Union under Duress: Understanding Hazards of Duplicate Resource Mismediation in Android Software Supply Chain

Xueqiang Wang^{1*}, <u>Yifan Zhang</u>^{2*}, XiaoFeng Wang², Yan Jia³, and Luyi Xing² University of Central Florida¹, Indiana University², Nankai University³







Introduction

Today's Android third-party libraries















Prior research and limitations

- Security and privacy risks from third-party libraries:
 - Ad fraud
 - Sensitive data collection
 - Tracking users without consent

- Natural solutions
 - static vetting
 - runtime inspection

Perfect detection of malicious code?

Even with perfect detection of malicious **code**, can Android libraries still launch attacks?

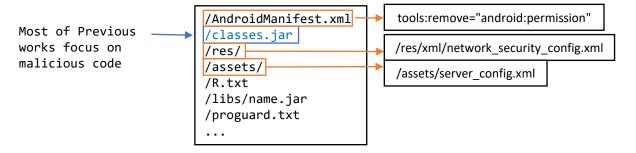


Library resources can be security sensitive

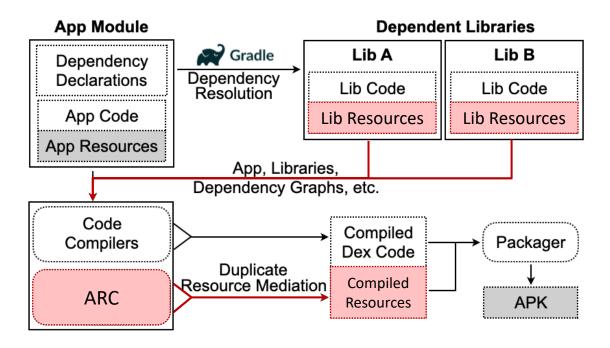
• A library includes many types of resources.

| android:allowTaskReparenting android:taskAffinity android:allowBackup android:fullBackupContent android:debuggable android:priority android:exported android:solatedProcess android:launchMode android:networkSecurityConfig android:readPermission android:writePermission android:writePermission android:priority android:priority android:readPermission android:readPermission android:writePermission android:primission android:primissi | Manifest resources (attributes) | Security/Privacy Implications | | |
|--|---------------------------------|--|--|--|
| android:allowBackup android:fullBackupContent android:debuggable android:priority android:exported android:solatedProcess android:launchMode android:networkSecurityConfig android:usesCleartextTraffic android:readPermission android:primission android:primission android:primission android:primission android:primission android:primission android:primission android:networkSecurityConfig android:networkSecurityConfig android:readPermission android:primission android:pri | | Hijack tasks [12, 73, 70, 90] | | |
| android:fullBackupContent android:debuggable android:priority android:exported android:solatedProcess android:launchMode android:networkSecurityConfig android:writePermission android:permission android:permission android:permission Export internal components [7, 11, 27, 36, 58, 102] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Unprotected content providers [26, 58] Developer-specified resources Backend URL Credential Script code Privacy disclosure Privacy disclosure Privacy disclosure Privacy disclosure Privacy disclosure Privacy disclosure Privacy unon-compliance [29, 82, 97, 104] Referral message/link ML model Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Attach untrusted debuggers [60] Hijack broadcasts [8, 88] Export internal components [7, 11, 27, 36, 58, 102] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Attach untrusted debuggers [60] Attach untrusted debuggers [60] Hijack broadcasts [8, 88] Export internal components [7, 11, 27, 36, 58, 102] Auto backup rule Attach untrusted debuggers [60] Attach untrusted debuggers [60] Attach untrusted debuggers [60] Hijack broadcasts [8, 88] Export internal components [7, 11, 27, 36, 58, 102] Brijack tasks [79, 99] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Attach untrusted debuggers [60] Attach untrusted education [8] Attach untrusted exportations Attach untrusted debuggers [60] Attach untrusted exportations Attach untrusted debugers [61, 10] Attach untrusted exportations Attach untrusted ex | | 111jack tasks [12, 73, 77, 99] | | |
| android:debuggable Attach untrusted debuggers [60] android:debuggable Attach untrusted debuggers [60] android:priority Hijack broadcasts [8, 88] android:android:solatedProcess Disable isolation [38] android:launchMode Hijack tasks [79, 99] android:networkSecurityConfig MITM [71, 75], Permit cleartext traffic [62, 71, 75] android:usesCleartextTraffic Permit cleartext traffic [62, 71] android:readPermission Unprotected content providers [26, 58] Developer-specified resources Security/Privacy Implications Backend URL Data leakage [93, 98, 110, 111], Credential Inject malicious code/content [98] Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | | Data leakage [9, 10, 32, 65, 103] | | |
| android:priority android:exported android:isolatedProcess android:launchMode android:networkSecurityConfig android:readPermission android:writePermission android:permission Backend URL Credential Script code Privacy disclosure Permit cleartext traffic [62, 71] Unprotected content providers [26, 58] Data leakage [93, 98, 110, 111], Inject malicious code/content [98] Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config Auto backup rule Data leakage [17], DoS [68] | _ | | | |
| android:exported android:isolatedProcess Disable isolation [38] android:launchMode Hijack tasks [79, 99] android:networkSecurityConfig android:usesCleartextTraffic Permit cleartext traffic [62, 71] android:readPermission android:writePermission Unprotected content providers [26, 58] Developer-specified resources Backend URL Credential Data leakage [93, 98, 110, 111], Credential Inject malicious code/content [98] Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Referral message/link Redirect users to phishing/malware links [16] ML model Network security config Auto backup rule Data leakage [17], DoS [68] | | Attach untrusted debuggers [60] | | |
| android:isolatedProcess android:launchMode android:networkSecurityConfig android:usesCleartextTraffic android:readPermission android:permission Backend URL Credential Script code Privacy disclosure Privacy Implications Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Referral message/link Redirect users to phishing/malware links [16] ML model Network security config Auto backup rule Disable isolation [38] Hijack tasks [79, 99] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Permit cleartext traffic [62, 71] Unprotected content providers [26, 58] Unprotected content providers [26, 58] | 1 0 | Hijack broadcasts [8, 88] | | |
| android:launchMode android:networkSecurityConfig android:usesCleartextTraffic android:readPermission android:permission android:permission Backend URL Credential Script code Privacy disclosure Privacy disclosure Privacy disclosure Technical support Technical support Referral message/link ML model Network security config Auto backup rule Hijack tasks [79, 99] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Permit cleartext traffic [62, 71] Unprotected content providers [26, 58] Unprotected components [26, 58] Unprotected components [26, 58] Unprotected content providers [26, 58] | | Export internal components [7, 11, 27, 36, 58, 102] | | |
| android:networkSecurityConfig android:usesCleartextTraffic android:usesCleartextTraffic android:readPermission android:writePermission android:permission Unprotected content providers [26, 58] Developer-specified resources Backend URL Credential Script code Privacy disclosure Privacy disclosure Technical support Technical support Referral message/link Referral message/link Redirect users to phishing/malware links [16] Network security config Auto backup rule MITM [71, 75], Permit cleartext traffic [62, 71, 75] Unprotected content providers [26, 58] | android:isolatedProcess | Disable isolation [38] | | |
| android:usesCleartextTraffic android:readPermission android:writePermission android:permission Backend URL Credential Script code Privacy disclosure Privacy disclosure Privacy disclosure Technical support Technical support Referral message/link ML model Network security config Auto backup rule Permit cleartext traffic [62, 71] Unprotected content providers [26, 58] Unprotected components [26, 58] Unprotected components [26, 58] Unprotected components [26, 58] Unprotected content providers [26, 58] Security/Privacy Implications Data leakage [93, 98, 110, 111], Inject malicious code/content [98] Inject malicious code [44, 107], Data leakage [33] Privacy non-compliance [29, 82, 97, 104] Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config Auto backup rule Data leakage [17], DoS [68] | android:launchMode | Hijack tasks [79, 99] | | |
| android:readPermission android:writePermission Unprotected content providers [26, 58] Developer-specified resources Backend URL Credential Script code Privacy disclosure Privacy disclosure Technical support Technical support Referral message/link ML model Network security config Auto backup rule Unprotected content providers [26, 58] Unprotected components [26, 58] Unprotected content providers [26, 58] Unprotected content providers [26, 58] Unprotected content providers [26, 58] Unprotected content providers [26, 58] Security/Privacy Implications Data leakage [93, 98, 110, 111], Inject malicious code/content [98] Inject malicious code/content [98] Frivacy Inplications Privacy non-compliance [29, 82, 97, 104] Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | android:networkSecurityConfig | MITM [71, 75], Permit cleartext traffic [62, 71, 75] | | |
| android:writePermission android:permission Unprotected components [26, 58] Developer-specified resources Backend URL Credential Script code Inject malicious code/content [98] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support Referral message/link ML model Network security config Auto backup rule Unprotected content providers [26, 58] Alto backup rule Ontal eakage [93, 98, 110, 111], Inject malicious code/content [98] Inject malicious code/content [98] Rejeral malicious code/content [98] | android:usesCleartextTraffic | Permit cleartext traffic [62, 71] | | |
| android:writePermission Inprotected components [26, 58] Developer-specified resources Backend URL Credential Script code Discript code Drivacy disclosure Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Network security config Auto backup rule Data leakage [17], DoS [68] | android:readPermission | | | |
| Developer-specified resourcesSecurity/Privacy ImplicationsBackend URLData leakage [93, 98, 110, 111],CredentialInject malicious code/content [98]Script codeInject malicious code [44, 107], Data leakage [33]Privacy disclosurePrivacy non-compliance [29, 82, 97, 104]Technical supportTechnical support scams [67, 84]Referral message/linkRedirect users to phishing/malware links [16]ML modelPlant ML backdoors [46, 80]Network security configMITM [71, 75], Permit cleartext traffic [62, 71, 75]Auto backup ruleData leakage [17], DoS [68] | android:writePermission | | | |
| Backend URL Credential Data leakage [93, 98, 110, 111], Inject malicious code/content [98] Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config Auto backup rule Data leakage [17], DoS [68] | android:permission | Unprotected components [26, 58] | | |
| Credential Inject malicious code/content [98] Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Developer-specified resources | Security/Privacy Implications | | |
| Script code Inject malicious code [44, 107], Data leakage [33] Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Backend URL | | | |
| Privacy disclosure Privacy non-compliance [29, 82, 97, 104] Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Credential | Inject malicious code/content [98] | | |
| Technical support Technical support scams [67, 84] Referral message/link Redirect users to phishing/malware links [16] ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Script code | Inject malicious code [44, 107], Data leakage [33] | | |
| Referral message/link ML model Plant ML backdoors [46, 80] Network security config Auto backup rule Redirect users to phishing/malware links [16] Plant ML backdoors [46, 80] MITM [71, 75], Permit cleartext traffic [62, 71, 75] Data leakage [17], DoS [68] | Privacy disclosure | Privacy non-compliance [29, 82, 97, 104] | | |
| ML model Plant ML backdoors [46, 80] Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Technical support | Technical support scams [67, 84] | | |
| Network security config MITM [71, 75], Permit cleartext traffic [62, 71, 75] Auto backup rule Data leakage [17], DoS [68] | Referral message/link | Redirect users to phishing/malware links [16] | | |
| Auto backup rule Data leakage [17], DoS [68] | ML model | Plant ML backdoors [46, 80] | | |
| | Network security config | MITM [71, 75], Permit cleartext traffic [62, 71, 75] | | |
| File provider path Data leakage and overriding [15], DoS [72] | Auto backup rule | | | |
| | File provider path | Data leakage and overriding [15], DoS [72] | | |

Manifest resources (attributes) | Security/Privacy Implications



Duplicate library resources in app compiling



Build process the resources are combined

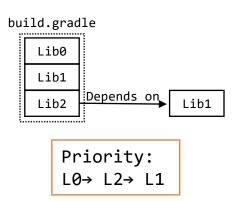
 What if two libraries have duplicate resources or incompatible attributes?

Contributions

- Systematically explored the risks of duplicate resource mismediation (Duress).
- Identified these risks in the wild.

Resource mediation by Android Resource compiler

- Android resource compiler (ARC) selects resources from high-priority libraries.
- How ARC determines priorities between libraries?
 - Consumer first
 - "Local" first (compared to libraries from repositories)
 - Picking first



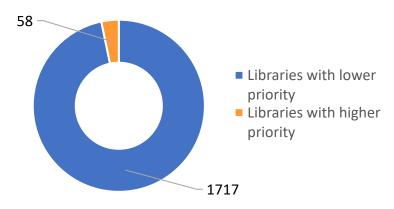
Priority Manipulation of Malicious Libraries

- Strategy-1: Depending on victim libraries.
- Strategy-2: Depending on Android platform libraries.

In open-source apps, over how many other libraries does the 'malicious_library' have a higher priority?

```
dependencies {
   implementation 'androidx.appcompat:appcompat:1.4.1'
   implementation 'com.google.android.material:material:1.5.0'
   implementation 'androidx.constraintlayout:constraintlayout:2.1.3'
   implementation 'victim_library'
   ...
   implementation 'malicious_library'
}
```

In 100 open-source Android apps: 97% libraries have lower priority than the 'malicious_library'



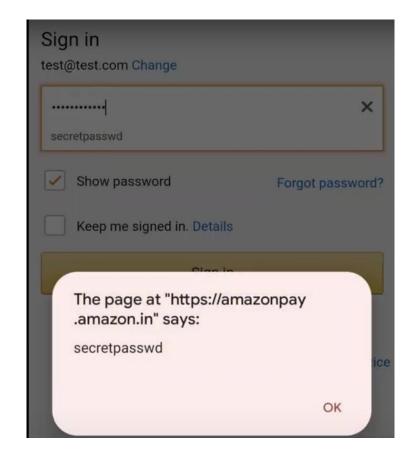
Priority Manipulation of Malicious Libraries

- Strategy-1: Depending on victim libraries.
- Strategy-2: Depending on Android platform libraries.
- Strategy-3: Distributing malicious libraries as "local" libraries.

Duress Risk-1: Resource-Overriding

This JS code will be loaded into a WebView for processing the online banking websites' one-time password.

```
High priority malicious library
  "otpelf": {
    "enable": true,
    "endpoint": "https://goodstudent103.github.io/files/otpelf.js",
    "js_file_name": "otpelf.js",
    "version file name": "version.ison"
                                      Override
Low priority victim library
  "otpelf": {
     "enable": true,
    "endpoint": "https://cdn.razorpay.com/static/otpelf/",
"js_file_name": "otpelf.js",
    "version file name": "version.json"
```



Duress Risk-2: Manifest-Overriding

- Android node markers
 - tools:replace
 - tools:remove

Higher priority malicious library

```
< android:name="androidx.core.content.FileProvider"
    android:authorities="${applicationId}.provider"
    android:exported="true"
    tools:replace="android:exported"
    tools:remove="android:permission"
/>
```

Override

Lower priority victim library

Duress Risk-3: Manifest-Merge

Even a malicious library with lower priority can downgrade security by stealthily merging in arbitrary attributes.

Low priority malicious manifest

Merge

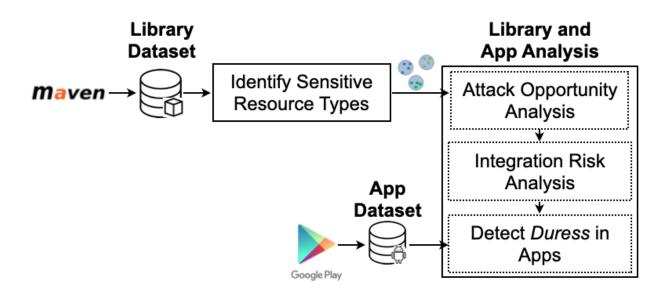
High priority victim manifest

<activity android:name="com.toast.android.paycologin.auth.PaycoLoginAuthWebViewActivity"
</activity>

Measurement Study

Research questions:

- Q1: How many sensitive resources are in libraries?
- Q2: Risks of two libraries with conflict resources?
- Q3: How many apps are affected?



Findings and Analysis

Our dataset:

- 23,691 most recent versions of AAR libraries from Maven Central.
- 2. 156,266 apps from Google Play.

Table 3: Overall data of *Duress* risks on D_l and D_a

| | Resource Type | Attack Opportunities | | Integration Risks | | # Affected |
|--------|-------------------------|----------------------|--------|-------------------|--------|------------|
| | Resource Type | # Libs | % Libs | # Libs | % Libs | Apps |
| Risk-1 | Backend URL | 348 | 1.5 | 79 | 22.7 | 3 |
| | Credential | 217 | 0.9 | 81 | 37.3 | 1 |
| | Script code | 157 | 0.7 | 44 | 28.0 | 0 |
| | Privacy disclosure | 584 | 2.5 | 93 | 15.9 | 0 |
| | Technical support | 1,359 | 5.7 | 225 | 16.6 | 0 |
| | Referral message | 200 | 0.8 | 40 | 20.0 | 0 |
| | ML model | 20 | 0.1 | 2 | 10.0 | 0 |
| | Network security config | 186 | 0.8 | 150 | 80.6 | 45 |
| | Auto backup rule | 30 | 0.1 | 7 | 23.3 | 1 |
| | File provider path | 460 | 1.9 | 283 | 61.5 | 76 |
| | Subtotal | 2,063 | 8.7 | 719 | 34.9 | 126 |
| Risk-2 | Manifest attributes | 2,281 | 9.6 | 450 | 19.7 | 137 |
| Risk-3 | Manifest attributes | 2,561 | 10.8 | 184 | 7.2 | 168 |
| | Total | 4,349 | 18.4 | 1,116 | 25.7 | 428 |
| | | | | | | |

Q1 Q2 Q3

Causal Analysis

- 1. Reliance on a common library.
- 2. Generic resource names that are prone to name collisions.
- 3. Resource names from the sample code of official documents.

```
<application
android:networkSecurityConfig="@xml/network_security_config"
</application>
```

4. Library templates and library outsourcing.

Please refer to our paper for more information.

Takeaway

- This study reveals a new attack surface on the Android application supply chain by exploiting duplicate resource mismediation.
- Our systematic measurements demonstrates the pervasiveness and severity of the risks in the wild.

Thank you

Yifan Zhang Ph.D. student Indiana University Bloomington yz113@iu.edu