



R2Fix: Automatically Generating Bug Fixes from Bug Reports



Chen Liu, **Jinqiu Yang**, Lin Tan
University of Waterloo

Munawar Hafiz
Auburn University

Motivation

- Developers often need to fix more bugs than time and resources allow [AnvikOOPSLA'05].
 - Mozilla bug database
 - 670,359 bug reports totally since 1998
 - 135 new bug reports daily on average
- The current bug-fixing process is manual.

Manual Bug Fixing Process

A Linux Kernel Bug Report

Bug 11975 - [linux/net/mac80211/debugfs_sta.c:202]: Buffer overrun

Description: **The trailing zero ('\0') will be written to state[4] which is out of bound.**

Buggy Code the Bug

```
char state[4];  
+++ b/net/mac80211/debugfs_sta.c  
@@ -199,7 +199,7 @@  
if (tid_static_rx[tid_num] == 1) {  
-    strcpy(state, "off");  
+...    strcpy(state, "off");
```

Remove the space character

Difficult & Time-Consuming to Fix Bugs

- Bugs take years to be fixed on average [EyolfsonMSR'11, KimMSR'06, ...].
- Developers spend almost half of their time fixing bugs [LaTozaCSE'06].

Ideal Goal vs. Realistic Goal

- Automatically generate patches for all bugs?
 - Only 17% - 34% of bug reports are fixed.
 - Some fixes are too complex.
- What about relatively simple bugs?
 - They cause security vulnerabilities.
 - Automatically fixing them will save developers' time and efforts.

Idea & Contribution

- R2Fix leverages past **fix patterns, machine learning, and program analysis** to automatically generate patches from free-form bug reports.
 - **57** correct patches generated, **5** for open unfixed bug reports (**4** accepted by the developers) in Linux, Mozilla and Apache
- Shorten bug-fixing time by **63** days
- Save developers' time and effort in fixing bugs
- R2Fix patches are never applied until confirmed by developers.

Fixes Have Common Patterns

- Allocate a longer buffer
- Assign fewer bytes to a buffer
- Modify the bound check condition

Fixed By



Bug Type	Linux	Mozilla
Overflow	86.6%	48.5%
Null Pointer	61.9%	70.0%
Memory Leak	53.8%	27.3%

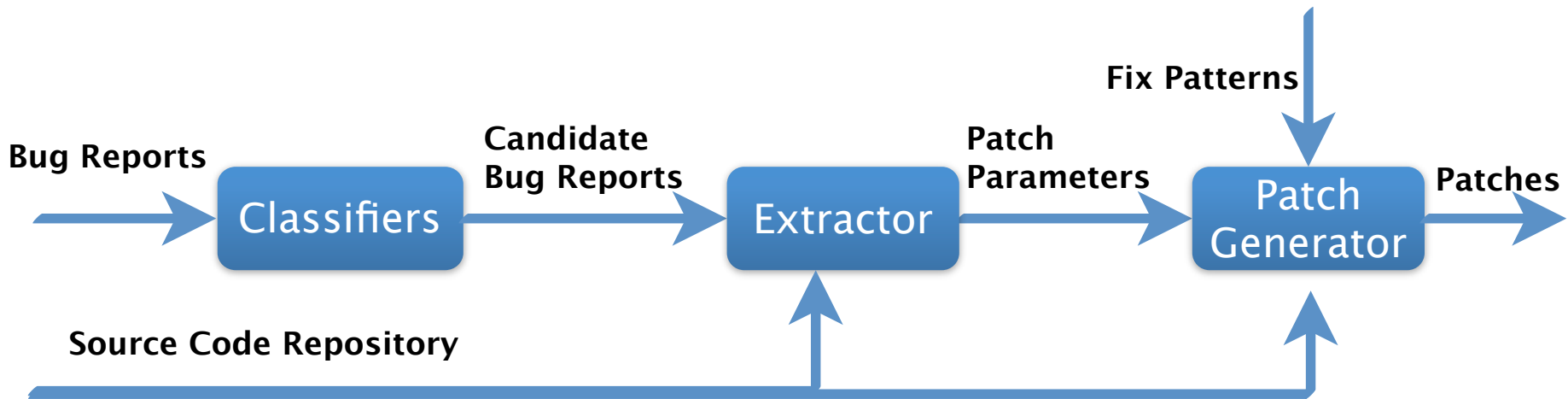
Check our paper for more fix patterns

Fix Pattern Examples

Pattern	Subpattern	Parameters
Overflow (6) FewerByte	<ul style="list-style-type: none">- sprintf(BUF, FMT, EXPR);+ snprintf(BUF, sizeof(BUF), FMT, EXPR);	none
NullPtr (): AddCheck	<ul style="list-style-type: none">+ if (PTR) FNC (... , PTR , ...);	FNC & PTR

Check our paper for more fix patterns

R2Fix Architecture



Classifiers

- Grep does not work.
- Applying machine learning outperforms Grep.

	Precision	Recall
Grep	19%	60%
Bayes	100%	65%

Extractor

- Two types of patch parameters to extract
 - Generic parameters: version, file name
 - Bug-type-specific information
 - For overflows: buffer names, buffer lengths, bound check condition

Patch Generator

- Fix patterns are applied to the target file:

R2Fix:

Bug 11975 - [linux/net/mac80211/debugfs_sta.c:202]: Buffer overrun
Description: The trailing zero ('\0') will be written to state[4] which is out of bound.

Developer:

equivalent

```
- strcpy(state, "off_");  
+ strcpy(state, "off");
```

Pattern	Subpattern	Param
Overflow: FewerByte	<pre>- strcpy(BUF, EXPR); + strncpy(BUF, EXPR, sizeof(BUF));</pre>	none

Evaluation Method

Software	LOC	Bug Reports	Fixed Bug Reports	Open Bug Reports
Linux	11.9M	16.4K	5.5K	2.6K
Mozilla	5.0M	599.8K	189.1K	67.1K
Apache	0.3M	5.4K	0.9K	1.0K

- Evaluated for three bug types:
 - Buffer Overflows, Null Pointer Bugs and Memory Leaks

Results

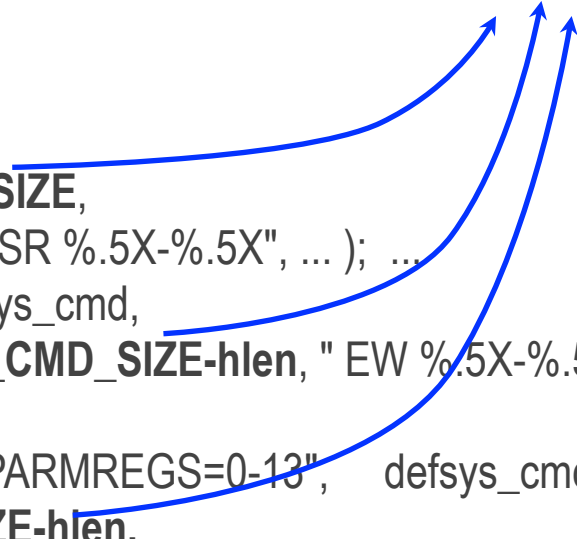
Bug Type	Candidate	Sample	Patched	Verifiable	Correct Patch	Patch Precision	Patches/Bug
Overflow	176	176	33	27	20	74.1%	1.1
NullPtr	1,284	327	31	29	19	65.5%	1.8
Leak	2,167	316	24	24	18	75.0%	1.3
Total	3,627	819	88	80	57	71.3%	1.3

- Generates **5** patches for unfixed bug reports (**4** accepted & committed by developers so far)
- Fixes **3** confirmed security vulnerabilities
- R2Fix patches are never applied until confirmed by developers.
- Could shorten bug fixing time by **63** days on average

A Complex Patch Example

```
--- a/arch/s390/kernel/early.c
+++ b/arch/s390/kernel/early.c
+ int hlen;...
+ char defsys_cmd[DEFSYS_CMD_SIZE]; ...
- sprintf(defsys_cmd,
+ hlen = snprintf(defsys_cmd, DEFSYS_CMD_SIZE,
    "DEFSYS %s 00000-%.5X EW %.5X-%.5X SR %.5X-%.5X", ... ); ...
- sprintf(defsys_cmd, "%s EW %.5X%.5X", defsys_cmd,
+ hlen += snprintf(defsys_cmd+hlen, DEFSYS_CMD_SIZE-hlen, " EW %.5X-%.5X",
    sinitrd_pfn, einitrd_pfn); ...
- sprintf(defsys_cmd, "%s EW MINSIZE=%.7iK PARMREGS=0-13", defsys_cmd,
+ snprintf(defsys_cmd+hlen, DEFSYS_CMD_SIZE-hlen,
    " EW MINSIZE=%.7iK PARMREGS=0- 13", min_size); ...
```

Control the number of
characters copied



The patch has already been **confirmed and committed** by the Linux kernel developers after we reported it.

Initial Developer Feedback

- Q-1: Would a patch automatically generated by R2Fix save developers' time in fixing the bug?
- Q-2: Would a patch automatically generated by R2Fix prompt a quicker response to the bug report?

Developers Find R2Fix Useful

- 4 of 7 developers answered that R2Fix can save their time in
 - Understanding the bug
 - Fixing the bug
- 6 of 7 developers agreed that they would respond quicker to a bug report with a R2Fix-generated patch attached.

Related Work

- Fault repair
 - Fix a faulty program by modifying the program to satisfy the violated specifications or test cases [AcurilCSE'08]
 - R2Fix does not require specifications or test cases.
- Failure diagnosis and fault localization
 - Find root causes and diagnostic information [ClauselCSE'10]
 - R2Fix takes the diagnosis process one step further.

Conclusions

- R2Fix automatically generates patches from bug reports written in natural language.
 - Generates 57 correct patches (5 for unfixed bug reports; 4 are accepted and committed)
- Shortens bug-fixing time by 63 days
- Saves developers' time and effort in fixing bugs