Facebook Infer

Seminar Formal Methods

Franz-Xaver Reichl

December 7, 2017

Infer: Overview

- Static program analyzer
- Maintained by facebook
- Deployed at large scale by facebook and other companies
- Free software (BSD3 license)
- Can treat various programming languages (Java/Android,C++,C,Objective-C)

Infer: History

- Basis: The research tools Smallfoot, Space Invader and Abductor
- 2009 Cristiano Calcagno, Dino Distefano and Peter O'Hearn founded Monoidics, where first version of infer was developed
- 2013 Monoidics bought by Facebook
- 2015 Facebook opensourced Infer

Possible applications of Infer

Infer contains several checkers including:

For all supported languages

- Detect null dereferenciations
- Detect resource leaks

For C\C++\Objective C

- Detect memory leaks

For C++

- Detect out of bound array access
- Detect if an assigned value is never used

And many more

Usage of Infer

For compilable code, basically following steps

- Write compilable code
- Apply Infer to the code
- Adapt Code
- Start again with the analysis (only changed Code has to be re-analysed)

Examples

- NullPointerExceptions
- Checking for null
- Resource Leaks

NullPointerException Detection Examples

- Infer can check for NullPointerException
- Example 1: possible intra procedural NPE is detected
  Reason: If args is empty array ⇒ str is null
- Example 2: possible inter procedural NPE is detected
  Reason: If args is empty array ⇒ foo returns null

NullPointerException Detection Examples

- Example 3: Model for the class ClassFromLib
- Without model: infer would detect an error
- With model: no error is reported
- Example 4: input can be null ⇒ possible dereferenciation of null.

NullPointerException Real World Example

- Example 5: illustration of large scale application of Infer
- If cursor at line 488 is empty, null is returned.
- Therefore at line 867 feedItemSelected is called with null.
- At line 486 null is dereferenced
- Also problems arising from the interaction of several procedures can be detected.

Checking for null

Infer is capable of various null checks:

- Check if fields that shall not be null get assigned to null.
- Check if fields that shall not be null are not initialised
- Check if methods return null although they should not.
- Check for overannotation with nullable
- Nullable annotations of subclass do not fit to annotations of superclass
- ...

Checking for null Examples

- Example 6: The argument of foo can be null but str shall not be null
- Example 7: str shall not be null but is not initialised.
- Example 8: foo can return null although it should not.

Checking for resource leaks

- Infer can check if resources are not closed.
- Example 9: The InputStream is not closed.
- Example 10: The InputStream is possibly not closed.

memory leaks in C++

- Infer can check for memory leaks in C/C++ or Objective C
- C/C++ analyser of infer did not work for me, therefore only few examples.
- Example 11: Infer should detect a memory leak
- Example 12: Infer should not detect a memory leak

Theoretical foundations - Separation Logic

- Allows to prove $s, h \models P$, s store, h heap P assertion
- Logical assertions
    - Predicate logic
    - New constructs (e.g. separating conjunction $*$)
- $s, h \models P * Q$ iff $s, h1 \models P$ and $s, h2 \models Q$
- For reasoning about program: extension of hoare logic
- Additional special inference rules

Theoretical foundations - Bi-Abduction

- Basic Problem: Find so called antiframe and frame s.t. $A * \mathit{antiframe} \vdash B * \mathit{frame}$ is valid.
- Detection of missing heap (antiframe) required for a specification
- Provides way to infer pre/postconditions (we need to know specifications of sub parts)

References

- Cristiano Calcagno and Dino Distefano. “Infer: An Automatic Program Verifier for Memory Safety of C Programs”. In: *NASA Formal Methods: Third International Symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011. Proceedings*. Ed. by Mihaela Bobaru et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 459–465. ISBN: 978-3-642-20398-5. DOI: 10.1007/978-3-642-20398-5_33. URL: https://doi.org/10.1007/978-3-642-20398-5_33.

- Cristiano Calcagno, Dino Distefano, and Peter O'Hearn. *Open-sourcing Facebook Infer: Identify bugs before you ship*. URL: https://code.facebook.com/posts/1648953042007882/open-sourcing-facebook-infer-identify-bugs-before-you-ship/ (visited on 11/23/2017).
- Facebook Open Source. *Getting started with Infer*. URL: http://fbinfer.com/docs/getting-started.html (visited on 11/23/2017).
- Facebook Open Source. *Infer Installation*. URL: https://github.com/facebook/infer/blob/master/INSTALL.md#pre-compiled-versions (visited on 11/23/2017).

Thank you for your attention!