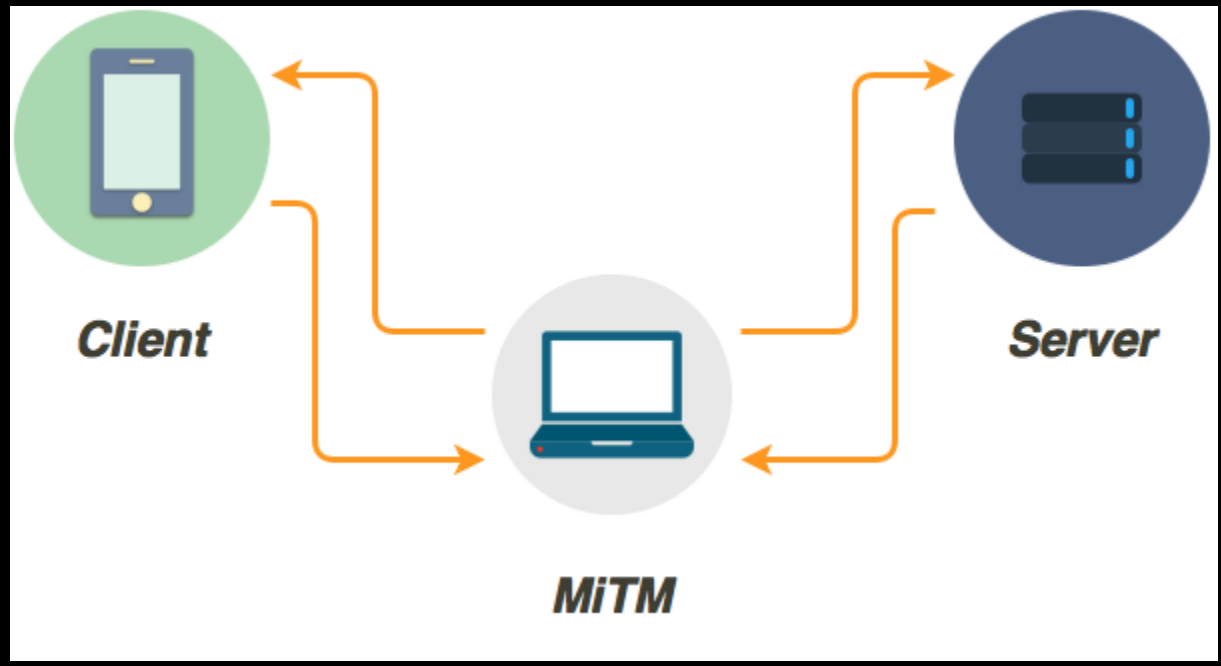
Android Mobile Pentest 101

Bài 6 – SSL Pinning

Mục tiêu: Hiểu vì sao bạn không bắt được request trên burpsuite ☺

Giới thiệu

- SSL Pinning là quá trình liên kết host với chứng chỉ X.509 certificate hoặc public key. Khi chứng chỉ hoặc key đã được chỉ định cho host, nó được gọi là 'pinned' với host.
- Phần mềm giao tiếp với server thông qua giao thức https và có pinning sẽ khiến kiểu tấn công Man-In-The-Middle attack thất bại, và cũng không lấy được dữ liệu dưới dạng clear text khi sử dụng các công cụ proxy (như burpsuite)



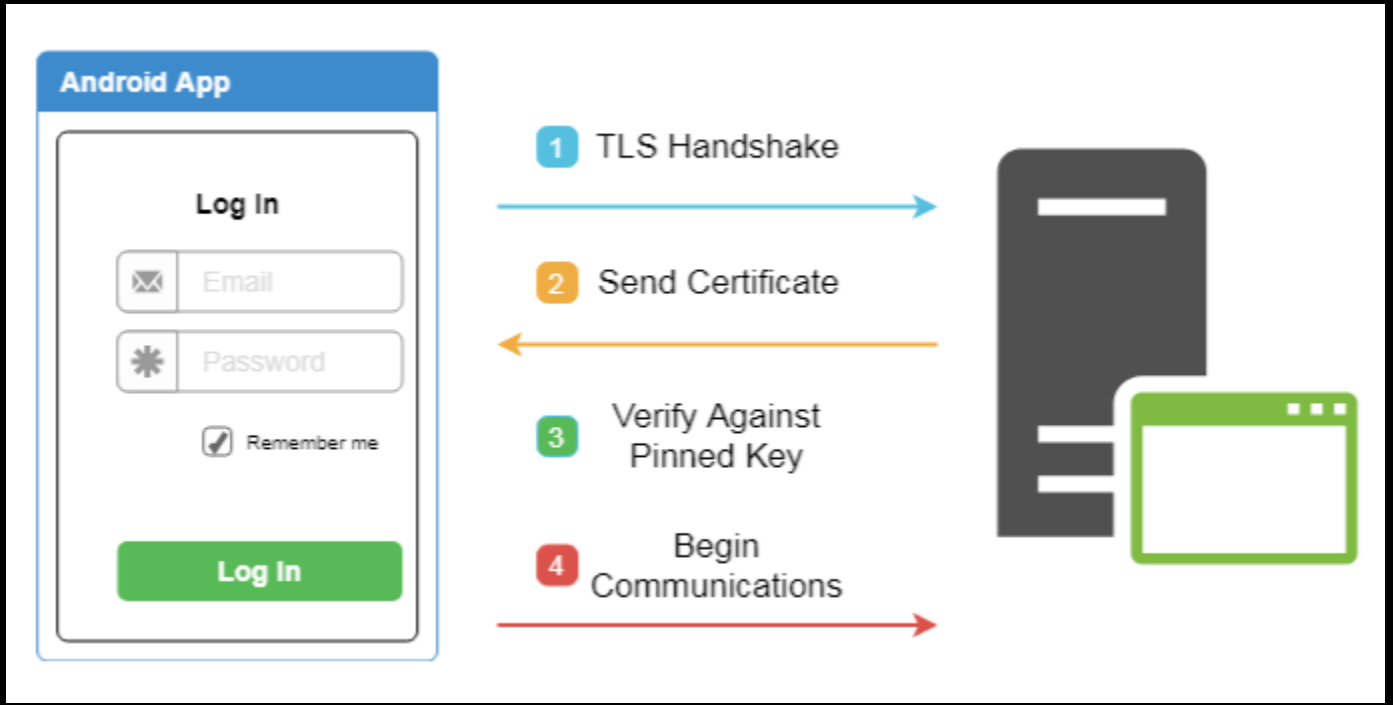
Giới thiệu

- Bây giờ chúng ta sẽ nói qua về pinning
- Có 3 lựa chọn dùng để pin:

1. Certificate Pinning (Chủ yếu nói về cái này)
2. Public Key
3. Hashing

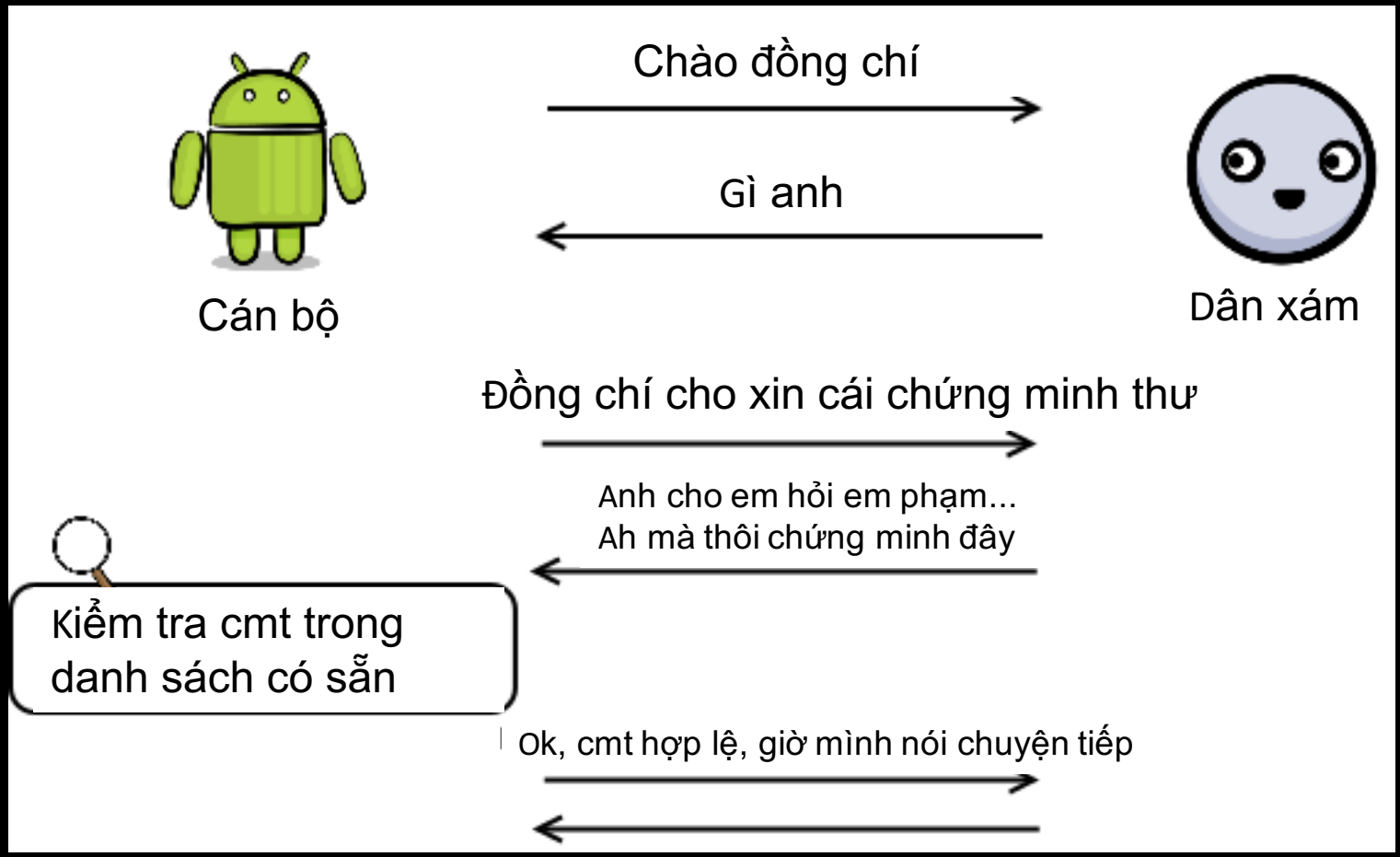
What To Pin -> Certificate

- Certificate dễ pin nhất
- Khi chương trình chạy lên và bắt đầu truy vấn, bạn sẽ nhận được một certificate từ website hoặc server
- Bạn dùng certificate đó để so sánh với certificate được pin vào app
- Nếu trùng thì app sẽ đồng ý tương tác với web/server



What To Pin -> Certificate

- Hoặc theo ngôn ngữ dân dã:



What To Pin -> Public Key

- Phức tạp hơn pin certificate
- Cần thực hiện nhiều bước hơn, vì phải tách key nằm trong certificate ra
- Cũng giống pin certificate, chương trình kiểm tra public key lấy ra từ certificate với key pin sẵn trong chương trình

What To Pin -> Hash

- Cho phép bạn giấu certificate hoặc public key
- Rất tiện để sử dụng, vì kiểu pin này thường cung cấp dưới dạng native api
- Còn có thể dùng để chứng thực danh tính tổ chức trong trường hợp bị giả mạo

Mấy slide tiếp theo nói về việc pin vào đâu trong app
(thông tin thêm thôi, bỏ qua cũng được ☺)

Where To Pin -> Leaf certificate

- Đảm bảo gần 100% chắc chắn rằng đây là chứng chỉ của bạn ngay cả khi Root CA bị tổn hại
- Nếu chứng chỉ trở thành không hợp lệ vì lý do nào đó (hoặc hết hạn hoặc bị tổn hại), ứng dụng sẽ bị ngưng cho đến khi có bản cập nhật mới
- Cho phép sử dụng các chứng chỉ tự ký

Where To Pin -> Root certificate

- Bạn tin tưởng vào cơ quan cấp chứng chỉ gốc
- Nếu CA bị tổn hại -> game over

Where To Pin -> Intermediate certificate

- Bạn tin tưởng rằng cơ quan cấp intermediate certificate không phát hành sai chứng chỉ cho (các) máy chủ của bạn
- Miễn là bạn còn sử dụng chứng chỉ của một nhà cung cấp thì mọi thay đổi đối với leaf certificate sẽ hoạt động mà không cần phải cập nhật ứng dụng của bạn

Thông tin thêm

- Một quan niệm sai lầm phổ biến về việc pin certificate là nó ngăn cản người dùng xem client-server communications
- OWASP's page on Certificate and Public Key Pinning[1] reads:

"You should pin anytime you want to be relatively certain of the remote host's identity or when operating in a hostile environment. Since one or both are almost always true, you should probably pin all the time."

- Do app có SSL Pinning, chúng ta sẽ không intercept được câu truy vấn gửi lên từ điện thoại bởi vì self-signed certificate tạo ra bởi tool proxy như burp không được tin cậy, hầu như tất cả các app sẽ không tương tác tiếp ☹

Detect Pinning

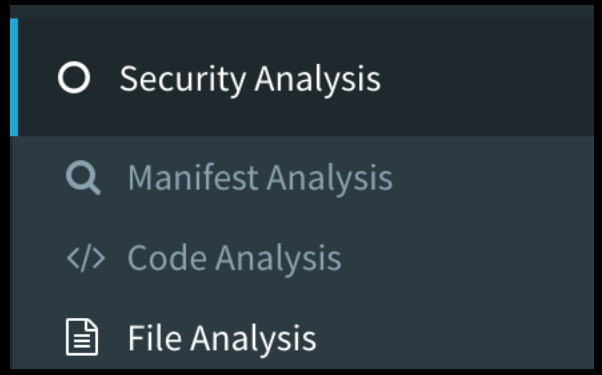
- Để kiểm tra xem app có ssl pinning hay không thường sử dụng các cách sau:

1. Chỉ intercept được request đầu tiên (hoặc không được request nào)
2. Tìm string “Trusted”

- Hoặc sử dụng MobSF

(menu trái) Security Analysis tab -> File Analysis.

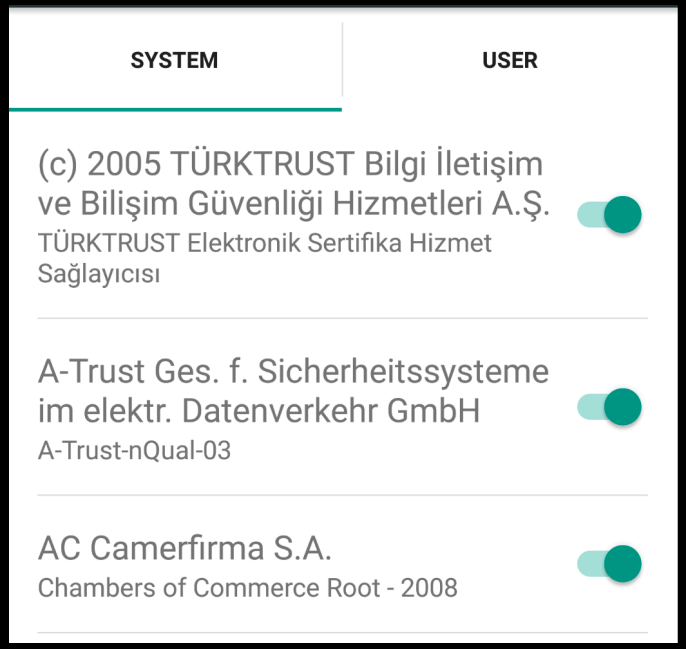
Nếu thấy "Certificate/Key Files Hard-coded inside the App” hoặc chỗ nào có chuỗi “Pinning” => Pinning



Bypass The Pinning

Method 1: Adding a Custom CA to the User Certificate Store

- Mặc định thì các kết nối bảo mật (sử dụng protocols như TLS and HTTPS) từ các app sẽ tin tưởng vào các pre-installed system CAs, và các app trên Android 6.0 (API level 23) trở xuống cũng tin tưởng vào user-added CA

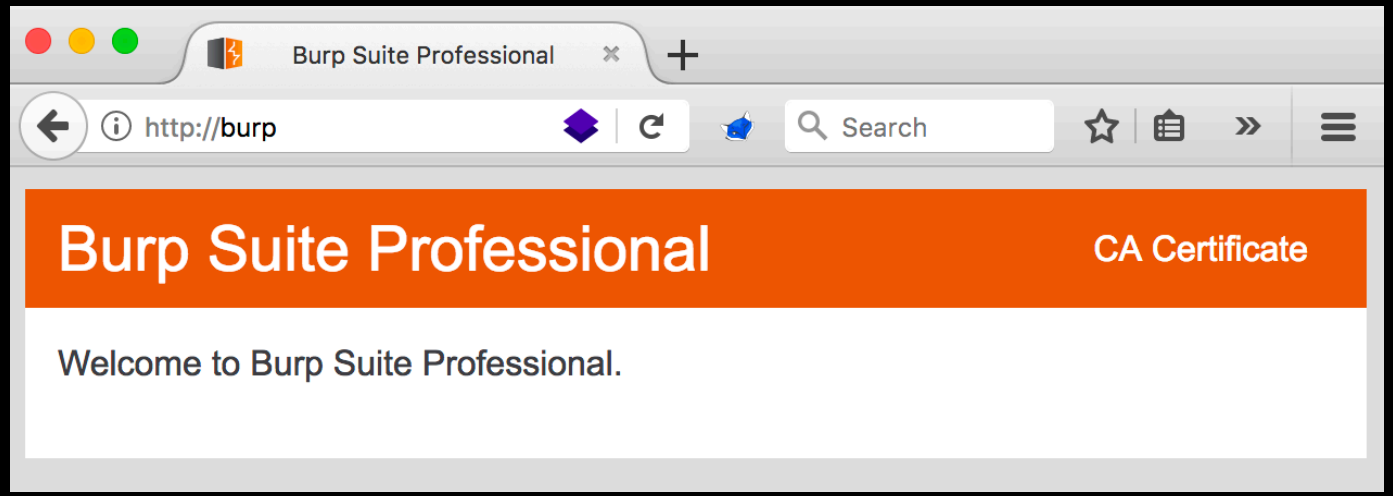


- Nếu chúng ta có 1 cái certificated trusted hợp lệ trong user CA ở máy android 6.0 api level 23- thì sẽ bypass được

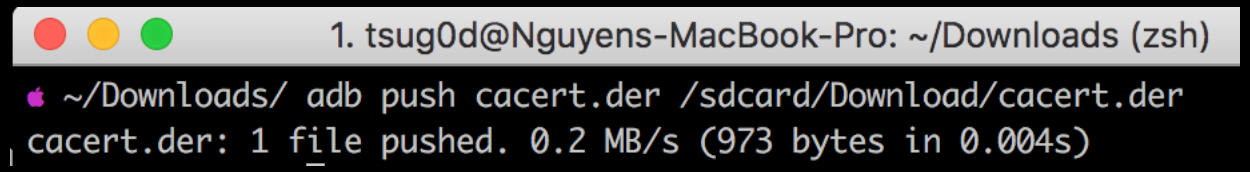
⇒ Let add our custom CA

Bypass The Pinning

- Đầu tiên download burp certificate (set the browser proxy via burp) bằng cách truy cập http://burp



- Rồi push nó lên điện thoại ảo:

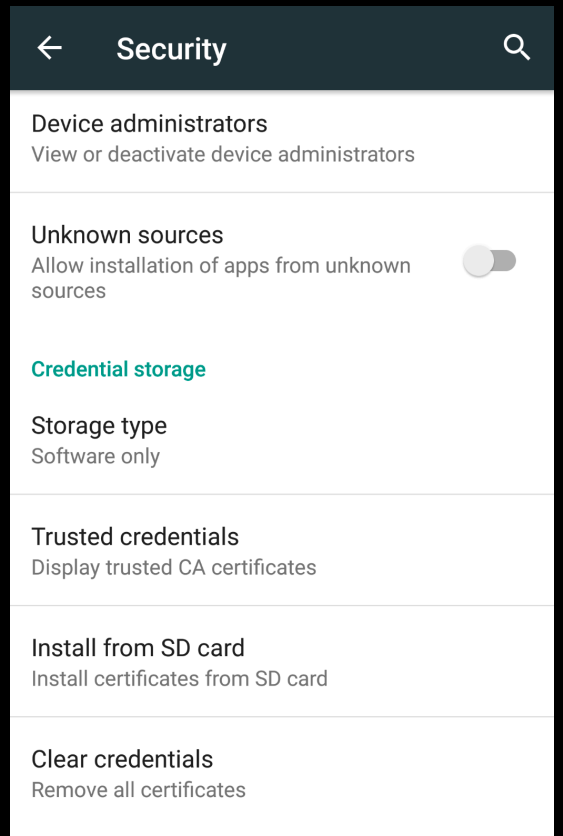


Bypass The Pinning

- Android không hỗ trợ định dạng .der, nên ta đổi nó thành .cer

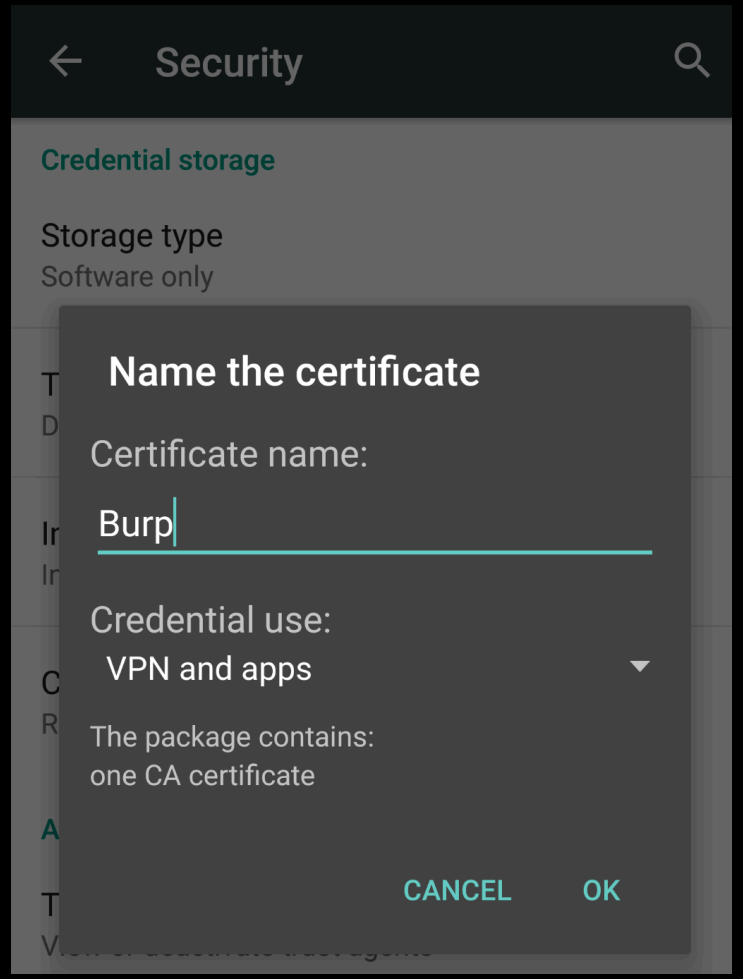
```
1. adb shell (adb)
 ~/Downloads/ adb shell
root@vbox86p:/ # cd sdcard/Download/
root@vbox86p:/sdcard/Download # mv cacert.der cacert.cer
```

- Giờ thì đi đến Settings -> Security -> Install from SD card



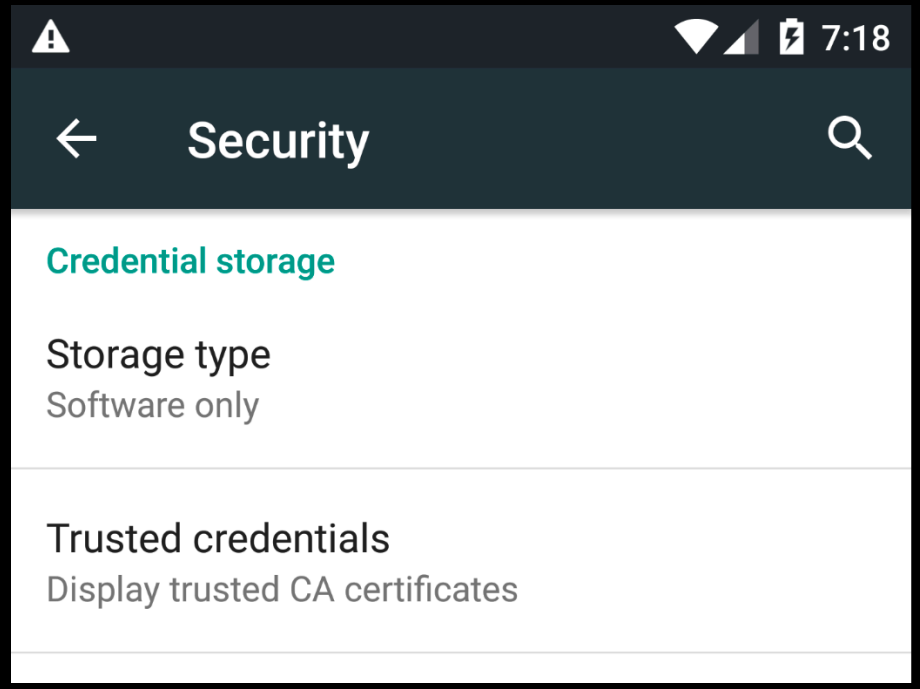
Bypass The Pinning

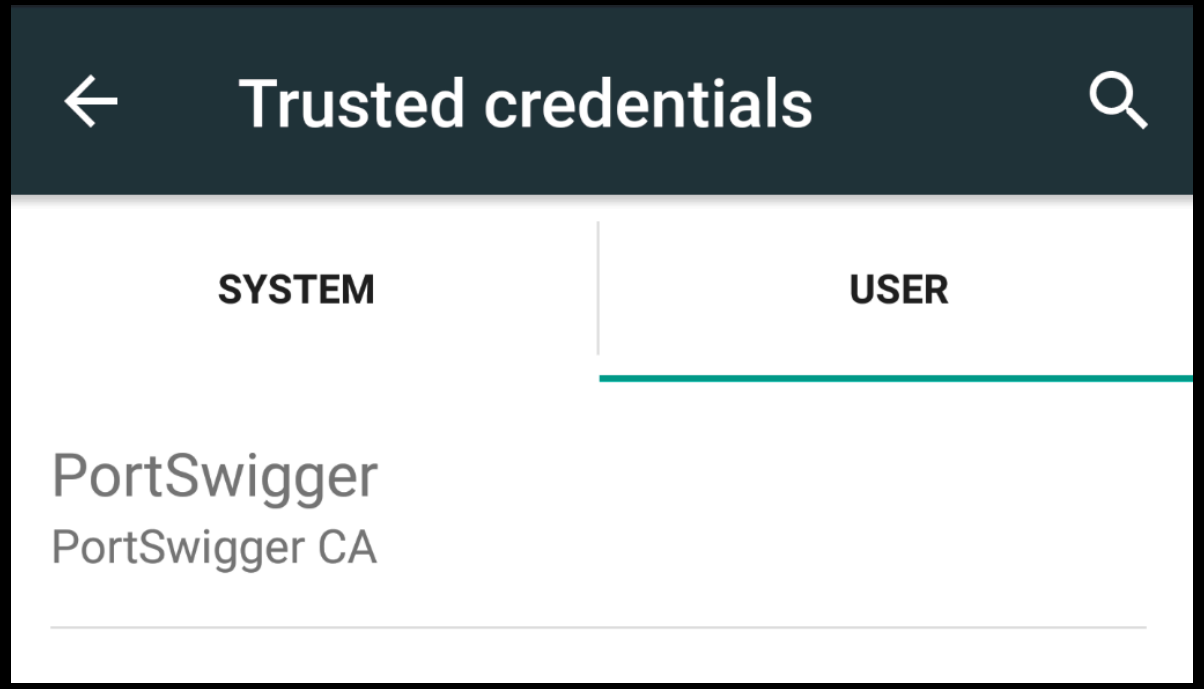
- Trong thư mục /sdcard/Download/, chúng ta thấy cert vừa up lên, click vào nó
- Điền như dưới, click ok



Bypass The Pinning

- Đến Trusted credentials kiểm tra xem cert đã được install chưa





- ssl request được proxied qua burpsuite sử dụng PortSwigger CA, là một valid cert installed, we pass

Bypass The Pinning

- Đôi khi người dev bắt ta sử dụng android 7 để tránh trường hợp trên, thường định nghĩa trong file AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.pinning_app.app"  platformBuildVersionCode="25"
platformBuildVersionName="7.0">
```

- Ta decompile nó sử dụng apktool, đổi thành:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.pinning_app.app"  platformBuildVersionCode="23"
platformBuildVersionName="6.0">
```

- Rồi recompile nó lại, nếu app chỉ check dựa trên valid certificate, kĩ thuật này sẽ giúp chúng ta bypass ssl pinning.

Bypass The Pinning

Method 2: Overwrite Packaged CA Certificate with Custom CA Certificate

- Đôi khi decompile file apk ra sẽ thấy 1 cái custom cert trong đó, có thể app sẽ dùng nó để check

- Ghi đè 'CustomCA.cer' certificate với cert của ta, từ đó làm cho app nghĩ rằng cert của ta hợp lệ

Bypass The Pinning

Method 3: Patch the app

- Decompile file apk, đọc code, tìm đoạn check ssl pinning, patch nó ☺
- Một số case-study thực tế:

1. Bypassing OkHTTP3 Certificate Pinning

https://blog.securityevaluators.com/bypassing-okhttp3-certificate-pinning-c68a872ca9c8

2. Bypassing certificate pinning/hardcoded ssl certificate/certificate pinning

https://www.youtube.com/watch?v=uEndLXB4tfA

3. Facebook Bypassing Certificate Pinning

https://blog.dewhurstsecurity.com/2015/11/10/mobile-security-certificate-pining.html

Bypass The Pinning

Method 4: Hook

- Frida time, nói ở lecture 8 ☺