Repairing Crashes in Android Apps

Shin Hwei Tan
Southern University of Science and Technology
shinhwei@hotmail.com

Xiang Gao, Zhen Dong and Abhik Roychoudhury
National University of Singapore
{gaoxiang | xhen.dog| abhik}@comp.nus.edu.sg

Lucas Roque

2018

I4Soft
Intelligence for Software

UFG

Introdução

- *Smartphones* tornaram-se altamente difundidos, por isso, é importante garantir a confiabilidade dos aplicativos em execução;
- Diversos trabalhos têm realizados análises estáticas e dinâmicas, e testes em aplicativos mobile;
- Várias técnicas automatizadas de reparo, foram propostas para reduzir o tempo e esforço na correção de software.

Introdução

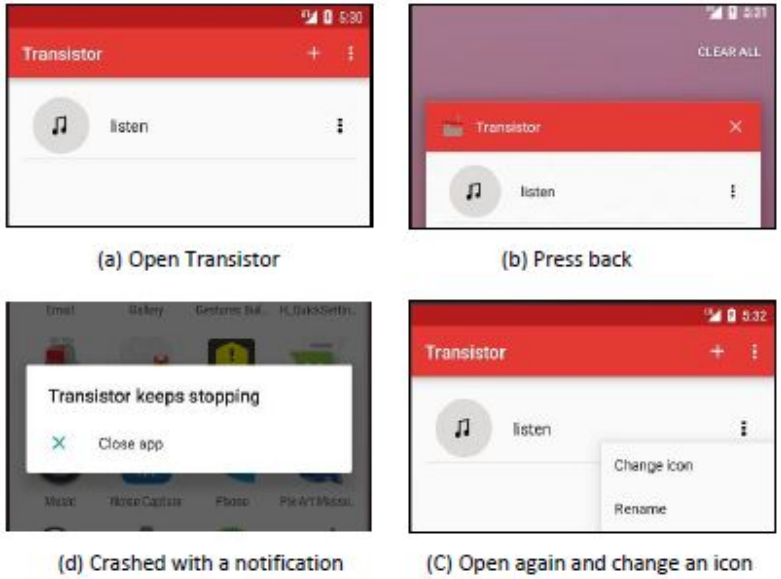
- As técnica atuais são baseadas no comportamento esperado, porém, na prática esse comportamento não é bem especificado;
- Tal fato pode não só produzir correções incompletas, como introduzir novos erros;
- Várias propriedades únicas de casos de teste para aplicativos móveis representam desafios únicos para este tipo de abordagem:
  - Frequentemente são uma sequência de comandos UI;
  - Dependência da disponibilidade de código fonte;
  - Necessidade de aplicação por desenvolvedores.

Proposta | Droix

- **Reparo para Android;**
- **Repara utilizando caso de testes baseados em UI;**
- **Transformação do ciclo de vida;**
- **Avaliação:** DroixBench 24 erros de 15 aplicativos Android.

Background

- A principal diferença do Java é que ele possui vários pontos de entrada.



(a) Open Transistor

(b) Press back

(d) Crashed with a notification

(C) Open again and change an icon

Background

```
FATAL EXCEPTION: main Process: org.y20k.transistor, PID: 2416
java.lang.IllegalStateException:
    Fragment MainActivityFragment{82e1bec} not attached to Activity
at android...startActivityForResult(Fragment.java:925)
at y20k...selectFromImagePicker(MainActivityFragment.java:482)
```

Listing 1: Stack trace for the crash in Transistor

```
    +if(getActivity()!=null)
482: startActivityForResult(pickImageIntent, REQUEST_LOAD_IMAGE);
```

Listing 2: Droix's patch for the crash in Transistor

```
    -startActivityForResult(pickImageIntent, REQUEST_LOAD_IMAGE);
482: +mActivity.startActivityForResult(pickImageIntent,
     REQUEST_LOAD_IMAGE);
```

Listing 3: Developer's patch for the crash in Transistor

Identificando causas do *Crash*

- Busca por causas comuns de *Crash*, analisando manual de aplicações Android no GitHub e documentação da API:
  - Busca pelo termo “android app”;
  - *Issues* fechadas com termo “crash”;
  - Extração de *issues* com pelo menos um *commit* associado a *crash*;
- Foram encontradas 1155 *issues* fechadas relacionadas a *crash*;
- 107 deles com correções correspondentes, de 15 aplicativos diferentes.

Identificando causas do *Crash*

- Quais são as possíveis causas e exceções que levam ao *Crash* de aplicativos para Android?
  - 40.19 % são NullPointerException;
  - 7.48 % são IllegalStateException;
- Como a complexidade do ciclo de vida da activity/fragment levam ao *Crash* de aplicativos para Android?
  - Estudos anteriores indicam que **47%** de NullPointerException são gerados devido a complexidade activity/fragment;

Identificando causas do *Crash*

Category	Specific reason	Description	GitHub Issues (%)	Frequent Exception Type	Category Total (%)
Lifecycle	Configuration changes	activity recreation during configuration changes	5.61	NullPointer	14.02
	Stateloss	transaction loss during commit	2.80	IllegalState	
	GetActivity	activity-fragment coordination	2.80	IllegalState	
	Activity backstack	inappropriate handling of activity stack	1.87	IllegalArgument	
	Save instance	uninitialized object instances in onSaveInstance() callback	0.93	IllegalState	
Resource	Resource-related	resource type mismatches	10.28	NullPointer	16.82
	Resource limit	limited resources	4.67	OutOfMemory	
	Incorrect resource	retrieve a wrong resource id	1.87	SQLite	
Callback	Activity-related	missing activities	7.48	NullPointer	17.76
	View-related	missing views	6.54	NullPointer	
	Intent-related	missing intents	3.74	NullPointer	
	Unhandled callbacks	missing callbacks	2.80	NullPointer	
Others	Missing Null-check	missing check for null object reference	12.15	NullPointer	52.34
	External Service/Library	defects in external service/library	8.41	NullPointer	
	Workaround	temporary fixes for defect	4.67	IndexOutOfBound	
	API changes	API version changes	2.80	SQLite	
	Others	project-specific defects	24.30	-	

Resolução de *Crash*

- Através de uma análise manual foram identificados 8 transformações que podem ser úteis no reparo:

Null

Transação

Comunicação

Recurso

Cast

Estado

Operator	Description
S1: GetActivity-check	Insert a condition to check whether the activity containing the fragment has been created.
S2: Retain object	Store objects and load them when configuration changes
S3: Replace resource id	Replace resource id with another resource id of same type.
S4: Replace method	Replace the current method call with another method call with similar name and compatible parameter types.
S5: Replace cast	Replace the current type cast with another compatible type.
S6: Move stmt	Removes a statement and add it to another location.
S7: Null-check	Insert condition to check if a given object is null.
S8: Try-catch	Insert try-catch blocks for the given exception.

Metodologia

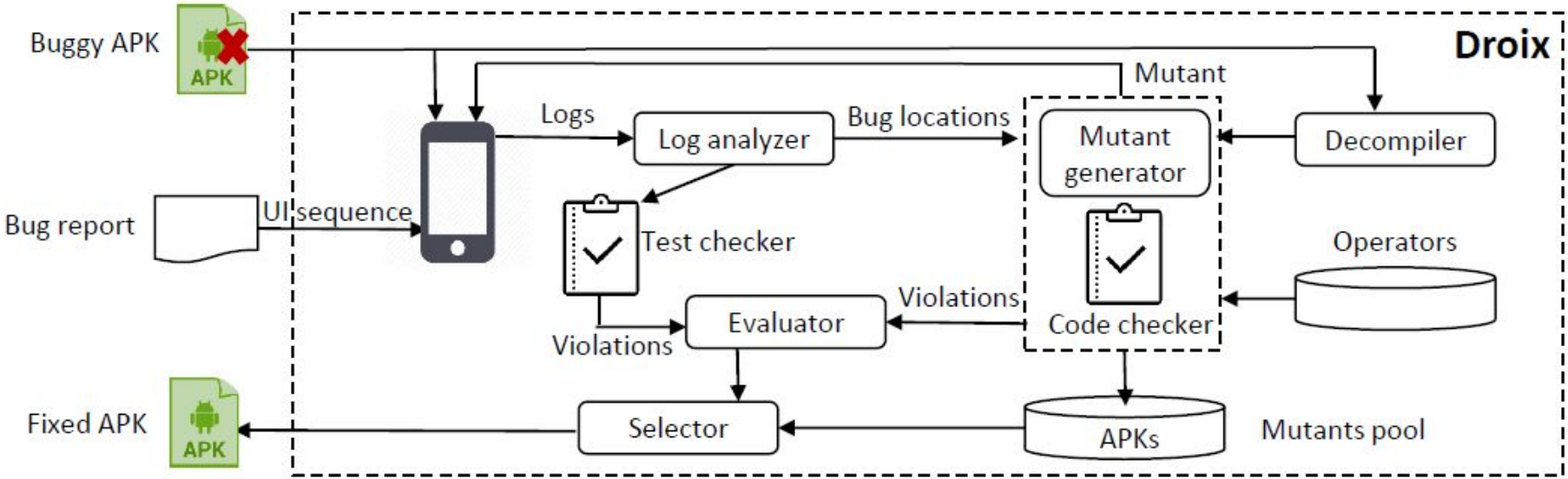
- Teste com sequências UI:
  - Frequentemente não incluídos;
  - Nem sempre confiável;
  - Aceita como entrada uma série de ações registradas com Monkey Runner, comandos ADB, ou *script* combinando as duas estratégias;
- Localização de falhas:
  - Utiliza o rastro do *crash*.
- Geração de mutantes:
  - Aplica uma das operações em cada linha do rastro.

Metodologia

- Validação de código e teste:
  - **Propriedades Code Level:** Verificadas antes da execução;
  - **Propriedades Test Level:** Verificadas durante e depois da execução.

Level	Type	Description
Code-level	Well-formedness	Verify that a mutated APK is compilable and the structural type of the program matches the requires context of the selected operator.
	Bug hazard	Checks whether a transformation violates Java exception-handling best practices.
	Exception Type	Checks whether a transformation matches a given exception type. (e.g., Insert Null-check should be used for fixing `NullPointerException` exclusively)
Test-level	Lifecycle	Checks that the event transition matches with the activity and fragment lifecycle model (Figure 1).
	Activity-Fragment	Checks that the interaction between a fragment and its parent activity matches the activity-fragment coordination model (dashed lines in Figure 1)
	Commit	Checks that a commit of a fragment's transactions is performed in the allowed states (i.e., after an activity's state is saved).

Metodologia



DroixBench

- 24 *crashes* reproduzíveis de 15 aplicações Android reais;
- Foi realizada uma nova busca, desconsiderando os aplicativos utilizados no estudo da identificação das operações de resolução;
- Também foram excluídas *issues* sem *commits* de correção, não resolvidas, e não Android;
- Posteriormente foram rejeitados defeitos seguindo os critérios:
  - Dependente de dispositivos;
  - Dependente de recursos;
  - Irreprodutíveis.

Avaliação

- **RQ1:** Quantas falhas em aplicativos Android o Droix pode consertar?

- **RQ2:** Qual a qualidade das correções geradas pelo Droix em comparação com os geradas pelos desenvolvedores?

Avaliação

- DroixBench;
- População: 40;
- Gerações: 10;

App Name	Description	Version	LOC	Type	TestEx(s)
Transistor	radio players	1.2.3	4K	NullPointer	42.1
		1.1.5	4K	IllegalState	40.1
Pix-art	photo editor	1.17.1	54K	NullPointer	37.2
		1.17.0	60K	NullPointer	42.0
PoetAssistant	poet writing helper	1.18.2	12K	NullPointer	42.3
		1.10.4	6K	SQLite	60.9
Anymemo	flashcard learning	10.10.1	29K	NullPointer	50.5
		10.9.922	33K	NullPointer	83.9
AnkiDroid	flashcard learning	2.8.1	73K	IllegalState	50.6
		2.7b1	73K	ClassCast	37.2
Fdroid	opensoure app repository	0.103.2	50K	IllegalState	38.7
		0.98	38K	SQLite	37.3
Yalp	app repository	0.17	11K	NullPointer	57.4
LabCoat	GitLab client	2.2.4	45K	NullPointer	49.2
GnuCash	finance expense tracker	2.1.4	42K	IllegalArgument	32.0
		2.1.3	40K	NullPointer	37.2
		2.0.5	37K	IllegalArgument	42.2
NoiseCapture	noise evaluator	0.4.2b	10K	NullPointer	42.5
		0.4.2b	10K	ClassCast	41.2
ConnectBot	secure shell client	1.9.2	26K	OutOfBounds	57.4
K9	email client	5.111	115K	NullPointer	42.2
OpenMF	Mifosx client	1.0.1	75K	IllegalState	134.0
Transdroid	torrents client	2.5.0b1	37K	NullPointer	45.9
Beem	communication tool	0.1.7rc1	21K	NullPointer	61.3

Avaliação

- Para cada defeito foram manualmente inspecionado o código fonte, e o comportamento das telas, entre a correção humana e a gerada pelo Droix;
- A qualidade das correções foram definidas seguindo os critérios:
  - Equivalente sintaticamente;
  - Equivalente semanticamente;
  - Comportamento de UI equivalente;
  - Incorreto;
  - Melhor.

Resultados

- 15 correções plausíveis;
- 9 defeitos não reparados;
- Análise manual revelou que seriam necessárias a edição de pelo menos 10 linhas.

App	Version	Time (s)	Fix type	Repair	Syntactic Equiv.	Semantic Equiv.	UI-behavior Equiv.	Others
Transistor	1.2.3 1.1.5	616 987	- GetActivity-check	√				better(⊕)
PixArt	1.17.1 1.17.0	1164 1525	- Null-check	√			△	
PoetAssistant	1.18.2 1.10.4	955 3600	Null-check -	√			△	
Anymemo	10.10.1 10.9.922	2104 1336	- Retain Object	√		⊙		
AnkiDroid	2.8.1 2.7b1	3600 3600	- Try-catch	√				text missing(×)
Fdroid	0.103.2 0.98	2293 518	Replace method -	√	★			
Yalp	0.17	2970	-					
LabCoat	2.2.4	2074	Null-check	√	★			
GnuCash	2.1.3 2.0.5 2.1.4	360 1492 3600	- Try-catch -	√			△	
ConnectBot	1.9.2	572	Try-catch	√				text missing(×)
NoiseCapture	0.4.2b 0.4.2b	340 520	Null-check Replace cast	√ √	★ ★			
K9	5.111	1718	Try-catch	√				crash(×)
OpenMF	1.0.1	3600	GetActivity-check	√	★			
Beem	0.1.7rc1	2378	Null-check	√	★			
Transdroid	2.5.0b1	1315	Null-check	√	★			
	24			15	7	1	3	4

Resultados

App	Version	Time (s)	Fix type	Repair	Syntactic Equiv.	Semantic Equiv.	UI-behavior Equiv.	Others
Transistor	1.2.3 1.1.5	616 987	- GetActivity-check	√				better(⊕)
PixArt	1.17.1 1.17.0	1164 1525	- Null-check	√			△	
PoetAssistant	1.18.2 1.10.4	955 3600	Null-check -	√			△	
Anymemo	10.10.1 10.9.922	2104 1336	- Retain Object	√		⊙		
AnkiDroid	2.8.1 2.7b1	3600 3600	- Try-catch	√				text missing(×)
Fdroid	0.103.2 0.98	2293 518	Replace method -	√	★			
Yalp	0.17	2970	-					
LabCoat	2.2.4	2074	Null-check	√	★			
GnuCash	2.1.3 2.0.5 2.1.4	360 1492 3600	- Try-catch -	√			△	
ConnectBot	1.9.2	572	Try-catch	√				text missing(×)
NoiseCapture	0.4.2b 0.4.2b	340 520	Null-check Replace cast	√ √	★ ★			
K9	5.111	1718	Try-catch	√				crash(×)
OpenMF	1.0.1	3600	GetActivity-check	√	★			
Beem	0.1.7rc1	2378	Null-check	√	★			
Transdroid	2.5.0b1	1315	Null-check	√	★			
	24			15	7	1	3	4

Resultados

- Uma correção clasificada como “Better”;
- Três como “Incorrect”.

App	Version	Time (s)	Fix type	Repair	Syntactic Equiv.	Semantic Equiv.	UI-behavior Equiv.	Others
Transistor	1.2.3 1.1.5	616 987	- GetActivity-check	√				better(⊕)
PixArt	1.17.1 1.17.0	1164 1525	- Null-check	√			△	
PoetAssistant	1.18.2 1.10.4	955 3600	Null-check -	√			△	
Anymemo	10.10.1 10.9.922	2104 1336	- Retain Object	√		⊙		
AnkiDroid	2.8.1 2.7b1	3600 3600	- Try-catch	√				text missing(×)
Fdroid	0.103.2 0.98	2293 518	Replace method -	√	★			
Yalp	0.17	2970	-					
LabCoat	2.2.4	2074	Null-check	√	★			
GnuCash	2.1.3 2.0.5 2.1.4	360 1492 3600	- Try-catch -	√			△	
ConnectBot	1.9.2	572	Try-catch	√				text missing(×)
NoiseCapture	0.4.2b 0.4.2b	340 520	Null-check Replace cast	√ √	★ ★			
K9	5.111	1718	Try-catch	√				crash(×)
OpenMF	1.0.1	3600	GetActivity-check	√	★			
Beem	0.1.7rc1	2378	Null-check	√	★			
Transdroid	2.5.0b1	1315	Null-check	√	★			
	24			15	7	1	3	4

Ameaças a validade

- Operadores utilizados;
- Apenas *Crashes* reproduzíveis;
- *Crashes* investigados;
- Qualidade do reparo.

Conclusões

- Foram estudadas 107 causas de *Crashes* em aplicativos Android;
- Foi proposto um *benchmark* com 24 erros reproduzíveis em 15 aplicações reais;
- O framework proposto possui potencial de uso por usuários não técnicos;
- Pode ser utilizado como plugin para melhor entendimento da API;
- Como trabalho futuro, pretende-se usá-lo como um aplicativo Android;

Perguntas?

Obrigado!