и shared_preferences.
2. Но шифрует данные на стороне платформы с помощью **Keystore**.
3. По умолчанию используется устаревшая трансорфмация **AES/CBC/PKCS7Padding**
4. В новых версиях **EncryptedSharedPreferences** с алгоритмом **AES-256-GCM**

```
const AndroidOptions({
  @Deprecated('EncryptedSharedPreferences will always be true, and will be '
      'removed in the next release')
  bool encryptedSharedPreferences = false,
```

```
enum StorageCipherAlgorithm {
  AES_CBC_PKCS7Padding,
  AES_GCM_NoPadding,
}
```

НА СТОРОНЕ CUPERTINO

1. Использует обычный **Keychain**.
2. Apple рекомендует хранить чувствительные данные, используя **Keychain**.
3. В сообществе iOS существует практика дополнительного шифрования данных.
4. FSS никак не шифрует данные! (см. **Secure Enclave** или **encrypt**).
5. ⚠️ По умолчанию FSS использует опасный параметр **kSecAttrAccessibleWhenUnlocked**.

ФЛАГИ ДОСТУПА KEYCHAIN 🔑

Флаги (**kSecAttrAccessible**) отвечают за то, каким образом вы можете получить данные из Keychain

ФЛАГИ ДОСТУПА KEYCHAIN 🔑

1. kSecAttrAccessible**WhenUnlocked** — когда устройство разблокировано
2. kSecAttrAccessible**AfterFirstUnlock** — разблокировано при первом включении

ФЛАГИ ДОСТУПА KEYCHAIN 🔑

1. kSecAttrAccessible**WhenPasscodeSetThisDeviceOnly** — самый надёжный
2. kSecAttrAccessible**WhenUnlocked**ThisDeviceOnly
3. kSecAttrAccessible**AfterFirstUnlock**ThisDeviceOnly

```
const AppleOptions({
  this.accountName = AppleOptions.defaultAccountName,
  this.groupId,
  this.accessibility = KeychainAccessibility.unlocked,
```

ЕЩЁ РАЗ

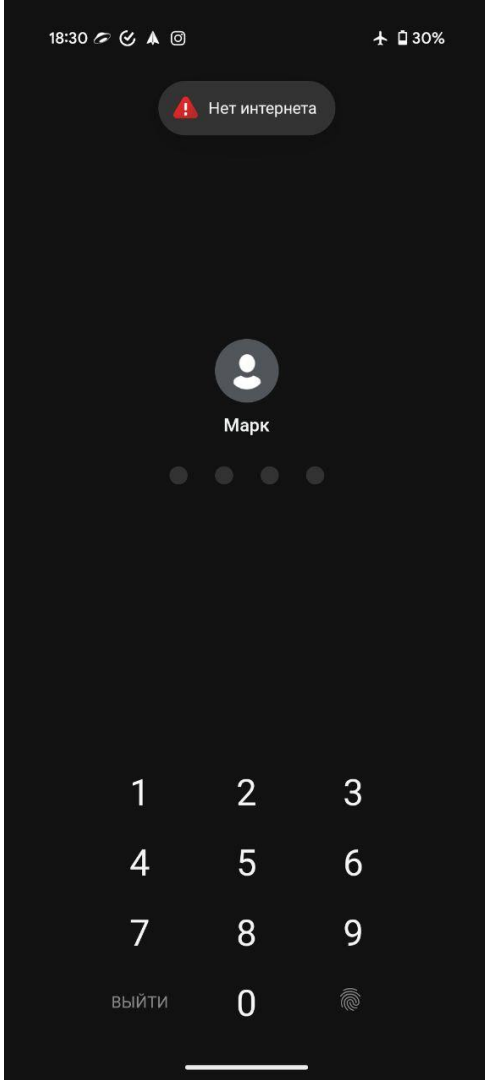
1. FSS хорошо работает на Android уже.
2. Обновите FSS и укажите флаг encryptedSharedPreferences на Android.
3. Данные на iOS по умолчанию бэкапятся, флаг “thisDeviceOnly”.
4. Обратите внимание, что данные на iOS не шифруются предварительно.

АВТОРИЗАЦИЯ ВНУТРИ

M3: Insecure Authentication/Authorization

PIN

1. **Левел 1:** зашить попытки ввода PIN-кода в коде Dart => обходим через перезапуск приложения => получаем брутфорс
2. **Левел 2:** храним попытки PIN-кода в постоянное хранилище => можем подменить количество => брутфорс
3. **Левел 3:** храним попытки в защищённом хранилище => подменить сложнее
4. **Левел 4:** храним и PIN и попытки на бэкенде => не обходится при защищённом соединении



Скриншот: приложение “Т-Банк”

БИОМЕТРИЯ

1. Самый популярный вид аутентификации
2. Может сыграть с вами злую шутку

local_auth 2.3.0

Published 5 months ago • flutter.dev Dart 3 compatible

SDK | FLUTTER PLATFORM | ANDROID IOS MACOS WINDOWS

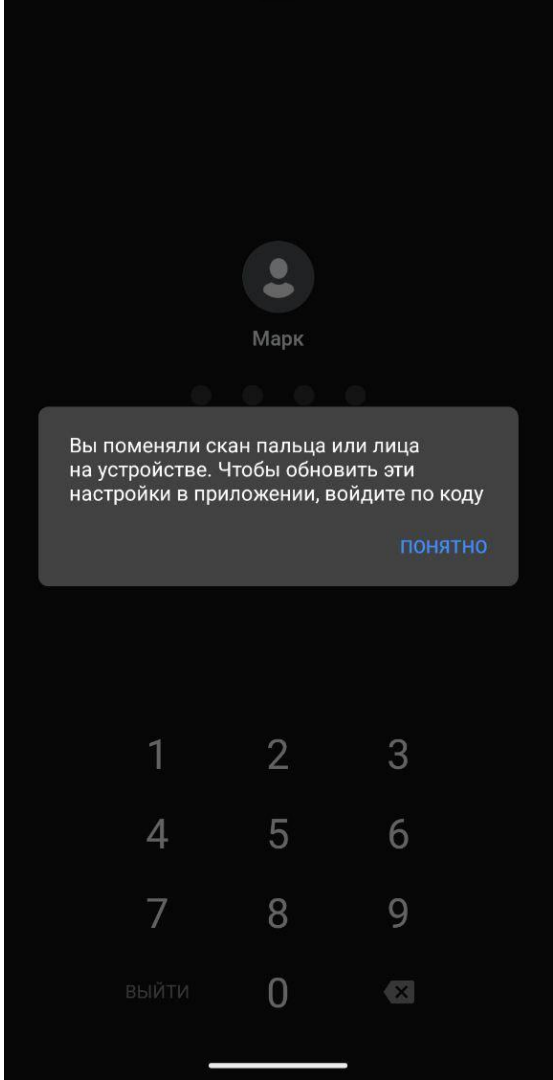
3.0K

Readme Changelog Example Installing Versions Scores

3.02k LIKES | 160 POINTS | 518k DOWNLOADS

LOCAL AUTH

1. Обходится с помощью подмены
2. Не реагирует на изменения биометрии в системе



Скриншот: приложение “Т-Банк”

БЕЗОПАСНАЯ ЛОГИКА

1. Генерация и хранение ключа
2. Проверка целостности ключа

ANDROID

1. Использование Keystore для шифрования и генерации ключей.
2. Использование флага `setInvalidatedByBiometricEnrollment`
3. Использование `BiometricPrompt.CryptoObject` и альтернативного `authenticate`

iOS

1. Использование Keychain и Secure Encalve для шифрования и генерации ключей.
2. Использование флага `biometryCurrentSet`
3. Использование `LAContext`

local_auth 2.3.0

Published 7 months ago • flutter.dev Dart 3 compatible

SDK | FLUTTER

PLATFORM | ANDROID IOS MACOS WINDOWS

3.09k LIKES | 160 POINTS | 767k DOWNLOADS

1. Самая популярная.
2. Использует `BiometricPrompt` и `LAContext` на платформе.
3. Не использует генерацию ключей.
4. Сам по себе небезопасен.

biometric_storage 5.0.1

Published 13 months ago • codeux.design Dart 3 compatible • Latest: 5.0.1 / Prerelease: 5.1.1-dev.1

SDK | FLUTTER PLATFORM | ANDROID IOS LINUX MACOS WEB WINDOWS

261

1. Подходит для хранения данных под защитой биометрии.
2. 🍏 На iOS использует Keychain, но не генерирует ключи. Сбрасывает биометрию.
3. 🪣 На Android Keystore + CryptoObject.
4. Внутри выглядит грязновато.

did_change_authlocal 0.0.6

Published 2 years ago • thongvo109.com Dart 3 compatible

SDK | FLUTTER PLATFORM | ANDROID IOS

22 LIKES | 140 POINTS | 15k DOWNLOADS

1. Очень мало лайков и давно не обновлялась.
2. Не проводит весь процесс биометрии, используется в связке с local_auth.
3. 🪣 На Android использует **AES/CBC/PKCS7Padding**
4. Внутри выглядит ещё более грязновато.

biometric_signature 6.2.0

Published 2 months ago • visionflutter.com Dart 3 compatible

SDK | FLUTTER PLATFORM | ANDROID IOS

20 LIKES | 160 POINTS | 76.5k DOWNLOADS

1. Также очень мало лайков.
2. 🪣 Очень неплохо реализовано на Android.
3. 🍏 На iOS используется Keystore + Secure Enclave, но ключ не инвалидируется.
4. Выглядит как хороший вариант.

ФРОНТЕНДЕРЫ ЛОХИ

Лучший способ хранить данные — делать это на бэкенде

САММАРИ

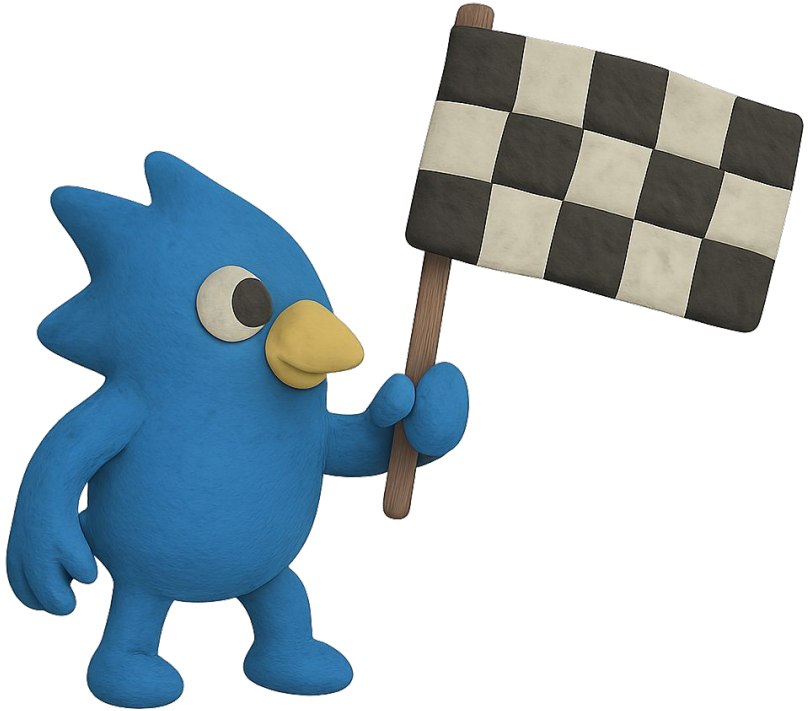
👊 Векторы атак на МП и OWASP TOP-10

🐦 Flutter хорошо справляется с атаками

☁️ Лучший способ защиты — ничего не хранить

🛡️ Превентивные меры защиты

👥 Сообществу необходимо развиваться



«Замки — это защита от добрых людей, а злые зайдут и без ключа»

«Замки — это защита от добрых людей, а злые зайдут и без ключа»