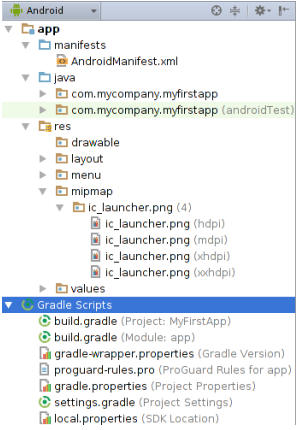
Detecting and Measuring Misconfigured Manifest in Android Apps

Yuqing Yang, Mohamed Elsabagh, Chaoshun Zuo,
Ryan Johnson, Angelos Stavrou, and Zhiqiang Lin

CCS 2022

The Android APK Structure



The Android Manifest File

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Configuration file

The Android Manifest File

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Configuration file
  - Components

The Android Manifest File

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Configuration file
  - Components
  - Security

The Android Manifest File

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Configuration file
  - Components
  - Security
  - Compatiblity
  - ...

What if it goes wrong...

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

What if it goes wrong...

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- No warning!

What if it goes wrong...

- What you think

What if it goes wrong...

- What you think

- What you have

Android Manifest Structure

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

Android Manifest Structure

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Elements
- Attributes
- Values

Android Manifest Structure: Constraints

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

Android Manifest Structure: Constraints

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- C1: Positional Constraints
- C2: Occurrence Constraints
  - A necessary (`android:name`)
  - B unique (`<application>`)
- C3: Value Type Constraints

Android Manifest Structure: Misconfigurations

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

Android Manifest Structure: Misconfigurations

```
01 <manifest package="com.example.app"...>
02  ...
03  <application ...>
04  ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter>
07     <action
08      android:name="com.amazon.*.NOTIFY"
09      android:permission="com.amazon.*.Permission.NOTIFY">
11     </action>
12    </intent-filter>
13   </receiver>
14  ...
15  </application>
16  ...
17 </manifest>
```

- Misplacement (C1, C2-A)
  - `<activity>` under `<action>`
- Absence (C2-B)
  - Missing `android:name`
- Type Error (C3)
  - `android:name=`**False**
- Unexpected
  - `<android:` **nmae**`>`

Validating Manifest File: XSD Schema [ ]

Validating Manifest File: XSD Schema [ ]

```
01  <xs:element name="intent-filter">
02    <xs:complexType mixed="true">
03      <xs:sequence>
04        <xs:element ref="action" minOccurs="1" />
05        <xs:element ref="category" />
06        <xs:element ref="data" />
07      </xs:sequence>
08      <xs:attribute name="autoVerify" type="xs:string"/>
09      ...
10    </xs:complexType>
11  </xs:element>
12  <xs:element name="action">
13    <xs:complexType mixed="true">
14      <xs:sequence>
15      </xs:sequence>
16      <xs:attribute name="name" type="xs:string"/>
17      ...
18    </xs:complexType>
19  </xs:element>
```

- Widely used
- Covers all manifest constraints
  - Positional: `<xs:element>`
  - Occurrence: `minOccurs`
  - Type: `type`

From Android Code...? [2]

From Android Code...? [2]

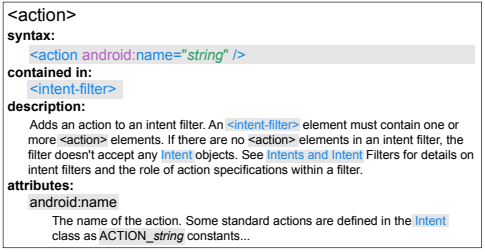
```
String nodeName = parser.getName();
if (nodeName.equals("action")) {
    String value = parser.getAttributeValue(
            ANDROID_RESOURCES, "name");
    if (value == null || value == "") {
        outError[0] = "No value supplied for <android:name>";
        return false;
    }
    XmlUtils.skipCurrentTag(parser);

    outInfo.addAction(value);
} else if (nodeName.equals("category")) {
```

- Ad-hoc
- Incomplete

From Documentation...? [3]

From Documentation...? [3]



<action>

syntax:

```
<action android:name="string" />
```

contained in:

<intent-filter>

description:

Adds an action to an intent filter. An <intent-filter> element must contain one or more <action> elements. If there are no <action> elements in an intent filter, the filter doesn't accept any Intent objects. See Intents and Intent Filters for details on intent filters and the role of action specifications within a filter.

attributes:

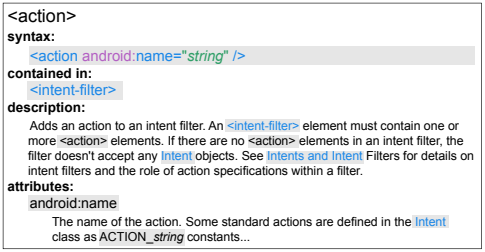
android:name

The name of the action. Some standard actions are defined in the Intent class as ACTION_*string* constants...

- Vague
- Implicit

Insights

Insights



<action>

syntax:

<action android:name="*string*" />

contained in:

<intent-filter>

description:

Adds an action to an intent filter. An <intent-filter> element must contain one or more <action> elements. If there are no <action> elements in an intent filter, the filter doesn't accept any Intent objects. See Intents and Intent Filters for details on intent filters and the role of action specifications within a filter.

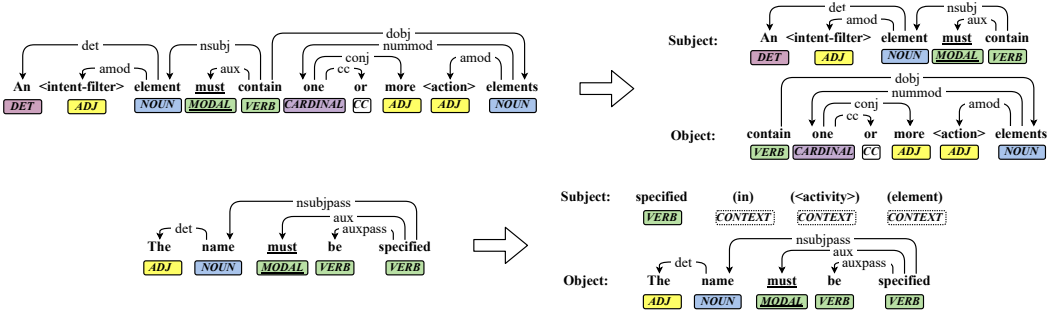
attributes:

android:name

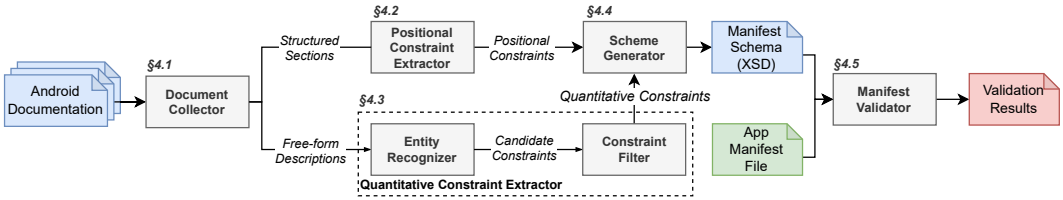
The name of the action. Some standard actions are defined in the Intent class as ACTION_*string* constants...

- Documentations are structured!
- Documentation Structure
  - Sections
  - Titles
- Sentence Structure
  - Subjects and Objects
  - Keywords Relate to Manifest

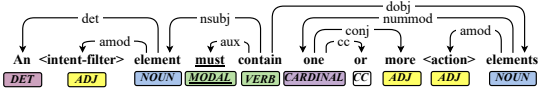
Example

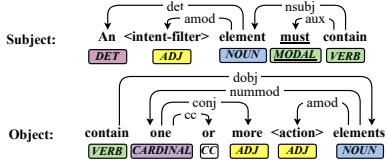

det
nsubj
dobj
amod
nummod
aux
conj
cc
amod
An <intent-filter> element must contain one or more <action> elements
DET ADJ NOUN MODAL VERB CARDINAL CC ADJ ADJ NOUN
Subject:
An <intent-filter> element must contain
DET ADJ NOUN MODAL VERB
Object:
contain one or more <action> elements
VERB CARDINAL CC ADJ ADJ NOUN
nsubjpass
det
aux
auxpass
The name must be specified
ADJ NOUN MODAL VERB VERB
Subject:
specified (in) (<activity>) (element)
VERB CONTEXT CONTEXT CONTEXT
Object:
The name must be specified
ADJ NOUN MODAL VERB VERB

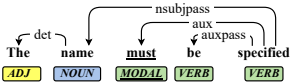
Architecture

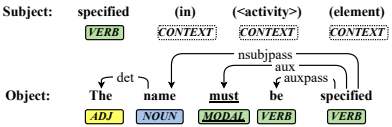


Entity Recognizer: Sentence Parsing [4]



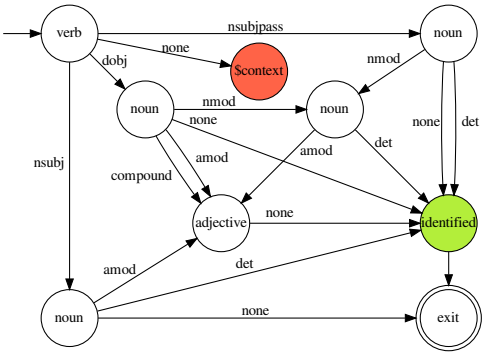




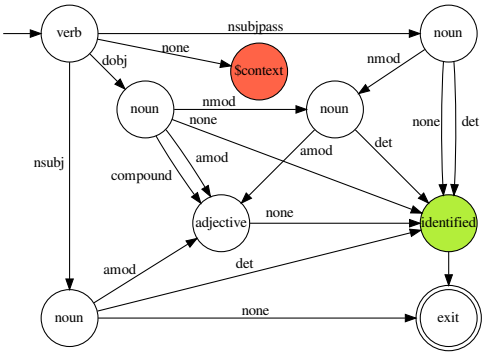


Entity Recognizer: Sentence Parsing [4]

Entity Recognizer: Sentence Parsing [4]



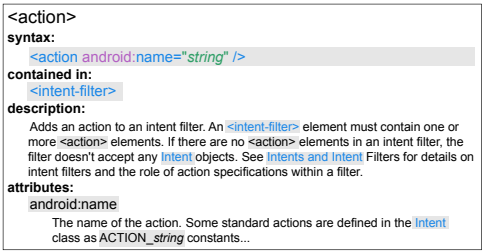
Entity Recognizer: Sentence Parsing [4]



- FSM-based parsing rule
- Starts from
- Moves to $context: resolve with context info
- Moves to exit:
  - Identified: current word is extracted
  - Not identified: abort this sentence

Entity Recognizer: Contextual Information

Entity Recognizer: Contextual Information



<action>

syntax:

<action android:name="*string*" />

contained in:

<intent-filter>

description:

Adds an action to an intent filter. An <intent-filter> element must contain one or more <action> elements. If there are no <action> elements in an intent filter, the filter doesn't accept any Intent objects. See Intents and Intent Filters for details on intent filters and the role of action specifications within a filter.

attributes:

android:name

The name of the action. Some standard actions are defined in the Intent class as ACTION_*string* constants...

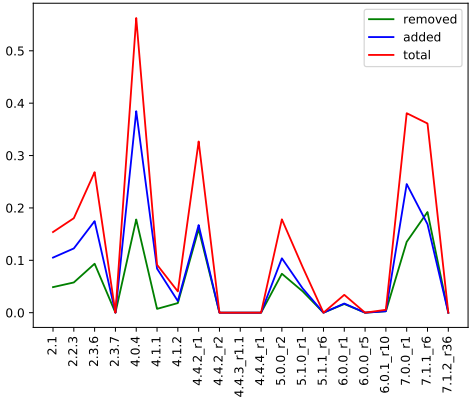
- Section-level Context
  - Section: `<activity>`
  - *The name must be specified*
- Paragraph-level Context
  - First sentence in paragraph:
  - *The name of the* **action**

Tool Stats

	Documentations Parsed					Sentences Recognized			Constraints Filtered			Constr.
Vers.	files	pages	sect.	para.	words	phrase	normal	passive	context	clause	word	Extra.
7.1.2+	26	190	348	849	28,765	404	1,326	256	2,379	139	34	254
7.1.2	26	158	308	687	25,585	361	1,135	235	2,104	126	21	219
7.1.1	26	158	308	687	25,585	361	1,135	235	2,104	126	21	219
7.0.0	26	157	305	672	25,292	358	1,115	232	2,078	125	21	216
6.0.1	26	148	302	665	25,294	361	1,119	233	2,094	122	22	217
6.0.0	26	148	302	665	25,294	361	1,119	233	2,094	122	22	217
5.1.1	26	148	301	656	25,025	362	1,108	227	2,076	123	21	216
5.1.0	26	148	301	656	25,025	362	1,108	227	2,076	123	21	216
5.0.0	26	146	298	643	24,592	352	1,094	224	2,058	122	20	213
4.4.4	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.4.3	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.4.2	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.1.2	26	138	286	589	22,009	321	971	208	1,834	115	14	194
4.1.1	26	138	285	585	21,867	317	963	207	1,821	115	14	193
4.0.4	26	128	283	598	23,235	348	1,019	218	1,933	122	15	191
2.3.7	24	109	262	514	19,552	288	881	186	1,651	109	12	178
2.3.6	24	109	262	514	19,552	288	881	186	1,651	109	12	178
2.2.3	24	95	262	507	19,459	284	888	192	1,632	110	12	179
2.1	24	92	257	487	18,331	269	838	180	1,548	105	12	174
1.6	24	89	256	482	17,756	264	804	176	1,501	102	12	172

Tool Stats

	Documentations Parsed					Sentences Recognized			Constraints Filtered			Constr.
Vers.	files	pages	sect.	para.	words	phrase	normal	passive	context	clause	word	Extra.
7.1.2+	26	190	348	849	28,765	404	1,326	256	2,379	139	34	254
7.1.2	26	158	308	687	25,585	361	1,135	235	2,104	126	21	219
7.1.1	26	158	308	687	25,585	361	1,135	235	2,104	126	21	219
7.0.0	26	157	305	672	25,292	358	1,115	232	2,078	125	21	216
6.0.1	26	148	302	665	25,294	361	1,119	233	2,094	122	22	217
6.0.0	26	148	302	665	25,294	361	1,119	233	2,094	122	22	217
5.1.1	26	148	301	656	25,025	362	1,108	227	2,076	123	21	216
5.1.0	26	148	301	656	25,025	362	1,108	227	2,076	123	21	216
5.0.0	26	146	298	643	24,592	352	1,094	224	2,058	122	20	213
4.4.4	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.4.3	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.4.2	26	143	292	612	22,846	340	1,006	210	1,900	120	19	200
4.1.2	26	138	286	589	22,009	321	971	208	1,834	115	14	194
4.1.1	26	138	285	585	21,867	317	963	207	1,821	115	14	193
4.0.4	26	128	283	598	23,235	348	1,019	218	1,933	122	15	191
2.3.7	24	109	262	514	19,552	288	881	186	1,651	109	12	178
2.3.6	24	109	262	514	19,552	288	881	186	1,651	109	12	178
2.2.3	24	95	262	507	19,459	284	888	192	1,632	110	12	179
2.1	24	92	257	487	18,331	269	838	180	1,548	105	12	174
1.6	24	89	256	482	17,756	264	804	176	1,501	102	12	172



Overall Result

- 1,853,862 Google Play Apps from AndroZoo [5]
- 692,106 Pre-installed Apps from SamMobile [6]

Google Play apps

Total installs	Misplaced element		Missing element		Misspelled element			Misplaced attribute		Missing attribute		Misspelled attribute			
	# Apps	# Misplaced	# Apps	# Missing	# Apps	# Cap.	# Typo	# Apps	# Misplaced	# Apps	# Missing	# Apps	# Prefix	# Cap.	# Typo
1B+	8	11	0	0	0	0	0	14	166	0	0	15	128	0	0
100M-1B	76	116	1	1	1	1	0	114	297	0	0	131	531	0	0
10M-100M	595	709	8	9	4	1	3	1,057	2,154	8	10	940	2,441	0	0
1M-10M	3,323	4,617	37	97	123	4	121	6,226	10,350	47	53	3,098	6,791	0	0
100k-1M	11,156	13,759	139	311	635	5	632	18,740	28,198	106	115	5,400	11,569	0	0
10k-100k	27,070	32,837	452	740	1,154	7	1,148	41,973	62,823	144	147	7,865	14,754	0	0
1k-10k	50,937	60,110	744	1,102	2,193	12	2,181	76,104	119,184	242	246	11,303	26,234	0	0
100-1k	65,252	72,285	854	1,124	1,553	4	1,558	107,344	154,858	339	343	15,992	55,119	0	0
0-10	69,482	76,645	422	516	251	5	246	127,018	173,644	562	565	16,904	47,486	1	4
total	227,899	261,089	2,657	3,900	5,914	39	5,889	378,590	551,674	1,448	1,479	61,648	165,053	1	4

Pre-installed apps

Firmware ver.	Misplaced element		Missing element		Misspelled element			Misplaced attribute		Missing attribute		Misspelled attribute			
	# Apps	# Misplaced	# Apps	# Missing	# Apps	# Cap.	# Typo	# Apps	# Misplaced	# Apps	# Missing	# Apps	# Prefix	# Cap.	# Typo
9	0	0	701	769	0	0	0	785	2,311	0	0	1,471	4,169	0	0
8	3	3	7,360	38,153	9	9	0	9,349	43,049	0	0	15,719	45,033	0	0
7	82	82	16,626	98,104	0	0	0	15,914	61,749	0	0	5,500	13,562	0	0
6	634	634	49,056	795,310	0	0	0	14,882	62,440	0	0	0	0	0	0
5	87	87	58,844	771,054	0	0	0	18,510	71,356	0	0	2	2	0	0
4	8	8	18,973	27,013	0	0	0	20,411	58,930	0	0	22,154	1,158	21,549	0
3	0	0	72	72	0	0	0	131	335	0	0	12	30	0	0
2	0	0	153	153	0	0	0	386	670	0	0	3	3	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
total	814	814	151,785	1,730,628	9	9	0	80,368	300,840	0	0	44,861	63,957	21,549	0

Security-related Misconfiguration

Type	Category	Name	AV	AC	PR	UI	S	C	I	A	Score*	Severity	# G	# P	Sample Impact
Element	Permission	permission	Local	Low	None	None	Unchanged	●	●	○	7.7	High	2,722	0	Component hijacking
		uses-permission	Local	Low	None	None	Unchanged	○	○	●	6.2	Medium	1,037	0	App crashing
Attribute	Compatibility	minSdkVersion	Local	Low	None	None	Unchanged	○	◐	●	6.8	Medium	2,156	408	Data leakage
		required	Local	Low	None	None	Unchanged	○	○	●	6.2	Medium	21,855	0	App crashing
	Functionality	allowBackup	Physical	Low	None	None	Unchanged	●	●	●	6.8	Medium	7,432	25,999	Data leakage
		enabled	Local	Low	None	None	Unchanged	○	○	◐	4	Medium	1,114	2	Data leakage
		excludeFromRecents	Local	High	None	None	Unchanged	◐	○	○	2.9	Low	2,395	12,013	Replay attack
		exported	Local	Low	None	None	Unchanged	◐	◐	◐	5.9	Medium	2,120	1,734	Component hijacking
		largeHeap	Local	Low	None	None	Unchanged	○	○	◐	4	Medium	7,086	3,950	App crashing
		multiprocess	Local	Low	None	None	Unchanged	◐	◐	◐	5.9	Medium	15,511	0	App crashing
		persistent	Local	Low	None	None	Unchanged	○	○	◐	4	Medium	16,429	2,391	App crashing
		priority	Local	High	None	None	Unchanged	○	○	◐	2.9	Low	2,477	6,907	Component hijacking
		taskAffinity	Local	Low	None	None	Unchanged	◐	◐	◐	5.9	Medium	555	5,291	Component hijacking
	Permission	permission	Local	Low	None	None	Unchanged	●	●	○	7.7	High	10,348	36	Component hijacking
		protectionLevel	Local	Low	None	None	Unchanged	●	●	○	7.7	High	6,839	6,787	Component hijacking

The Amazon Case: Official Mistaken Snippets [7]

PERMISSION(Top-Five Categories)

	App category	# App
Payment	Game	6,406
	News	621
	Education	488
	Books	255
	Personalization	237
Cloud Msg	Lifestyle	104
	Sports	61
	Entertainment	55
	Tools	55
	Books	47
SMS Msg	Tools	11
	Productivity	10
	Communication	6
	Social	3
	Lifestyle	1

Levon@Amazon 回答済 • Feb 22 2017 時刻 10:22 AM

The solution would be to include the receiver and have the NOTIFY action and permission set. Open your AndroidManifest.xml file, and add the following (you can place it after all of your <activity> entries, just before </application> end tag:

```
1. <!-- Amazon IAP v2.x -->
2. <receiver android:name = "com.amazon.device.iap.ResponseReceiver">
3.   <intent-filter>
4.     <action android:name = "com.amazon.inapp.purchasing.NOTIFY"
5.       android:permission = "com.amazon.inapp.purchasing.Permission.NOTIFY" />
6.   </intent-filter>
7. </receiver>
```

1 · 1 を非表示 1

Mitigation

- Developers: Be careful for online snippets!!
- Third-party Providers: Double-check provided snippets
- Android: Provide systematic configuration checking

References I

XML schema languages.
https://en.wikipedia.org/wiki/XML_schema#Languages, 2021.
(Accessed on 2021-01-18).

Android package parser.
http://androidxref.com/9.0.0_r3/xref/frameworks/base/core/java/android/content/pm/PackageParser.java#parseVerifier, 2021.
(Accessed on 2021-01-12).

action — android developers.
https://developer.android.com/guide/topics/manifest/action-element, 2021.
(Accessed on 2022-09-13).

Overview - corenlp.
https://stanfordnlp.github.io/CoreNLP/, 2021.
(Accessed on 2022-09-13).

androzoo home.
https://androzoo.uni.lu/, 2022.
(Accessed on 2022-09-13).

SamMobile - Your authority on all things Samsung.
https://www.sammobile.com/, 2021.
(Accessed on 2021-05-30).

References II

Purchasing Listener doesn't get called.
https://forums.developer.amazon.com/questions/16519/purchasinglistener-doesnt-get-called.html, 2021.
(Accessed on 2021-01-18).

Q&A

- Context filter:
  - Extracted parent and child have to be in dictionary.
    - e.g., `['foo','bar']` ✗
  - Extracted child entity has to be one of parents' actual children
    - e.g., `['action','activity']` ✗
- Sentence filter:
  - Sentence must not have adverbial clause voiding constraint necessity
    - e.g.,'*You* **should always** *declare this attribute* **if** *you want to configure [...]*'✗
- Word filter:
  - Sentence must contain model verb
    - e.g., *The name* **must** *be specified.*✓