Защищаем себя и пользователей

(руководство по безопасности для iOS)

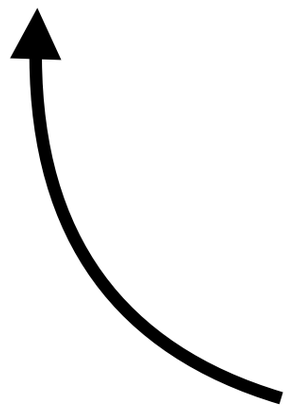
Вадим Дробинин

@Valzevul

В двух словах

- Что мы будем защищать?
- Какие бывают атаки?
- Примеры атак
- Как проверить приложение?
- Способы защиты
- Что дальше?

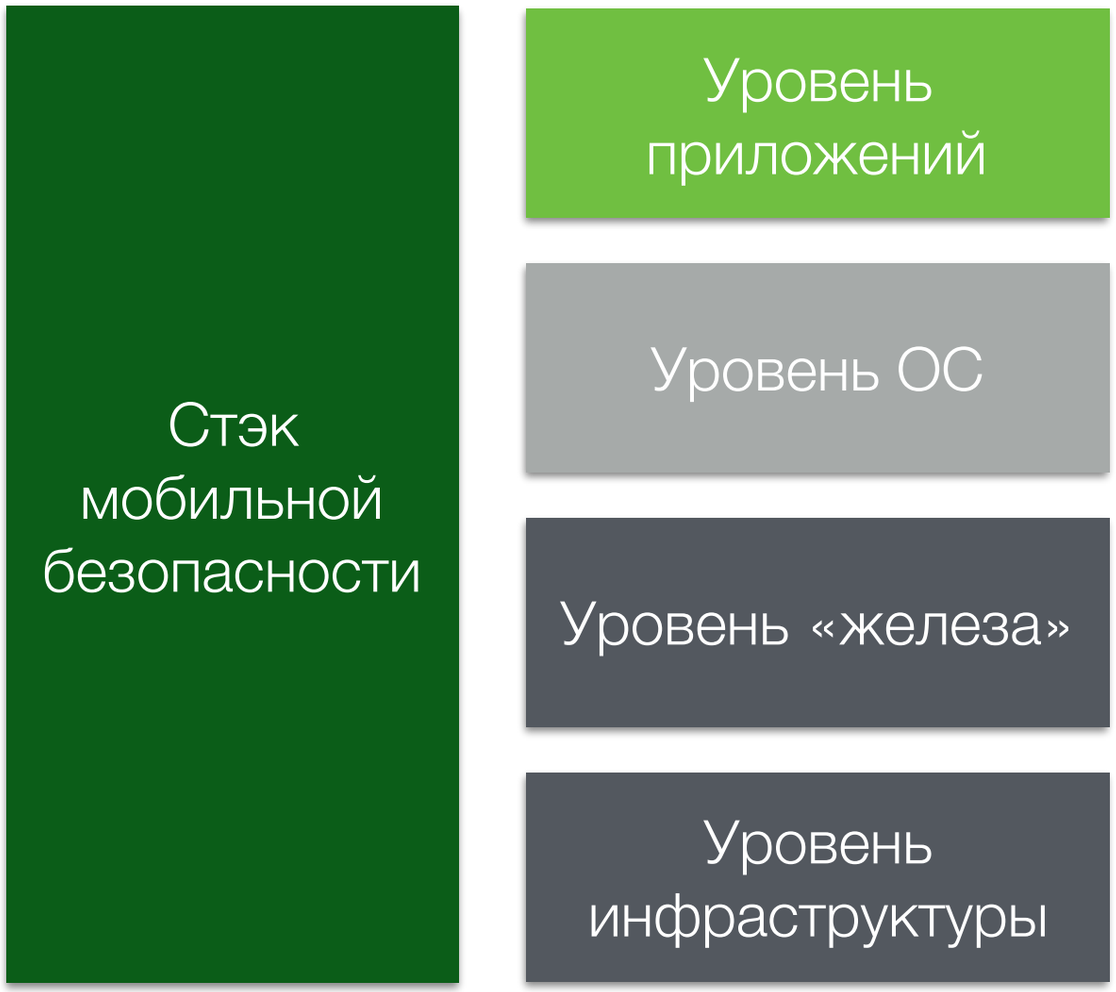
Мобильные устройства — основной источник личных данных пользователей



и мы не умеем их защищать

@Valzevul

Что мы будем защищать?



- **???**

- Версия OS
- Root-доступ

- Устройство
- Прошивка

- CDMA, GSM
- GPS
- SMS, MMS

Уровень приложений

Transport Layer Security

- NSURLConnection и NSURLSession требуют ATS
- ATS требует TLS 1.2 и сертификаты
- Приложения должны соответствовать *

Защита данных

- Всё шифруется с помощью уникального ключа в 256 бит
- Ключи «оборачиваются» в ключи классов
- Класс = политика безопасности

Уровень приложений

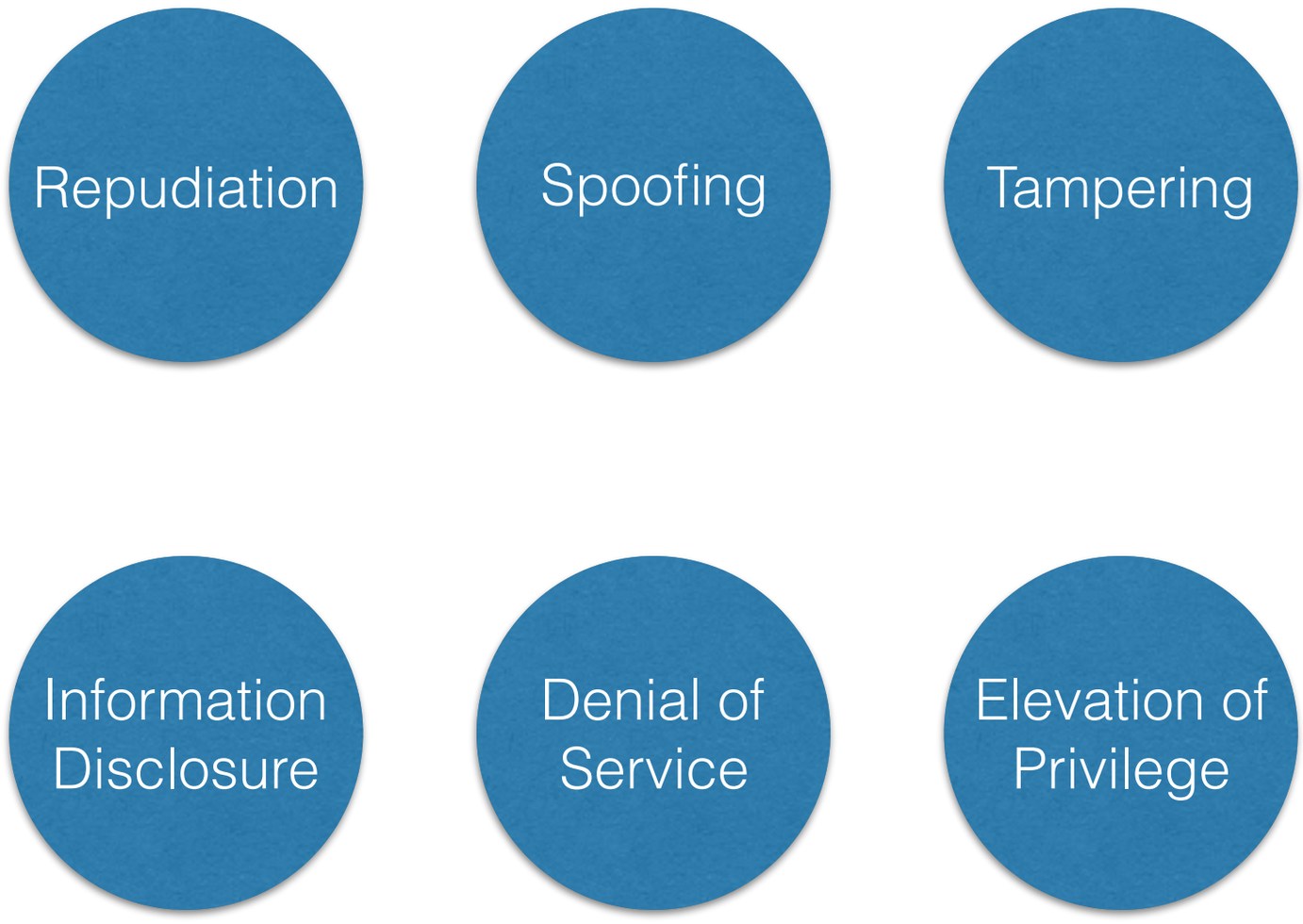
Transport Layer Security

С iOS9 сложно налажать в зашифрованной передаче данных

Защита данных

Почти все файлы надежно зашифрованы на диске

Какие бывают атаки?



Какие бывают атаки?

Какие бывают атаки?

@Valzevul

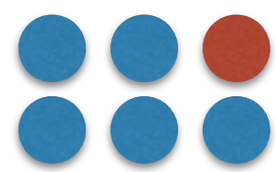
Какие бывают атаки?

Изменение локальных данных

Tampering (атаки искажения)

Незащищенная Wi-Fi сеть

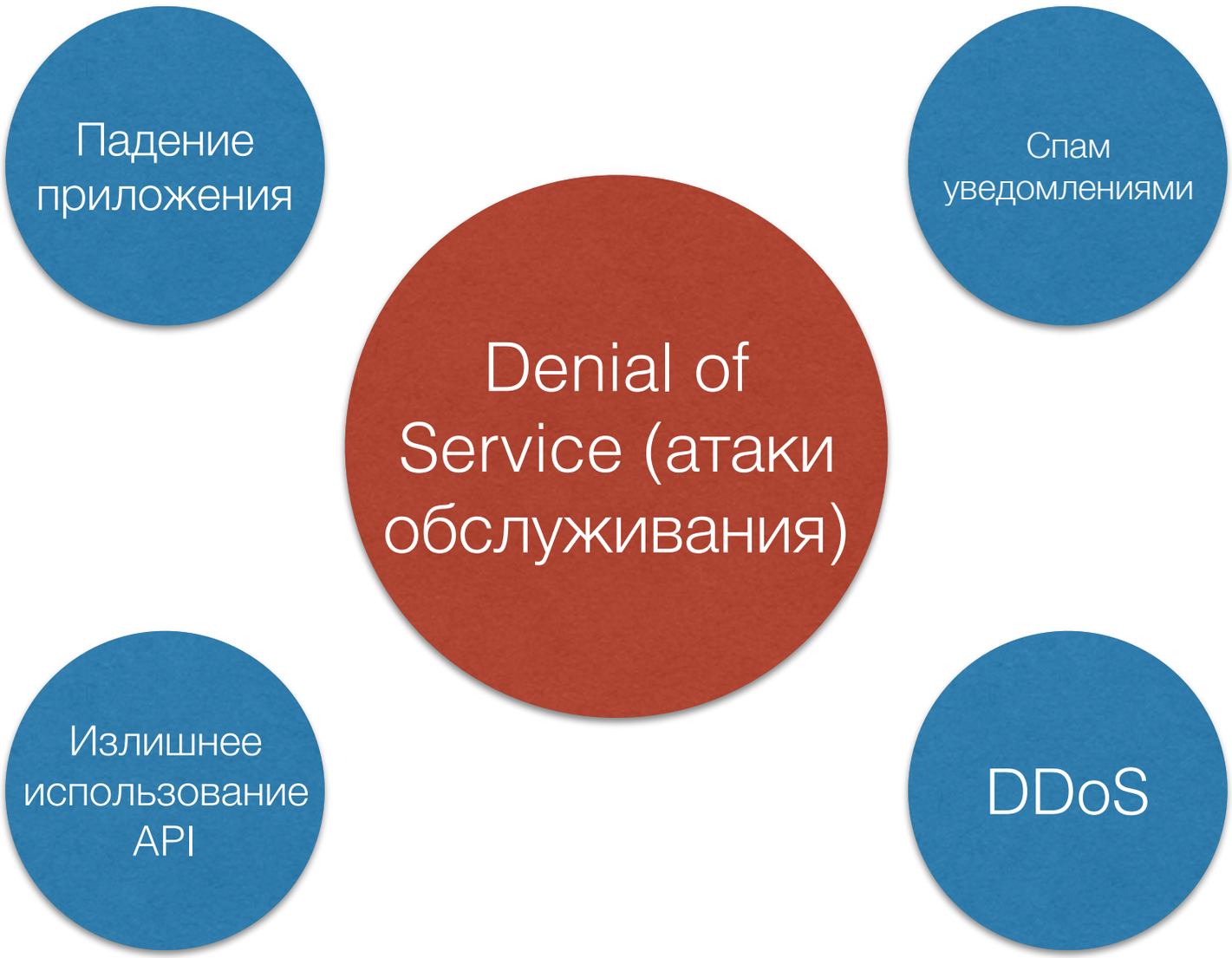
Взлом мобильной сети



Какие бывают атаки?

@Valzevul

Какие бывают атаки?



@Valzevul

Какие бывают атаки?

@Valzevul

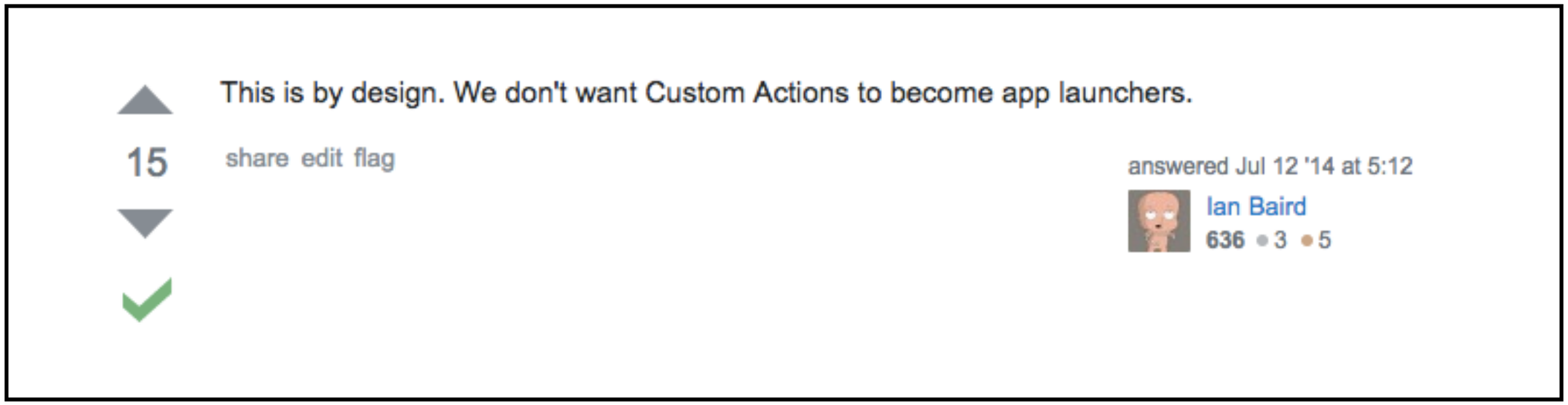
Примеры атак

- Information Disclosure (1):
  - Бэкапы в iTunes не шифруются по-умолчанию
  - Вирус BackStab
- Information Disclosure (2):
  - Никто не шифрует данные под PIN
  - Elcomsoft iOS Forensic Toolkit

Примеры атак

- Information Disclosure (3):
  - UIPasteboard (1Password, токены, URLы)
  - Кэш
- Elevation of Privilege:
  - Ad-hoc → можно использовать Private APIs
  - Вирусы для EnPublic (CVE-2014-1276)

Elevation of Privilege



github.com/valzevul/ElevationOfPrivilegeHack

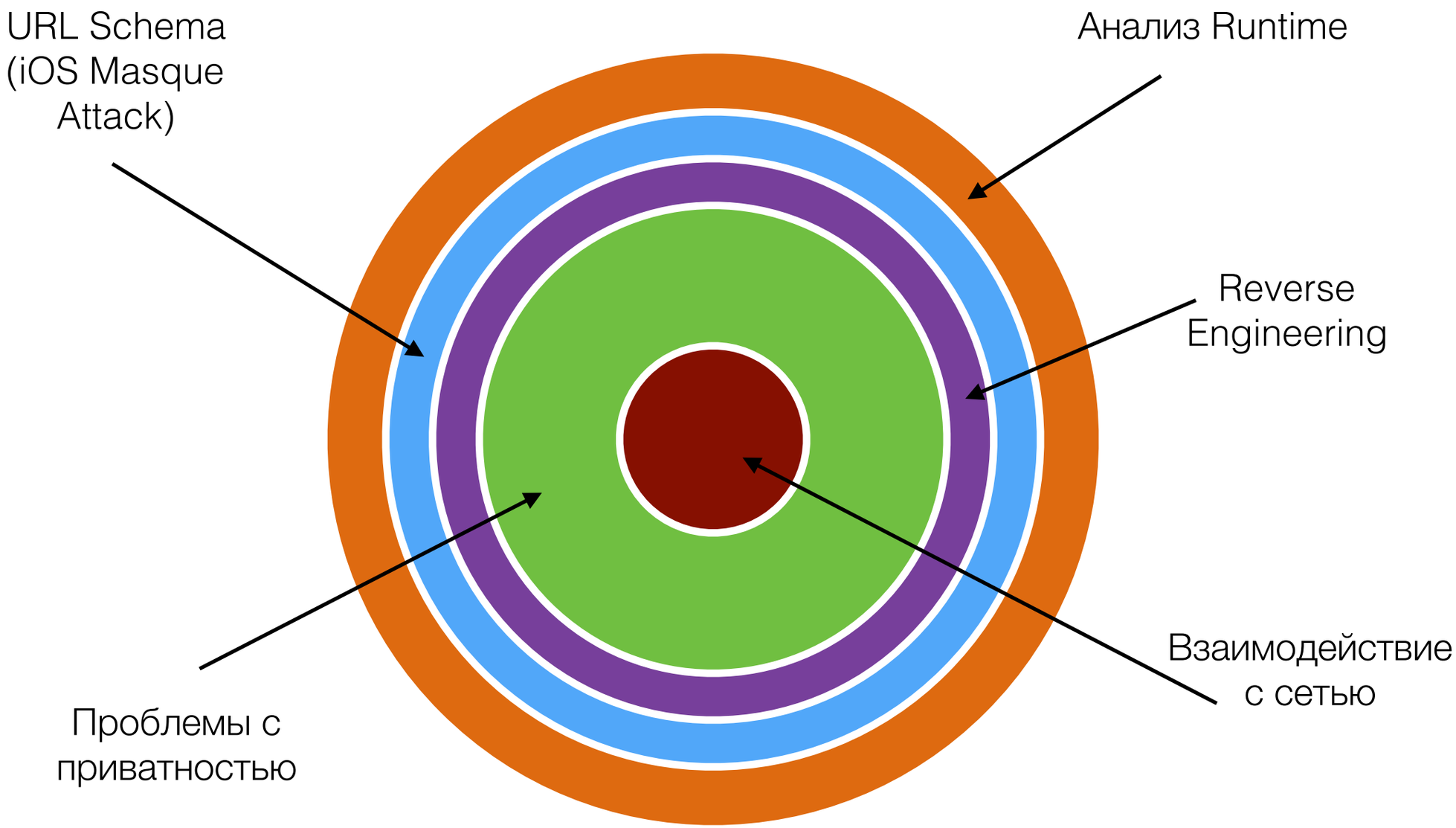
Как проверить приложение?

- White-box vs. Black-box;
- Личные данные (PII, personal or identifying information);
- Penetration-тесты («пентесты»).

PII

- Логины, пароли, геолокация, адрес, связь с социальными сетями;
- Имя девайса, имя сети, UDID;
- Данные приложения, логи и cookies.

Пентесты


URL Schema
(iOS Masque
Attack)
Анализ Runtime
Reverse
Engineering
Взаимодействие
с сетью
Проблемы с
приватностью

Пентесты

- Окружение:
    - iDevice
    - Сеть
    - Jailbreak
- Утилиты:
    - BigBoss Recommended Tools
    - OpenSSH
    - Clutch
    - Class-Dump
    - Cycript
    - Keychain dumper
    - …

Как защитить приложение?

- TLS и Certificate Pinning
  - Secure Networking by Apple
  - TrustKit
- Шифрование
  - Шифруйте всё (атрибуты NSData и NSFileManager)
  - Используйте Keychain
  - Не используйте Preferences, Cookies, /Library и /Documents

Как защитить приложение?

- Запретите синхронизацию
  - NSURLIsExcludedFromBackupKey
- Очищайте «скриншоты»
  - applicationDidEnterBackground → hidden
- Не пишите в NSLog
- Избегайте кэша клавиатуры
  - secureTextEntry
  - UITextAutocorrectionTypeNo

Как защитить приложение?

- Jailbreak-detection:
  - Проверьте наличие файлов MobileSubstrate.dylib, ssh, …
  - Попробуйте открыть Cydia.app
  - Проверьте вызов fork()
  - Проверьте родителя через sysctl (если не запущен или это ядро, вас дебажат!)
  - Обфусцируйте код

Что дальше?

@Valzevul

Что дальше?

- https://www.slideshare.net/eightbit/owasp-melbourne-introduction-to-ios-application-penetration-testing
- https://www.slideshare.net/OWASP_Poland/introduction-to-ios-penetration-testing

- Apple Pay: Inspect, Set Up, Promote (Vadim Drobinin, https://vk.cc/6iPXEe)
- Usability vs. Security (Josiah Renaudin, https://vk.cc/6j2i75)
- Demystifying Apple 'Pie' & TouchID (Sebas Guerrero, https://vk.cc/6iPY3f)
- iOS Headers, http://developer.limneos.net/

Узнавайте в кальянных и на конференциях

Вопросы и хейт-мейлы

@Valzevul

vadim@drobinin.com