Impact of Tool Support in Patch Construction
Anil Koyuncu, Tegawendé F. Bissyandé, Dongsun Kim, Jacques Klein, Martin Monperrus, Yves Le Traon

To cite this version:

HAL Id: hal-01575214
https://hal.archives-ouvertes.fr/hal-01575214
Submitted on 18 Aug 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Impact of Tool Support in Patch Construction

Anil Koyuncu
SnT, University of Luxembourg - Luxembourg

Tegawendé F. Bissyandé
SnT, University of Luxembourg - Luxembourg

Jacques Klein
SnT, University of Luxembourg - Luxembourg

Dongsun Kim
SnT, University of Luxembourg - Luxembourg

Martin Monperrus
Inria, University of Lille - France

Yves Le Traon
SnT, University of Luxembourg - Luxembourg

ABSTRACT

In this work, we investigate the practice of patch construction in the Linux kernel development, focusing on the differences between three patching processes: (1) patches crafted entirely manually to fix bugs, (2) those that are derived from warnings of bug detection tools, and (3) those that are automatically generated based on fix patterns. With this study, we provide to the research community concrete insights on the practice of patching as well as how the development community is currently embracing research and commercial patching tools to improve productivity in repair. The result of our study shows that tool-supported patches are increasingly adopted by the developer community while manually-written patches are accepted more quickly. Patch application tools enable developers to remain committed to contributing patches to the code base. Our findings also include that, in actual development processes, patches generally implement several change operations spread over the code, even for patches fixing warnings by bug detection tools. Finally, this study has shown that there is an opportunity to directly leverage the output of bug detection tools to readily generate patches that are appropriate for fixing the problem, and that are consistent with manually-written patches.

CCS CONCEPTS
-Software and its engineering → Software maintenance tools;
  Software configuration management and version control systems;
  Software version control;

KEYWORDS
Repair, Debugging, Patch, Linux, Empirical, Tools, Automation

1 INTRODUCTION

Patch construction is a key task in software development. In particular, it is central to the repair process when developers must engineer change operations for fixing the buggy code. In recent years, a number of tools have been integrated into software development ecosystems, contributing to reducing the burden of patch construction. The process of a patch construction indeed includes various steps that can more or less be automated: bug detection tools for example can help human developers characterize and often localize the piece of code to fix, while patch application tools can systematize the formation of concrete patches that can be applied within an identified context of the code.

Tool support however can impact patch construction in a way that may influence acceptance or that focuses the patches to specific bug kinds. The growing field of automated repair [20, 24, 29, 33], for example, is currently challenged by the nature of the patches that are produced and their eventual acceptance by development teams. Indeed, constructed patches must be applied to a code base and later maintained by human developers.

This situation raises the question of the acceptance of patches within a development team, with regards to the process that was relied upon to construct them. The goal of our study is therefore to identify different types of patches written by different construction processes by exploring patches in a real-world project, to reflect on how program repair is conducted in current development settings. In particular, we investigate how advances in static bug detection and patch application have already been exploited to reduce human efforts in repair.

We formulate research questions for comparing different types of patches, produced with varying degrees of automation, to offer to the community some insights on i) whether tool-supported patches can be readily adopted, ii) whether tool-supported patches target specific kinds of bugs, and iii) where further opportunities lie for improving automated repair techniques in production environments.

In this work, we consider the Linux operating system development since it has established an important code base in the history of software engineering. Linux is furthermore a reliable artifact [17] for research as patches are validated by a strongly hierarchical community before they can reach the mainline code base. Developers involved in Linux development, especially maintainers who are in charge of acknowledging patches, have relatively extensive experience in programming. Linux’s development history constitutes a valuable information for repair studies as a number of tools have been introduced in this community to automate and systematize...
various tasks such as code style checking, bug detections, and systematic patching. Our analysis unfolds as an empirical comparative study of three patch construction processes:

- **Process H**: In the first process, developers must rely on a bug report written by a user to understand the problem, locate the faulty part of source code, and manually craft a fix. We refer to it as Process H, since all steps in the process appear to involve human intervention.

- **Process DLH**: In the second process, static analysis tools first scan the source code and report on lines which are likely faulty. Fixing the reported lines of code can be straightforward since the tools may be very descriptive on the nature of the problem. Nevertheless, dealing with static debugging tools can be tedious for developers with little experience as these tools often yield too many false positives. We refer to this process as Process DLH, since Detection and Localization are automated but human intervention is required to form the patch.

- **Process HMG**: Finally, in the third process, developers may rely on a systematic patching tool to search for and fix a specific bug pattern. We refer to this process as Process HMG, since human input is needed to express the bug/fix patterns which are matched by a tool to a code base to generate a concrete patch.

We ensure that the collected dataset does not include patch instances that can be attributed to more than one of the processes described above. Our analyses have eventually yielded a few implications for future research:

**Acceptance of patches**: development communities, such as the Linux kernel team, are becoming aware of the potential of tool support in patch construction i) to gain time by prioritizing engineering tasks and ii) to attract contributions from novice developers seeking to join a project.

**Kinds of bugs**: Tool-supported patches do not target the same kinds of bugs as manual patches. However, we note that patches fixing warnings outputted by bug detection tools are already complex, requiring several change operations over several lines, hunks and even files of code.

**Opportunities for automated repair**: We have performed preliminary analyses which show that bug detection tools can be leveraged as a stepping stone for automated repair in conjunction with patch generation tools, to produce patches that are consistent with human patches (for maintenance), correct (derived from past experience of fixing a specific bug type) and thus likely to be rapidly accepted by development teams.

2 BACKGROUND

Linux is an open-source operating system that is widely used in environments ranging from embedded systems to servers. The heart of the Linux operating system is the Linux kernel, which comprises all the code that runs with kernel privileges, including device drivers and file systems. It was first introduced in 1994, and has grown to over 28 thousand bug reports were filed in the kernel tracking system to report and manage bugs. As of November 2016, over 28 thousand bug reports were filed in the kernel tracking system, with about 6,000 marked as highly severe or even blocking.

The Linux community has also built, or integrated, a number of tools for improving the quality of its source code in a systematic way. For example, The mainline code base includes the coding style checker checkpatch, which was released in July 2007, in Linux 2.6.22. The use of checkpatch is supported by the Linux kernel guidelines for submitting patches, and checkpatch has been regularly maintained and extended since its inception. Sparse is another example of the tools built by Linus Torvalds and colleagues to enforce type checking.

Commercial tools, such as Coverity, also often help to fix Linux code. More recently, researchers at Inria/LiP6 have developed the Coccinelle project for Linux code matching and transformation. Initially, the project was designed to help developers perform collateral evolutions. It is now intensively used by Linux developers to apply fix patterns to the whole code base.

3. **Acceptance of patches**: development communities, such as the Linux kernel team, are becoming aware of the potential of tool support in patch construction i) to gain time by prioritizing engineering tasks and ii) to attract contributions from novice developers seeking to join a project.

2. **Kinds of bugs**: Tool-supported patches do not target the same kinds of bugs as manual patches. However, we note that patches fixing warnings outputted by bug detection tools are already complex, requiring several change operations over several lines, hunks and even files of code.

3. **Opportunities for automated repair**: We have performed preliminary analyses which show that bug detection tools can be leveraged as a stepping stone for automated repair in conjunction with patch generation tools, to produce patches that are consistent with human patches (for maintenance), correct (derived from past experience of fixing a specific bug type) and thus likely to be rapidly accepted by development teams.
3 METHODOLOGY

Our objective is to empirically check the impact of tool support in the patch construction process in Linux. To achieve this goal, we must collect a large, consistent and clean set of patches constructed in different processes. Specifically, we require:

1. patches that have been a-priori manually prepared by developers based on the knowledge of a potential bug, somewhere in the code. For this type of patches, we assume that a user may have reported an issue while running the code. In the Linux ecosystem, such reporters are often kernel developers.
2. patches that have been constructed by using the output of bug finding tools, which are integrated into the development chain. We consider this type of patches to be tool-supported, as debugging tools often provide reliable information on what the bug is (hence, how to fix it) and where it is located.
3. patches that have been constructed, by a tool, based fully on change rules. Such fixes, validated by maintainers, are actually based on templates of fix patterns which are used to i) match (i.e., locate) incorrect code in the project and ii) generate a corresponding concrete fix.

3.1 Dataset Collection

To collect patches constructed via Process H, hereafter referred to as H patches, we consider patches whose commits are explicitly linked to a bug report from the kernel bugzilla tracking system and any other Linux distributions bug tracking systems. We consider that such patches have been engineered manually after a careful consideration of the report filed by a user, and often after a replication step where developers dynamically test the software.

Until Linux 4.8, we have found 5,758 patches fixing defects described in bug reports. Unfortunately, for some of the patches, the link to its bug report in the commit log was not accessible (e.g., because of restriction in access rights of some Redhat bug reports or because the web page was no longer live). Consequently, we were able to collect 4,417 bug patches corresponding to a bug report (i.e., ~77% of H patches). Table 1 provides statistics on the bugs associated with those patches.

Table 1: Statistics on H patches in Linux Kernel.

<table>
<thead>
<tr>
<th>Severity</th>
<th># reports</th>
<th># patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td>965</td>
<td>1,052</td>
</tr>
<tr>
<td>Medium</td>
<td>2,961</td>
<td>3,163</td>
</tr>
<tr>
<td>Minor</td>
<td>138</td>
<td>136</td>
</tr>
<tr>
<td>Enhancement</td>
<td>47</td>
<td>66</td>
</tr>
<tr>
<td>Total</td>
<td>4,351</td>
<td>4,417</td>
</tr>
</tbody>
</table>

First, we note that the severity of most bugs (2,961, i.e., 72.0%) is medium, and H patches have fixed substantially more severe bugs (965, i.e., 23.5%) than minor bugs (138, i.e., 3.3%). Only 47 (1.1%) bug reports represent mere enhancements. Second, exploring the data shows that there is not always a 1 to 1 relationship between bug reports and patches: a bug report may be addressed by several patches, while a single patch may relate to several bug reports. Nevertheless, we note that 4,270 out of 5,265 (i.e., 89%) patches address a single bug report. Third, a large number of unique developers (1,088 out of 18,733= 6.95%) have provided H patches to fix user bug reports. Finally, H patches have touched about 17% (= 9,650/57,195) of files in the code base. Overall, these statistics suggest that the dataset of H patches is diverse as they are indeed written by a variety of developers to fix a variably severe set of bugs spread across different files of the program.

We identify patches constructed via Process DLH, hereafter referred to as DLH patches, by matching in commit logs messages on the form "found by <tool>"8

where <tool> refers to a tool used by kernel developers to find bugs. In this work, we consider the following notable tools, for static analysis:

- **checkpatch**: a coding style checker for ensuring some basic level of patch quality.
- **sparse**: an in-house tool for static code analysis that helps kernel developers to detect coding errors based on developer annotations.
- **Linux driver verification (LDV) project**: a set of programs, such as the Berkeley Lazy Abstraction Software verification Tool (BLAST) that solves the reachability problem, dedicated to improving the quality of kernel driver modules.
- **Smatch**: a static analysis tool.
- **Covexity**: a commercial static analysis tool.
- **Cppcheck**: an extensible static analysis tool that feeds on checking rules to detect bugs.

and for dynamic analysis:

- **Strace**: a tracer for system calls and signals, to monitor interactions between processes and the Linux kernel.
- **Syzkaller**: a supervised, coverage-guided Linux syscall fuzzers for testing untrusted user input.
- **Kasan**: the Linux Kernel Address SANitizer is a dynamic memory error detector for finding use-after-free and out-of-bounds bugs.

After collecting patches referring to those tools, we further check that commit logs include terms "bug" or "fix", to focus on bug fix patches. Table 2 provides details on the distribution of patches produced based on the output of those tools.

Table 2: Statistics on DLH patches in Linux Kernel.

<table>
<thead>
<tr>
<th>Tool</th>
<th># patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkpatch</td>
<td>292</td>
</tr>
<tr>
<td>LDV</td>
<td>220</td>
</tr>
<tr>
<td>Coverity</td>
<td>84</td>
</tr>
<tr>
<td>strace</td>
<td>4</td>
</tr>
<tr>
<td>kasan</td>
<td>1</td>
</tr>
<tr>
<td>total</td>
<td>4,417</td>
</tr>
</tbody>
</table>

Checkpatch and the Linux driver verification project tools are the most mentioned in commit logs. The Covexity commercial tool and the sparse internal tool also helped to find and fix dozens of bugs in the kernel. Finally, we note that static tools are more frequently referred to than dynamic tools.

**HMG patches** in Linux are mainly carried out by Coccinelle, which was originally designed to document and automate collateral evolutions in the kernel source code [35]. Coccinelle is built on an approach where the user guides the inference process using patterns of code that reflect the user’s understanding of the conventions and design of the target software system [23].

Static analysis by Coccinelle is specified by developers who use control-flow sensitive concrete syntax matching rules [9]. Coccinelle provides a language, SmpL9, for specifying search and transformations referred to as semantic patches. It also includes a transformation engine for performing the specified semantic patches. To

8We also use "generated by <tool>" since the commit authors also often refer to warnings as "generated by" a given tool.
9Semantic Patch Language.
avoid confusion with semantic patches in the context of automated repair literature, we will refer to Coccinelle-generated patches as SmPL patches.

```
1 @@
2 expression E;
3 Constant c;
4 type T;
5 @@
6 +kzalloc(sizeof(int), GFP_KERNEL);
7 +kzalloc(sizeof(T), GFP_KERNEL);
8 +kzalloc(sizeof(T), GFP_KERNEL);
9 +kzalloc(sizeof(T), GFP_KERNEL);
10 +kzalloc(sizeof(T), GFP_KERNEL);
11 +kzalloc(sizeof(T), GFP_KERNEL);
```

(a) Example of SmPL templates.

(b) C code matching the template on the left. (iso-kzalloc.c)

Figure 2: Illustration of SmPL matching and patching.

Figure 1 illustrates a SmPL patch example. This SmPL patch is aimed at changing all function calls of kzalloc to kalloc with a reorganization of call arguments. For more details on how SmPL patches are specified, we refer the reader to the project documentation. Figure 2 represents the concrete Unix diff generated by Coccinelle engine and which is included in the patch to forward to mainline maintainers.

```
diff =
--- iso-kzalloc.c
+++ /tmp/cocci-output-52882-062587-iso-kzalloc.c
@@ -1,7 +1,7 @@
0 void main(int i)
1 {
2   type T;
```

Figure 2: Patch derived from the SmPL template in Figure 1a.

In some cases, the fix is not directly implemented in the SmPL patch (which is then referred to as SmPL match). Nevertheless, since each bug pattern must be clearly defined with SmPL, the associated fix is straightforward to engineer. Overall, we have collected 4,050 HMG patches mentioning “coccinelle” or “semantic patch” and applied to C code.

### 3.2 Research Questions

We now enumerate and motivate our research questions in the context of the three processes of patch construction:

**RQ1** How does the developer community react to the introduction of bug detection and patch application tools?

With this research question, we check that the temporal distributions of patches in each patch construction process are in line with the upstream discussions for accepting patches. Such discussions may shed light on the proportions of tool-supported patches that are pushed by developers but that never get into the code base.

**RQ2** Who is using bug detection and patch application tools?

In this research question, we investigate the profile of patch authors in the different patch construction processes.

**RQ3** What is the impact of patch construction process in the stability of patches?

We investigate the stability, i.e., whether or not the patch is reverted after being propagated in the mainline tree, of accepted patches to highlight the reliability of each patch application tool within the community.

---

We have controlled with a random subset of 100 commits that this grep-based approaches yielded indeed only relevant patches constructed by Coccinelle.

```
20We have controlled with a random subset of 100 commits that this grep-based approaches yielded indeed only relevant patches constructed by Coccinelle.

**RQ4** Do the patch construction processes target the same kind of bugs?

We approximate the categorization of bugs with two metrics related to (1) the locality of the fixes as well as (2) the nature and number of change operators of the patch.

### 4 EMPIRICAL STUDY FINDINGS

#### 4.1 Descriptive Statistics on the Data

We first provide statistics on how the different patch construction processes are used by developers over time and across project modules. Temporal distribution of patches may shed some light on the adoption of a patch construction process by kernel maintainers. Spatial distributions on the other hand may highlight the acceptance of a process based on the type (i.e., to some extent the critical nature of the code) to fix.

**Temporal distribution of patches.** We compute the temporal distribution of patches since Linux 2.6.12 (June 2005) until Linux 4.8 (October 2016) and outline them in Figure 3. Note that although Linux 2.6.12 was released in June 2005, a few commit patches in the code base pre-date this release date.

```
Figure 3: Temporal distributions of patches.
```

Overall, H patches are consistently applied over time with approximately 50 fixes per month. DLH patches have been very slow to take up. Indeed, the number of patches built based on bug finding tools has been narrow for several years, with a slight increase in recent years, partly due to the improvements made for reducing false positives. Finally, HMG patches have rapidly increased and now account for a significant portion of patches propagated to the mainline code base.

```
Figure 4: Temporal distributions of DLH patches broken down by tool.
```

Figure 4 represents the detailed temporal evolutions of DLH patches. Checkpatch, after a slow adoption, is now commonly used,
followed by Coverity, which regularly contributes to fix vulnerabilities and common operating system errors. Linux driver verification project tools and Smatch find fewer issues in mainline code base; such tools are indeed extensively used by developers before code is committed in the code base.

**Spatial distribution of patches.** We compute the spatial distribution of patches across Linux sub-systems. Linux Kernel’s code is split into several folders, each roughly containing all code related to a specific sub-system such as file systems, device drivers, architectures, networking, etc. We investigate the scenarios of patches with regards to the folders where the files are changed and the results are shown in Figure 5. Most patches are targeted to device drivers code, and code in early development (i.e., in staging) that is not yet part of the running kernel. It is noteworthy that header code (include), core kernel code (kernel), and to some extent file system code (fs), which have been extensively tested over the years, remain repaired mainly in an all-human process.

Driver code in general, and drivers/staging/ code, in particular, appear to be the place where tool support is most prevalent. Percentages distribution in Figure 5b shows that half (46%) of DLH patches are targeted at staging code. 39% of DLH patches are applied to driver code. Several studies [12, 37, 38] have already shown that driver and staging code contained most kernel errors identified by static analysis tools. Similarly, HMG patches are applied in a large majority in drivers code and staging code.

### 4.2 Acceptance of Patches (RQ1)

We investigate the reaction of the developer community to the introduction of bug finding and patch application tools. To that end, we explore, first, the delays in integrating commits, then, the gaps between the number of patches proposed to the Linux community and those that are finally integrated.

**Delay in commit acceptance.** Kernel patches are change suggestions proposed by developers to maintainers who often need time to review them before propagating the changes to the mainline code base. Thus, depending on several factors—including the criticality of the bug, complexity of the fix, reliability of the suggested fix, and patch quality—there can be a more or less significant delay in commits.

We compute a delay in commit acceptance as the time difference between the author contribution date and the commit date (i.e., when the maintainer propagated the patch to mainline tree). Figure 6 shows the distribution of delays in the three different patch construction processes. Overall, H patches appear to be more rapidly propagated (median = 2 days) than DLH (median = 4 days) and HMG patches (median = 4 days). A patch represents the conclusion of an email exchange between the patch author and the relevant maintainers about the correctness of the proposed change. As the discussion takes place in natural language, it is difficult to categorize how the use of bug finding and patching tools are valued in the process. Nevertheless, we can use the mailing list to study the frequency at which developers specifically mention bug finding tools when a patch is first submitted. Then, we can correlate this frequency on a monthly basis with the corresponding statistics on accepted DLH patches related to the specific tools.

We have crawled all emails archived in the Linux Kernel Mailing List (LKML) using Scrapy. We use heuristics to differentiate message replies from original mail content: we consider lines starting with ‘>’ as part of a previous conversation. Finally, we naively search for the tool name reference in the message text. In total, we crawled 1,601,606 original email messages and 885,814 reply messages.
messages. As examples, we provide in Figures 7a and 7c the distributions per month of the number of patches that were submitted through LKLM mentioning checkpatch or coccinelle respectively, as well as the number of maintainer replies referencing those tools, and the number of related commits accepted into the mainline git tree. To ease observation, we compute in Figures 7b and 7d the integration gap as a percentage between the number of patches submitted to LKLM and the number of patches that are eventually integrated. We draw the slope of the evolution of this gap over time. While checkpatch presents roughly the same gap, the gap is clearly reducing for coccinelle. We have computed the slope for the different sets of tool-supported patches and checked that it was negative for 3 out of 4 of the tools: the gap is thus closing over time for most tool-supported processes.

Tool-supported patches (DLH and HMG alike) have been overall accepted at an increasing rate by Linux developers. Integration of such patches by maintainers remains, however, slower than that of traditional H patches.

### 4.3 Profile of Patch Authors (RQ2)

We investigate the speciality and commitment of developers who rely on patch application and bug finding tools to construct patches. Speciality is defined as a metric for characterizing the extent to which a developer is focused on a specific subsystem. We compute it as the percentage of patches, among all her/his patches, which a developer contributes to a specific subsystem. Thus, speciality is measured with respect to each Linux code directory. We then draw, in Figure 8, the distributions of speciality metric values of developers for the different types of patches: e.g., for an automated patch applied to a file in a subsystem, we consider the commit author speciality w.r.t that subsystem.

**Figure 8: Speciality of developers Vs. Patch types.**

H patches are mostly provided by specialized developers. This may imply that the developers focus on implementing specific functionalities over time. Similarly, DLH patches appear to be mostly applied by specialized developers (even slightly more specialized than those who made H patches). This finding is inline with the requirements for developers to be aware of the idiosyncrasies of the programming of a particular subsystem to validate the warnings of bug detection tools and sift through various false positives to produce patches that are eventually accepted by maintainers. HMG patches, on the other hand, are performed by developers on subsystem code which they are not known to be specialized on.

To measure developer commitment, we follow the approach of Paxil et al. [38] and compute, for each developer, the product of (1) the number of patches (H, DLH or HMG) that have been integrated into Linux and (2) the number of days between the first patch and the last patch. This metric favours both developers who have contributed many patches over a short period of time and developers who have contributed fewer patches over a longer period of time: e.g., a developer who gets 10 commits integrated during one year, will have the same degree of commitment as another developer who gets 40 commits integrated in 3 months.

Developer commitment is studied here as an approximation of developer expertise, since the more a developer works on the Linux project or with a tool, the more expertise the developer may be assumed to acquire (on the Linux project and/or with the use of the tool). Figure 9 shows the distribution of commitment scores of developers for the different types of patches.

**Figure 9: Commitment of developers Vs. Patch types.**

DLH patches are shown to be produced by developers with a more varying degree of commitment (greater standard deviation). The median value of commitment is further lower than the median commitment for HMG patches. Finally, overall, the distributions of commitment values of developers indicate that H patch authors present lesser commitment than HMG patch authors.

We then use Spearman’s ρ [43] to measure the degree of correlation between the commitment of developers and the number of tool-supported patches that they submit. We focus on specialized developers of two very different kinds of code: mature file system (fs) code and early-development (staging) code. The correlation is then revealed to be higher (ρ = 0.42) for staging than for fs (ρ = 0.11). We also note that 64% of developers committing code in staging stick to this part of the code for over half of their contributions. Finally, developers specialized in kernel have never relied on tool support to produce a patch.

Bug detection tools are generally used by developers with (to some extent) knowledge of the code. Patch application tools, on the other hand, enable developers to remain committed to contributing patches to the code base.

### 4.4 Stability of Patches (RQ3)

Although patches are carefully validated before they are integrated to the mainline code base, a patch might be simply incorrect and thus the relevant code may require further changes, or the patch may simply be reverted. However, it is challenging to precisely detect and resolve such a change in recently patched code hunks. Even this requires heuristics that may prove to be error-prone. Thus, in this study, we focus on commits whose reverting is explicit.

It is common for software developers to cancel patches that they hastily committed to the code base. The `git revert` command is an excellent means for developers to roll back their commits. However, given the hierarchical organization in Linux, when a patch has reached the mainline, a simple revert (using `git commands`) is uncommon. The submitting developer (or another one) must write another patch explaining the need to revert. This patch again goes through the process to be accepted in the mainline. In this setting, the revert of a commit is likely strongly justified. We search for

---

16 We considered only tools associated to at least 50 patches.

17 speciality metric value greater than 50%
4.5 Bug Kinds (RQ4)

We study bug kinds in two dimensions: the spread of buggy code and the complexity of the bugs. We investigate the locality of patches as an approximation of the spread of buggy code, and the change operations at the level of Abstract syntax tree nodes modifications to approximate complexity of bugs.

4.5.1 Locality of Patches. The locality of patches is a key dimension for characterizing patches. Patch size has been measured in the literature [8, 38] in terms of the number of code locations that it involves, while several state-of-the-art automated repair approaches mostly focus on single/limited code changes to fix software. The Linux project is a particularly adequate study subject for this comparison since developers are often reminded that they must “solve a single problem per patch”\(^\text{19}\). Fix operations are then generally separated from cosmetic changes.

A bug fix patch may involve changes across files. Figure 11 shows that most fixes are localized to a single file independently of the way they are constructed.

4.5.2 Change Operations in Patches. In general, line-based diff tools, such as the GNU Diff, are limited in the expression of the kinds of changes that can be identified since they consider only adds and removes, but no moves and updates [36]. Thus, to investigate change operations performed by patches, we rely on approaches that compute modifications based on abstract syntax trees (AST) [21]. Such approaches produce fine-grained results at the level of individual nodes. For this study, we consider an extended version of the open-source GumTree [14] with support for the C language [36]. This tool specifically takes into account additions, deletions, updates and moves of individual tree nodes, and has the goal of producing results that are easier for users to understand than those of GNU Diff.

The output of GumTree is an edit script enumerating a sequence of operations that must be carried out on an AST tree to yield the other tree. To that end, GumTree implements a mapping algorithm between the nodes in two abstract syntax trees. This algorithm is inspired by the way developers manually look at changes between two files, first searching for the largest unmodified chunks of code (i.e., isomorphic subtrees) and then identifying modifications (i.e., given two mapped nodes, find descendants that share a large percentage of common mappings, and so on). Given those mappings, GumTree leverages an optimal and quadratic algorithm [11] to

---

\(\text{18}\) We use git show ‘+sha’ | grep -E ‘\(\text{[0-9a-f]}\)+ | commit \(\text{[0-9a-f]}\)+ | \(\text{[0-9a-f]}\)(40)\)+

\(\text{19}\) see Documentation/SubmittingPatches

compute the edit script. More details on the algorithm can be found in the original articles [11, 14].

For simplicity, in this paper, we express change operations in their abstract form as a triplet “scope/element/action” where scope represents the type of node (e.g., the program, an if block, a compound block, a generic list, an identifier, etc.) where the change occurs, element represents the element (e.g., an expression, a declaration, a generic string, a compound block, an if block, etc.) that is changed and action represents the move/update/add/delete operators that are used. This abstract representation indeed does not take into account any variable names and functions involved (and available in the output of GumTree). Figure 16 shows a patch example for a change operation where a new if block code is inserted.

diff --git a/drivers/gpu/drm/i915/intel_display.c b/.../drm/1915/intel_display.c
index 6e0d828..182f849 100644
--- a/drivers/gpu/drm/i915/intel_display.c
+++ b/drivers/gpu/drm/i915/intel_display.c
@@ -13351,6 +13351,9 @@ int intel_atomic_prepare_commit(struct drm_device *dev,
     ret = intel_crtc_wait_for_pending_flips(crtc);
     return ret;
   case DRM_IOCTL_ATOMICnesota_prepare_commit:
-     continue;
-     if (state->legacy_cursor_update)
-         return -EINVAL;
+     continue;
+     if (state->legacy_cursor_update)
+         return -EINVAL;
     state->cursor_info->dont_update.setCursor(crtc, state)
     for_each_crtc_in_state(state, crtc, crtc_state, 1) {
         if (state->legacy_cursor_update)
             continue;
     }
   case DRM_IOCTL_ATOMICiplina_prepare_commit:
     return -EINVAL;
   case DRM_IOCTL_ATOMICleton_commit:
     ret = intel_crtc_wait_for_pending_flips(crtc);

Figure 16: Example of Compound/If: add - Add an if block.

Figure 14 illustrates the distributions of the number of operations that are performed in a patch, to limit the bias of changes that are identically performed in several files (e.g., Coccinelle collateral evolutions), we focus on patches that touch a single file, then on patches that are limited to a single hunk. All distributions are long-tail, revealing that most patches apply very few operations in terms of number and variety. While the three processes have similar average (median) values of change operations performed on a file, HMG patches appear to implement changes with a consistent number of operations (limited standard deviation). On the other hand, when we consider change operations at the hunk level, DLH patches apply fewer operations than HMG patches.

5 DISCUSSIONS

We discuss the implications of our findings for the software engineering research community, in particular, the automated repair field, and enumerate the threats to validity that this study carries.

5.1 Implications

As the field of automated repair is getting mature, the community has started to reflect (i) on whether to build human-acceptable or readable patches [20, 32], (ii) on the suitability of automated repair fixes [41], (iii) on the relevance of patches produced by repair tools [51]. Our work continues this reflection from the perspective of the acceptance of tool-support in patch construction. We further acknowledge that HMG patches considered in this study are not constructed in the same spirit as in automated repair: indeed, automated repair approaches make no a-priori assumption on what and where the fault is, while tools such as Coccinelle [9] produce patches based on fix patterns that match buggy code locations. Nevertheless, given the lack of integration of automated repair in a real-world development process, we claim that investigating Linux patch cases can offer insights which can be leveraged by the research community to understand how the developer community cooperate and collaborate.
can accept tool-supported patches, and the automation of what kind of fixes can be readily accepted in the community.

On manual Vs. tool-supported patches. As illustrated in Section 4.1, tool-supported patch construction is becoming frequently and widely used in the Linux Kernel development. In particular, HMG patches account for a larger portion of recent program changes than H patches. This suggests that both (1) developers gradually accept to use patch application tools such as Coccinelle [9] since they are effective to automatically change similar code fragments and (2) there are many (micro) code clones [46] in the code base. Regarding spatial distribution, DLH and HMG patches are committed to 'staging' (22-47%) while H patches in 'staging' account for only 1%. This may indicate that experimental features have more opportunities for tools to help write bug fixing patches. It implies indeed that, for early development code, the community almost exclusively relies upon tools to solve common bugs (e.g., in relation with programming rules, styles, code hardening, etc.) by novice programmers (i.e., not necessary specialized in kernel code), before expert developers can take over. Thus, reliable automated debugging techniques could be beneficial in a production development chain as debugging aids. This finding comforts the human study recently conducted by Tao et al. [45] which suggested that automated repair tools can significantly help debugging tasks.

On the delay in patch acceptance. We have observed a delay in the acceptance of tool-supported patches by maintainers. However, given the differences in change operations with fully manual patches, it is likely the case that tool-supported patches are fixing less severe bugs, which makes their integration a less crucial issue for maintainers.

Furthermore, negative percentages in evolution gap between submission and acceptance (cf. Figure 7) suggests that there are many HMG patches that are integrated into the mainline code base without being discussed by maintainers. This finding implies that once the fix pattern has been validated, patches appear to be accepted systematically.

On the nature of bugs being fixed. The study of patch locality shows results that are in line with a previous study [51] which revealed that most fix patches only change a single file. Nevertheless, we have found that, in practice, even tool-supported patches, in a large majority, modify several lines to fix warnings by bug detection tools (which, by the way, generally flag a single line in the code). Although patch size does not, by any means, imply ease of realization, our results suggest that there are considerable numbers of repair targets and shapes that automated repair should aim for.

It is also noteworthy that the spread of change operations over several files may carry different implications for the patch construction processes. For example, while a cocinnelle patch may be applying the same change pattern over several files to fix an API function usage, a human patch modifying several files may actually carry data and behavior dependencies among the changes.

5.2 Exploiting Patch Redundancies

A large body of the literature on program repair has discussed findings on the repetitiveness/redundancy of code changes in real-world software development [3, 34]. Unfortunately, such findings are not readily actionable in the context of automated repair since they do not come with insights on how such redundant patches will be leveraged in practice. Indeed, although it is possible to abstract redundant patches to recommend bug fix actions [5], only a few research directions manage to contextualize them, to some extent, for repair scenarios [26]. Actually, researchers discuss such redundancies for enriching the repair space with change operations that are more likely to be appropriate fix operations.

With this study, we see concrete opportunities for exploiting patch redundancies for systematically building patches and applying (or recommending) them to a specific identified and localized buggy piece of code. Indeed, bug detection tools, which are used by various developers who then craft fixes based on specific warnings, and patch application tools, which are based on fix patterns, can be leveraged in an automated repair chain. The former will be used in the bug detection and localization steps while the latter will focus on building concrete patches based on patterns found in a database of human fixes created to address warnings by bug detection tools.

To demonstrate the feasibility of this research direction, we have conducted a study for searching redundancies in patches constructed following warnings by bug detection tools, and investigating the possibility of producing a generic patch which could have been used to derive these concrete patches. Nevertheless, although generic patch inference has been a very fertile research direction in the past [1, 2, 30, 31], we have experimented available tool supports and found that they do not scale in practice. We have thus devised a process to split the set of patches into clusters, each containing patches presenting similar change operations. Figure 17 depicts the overall process. Based on GumTree sequences of change operations, we rely on a sequential pattern mining tool to extract maximal sequential patterns. We use a fast implementation of VMSP [15] to find recurrent change patterns at the level of the abstract change operations expressed in Section 4.5. Then, we build clusters of patches based on the elicited patterns, and leverage SpDiff [1] to attempt the inference of a unique SmPL patch which could instantiate the common redundant concrete repair actions performed in the patches.

With this process, starting with a set of 571 DLH patches, we were able to build 37 clusters based on change operations patterns. Among the clusters, 10 led to the generation of a common generic patch. We then manually investigated the commit messages associated with the patches in clusters that produced a generic patch, and found that they indeed largely dealt with the same bug type. This final check confirms, to some extent, the potential to collect fix patterns from human repair processes to build an automated repair chain leveraging bug detection tools.
5.3 Threats to Validity

We have identified the following threats to validity to our study:

*External validity* – We focus on Linux only. It is, however, one of the largest development projects, one of the most diverse in terms of developer population, with a significant history for observing trends, and implementing strict patch submission guidelines that try to systematize the tracking of change information. To the best of our knowledge, Linux is the best candidate for observing various patch construction processes, as it encourages the use of tools for bug detection and patching.

*Construct validity* – We rely on a number of heuristics to collect and process our datasets. We have nevertheless, by design, chosen to be conservative in the way we collect patches in each process with the objective of having reliable and distinctive sets for each process, to further enable replication.

*Internal validity* – The metrics that we leverage to elicit the differences among the different processes may lead to biased results. However, those metrics were also used in the literature.

6 RELATED WORK

6.1 Program Repair

6.1.1 *Studies on Human-Generated Patches.* Studies on patches, generated by human developers, focus on investigating existing patches fully written by developers (i.e., H patches) rather than devising a new technique. Pan et al. explored syntactic bug fix patterns in seven Java projects [39]. This study extracted 27 bug fix patterns. Martinez and Monperrus identified common programrepair actions (patterns) [27], and Zhong and Su reported statistics on 9,000 real bug fixing patches collected from Java open source projects [51]. These studies examined features of real bug fixes against whether automated repair techniques can be applied to those bugs. In addition, Barr et al. formulated a hypothesis called “plastic surgery hypothesis” [3]. They studied how many changes can be graftable by using snippets that can be found in the same code base where the changes are made.

6.1.2 *Studies on Tool-aided Patches.* As discussed in Sections 1 and 3, generating tool-aided patches indicates that developers create program patches with an aid of tools, rather than generating patches from scratch. Tao et al. supposed that automated repair tools can provide aids to debugging tasks [45]. They adopted Par [20] as a patch recommendation tool and gave patches generated by the tool to experiment participants. The findings include that automatically generated patches can significantly help debugging tasks. MintHint [18] is a semi-automatic repair technique, which can help developer find correct patches. This technique does statistical correlation analysis to locate program expressions likely to perform repaired program executions.

6.1.3 *Automated Patch Generation.* Generating patches with automated tools implies minimizing a developer’s effort in debugging. It often indicates that fully automated procedures including fault localization, code modification, and patch verification. Recent endeavors achieved an impressive progress as follows.

Weimer et al. [48] proposed GenProg, an automatic patch generation technique based on genetic programming [22]. This technique randomly mutates buggy statements to generate several different program variants that are potential patch candidates. In 2012, the authors extended their previous work by adding a new mutation operation, replacement and removing the switch operation [24]. SemFix [33] leverages program synthesis to generate patches. The technique assumes that buggy predicates are an unknown function to be synthesized. The technique is successful for several bugs, but it is only applicable to “one-line bug”, in which only one predicate is buggy. DirectFix [28] and Angelix [29] extended SemFix so that it can generate patches for bugs in larger and complex (w.r.t the search space) programs in a simpler way. PAR [20] automatically generates patches by using fix patterns learned from human-written patches. This technique is inspired by the fact that patches are redundant.

6.2 Patch Acceptability

Fry et al. conducted a human study to indirectly measure the quality of patches generated by GenProg by measuring patch maintainability [16]. They presented patches to participants and asked maintainability related questions developed by Sillito et al. [40]. They found that machine-generated patches [24] with machine-generated documents [10] are comparable to human-written patches in terms of maintainability. PAR [20] is presented to deal with nonsensical patches. The approach generates patches based on fix patterns, which are learned from human-written patches. The fix patterns generalize common repair actions from more than 60,000 real bug fixes enabling PAR to avoid generating nonsensical patches.

6.3 Program Matching and Transformation

SYDIT [30] automatically extracts an edit script from a program change. In its scenario, a user must specify the program change to extract the edit script from. Coccinelle [9], on the other hand, directly lets the user specify the edit script in a user-friendly language, and performs the transformation by matching the change pattern with code context. It has been used in several debugging tasks in the literature [4–7, 37]. LASE [31] differs from SYDIT as it can generate a generalized edit script based on multiple changes of Java programs. Another approach in this direction is SpDiff [1, 2] supports the extraction of a subset of common changes (i.e., SmPL patches that are fed to Coccinelle) from several concrete patches.

7 CONCLUSION

We have studied the impact of tool support in patch construction, leveraging real-world patching processes in the Linux kernel development project. We investigated the acceptance of tool-supported patches in the development chain as well as the differences that may exist in the kinds of bugs that such patches fix in comparison with traditional all-hand written patches. We show that in the Linux ecosystem, bug detection and patch application tools are already heavily used to unburden developers, and already enable relatively complex repair schema, contrasting with a number of repair approaches in the state-of-the-art literature of automated repair. An artefact dataset on this study is available at https://goo.gl/f1mRMM.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their helpful comments and suggestions. This work was supported by the Fonds National de la Recherche (FNR), Luxembourg, under projects RECOMMEND C15/IS/10449467 and FIXPATTERN C15/IS/9964569.

