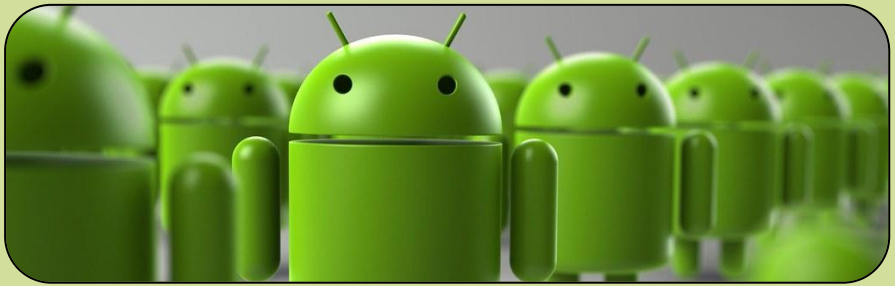
CIS 446 Final Project

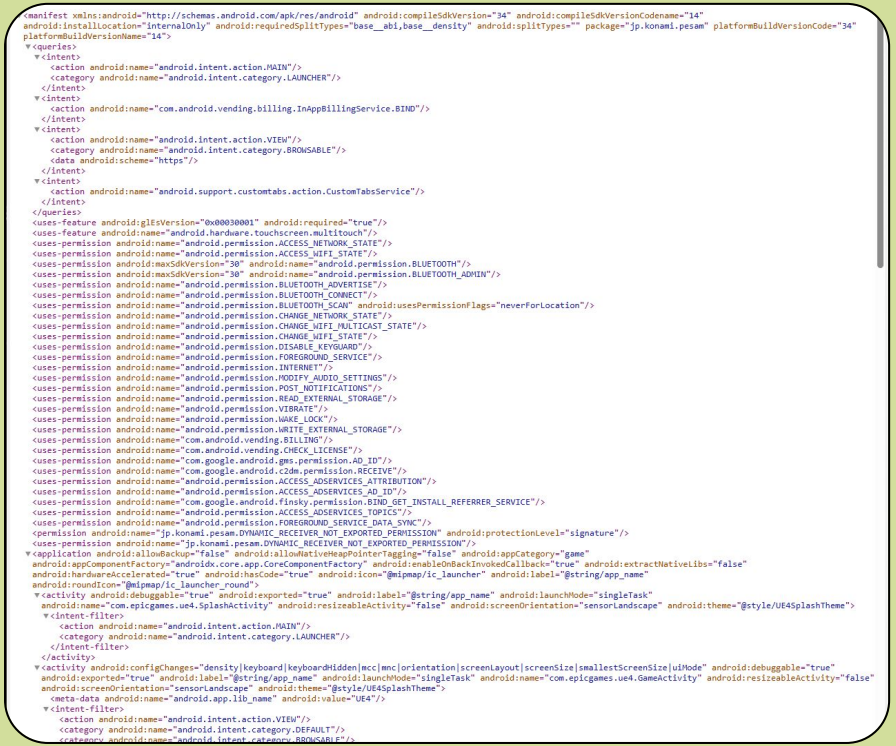
Smartphone App Static Analysis



Michael Luong | Manaswitha Kalapuram | Daisy Sinani

Introduction

SSL/TLS is the de facto standard for secure internet connections.
However, developers have varied knowledge, and many applications are suspected to be flawed in certificate validation.
For CIS 446/546 Final Project, we are instructed to decompile some Android applications and inspect their XML files, to determine whether those apps are configured securely using NSC.



Method

Applications' APK files are downloaded from the chosen source of choice. The file is then decompiled using either an online decompiler, or APKtool. Using static code analysis, we look at the apps' AndroidManifest.xml, and/or network_security_config.xml to determine whether the application utilized NSC.
Each member of the group chose a different category of apps, ensuring a broader coverage, to better understand how and why NSC are utilized.

Apktool

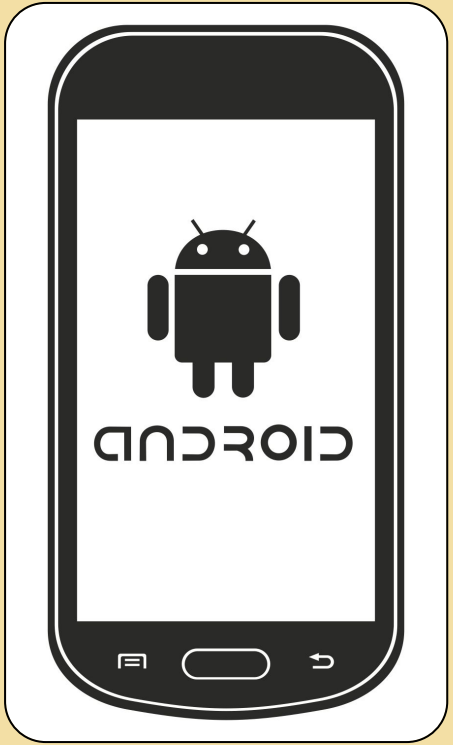
A tool for reverse engineering Android apk files

```
$ apktool d test.apk
I: Using Apktool 2.11.1 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with
I: Loading resource table from file:
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.11.1 on test
I: Checking whether sources has chan
I: Smaling smali folder into classes
I: Checking whether resources has ch
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Terminology

In this project, as we are exploring some concepts about Android's NSC, it is important to understand some key terms used throughout the study. Here are some terms that you may encounter in this presentation:

- NSC: Network Security Configuration, configuration-based approach to increase custom certificate validation logic security and implemented safeguards in Google Play to block insecure applications.
- clearTextTrafficPermitted: flag to set whether the app allows clear text traffic, which is data transmitted without encryption.
- Certificate Pinning: a security mechanism, ensuring that a client only communicates with a trusted server by verifying its digital certificate with a trusted...
- Certificate Authority: a trusted company or organization that acts to validate the identities of entities and issue digital certificates.



Student 1

Michael Luong

Category: Games

App and Decompile Tool information	App #	1	2	3	4	5	6	7	8	9	10
	Download from	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com	apkpure.com
	App Name	Roblox	Among Us	Brawl Stars	Hello Neighbor	PUBG Mobile	eFootball 2025	Subway Surfer	Clash Royale	Clash of Clans	Free Fire
	Version Number	2.665.684	2024.10.29	60.42	2.3.15	3.7.0	9.3.0	3.44.0	100455000	17.126.15	1.109.1
	Target Android Version	Android 6.0+ (M, API 23)	Android 6.0+	Android 7.0+	Android 8.0+ (Oreo, API 26)	Android 5.0+ (Lollipop, API 21)	Android 7.0+ (N, API 24)	Android 6.0+ (M, API 23)	Android 7.0+ (N, API 24)	Android 5.0+ (Lollipop, API 21)	Android 5.1+ (Lollipop MR1, API 22)
	Developer information	Roblox Corporation	Innersloth LLC	Supercell	tinyBuild	Level Infinite	KONAMI	SYBO Games	Supercell	Supercell	Garena International
	No. of reviews	14363	3651	11005	3279	62288	26364	3970	4911	12930	37013
	No. of downloads	60M+	10M+	30M+	6M+	100M+	30M+	20M+	10M+	30M+	100M+
	App permissions	25	5	17	24	38	29	18	18	16	32
	Decompiler tool used	decompiler.com	decompiler.com	decompiler.com	apktool	apktool	apktool	apktool	apktool	apktool	apktool
Analyze Network Security Configuration (NSC)	Adopt NSC or not	Yes	No	Yes	Yes	Yes	No	Yes	No	No	Yes
	Implemented custom NSC setting(s)	Yes	No	Yes	Yes	Yes	No	Yes	No	No	Yes
	Empty NSC file	No	Yes	No	No	No	Yes	No	Yes	Yes	No
	Explicitly declare the cleartextTrafficPermittedFlag	No	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes
	Has Certificate Pinning	No	No	No	No	No	No	No	No	No	No
	CA Configurations	Yes	No	Yes	No	No	No	No	No	No	Yes
	User-Installed Certificates	No	No	No	No	No	No	No	No	No	No
	(Optional) Debug Overrides										

Student 1

Michael Luong

Category: Games

Findings:

- 7/10 games decompiled adopted NSC and utilized custom NSC settings.
- 6/10 games explicitly declare the clearTextTraffic flag explicitly, with all of them allowing the traffic.
- None of the games have certificate pinning.
- 2/10 utilize Certificate Authority configurations.
- None of the games allow user-installed certificates.

Student 2

Daisy Sinani

Category: Bank

	App #	1	2	3	4	5	6	7	8	9	10
App and Decompile Tool information	Download from	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure
	App Name	PayPal	KBZPay	Airtel Thanks: Recharge & Ba	WavePay	Easypaisa	BitMart	Google Wallet	Google Pay: Save and Pay	Qi Services	Touch 'n Go eWallet
	Version Number	8.80.0	5.8.1	4.114.2	2.4.0	2.9.84	3.2.10	25.12.740385114	272.1.2	5.4.29	1.8.5.1.2
	Target Android Version	Android 6.0+ API 34	Android 8.0+ API 26	Android 6.0+ (M, API 23)	Android 5.0+ API 2	Android 6.0+ (M, API 23)	Android 6.0+ (API 23)	Android 9.0+ API 28	Android 6.0+ API (M, API	Android 5.0+ API 21	Android 5.0+ API 21
	Developer information	PayPal Mobile	KBZ Bank	Airtel	Wave Money	Telenor Microfiance Bank Limi	GBM Foundation Compar	Google LLC	Google LLC	THE INTERNATIO NAL SMART CARD CO LLC	TNG Digital Sdn Bhd
	No. of reviews	563	39	52	44	42	1	195	17	30	8
	No. of downloads	6M+	500k+	300K+	600K+	1M+	20K+	3M+	500K+	200K+	200K+
	App permissions	38	48	58	30	34	33	32	28	25	49
	Decompiler tool used	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler	Online Decompiler
Analyze Network Security Configuration (NSC)	Adopt NSC or not	Yes, <network-security-config>	No, but has android:usesClea tTraffic="true"	Yes, <network-security-confic android:networkSecurityConfi @xml/network_security_confi	No	No	Yes, android:network SecurityConfig ="@xml/network_securit y_config"	No, but has android :usesCleartextTraffi c="false"	Yes, android:networkSecu Config ="@xml/gpay_app network_security_config"	No, but has android:usesClear textTraffic="true"	Yes, android:networkSecurity Config="@xml/network_ security_config_prod"
	Implemented custom NSC setting(s)	Yes, <base-config>, <domain-config>, <pin-set>,	No	Yes, <base-config>, <debug -overrides>, <trust-anchors>	No	No	Yes, has android:network SecurityConfig	No	Yes, has android:network SecurityConfig	No	Yes, <base-config> , <trust-anchors>, <certificates>, <debug-overrides>
	Empty NSC file	No	Yes	No	Yes	Yes	No	Yes	No	Yes	No
	Explicitly declare the cleartextTrafficPermitte dFlag	Yes, cleartextTraffic Permitted ="false"	Yes, android:usesCleartextTra ="true"	Yes, cleartextTraffic Permitted "true"	No	No	Yes, android:usesCleartex Traffic="false"	Yes, android:usesCleartextTra ="false"	Yes, android:usesCleartex Traffic="false"	Yes, android:uses CleartextTraffic ="true"	Yes, cleartextTrafficPermitted ="false"
	Has Certificate Pinning	a) Yes b) For www.paypalobjects.com: Pin 1: r/mlkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5 Pin 2: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY Pin 3: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PI Pin 4: Wd8xe/qfTwq3ylFNd3lpaqLHZbh2ZNCLluVzmeNI Pin 5: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8F Pin 6: InsM2T/O9/JB4sJFdnrpsFp3awZJ+ZZbYpCWhGloa For paypal.com: Pin 1: r/mlkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5 Pin 2: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY Pin 3: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PI Pin 4: Wd8xe/qfTwq3ylFNd3lpaqLHZbh2ZNCLluVzmeNI Pin 5: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8F Pin 6: InsM2T/O9/JB4sJFdnrpsFp3awZJ+ZZbYpCWhGloa For www.paypal.me: Pin 1: r/mlkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5 Pin 2: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY Pin 3: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PI s		No	No	No	No	No	No	No	No
	CA Configurations	No	No	Yes, <trust-anchors> <certificates src="us </trust-anchors>	No	No	No	No	No	No	Yes, <certificates overridePins="true" src="system"/> <certificates overridePins="true"
	User-Installed Certificates	No	No	Yes, <certificates src="user"/>	No	No	No	No	No	No	No
	(Optional) Debug										

Student 2

Daisy Sinani

Category: Bank

Findings:

- Apps range from Android version 5.0 all the way up to Android 9.0
- 5/10 of apps adopted NSC and used custom NSC settings
- 8/10 of apps explicitly declared the cleartext Traffic Permitted Flag with half of them set to false
- 1/10 of apps has certificate pinning
- 2/10 of apps has certificate authority configurations
- 1/10 of apps has user-installed certificates

Student 2

Daisy Sinani

Category: Bank

Feature	PayPal	KBZ Pay
Developer	Global	Regional
Downloads	6 million+	500K+
Permissions	38	48
Certificate Pinning	Yes	No
Encrypted Data	HTTPS	HTTP

Student 3

Manaswitha Kalapuram

Category: Social

		1	2	3	4	5	6	7
App and Decompile Tool information	App #	1	2	3	4	5	6	7
	Download from	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure
	App Name	Instagram	Chamet - Live Video Chat	Threads	X	OmeTV – Video Chat Al	Sinterest	Lynck
	Version Number	373.0.0.43.67	4.2.0	375.0.0.1.107	10.87.0-release.0	605095	1.2	1.4.6
	Target Android Version	Android 9.0+ Android OS	Android 5.0+ (Lollipop, API 21)	Android 9.0+ (P, API 28)	Android 8.0+ (Oreo, API 26)	Android 5.0+ (Lollipop,	Android 5.0+ (Lollipop, Al	Android 6.0+ (M,
	Developer information	Tammy Palma	Piero Lopez Condori	Instagram	X Corp.	Eduard Mogda	Tim Strobel	Tyav Simon
	No. of reviews	11K	50	98	2.9K	258	0	0
	No. of downloads	100M+	900K+	1M+	30M+	5M+	1K+	1K+
	App permissions	70	40	44	63	19	19	41
	Decompiler tool used					https://www.decompiler.com/		
Analyze Network Security Configuration (NSC)	Adopt NSC or not	Yes android:networkSecurityConfig="@xml/fb_	Yes android:networkSecurityConfig="@xm	Yes android:networkSecurityConfig="@xml/fb_net	No, Not Found	Yes android:networkSecu	No, Not Found	No, Not Found
	Implemented custom NSC setting(s)	Yes <network-security-config> <base-config cleartextTrafficPermitted="true"> <trust-anchors> <certificates src="system"/> <certificates overridePins="true" src="user"/> </trust-anchors> </base-config>	Yes <network-security-config> <domain-config cleartextTrafficPermitted=" ... </domain-config>	Yes <network-security-config> <base-config cleartextTrafficPermitted="true"> <trust-anchors> <certificates src="system"/> <certificates overridePins="true" src="user"/> </trust-anchors> </base-config>	No, Not Found	Yes <base-config> <trust-anchors> <certificates src="@raw/ <certificates src="@raw/ <certificates src="@raw/ <certificates src="@raw/ <certificates src="@raw/ <certificates src="system	No, Not Found	No, Not Found
	Empty NSC file	No	No	No	Yes	No	Yes	Yes
	Explicitly declare the cleartextTrafficPermittedFlag	Yes <base-config cleartextTrafficPermitted="tr	Yes <domain-config cleartextTrafficPermitt	Yes <domain-config cleartextTrafficPermitted="fal <base-config cleartextTrafficPermitted="true">	No, Not Found	No explicit declaration	Yes, found in AndroidMan	No, Not Found
	Has Certificate Pinning	Yes <pin-set expiration="2026-03-31"> <pin digest="SHA-256">x4QzPSC810K5/cMjb <pin digest="SHA-256">ICGRfpgmOUXIWcC <pin digest="SHA-256">grX4Ta9HpZx6tSHkn <pin digest="SHA-256">58qRu/uxh4gFezqAcI <pin digest="SHA-256">r/mIkG3eEpVdm+u/k <pin digest="SHA-256">i7WTqTvh0OioIruIfF <pin digest="SHA-256">uUwZgwDOxcBXrQc <pin digest="SHA-256">WoiWRyIOVNa9ihaB <pin digest="SHA-256">Wd8xe/qfTwq3ylFNd <pin digest="SHA-256">ape1HIIZ6T5d7GS61 <pin digest="SHA-256">oC+voZLIy4HLE0FV <pin digest="SHA-256">K87oWBWM9UZfyd <pin digest="SHA-256">cGuxAXyFXFkWm6 <pin digest="SHA-256">aCdH+LpiG4fN07wp <pin digest="SHA-256">rn+WLLnmp9v3uDP <pin digest="SHA-256">C5+lpZ7tcVwmwQIN <pin digest="SHA-256">diGVwiVYbubAI3RW <pin digest="SHA-256">o4PO2G2cbkZhZ82+	No, Not Found	Yes <pin-set expiration="2026-04-02"> <pin digest="SHA-256">x4QzPSC810K5/cMjb05C <pin digest="SHA-256">ICGRfpgmOUXIWcQ/H <pin digest="SHA-256">grX4Ta9HpZx6tSHkmCr <pin digest="SHA-256">58qRu/uxh4gFezqAcERu <pin digest="SHA-256">r/mIkG3eEpVdm+u/ko/cv <pin digest="SHA-256">i7WTqTvh0OioIruIfFR4k <pin digest="SHA-256">uUwZgwDOxcBXrQcntw <pin digest="SHA-256">WoiWRyIOVNa9ihaBciR <pin digest="SHA-256">Wd8xe/qfTwq3ylFNd3Ip <pin digest="SHA-256">ape1HIIZ6T5d7GS61YB <pin digest="SHA-256">oC+voZLIy4HLE0FVT5v <pin digest="SHA-256">K87oWBWM9UZfyddvD <pin digest="SHA-256">cGuxAXyFXFkWm61cF <pin digest="SHA-256">aCdH+LpiG4fN07wpXtX <pin digest="SHA-256">rn+WLLnmp9v3uDP7GP <pin digest="SHA-256">C5+lpZ7tcVwmwQIMcR <pin digest="SHA-256">diGVwiVYbubAI3RW4h <pin digest="SHA-256">o4PO2G2cbkZhZ82+Jem	No, Not Found	No, Not found	No	No, Not Found
	CA Configurations	Yes <trust-anchors> <certificates src="system"/> <certificates overridePins="true" src="user"/> </trust-anchors>	Yes <trust-anchors> <certificates src="system"/> </trust-anchors> <trust-anchors> <certificates src="system"/>	Yes <trust-anchors> <certificates src="system"/> <certificates overridePins="true" src="user"/> </trust-anchors>	No, Not Found	Yes <certificates src="sy	No	No, Not Found
	User-Installed Certificates	No <certificates src="system"/>	Yes	Yes <certificates src="system"/> <certificates overridePins="true" src="user"/>	No, Not Found	No	No	No, Not Found
	(Optional) Debug Overrides	No, Not Found	Yes <debug-overrides> <trust-anchors> <certificates src="user"/> <certificates src="system"/> </trust-anchors>	No	No, Not Found	No	No	No, Not Found

		8	9	10	11	12	13	14	15
App and Decompile Tool information	App #	8	9	10	11	12	13	14	15
	Download from	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure	APK Pure
	App Name	네이버 카페 - Nave	TikTok	HiFun聊天 - 聊天	Facebook Lite	TikTok Lite - Sa	Facebook	Grindr - Gay Dati	WhatsApp Messenger
	Version Number	25.0331.0	39.2.1	1.15.0	455.0.0.0.4	38.6.1	507.0.0.66.49	25.5.0	2.25.9.79
	Target Android Version	Android 9.0+ (P, AP	Android 5.0+ (Loll	Android 7.0+ (N,	Android 8.0+ (Oreo, A	Android 5.0+ (L	Android 11.0+ (F	Android 8.0+ (Or	Android 5.0+ (Lollipop, API 2
	Developer information	Claudio Pereira	Runcan Vlad	คนโสด จำ	Meta Platforms, Inc.	Hamode Xb	Nay Lin Thu Ya	Grindr LLC	Google Play
	No. of reviews	3	8.8K	0	2K	300	14K	167	5.4K
	No. of downloads	40K+	70M+	1K+	30M+	7M+	100M+	2M+	100M+
	App permissions	50	51	31	64	63	90	34	81
	Decompiler tool used								
Analyze Network Security Configuration (NSC)	Adopt NSC or not	Yes android:network	Yes android:netwo	Yes android:netw	Yes android:networkSe	Yes android:netw	Yes android:netw	Yes android:netw	Yes android:networkSecurityC
	Implemented custom NSC setting(s)	Yes <network-secur <base-config clearte <trust-anchors> <certificates src="sy </trust-anchors> </base-config>	Yes <network-secu <base-config cleart <trust-anchors> <certificates overri </trust-anchors> </base-config>	Yes <base-config	Yes <network-security <base-config cleartext <trust-anchors> <certificates src="syst <certificates overrideP </trust-anchors> </base-config>	Yes <network-se <base-config cle <trust-anchors> <certificates ove </trust-anchors> </base-config>	Yes <network-se <base-config cle <trust-anchors> <certificates src= <certificates ove </trust-anchors> </base-config>	No	Yes <network-security-config> <base-config cleartextTrafficPe </network-security-config>
	Empty NSC file	No	No	No	No	No	No	Yes <network-sec	No
	Explicitly declare the cleartextTrafficPermittedFlag	Yes <base-config cl	Yes <base-config c	Yes <base-config	Yes <domain-config cl	Yes <base-confi	Yes, it is declare	Yes, found in And	Yes <base-config cleartextTraf
	Has Certificate Pinning	No	No, Not Found	No, Not Found	Yes <pin-set expiration <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25 <pin digest="SHA-25	No, Not Found	Yes <pin-set exp <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH <pin digest="SH	No	No, Not Found
	CA Configurations	Yes <trust-anchors> <certificates src="sy </trust-anchors> <tr <certificates src="us	Yes <certificates o	Yes <trust-anchor <certificates src=" <certificates src=" </trust-anchors>	Yes <certificates src=" <certificates overrideP	Yes <trust-ancho <certificates ove </trust-anchors>	Yes <certificates <certificates ove	No	No, Not Found
	User-Installed Certificates	Yes <trust-anchors> <certificates src="us </trust-anchors>	No	Yes <trust-anchor <certificates src=" <certificates src=" </trust-anchors>	No <trust-anchors> <certificates src="syst <certificates overrideP </trust-anchors>	Yes <trust-ancho <certificates src= </trust-anchors>	No	No	No, Not Found
	(Optional) Debug Overrides	Yes <debug-overrid <trust-anchors> <certificates src="us </trust-anchors> </debug-overrides>	Yes <debug-overri <trust-anchors> <certificates src="u </trust-anchors> </debug-overrides>	Yes <debug-overr <trust-anchors> <certificates src=" <certificates src=" </trust-anchors>	No, Not found	Yes <debug-ove <trust-anchors> <certificates src= </trust-anchors> </debug-overrid	No, Not Found	No	No

Student 3

Manaswitha Kalapuram

Category: Social

List of APK apps

- Instagram
- Chamet - Live Video Chat
- Threads
- X
- OmeTV – Video Chat Alternative
- Sinterest
- Lynck
- 네이버 카페 - Naver Cafe
- TikTok
- HiFun嗨翻 - 聊天交友約會語音軟體App
- Facebook Lite
- TikTok Lite - Save Data & Fast
- Facebook
- Grindr - Gay Dating & Chat
- WhatsApp Messenger

Student 3

Manaswitha Kalapuram

Category: Social

Findings:

- App versions range from Android 5.0 to Android 11.0.
- 12/15 apps use Network Security Configuration (NSC), and most of them include custom NSC settings.
- 12/15 apps clearly declare the cleartextTrafficPermitted flag.
- 5/15 apps have implemented certificate pinning.
- 11/15 apps define certificate authority (CA) configurations.
- 8/15 apps support user-installed certificates..

Challenges

Online Decompiler Limitation

For some APKs on the heavier side, most of the time, the file won't be uploaded correctly, which leads to the online decompiler not working correctly. The APK file doesn't get decompiled in its entirety, which leads to missing AndroidManifest.xml file and/or directories.

Malicious APK files

Some APKs downloaded from online sources tripped off the Windows Security alarm, which means that the files might edited for malicious purposes and intentions.

Results Across Diff. App Categories

- Social apps show the highest adoption of NSC, followed by Games, and then Bank apps
    - Strong commitment to securing network traffic, which is crucial for apps handing user data and communication
- Social apps had 11/15 CA configurations, meanwhile Banks and Game apps had 2/10
    - High prevalence of CA configurations suggests that these apps are more diligent in verifying the legitimacy of servers they communicate with, which is important for because social apps handle sensitive personal info

Results Across Diff. App Categories

- Game apps had lowest number of not explicitly mentioning cleartext traffic (Game apps 0/10) (Social apps 2/15) (Bank apps 5/10)
    - Games are the least cautious when it comes to cleartext traffic. Unencrypted traffic is a major security risk. ‘
    - Indicates games prioritize user experience or performance over security

Results Across Diff. App Categories

- Bank apps are most restrictive when it comes to cleartext traffic with half of the apps not permitting it
- Bank apps are still relatively weak in adopting certificate pinning (1/10)
- Only 2/10 bank apps have CA configurations, suggesting that banks might not be doing enough to establish a trust model with their servers