Projet :

sécurité mobile

Sujet :

Android: Déterminer la prévalence de mis-configuration de la sécurité réseau

NOTRE ÉQUIPE :

Raffass Mouad

Jalal Yassir

Settou Ayoub

But du projet :

Analyser à quelle fréquence des erreurs de configuration de la sécurité réseau se produisent sur des appareils Android. En examinant ces erreurs, nous cherchons à comprendre comment elles peuvent affecter la sécurité des dispositifs Android

Étapes :

Création d’une tool pour extraire les fichiers NSC de l’apk

L’analyse du fichier NSC pour détecter les mis-configurations

NSC ?

La ‘fonctionnalité de Configuration de sécurité’ réseau permet aux applications de personnaliser leurs paramètres de sécurité réseau dans un fichier de configuration déclaratif sans modifier le code de l'application. Ces paramètres peuvent être configurés pour des domaines spécifiques et pour une application particulière. Les principales capacités de cette fonctionnalité sont les suivantes :

- **Custom trust anchors**
- **Debug-only overrides**
- **Cleartext traffic opt-out**
- **Certificate pinning**

Étape 1 :

D’abord on a crée une tool avec le code :

~/Desktop/wtsp/tool.sh - Mousepad

File Edit Search View Document Help

```
1 #!/bin/bash
2 a=$(python3 tool)
3 echo "$a"
4 cat res/$a.xml
5
6
```

~/Desktop/wtsp/tool - Mousepad

File Edit Search View Document Help

```
1 import re
2
3
4 manifest_file_path = "AndroidManifest.xml"
5
6
7 with open(manifest_file_path, 'r', encoding='utf-8') as manifest_file:
8     manifest_content = manifest_file.read()
9
10 match = re.search(r'android:networkSecurityConfig\s*=\s*["\']@(\S+)["\']',
   manifest_content, re.IGNORECASE)
11
12 if match:
13     value_after_equals = match.group(1).strip()
14
15     def a():
16         return value_after_equals
17
18 else:
19     print("Pattern not found or no value after
   'android:networkSecurityConfig=' in the manifest.")
20 print(a())
21
```

Ce code est spécifiquement conçu pour extraire le chemin du fichier de configuration de sécurité réseau (`**networkSecurityConfig**`, abrégé en NSC) d'une application Android (APK). L'attribut `**android:networkSecurityConfig**` dans le fichier AndroidManifest.xml de l'APK pointe vers le fichier de configuration de sécurité réseau associé à cette application.

En extrayant cette information, le code permet d'obtenir dynamiquement le chemin vers le fichier NSC, ce qui peut être utile pour divers scénarios de développement ou d'analyse, tels que la vérification des paramètres de sécurité, la modification dynamique de la configuration, ou toute autre tâche nécessitant l'accès au fichier NSC d'une APK.

Étape 2 :

L’utilisation de notre tool pour l’analyse du fichier nsc sur quelques applications mobile.
Par exemple :


whatsapp


Spotify


Roblox


Secure VPN


SHAREit

Exemple 1 : whatsapp

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd wtsp

┌──(kali㉿kali)-[~/Desktop/wtsp]
└─$ ./tool.sh
xml/APKTOOL_DUMMYVAL_0x7f180006
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

Exemple 2 : Spotify

```
┌──(kali㉿kali)-[~/Desktop/spotify]
└─$ ./tool.sh
xml/network_security_config
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">appspot.com</domain>
        <domain includeSubdomains="true">facebook.com</domain>
        <domain includeSubdomains="true">genius.com</domain>
        <domain includeSubdomains="true">google.com</domain>
        <domain includeSubdomains="true">googleapis.com</domain>
        <domain includeSubdomains="true">instagram.com</domain>
        <domain includeSubdomains="true">qualtrics.com</domain>
        <domain includeSubdomains="true">scdn.co</domain>
        <domain includeSubdomains="true">slack.com</domain>
        <domain includeSubdomains="true">spotify.com</domain>
        <domain includeSubdomains="true">spotify.net</domain>
        <domain includeSubdomains="true">spotifyinternal.com</domain>
        <domain includeSubdomains="true">twitter.com</domain>
    </domain-config>
</network-security-config>
```

Exemple 3 : Roblox

```
┌──(kali㉿kali)-[~/Desktop/roblox]
└─$ ./tool.sh
xml/network_security_config
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config>
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

Exemple 4 : Secure VPN

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd vpnsecure

┌──(kali㉿kali)-[~/Desktop/vpnsecure]
└─$ ./tool.sh
xml/network_security_config
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">127.0.0.1</domain>
    </domain-config>
```

Exemple 5 : SHAREit

```
┌──(kali㉿kali)-[~/Desktop/sharefiles]
└─$ ./tool.sh
xml/o
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">127.0.0.1</domain>
    </domain-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

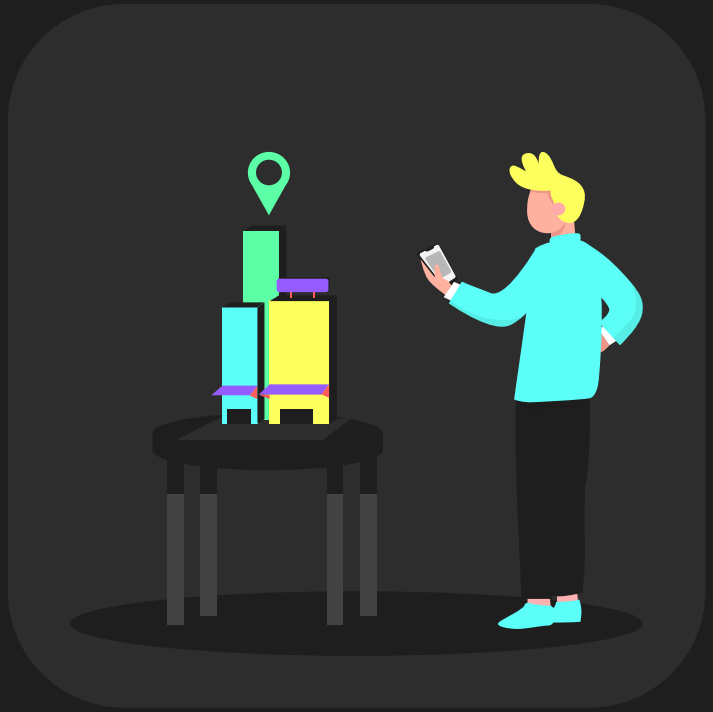
Exemple supplémentaire : Telegram

```
C:\Users\hp\OneDrive\Desktop\apk test>cd telegram

C:\Users\hp\OneDrive\Desktop\apk test\telegram>py tool.py
Pattern not found or no value after 'android:networkSecurityConfig=' in the manifest.
```

Pas de fichier nsc

Un développeur peut choisir de ne pas utiliser de fichier **network_security_config.xml** ou de le configurer de manière à autoriser certaines actions qui pourraient être considérées comme moins sécurisées (par exemple, autoriser le trafic en clair). Cependant, la sécurité globale de l'application dépend de divers facteurs, dont la manière dont elle gère les données, la sécurité des communications réseau, l'utilisation de protocoles sécurisés tels que HTTPS, etc.
En résumé, la présence ou l'absence du fichier **network_security_config.xml** ne fournit qu'une partie de l'image en matière de sécurité. Pour évaluer la sécurité d'une application Android, il est important de prendre en compte l'ensemble de la configuration de sécurité, les bonnes pratiques de développement et d'autres aspects liés à la sécurité.



Fin du presentation

Merci pour votre attention !