Análise a Aplicações Mobile

António Pinto
apinto@estg.ipp.pt

Novembro 2024 (v3)

Sumário

Aplicações móveis

para *smartphones*, *tablets*, ...

- Pessoas usam constantemente **múltiplas aplicações** móveis, **múltiplas vezes** ao dia
- **Quantidade de informação** sobre o utilizador existente no telemóvel é avassaladora
- Algumas aplicações **aproveitam-se** desta fonte de informação
- Muitas destas tem como **única** fonte de receita a **publicidade**
- Pode ser um **forte auxílio** na investigação digital forense

Controlo por permissões

- Mecanismo dos sistemas operativos mobile que permitem algum nível de controlo sobre a atuação das aplicações
- Condiciona o acesso a funcionalidades de *hardware* (câmara, GPS) ou a dados (fotos, informação pessoal) mediante autorização do utilizador
- É um mecanismo útil, mas com limitações
- Problemas e abusos (*malware*) levou a alterações ao seu funcionamento
  - Aceitação de permissões (até ao KitKat) era em bloco
  - Versões recentes Android permitem tratamento individual

Controlo por permissões

Android: Modo de funcionamento

- Programadores indicam as permissões necessárias ao funcionamento das aplicações
- Lista de permissões incluída no manifesto das aplicações
- Utilizador, ao instalar aplicações, pode consultar as permissões solicitadas
- Utilizador decide se autoriza cada permissão, quando solicitado pela aplicação e de forma individual

Grupos de permissões

Android

- Disponíveis 2 níveis de permissões: normais e perigosas
- Permissões **normais** englobam atividades que envolvem **muito baixo risco** para a privacidade dos utilizadores (ex.: mudar *timezone*)
- Permissões **perigosas** englobam atividades que envolvem **dados dos utilizadores** ou a capacidade de **influenciar o funcionamento** de outras aplicações
  - Requerem autorização explicita do utilizador

Grupos de permissões

Android

- Autorização pode ser dada
  - No momento de **instalação** (Android 5.1 ou inferior)
  - **Durante a utilização** (Android 6 ou superior)
- Mas sempre para todas as **permissões do grupo**!

Permissões perigosas

(e respetivos grupos)

Grupo	**Permissões**
CALENDAR	READ_CALENDAR, WRITE_CALENDAR
CAMERA	CAMERA
CONTACTS	READ_CONTACTS, WRITE_CONTACTS, GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE, CALL_PHONE, READ_CALL_LOG WRITE_CALL_LOG, ADD_VOICEMAIL, USE_SIP PROCESS_OUTGOING_CALLS
SENSORS	BODY_SENSORS
SMS	SEND_SMS, RECEIVE_SMS, READ_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS
STORAGE	READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE

Apps potencialmente perigosas

Aplicações que

1. Enganam o utilizador para que autorize permissões que não necessitam
2. Escondem comportamento malicioso por detrás de permissões legitimas
3. Tentam levar o utilizador a fornecer informação sensível (ex.: cartão de crédito)

Apps potencialmente perigosas

Proteção passa por

- Usar apenas lojas fidedignas (Ex.: Google, Amazon)
- Analisar criteriosamente as permissões antes da sua instalação
  - Quando em dúvida, validar comentários, classificação, página do programador
- Analisar o comportamento da aplicação em tempo de execução

Análise de comportamento

(ponto de vista dos utilizadores)

- Aplicações podem ser analisadas também quanto ao seu comportamento, validando
  - Em que situações solicitam autorização para permissões
  - Que tipo de comunicações usam (HTTP, HTTPS, outras)
  - Que tipo de API (ou *web* APIs) são utilizadas e para que servem
  - Que informações recolhem

Análise de comportamento

(ponto de vista das *Apps*)

- Análise possibilita também a descoberta de problemas na forma como são implementadas
  - Uso de APIs sem autenticação
  - Possibilidade de extração de informação de outros utilizadores

Análise de comportamento

(ponto de vista das comunicações)

- Generalidade das Apps
  - Usa HTTPS como forma de comunicação segura com os seus serviços
  - Solicita autenticação aos utilizadores (muitas vezes OAuth)
- Levanta algumas considerações
  - Captura de tráfego de rede para análise não é viável por estar encriptado
  - Não é possível utilizar *Apps* e respetivas APIs sem credenciais

Análise de comunicações

- Captura de tráfego de rede permite analisar
  - Pedidos não cifrados
  - Equipamentos utilizados
- Ideal é poder-se analisar todos os pedidos efetuados, mesmo os cifrados (HTTPS)
  - Solução passa por utilizar *software* específico para o efeito

Análise de comunicações

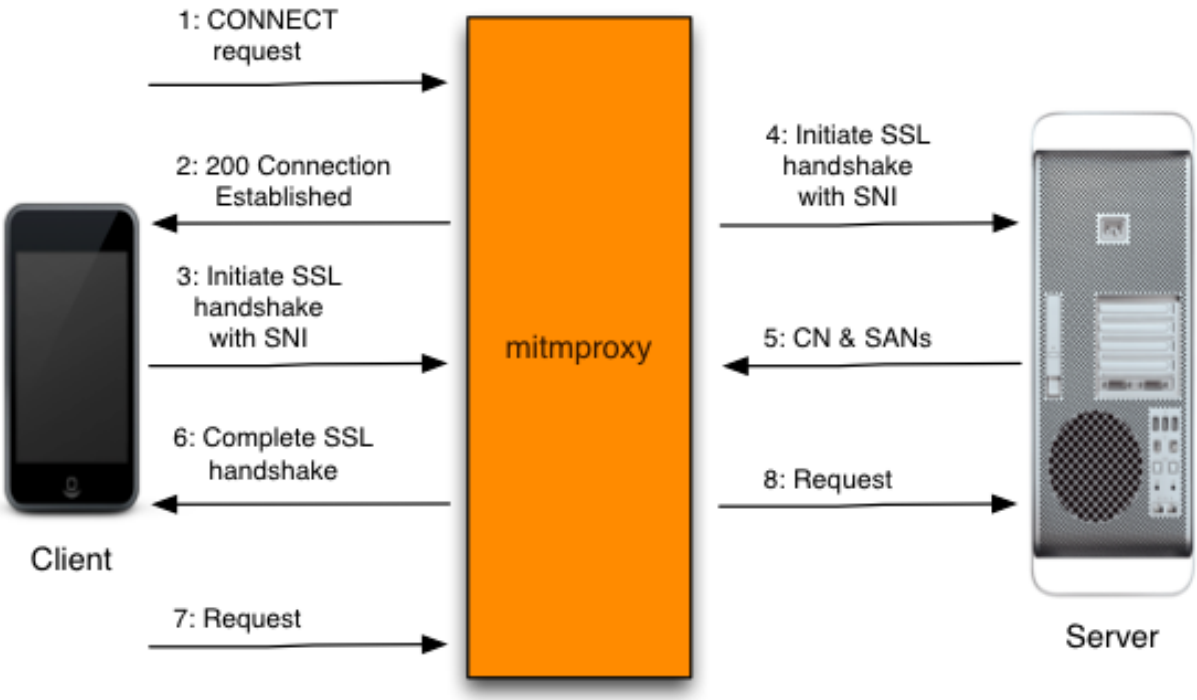
A partir do *browser*

- Análise de comunicações *web* com *browser* é simples
- Existem *add-ons* que possibilitam a análise aos pedidos HTTP enviados/recebidos
- Ferramentas de desenvolvimento dos próprios *browsers*
- Como executam no *browser*, a cifra das comunicações não impede o seu uso

Análise de comunicações

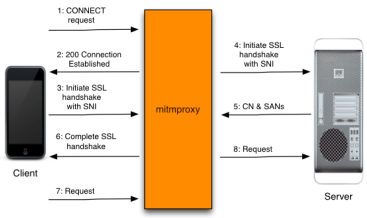
mitmproxy `https://mitmproxy.org`

- **mitmproxy** suporta a interceção e análise de HTTPS



mitmproxy

Funcionamento



1. Cliente liga-se ao mitmproxy e faz pedido de ligação
2. mitmproxy responde **200 Ok**, simulando conclusão da ligação
3. Cliente assume estar ligado ao servidor real e inicia ligação segura (TLS) indicando SNI[a]
4. mitmproxy cria ligação segura ao servidor real usando o SNI
5. Servidor responde, indicando os campos CN e SAN, utilizados para gerar certificado forjado
6. mitmproxy gera certificado forjado e conclui ligação segura com o cliente (suspenso desde passo 3)
7. Cliente envia o pedido cifrado HTTP para o mitmproxy
8. mitmproxy reenvia pedido para o servidor real

[a] `https://en.wikipedia.org/wiki/Server_Name_Indication`

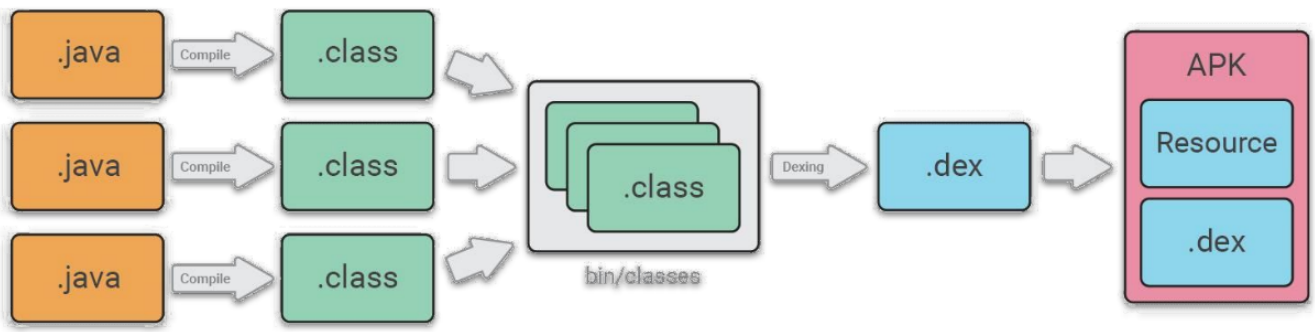
Conteúdos

Aplicações Android

- Aplicações Android são distribuídas em **ficheiros APK**
- APK não são mais do simples **ficheiros ZIP**, contendo o código de outros recursos da aplicação, organizado em pastas
- É possível obter-se **muita informação** sobre uma aplicação pela simples análise do conteúdo dos APK

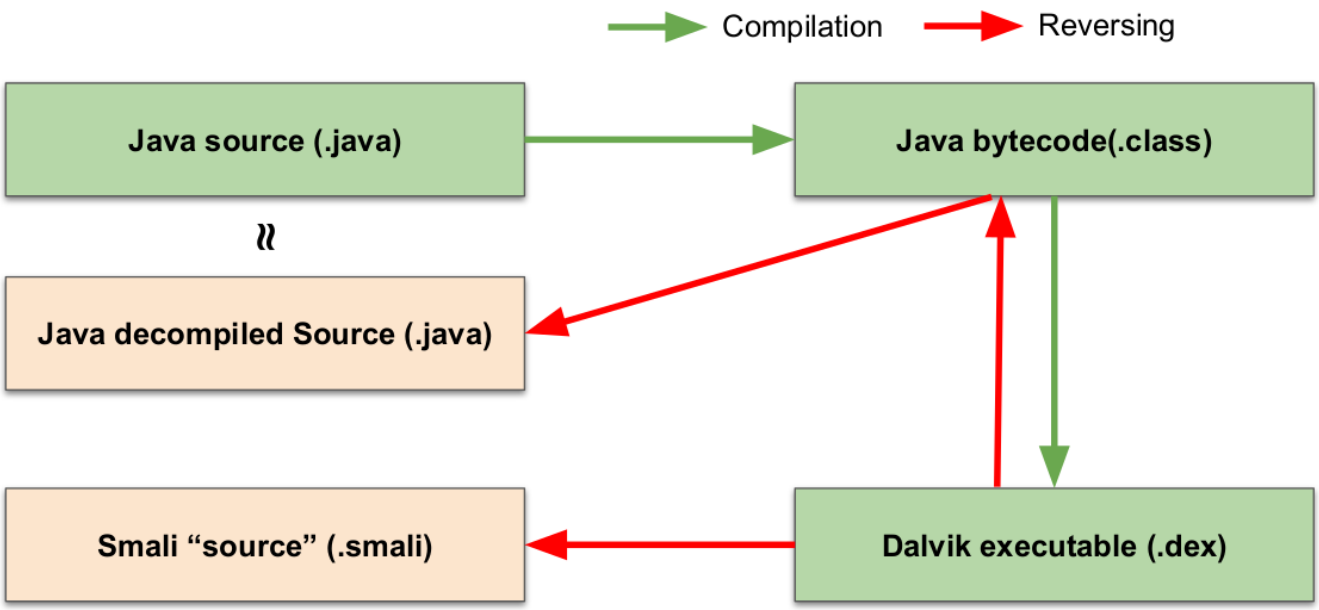
Compilação de aplicações Android

(visão simplificada)



Descompilação de aplicações Android

(visão simplificada)



Ferramentas disponíveis

- Android studio (`https://developer.android.com/studio`)
- APK Tool (`https://ibotpeaches.github.io/Apktool/`)
- **JADX-GUI** (`https://github.com/skylot/jadx`)
- Bytecode Viewer (`https://github.com/Konloch/bytecode-viewer`)
- dex2jar (`https://github.com/pxb1988/dex2jar`)

Como obter APK

- `https://apk-dl.com`
- `https://www.aptoide.com`
- `https://www.apkmonk.com`
- Extraindo de um telemóvel

```
$ adb shell pm list packages
$ adb shell pm path com.package.name
$ adb pull /full/path/to/apk
```


Exercício #2

Análise de código de aplicação mobile (15 minutos)

Analise a aplicação disponibilizada no mobile_app.zip usando o JADX-GUI.

Submeta a sua análise crítica pelo **moodle** (um ficheiro PDF).