Detecting and Measuring Misconfigured Manifests in Android Apps

Yuqing Yang [1] Mohamed Elsabagh [2] Chaoshun Zuo [1] Ryan Johnson [2]
Angelos Stavrou [2] Zhiqiang Lin [1]

[1]The Ohio State University

[2]Quokka (formerly Kryptowire)

CCS 2022

The Ohio State University
Computer Security Laboratory

Quokka

The Android Manifest File

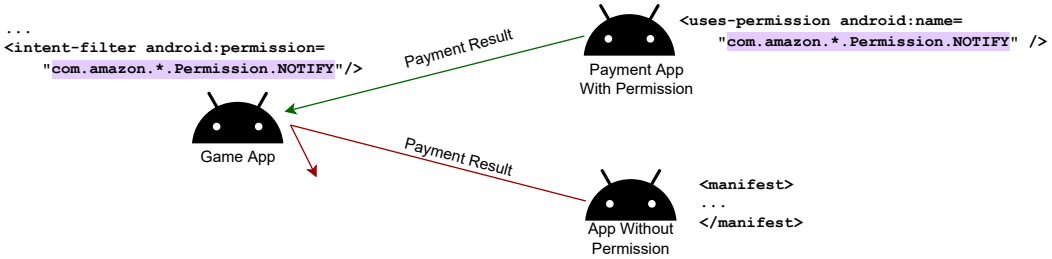
Components

Functionality

Security

```
01 <manifest package="com.example.app"...>
02 ...
03  <application android:allowBackup=True>
04 ...
05   <receiver android:name="com.amazon.*">
06    <intent-filter
        android:permission="com.amazon.*.Permission.NOTIFY">
07     <action
         android:name="com.amazon.*.NOTIFY"/>
08     </action>
09    </intent-filter>
10   </receiver>
11 ...
12  </application>
13  <uses-permission
       android:name="com.amazon.*.Permission.NOTIFY"
       android:maxSdkVersion="18" />
14 ...
15 </manifest>
```

Manifest File Can Be Security-sensitive



What if it goes wrong...

```
<manifest package="com.example.app"...>
...
 <application android:allowBackup=True>
...
  <receiver android:name="com.amazon.*">
   <intent-filter
    android:permission="com.amazon.*.Permission.NOTIFY">
    <action
     android:name="com.amazon.*.NOTIFY"
     android:permission="com.amazon.*.Permission.NOTIFY">
    </action>
   </intent-filter>
  </receiver>
...
 </application>
 <uses-permission
    android:name="com.amazon.*.Permission.NOTIFY"
    android:maxSdkVersion="18" />
...
</manifest>
```

What if it goes wrong...

```
<manifest package="com.example.app"...>
...
 <application android:allowBackup=True>
...
  <receiver android:name="com.amazon.*">
   <intent-filter
    android:permission="com.amazon.*.Permission.NOTIFY">
    <action
     android:name="com.amazon.*.NOTIFY"
     android:permission="com.amazon.*.Permission.NOTIFY">
    </action>
   </intent-filter>
  </receiver>
...
 </application>
 <uses-permission
    android:name="com.amazon.*.Permission.NOTIFY"
    android:maxSdkVersion="18" />
...
</manifest>
```

- No warning at installation

What if it goes wrong...

```
<manifest package="com.example.app"...>
...
 <application android:allowBackup=True>
...
  <receiver android:name="com.amazon.*">
   <intent-filter
    android:permission="com.amazon.*.Permission.NOTIFY">
    <action
     android:name="com.amazon.*.NOTIFY"
     android:permission="com.amazon.*.Permission.NOTIFY">
    </action>
   </intent-filter>
  </receiver>
...
 </application>
 <uses-permission
    android:name="com.amazon.*.Permission.NOTIFY"
    android:maxSdkVersion="18" />
...
</manifest>
```

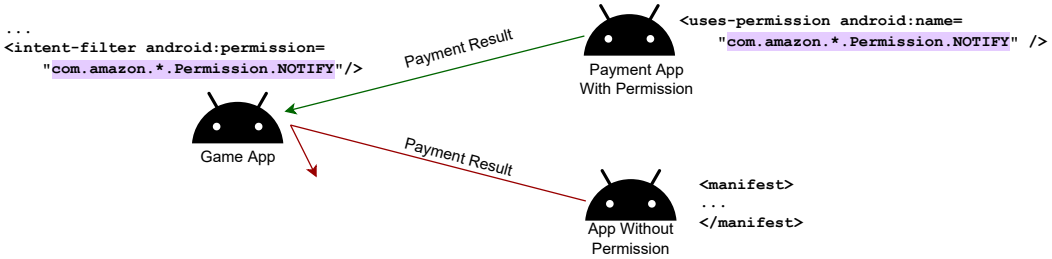
- No warning at installation
- Application executes normally

What if it goes wrong...

```
<manifest package="com.example.app"...>
...
 <application android:allowBackup=True>
...
  <receiver android:name="com.amazon.*">
   <intent-filter
    android:permission="com.amazon.*.Permission.NOTIFY">
    <action
     android:name="com.amazon.*.NOTIFY"
     android:permission="com.amazon.*.Permission.NOTIFY">
    </action>
   </intent-filter>
  </receiver>
...
 </application>
 <uses-permission
    android:name="com.amazon.*.Permission.NOTIFY"
    android:maxSdkVersion="18" />
...
</manifest>
```

- No warning at installation
- Application executes normally
- Security configuration ineffective!

What if it goes wrong...



What if it goes wrong...

```
...
<intent-filter >
  <action android:permission=
    "com.amazon.*.Permission.NOTIFY"/>
</intent-filter>
```

Game App

Payment Result

Payment App
With Permission

```
<uses-permission android:name=
    "com.amazon.*.Permission.NOTIFY" />
```

Payment Result

App Without
Permission

```
<manifest>
...
</manifest>
```

What if it goes wrong...

- What you think

What if it goes wrong...

- What you think

- What you have

Section Summary

- Manifest file can be security-critical

Section Summary

- Manifest file can be security-critical
- Malformed security configuration are ineffective without warning

Section Summary

- Manifest file can be security-critical
- Malformed security configuration are ineffective without warning
- Ineffective configuration creates vulnerabilities

Yes, but what is "Schema"?

- "An XML Schema describes the structure of an XML document.[1]"
- Also referred to as XML Schema Definition (XSD)[2].

Positional Constraint

Occurrence Constraint (Max)

Occurrence Constraint (Min)

```
<xs:element name="intent-filter">
<xs:complexType mixed="true">
<xs:sequence>
<xs:element ref="action" minOccurs="1" />
<xs:element ref="category" />
<xs:element ref="data" />
</xs:sequence>
<xs:attribute name="autoVerify" type="xs:string"/>
...
</xs:complexType>
</xs:element>
<xs:element name="manifest">
<xs:complexType mixed="true">
<xs:sequence>
<xs:element ref="application" maxOccurs="1" />
</xs:sequence>
<xs:attribute name="name" type="xs:string"/>
...
</xs:complexType>
</xs:element>
```

Android Manifest Structure: Misconfigurations

Misplacement

Absense

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

From Android Code...? [3]

From Android Code...? [3]

```
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

From Android Code...? [3]

```
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!

From Documentation!

<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...

1. Documentations are structured!

From Documentation!

<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...

1. Documentations are structured!
2. Documentation Structure
   - Sections
   - Titles

From Documentation!

<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.

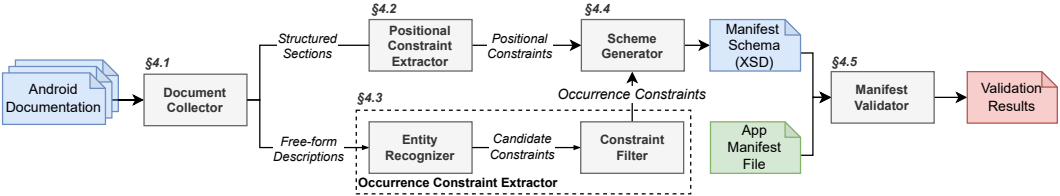
attributes:

android:name

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

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

Architecture



Positional Constraint Extractor

<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...

Positional Constraint Extractor

<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...

1. Current element: `<action>`

Positional Constraint Extractor

<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...

1. Current element: `<action>`
2. Parent element:
   - `<intent-filter>`

Positional Constraint Extractor

<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.

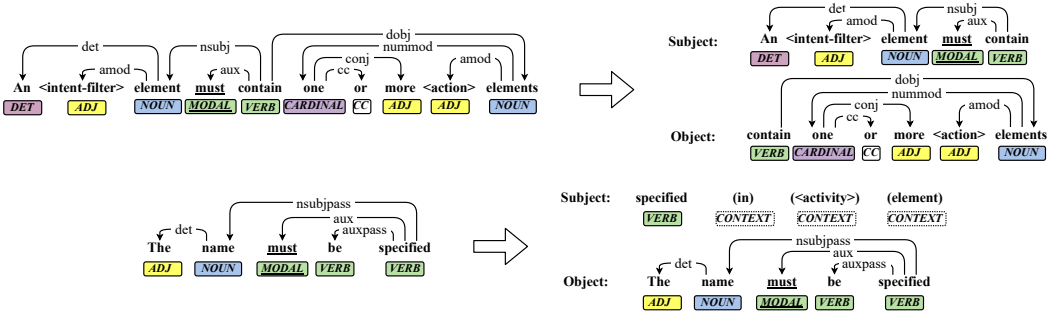
attributes:

android:name

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

1. Current element: `<action>`
2. Parent element:
   - `<intent-filter>`
3. Child Attribute:
   - `android:name`

Occurrence Constraint Extractor



Collected Documentation

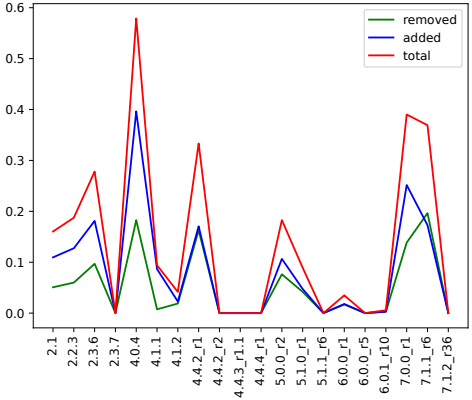
- 20 versions of documentations
  - 1 online version

Collected Documentation

- 20 versions of documentations
  - 1 online version
  - 19 historical versions (1.6 to 7.1.2)

Collected Documentation

- 20 versions of documentations
  - 1 online version
  - 19 historical versions (1.6 to 7.1.2)
  - Online version:
    - 190 pages
    - 1,986 sentences
    - 254 constraints



Overall Result

- 1,853,862 Google Play Apps from AndroZoo [4]

Overall Result

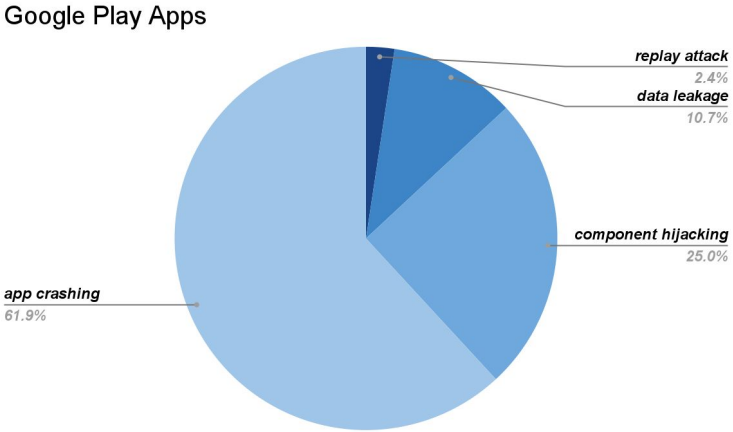
- 1,853,862 Google Play Apps from AndroZoo [4]
- 692,106 Pre-installed Apps from SamMobile [5]

Overall Result

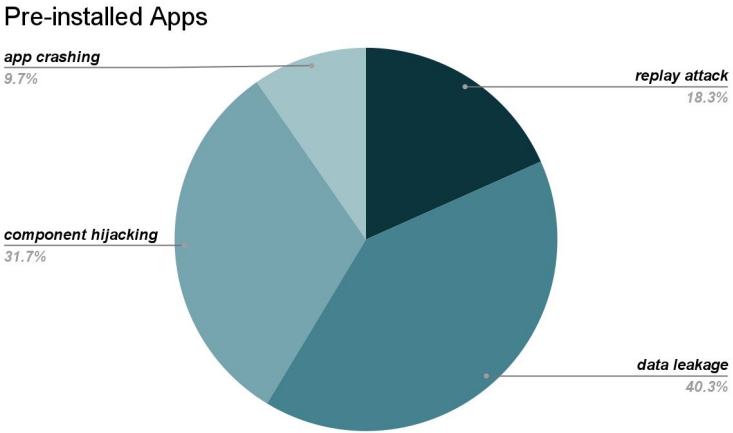
- 1,853,862 Google Play Apps from AndroZoo [4]
- 692,106 Pre-installed Apps from SamMobile [5]
- 84,117 (13.80%) Google Play Apps and 56,611 (22.95%) Pre-installed Apps are misconfigured with security concerns.

Type	Category	Name	AV	AC	C	I	A	Score*	Severity	# G	# P	Sample Impact
Element	Permission	permission	Local	Low	●	●	○	7.7	High	2,722	0	Component hijacking
		uses-permission	Local	Low	○	○	●	6.2	Medium	1,037	0	App crashing
Attribute	Compatibility	minSdkVersion	Local	Low	○	◐	●	6.8	Medium	2,156	408	Data leakage
		required	Local	Low	○	○	●	6.2	Medium	21,855	0	App crashing
	Functionality	allowBackup	Physical	Low	●	●	●	6.8	Medium	7,432	25,999	Data leakage
		enabled	Local	Low	○	○	◐	4	Medium	1,114	2	Data leakage
		excludeFromRecents	Local	High	◐	○	○	2.9	Low	2,395	12,013	Replay attack
		exported	Local	Low	◐	◐	◐	5.9	Medium	2,120	1,734	Component hijacking
		largeHeap	Local	Low	○	○	◐	4	Medium	7,086	3,950	App crashing
		multiprocess	Local	Low	◐	◐	◐	5.9	Medium	15,511	0	App crashing
		persistent	Local	Low	○	○	◐	4	Medium	16,429	2,391	App crashing
		priority	Local	High	○	○	◐	2.9	Low	2,477	6,907	Component hijacking
		taskAffinity	Local	Low	◐	◐	◐	5.9	Medium	555	5,291	Component hijacking
	Permission	permission	Local	Low	●	●	○	7.7	High	10,348	36	Component hijacking
		protectionLevel	Local	Low	●	●	○	7.7	High	6,839	6,787	Component hijacking

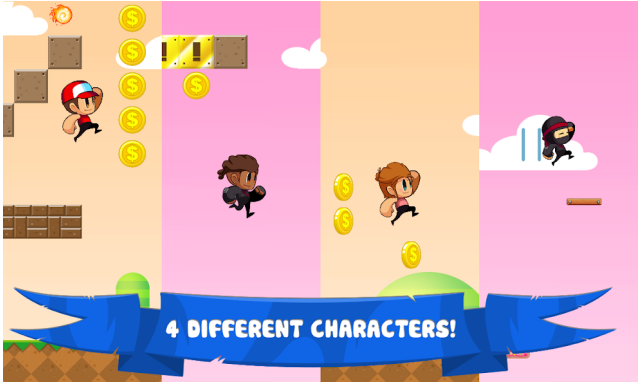
Security-related Misconfiguration



Security-related Misconfiguration



Case Study: a game with 10M+ installs



Case Study: a game with 10M+ installs

```
...
<intent-filter >
  <action android:permission=
    "com.amazon.*.Permission.NOTIFY"/>
</intent-filter>
```

Game App

Payment Result

Payment App
With Permission

```
<uses-permission android:name=
    "com.amazon.*.Permission.NOTIFY" />
```

Payment Result

App Without
Permission

```
<manifest>
...
</manifest>
```

Root Cause: Official Mistaken Snippets [6]

Impact: App defrauding (buy item once, get infinite refills)

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

Conclusion

- Manifest files are as important as app code.

Conclusion

- Manifest files are as important as app code.
- Misconfigured Manifest files can lead to severe security weaknesses.

Conclusion

- Manifest files are as important as app code.
- Misconfigured Manifest files can lead to severe security weaknesses.
- Developers should be careful with copied snippets when developing apps.

Thank You

Detecting and Measuring Misconfigured Manifests in Android Apps

Yuqing Yang [1] Mohamed Elsabagh [2] Chaoshun Zuo [1] Ryan Johnson [2]
Angelos Stavrou [2] Zhiqiang Lin [1]

[1]The Ohio State University

[2]Quokka (formerly Kryptowire)

CCS 2022

References I

XML schema.
https://www.w3schools.com/xml/xml_schema.asp, 2022.
(Accessed on 2022-11-8).

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).

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

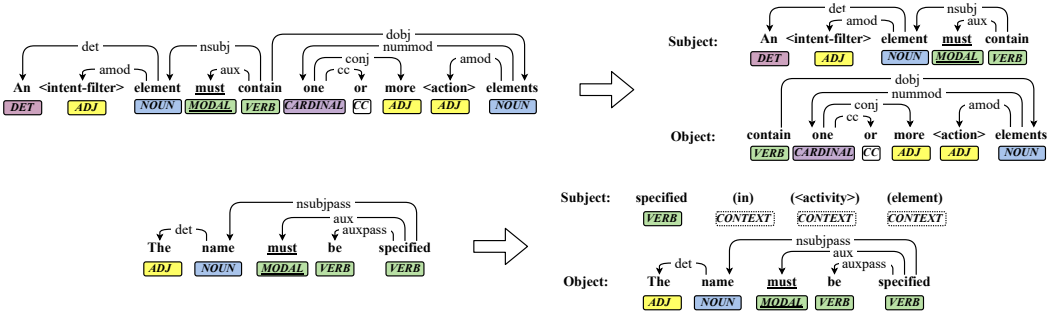
SamMobile - Your authority on all things Samsung.
https://www.sammobile.com/, 2021.
(Accessed on 2021-05-30).

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

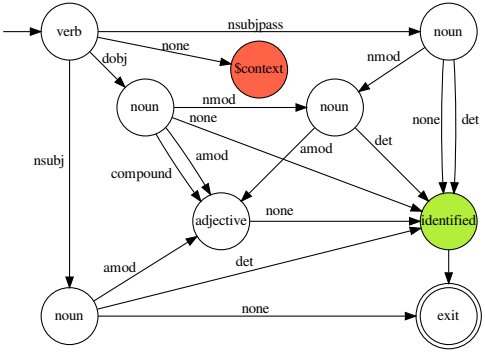
References II

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

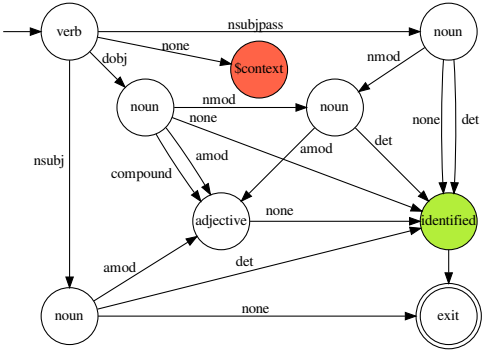
State-based Sentence Prasing [7]



State-based Sentence Parsing [7]



State-based Sentence Parsing [7]



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

Contextual Information Extraction

Contextual Information Extraction

<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**

Domain-aided Constraint Generation

- 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.*✓

Documentation Analysis

	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

Documentation Analysis

	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