Digital Security

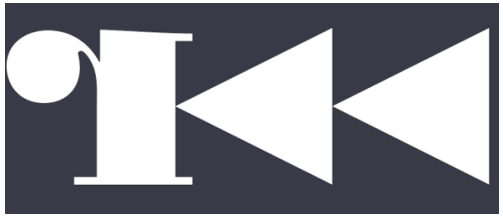
Последние фичи безопасности в iOS и Android

Борис @dukeBarman Рютин
Digital Security

Digital Security

whoami

- Исследователь информационной безопасности в **Digital Security**
- Редактор рубрики в журнале **Xakep**
- Участник R0 Crew и модератор проекта (**reverse4you**)
- Евангелист **radare2**
- Анализ **мобильных** приложений для Android и iOS
- Докладчик на различных **конференциях**
- **…**



План

1. Общий взгляд на безопасность мобильных приложений
2. Новые механизмы в iOS
3. Новые механизмы в Android

Б - безопасность

Модели злоумышленника

1. Злоумышленник с физическим доступом к устройству

2. Злоумышленник, не имеющий доступа к устройству, находящийся рядом* с жертвой

3. Злоумышленник, установивший вредоносное ПО на устройство жертвы

* - рядом это понятие относительное.

iOS

iOS

- Touch ID по умолчанию теперь используют 6-значный пароль вместо 4-х
- Добавилась двухфакторная авторизация для iCloud
- Поддержка IKEv2
- Добавилось диалоговое окно при попытке открытия приложением другого приложения

iOS

- Добавилась возможность удалить сторонние приложения для обновления ОС
- Добавили сертификат разработчика

App Transport Security (ATS)

iOS

- Контроль работы по открытым каналам передачи данных
- Запрещает работу по незащищённому каналу
- Появилось iOS 9.0
- По умолчанию включено для `NSURLConnection`, `CFURL` и `NSURLSession` API

Исключения для ATS

iOS

- `NSExceptionDomains` в `Info.plist`
- Типы исключений:
  - `NSExceptionMinimumTLSVersion`
  - `NSExceptionRequiresForwardSecrecy`
  - `NSExceptionAllowsInsecureHTTPLoads`
  - `NSRequiresCertificateTransparency`
  - `NSIncludesSubdomains`
  - `NSThirdPartyExceptionMinimumTLSVersion`
  - `NSThirdPartyExceptionRequiresForwardSecrecy`
  - `NSThirdPartyExceptionAllowsInsecureHTTPLoads`

Примеры работы с ATS

iOS

ATS для всех, с одним исключением

▼ NSAppTransportSecurity	Dictionary	(1 item)
▼ NSExceptionDomains	Dictionary	(1 item)
▼ media.example.com	Dictionary	(2 items)
NSIncludesSubdomains	Boolean	YES
NSExceptionsAllowsInsecureHTTPLoads	Boolean	YES

ATS отключена, с одним исключением

▼ NSAppTransportSecurity	Dictionary	(2 items)
NSAllowsArbitraryLoads	Boolean	YES
▼ NSExceptionDomains	Dictionary	(2 items)
▼ secure.example.com	Dictionary	(1 item)
NSExceptionsAllowsInsecureHTTPLoads	Boolean	NO

Android

Android list

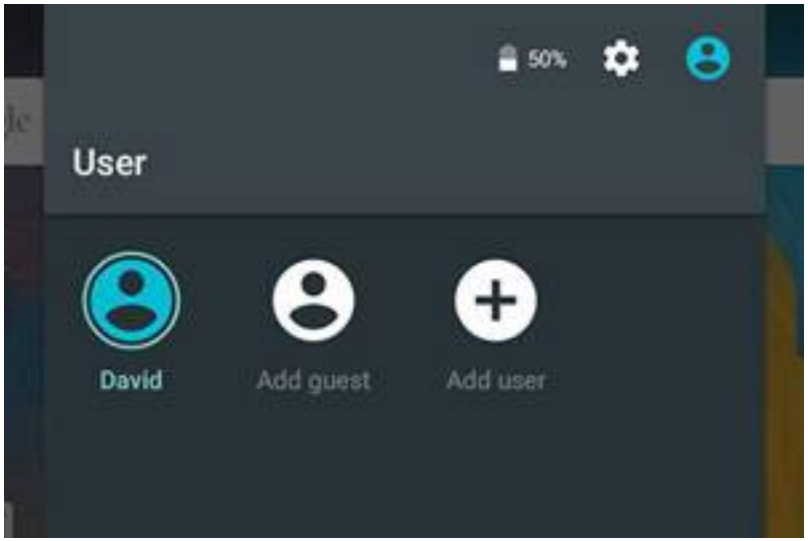
- Android 5.0 == API 21 == Android L(ollipop)
- Android 5.1 == API 22 == Android L(ollipop_MR1)
- Android 6.0 == API 23 == Android M(arshmallow)
- Android N?

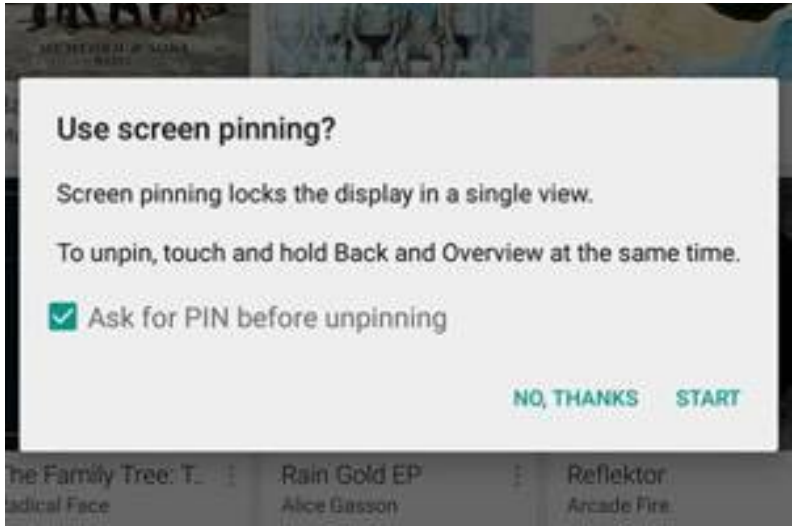
Новая модель разрешения с Android M

- Запрос разрешений в Post-install/run-time
  `ContextCompat.checkSelfPermission`
- Можно отзывать разрешения
  `Settings -> Apps -> app-name -> Permissions`
- Группы разрешений:
  `normal, dangerous, signature, signatureOrSystem, system, development, appop`
- Если target SDK < Android M, то все работает как и раньше (но может отзывать разрешения)

Мультипользователи с Android 5.0

- Поддержка мультиаккаунтов и профайлов
- Гостевой режим
- Screen pinning
- Smart Lock

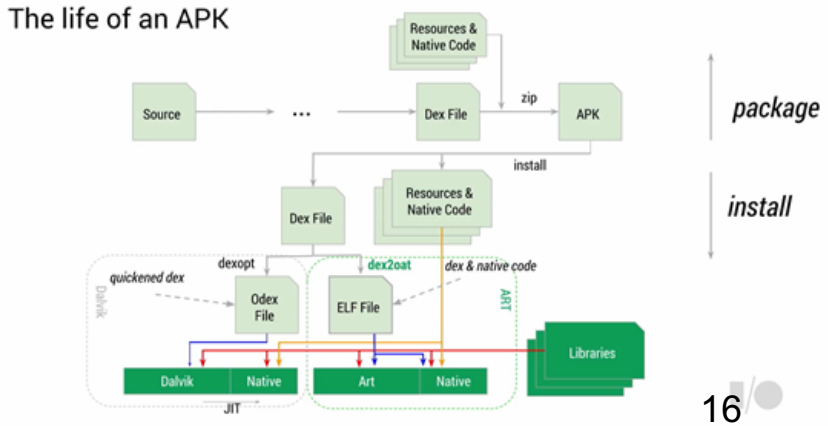




Android Runtime (ART)

- Впервые появился в Android 4.4
- С Android 5.0 заменил Dalvik
- ART компилирует (ahead-of-time (AOT)) приложение во время установки
- Обратная совместимость
- С Android 6.0 обработка прав на newInstance()

- Danger:
  - Если JNI
  - Нестандартный код
  - Очистка памяти…



Security-Enhanced Linux (SELinux)

- Мандатное управление доступом (Mandatory Access Control, MAC)
  - Все что не разрешено, то запрещено
  - Discretionary access control (DAC)
- Впервые появилось в версии Android 4.3
  - Permissive mode (журнал)
- Полная поддержка с Android 5.0
  - Enforcing mode for all domains (кроме kernel и init)

Other SE(curity) с Android 5.0

- FORTIFY_SOURCE– libc функции: `stpcpy()`, `stpncpy()`, `read()`, `recvfrom()`, `FD_CLR()`, `FD_SET()` и `FD_ISSET()`
- non-PIE linker support removed
- Cryptography SSL/TLS – включены TLSv1.1 & TLSv1.2
- Bugs...bugs...bugs...

Storage Access Framework

- Появилась в Android 4.4
- Улучшилась поддержка в Android 5.0
- Сторонние приложения могут запросить доступ к отдельным файлам или директориям
- Взаимодействите через `Intent.ACTION_OPEN_DOCUMENT_TREE`
- В 6.0 шифрование и улучшение доппамяти

Auto Backup в Google Drive с Android M

- Происходит каждые 24 часа
- Похоже на ADB backup
  - Отключается с помощью “`android:allowBackup`” в значении `false` в `AndroidManifest.xml` или указываем через `android:fullBackupContent`
- В backup не попадают файлы:
  - С внешнего носителя `getCacheDir()` и `getCodeCacheDir()`
  - С кэша `getExternalFilesDir()`
  - Обрабатываемые как не для backup `getNoBackupFilesDir()`

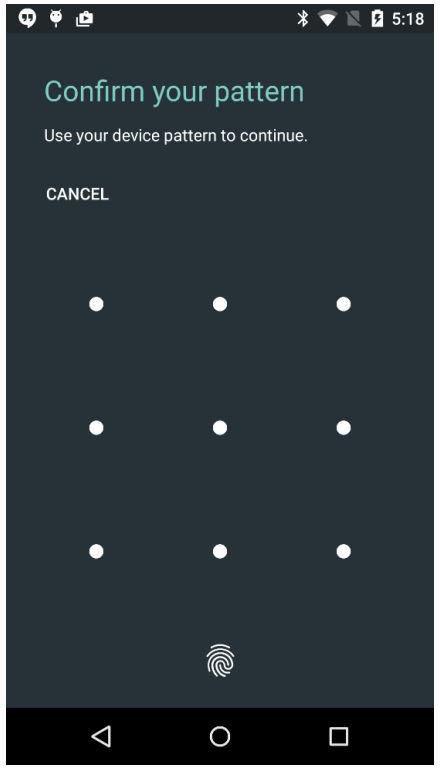
Confirm Credentials с Android 6.0

- Проверка перед важным действием, что устройство у пользователя (или как давно пользователь разблокировался)

```
setUserAuthenticationValidityDurationSeconds()
createConfirmDeviceCredentialIntent()
```

- Хорошо только в сочетании с ключами:

```
KeyGenerator или KeyPairGenerator
```



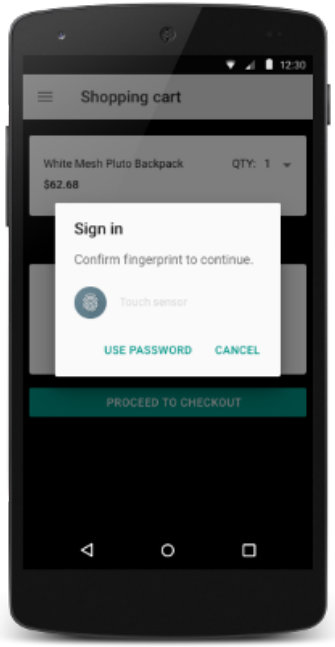
Fingerprint API с Android 6.0

- Класс `FingerprintManager` и метод `authenticate()`

```
<uses-permission
 android:name="android.permission.USE_FINGERPRINT" />
```

- Тестирование:

```
adb -e emu finger touch (API => 24)
```



Уведомления с Android 5.0

- Элементы на экране блокировки (by default)
- `setPublicVersion()`- для включения сокрытия
- `setVisibility()` и задайте видимость уведомления:
  - `VISIBILITY_PRIVATE`: показывать основные сведения, такие как значок, но скрывать все остальные
  - `VISIBILITY_PUBLIC`: показывать всё уведомление
  - `VISIBILITY_SECRET`: ничего, кроме иконки

Нововведения в WebView с Android 5.0

- `setMixedContentMode()` – установка режима со смешенным контентом
  - MIXED_CONTENT_NEVER_ALLOW – по умолчанию для API Level >= 21
  - MIXED_CONTENT_ALWAYS_ALLOW – по умолчанию для API Level < 21
  - MIXED_CONTENT_COMPATIBILITY_MODE
- `setAcceptThirdPartyCookies()` – работа со сторонними cookies
  - Для APLI Level < 21 – разрешено по умолчанию
  - Для API Level >= 21 – запрещено по умолчанию
- WebViews получают обновления через Google Play
- Класс `PermissionRequest` - доступ к защищенным ресурсам, таким как камера и микрофон

android.os.StrictMode API с Android M

- Запрет на отправку данных по незащищенному каналу
- `detectCleartextNetwork()`
  - `penaltyDropBox()` – запись в лог
  - `penaltyDeathOnCleartextNetwork()` – crash

Новый атрибут сетевой безопасности

- С Android 6.0
- `<application android:usesCleartextTraffic=["true" | "false"]>`
  - По умолчанию `true`, если не определен.
  - Если в `false`, то приложение упадет при работе через HTTP вместо HTTPS.
- Появление нового класса `NetworkSecurityPolicy` `isCleartextTrafficPermitted()`

CookieManager class с Android 5.1

- Управляет cookies приложения внутри WebView
- Методы:
  - `removeAllCookie()`
  - `setAcceptThirdPartyCookies(WebView, boolean)`
  - `acceptThirdPartyCookies(WebView)`
  - `setAcceptCookie(boolean)`
  - `removeSessionCookie()`
  - `removeExpiredCookie()`
  - `setCookie(String, String)`
  - `getCookie(String)`
  - `acceptCookie()`
  - …

App Linking с Android M

- Только определенное приложение может обрабатывать URL и должен быть доступен сайт
- Если приложение не установлено, то появится окно открыть с помощью...

```
<intent-filter
android:autoVerify="true">...
<data android:scheme="http"
android:host="www.android.com" /> ...
</intent-filter>
```

Безопасная работа с Service с Android 5.0

- Модифицировано поведение `Context.bindService()`
- Необходимо использование явного Intent

```
intent.setPackage("com.example.app");
```

Защита от tapjacking с Android 5.0

- Необходимо установить атрибут для View

```
android:filterTouchesWhenObscured="true“
```

- Или програмным путем

```
view.setFilterTouchesWhenObscured(true);
```

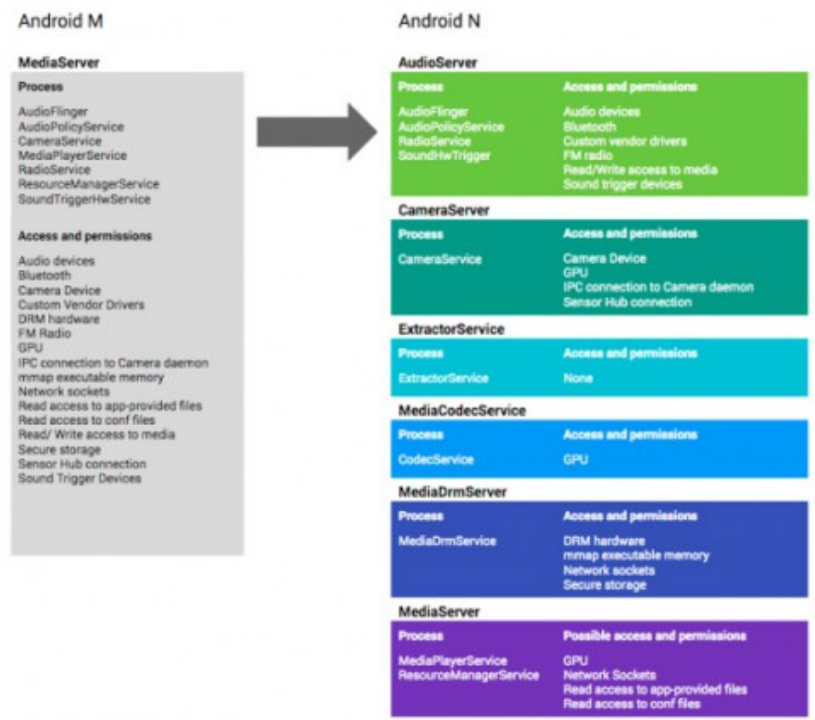
Это позволяет быть уверенным, что тачи не будут отправлены вашему activity, когда View другого приложения перекрывает ваше activity.

IPC и Manifest

- Безопасность в Android начинается с AndroidManifest.xml
  - Настройки проекта
    `android:debuggable=["true" | "false"]`
  - Запрашиваемые права
    `<uses-permission>`
  - Доступ к компонентам
    `android:exported=["true" | "false"]`

Новые фичи. Android N

- Явно указать - используется открытый траффик или нет
- Разделение MediaServer
- !User-сертификаты
- Storage Encryption
- Seccomp – Sandbox
- Улучшение ASLR
- Проверка BOOT



Заключение

iOS ANDROID

- Мобильные ОС развиваются постоянно
- Механизмы безопасности также совершенствуются
- Заимствуют лучшее!?...

P.S.

Следим за изменениями:

- iOS:
  - https://developer.apple.com/library/ios/releasenotes/General/WhatsNewIniOS/Articles/iOS9_3.html
  - https://developer.apple.com/library/ios/releasenotes/General/iOS90APIDiffs/
- Android:
  - http://changes.droidsec.org/
  - http://androidtamer.com/android-security-enhancements/
  - https://source.android.com/security/

Digital Security

Последние фичи безопасности в iOS и Android

Спасибо за внимание!

Вопросы?

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47

b.ryutin@dsec.ru

@dukeBarman