

Homework 7

ECE 590: Towards More Reliable Software

Jeff Fan || zf70@duke.edu
February 27, 2024

Question 1:

Project/Repository: Linux Kernel

Issue 218173-Kernel 6.6 onwards hangs on "loading initial ramdisk" [1]

Classification: NAM-ENV

Justification:

Bug Activation: The issue's activation seems to depend on the system's environment, including the kernel version (6.6 onwards) and possibly specific hardware configurations, rather than a specific sequence of operations.

Error Propagation: The failure, characterized by the system hanging during the boot process, indicates that the bug's impact is immediate upon encountering the specific environmental conditions rather than following a sequential order of operations.

Failure Occurrence: The consistent reproducibility of the failure across various configurations underlines the environmental dependency of the bug, reinforcing the NAM-ENV classification. This perspective is supported by the bug manifesting in relation to environmental factors such as kernel version and hardware interactions, rather than a fixed sequence of events.

Issue 89611 - Kernel Panic in b44 Driver [2]

Classification: NAM-SEQ

Justification:

Bug Activation: This issue is activated by a specific sequence of network traffic patterns, which indicates that the sequencing (or relative order) of operations is crucial for the fault to manifest. This aligns with the NAM-SEQ classification, where the activation and/or error propagation is influenced by the sequencing of operations.

Error Propagation: The error's propagation through the system until it causes a kernel panic suggests a complex interplay that is dependent on the order in which

network traffic is processed by the b44 driver. This complexity and sequence dependency further support the NAM-SEQ classification.

Failure Occurrence: The failure, a kernel panic, occurs in a nondeterministic manner but is closely tied to the sequence and nature of network operations rather than environmental factors, timing of inputs, or a time lag between activation and failure. This specificity to operational sequences justifies the classification as NAM-SEQ, emphasizing the critical role of the operation order in triggering the bug.

Issue 53031 - kswapd in uninterruptible sleep state [3]

Classification: ARB-MEM

Justification:

Bug Activation: This issue is activated under conditions where the system's memory usage approaches a critical level, specifically when the page cache fills up while a significant amount of free memory (about 150MB, presumed to be the high watermark) still remains. This scenario indicates a gradual accumulation of memory usage leading to the problem, which is a hallmark of aging-related bugs, particularly those affecting memory management (ARB-MEM).

Error Propagation: The error propagates through the system's memory management subsystem, with kswapd entering an uninterruptible sleep state and failing to free up memory as would normally be expected. This behavior suggests that the system's ability to manage memory effectively degrades over time, leading to a situation where critical processes become unresponsive.

Failure Occurrence: The failure manifests as a significant system slowdown or potential unresponsiveness, given that kswapd is a critical kernel thread responsible for managing memory swapping. This problem directly impacts the system's performance and stability, aligning with the characteristics of an ARB-MEM, where memory resources are not managed or freed correctly, leading to system degradation over time.

Issue 211585 - Laptop hangs on second suspend unless a file is written to second disk - Intel Core i7-5500U Acer Aspire R13 [4]

Classification: BOH

Justification:

Bug Activation: The issue occurs consistently on the second suspend attempt, indicating a deterministic pattern rather than being influenced by timing or environmental factors.

Error Propagation: The behavior of the laptop hanging on the second suspend

is deterministic and not influenced by external factors or variations in system state. It consistently occurs regardless of system configuration or usage.

Failure Occurrence: The problem manifests consistently on the second suspend attempt, suggesting a systematic flaw rather than variability in timing or environment.

In summary, the behavior of the laptop hanging on the second suspend appears to be a deterministic flaw in the system's power management behavior, unaffected by environmental or timing factors. Therefore, it aligns with the classification of a Bohrbug (BOH).

Project/Repository: MySQL

Issue 71204 - Timing for stages in P_S is different from what SHOW PROFILE reports [5]

Classification: NAM-TIM

Justification:

Bug Activation: The bug is triggered when there is a discrepancy between the timing for stages in Performance Schema (P_S) and what SHOW PROFILE reports. This indicates that the bug's activation is closely associated with timing discrepancies between these two mechanisms for profiling.

Error Propagation: The error likely propagates within the mechanisms responsible for profiling and timing measurement within MySQL. It may involve discrepancies in how timing data is collected, processed, and reported by Performance Schema and SHOW PROFILE.

Failure Occurrence: The failure occurs consistently when comparing the timing data reported by Performance Schema with that reported by SHOW PROFILE. This indicates that the bug's manifestation is predictable and reproducible when analyzing performance data through these two mechanisms.

Given that the bug's activation is directly related to timing discrepancies between Performance Schema and SHOW PROFILE, its error propagation likely involves mechanisms responsible for timing measurement and reporting within MySQL, and its occurrence is consistent and reproducible when analyzing performance data, it aligns with the NAM-TIM classification. This classification signifies that the bug's behavior is influenced by timing issues in performance profiling mechanisms within MySQL.

Issue 2261 - Can't use @user_variable as FETCH target in stored procedure [6]

Classification: NAM-ENV**Justification:**

Bug Activation: The bug is triggered when attempting to use @user_variable as a FETCH target in a stored procedure. This indicates that the bug's activation is closely tied to environmental conditions, specifically the usage of user-defined variables within stored procedures.

Error Propagation: The error likely propagates within the stored procedure execution context and is limited to the scope of FETCH operations involving @user_variables. There is no indication that this error affects other parts of the system or propagates beyond the stored procedure.

Failure Occurrence: The failure occurs consistently when attempting to use @user_variable as a FETCH target in stored procedures. This indicates that the bug's manifestation is predictable and reproducible within the specific context of stored procedure execution.

Given that the bug's activation is closely tied to the usage of user-defined variables within stored procedures, its error propagation is limited to the scope of FETCH operations, and its occurrence is consistent and reproducible within the stored procedure context, it aligns with the NAM-ENV classification. This classification signifies that the bug's behavior is influenced by environmental conditions, specifically the usage of @user_variables within stored procedures.

Issue 107991 - Clone_persist_gtid causes memory leak [7]**Classification: ARB-MEM****Justification:**

Bug Activation: The bug is activated when using the Clone_persist_gtid function, which causes a memory leak. Specifically, the memory leak occurs within this function, indicating that the bug's activation is associated with memory management processes rather than environmental conditions or specific sequences of actions.

Error Propagation: The error likely propagates within the Clone_persist_gtid function and potentially affects other memory-related operations within the code-base. Memory leaks typically propagate as the program executes, consuming memory resources and potentially leading to system instability or crashes.

Failure Occurrence: The failure occurs gradually over time as the Clone_persist_gtid function is repeatedly used without proper memory deallocation. This gradual accumulation of memory leaks may lead to system instability or performance degradation, depending on the frequency and intensity of function usage.

Given that the bug's activation is related to memory management processes,

its error propagation involves the gradual accumulation of memory leaks within the function and potentially throughout the codebase, and its failure occurrence is characterized by gradual system degradation over time, it aligns with the ARB-MEM classification. This classification indicates that the bug is aging-related and primarily affects memory management within the system.

Issue 86043 - Can't use BigInt or Double as userId instead of Int32 (default) [8]

Classification: BOH

Justification:

Bug Activation: The fault is activated when attempting to use BigInt or Double as the userId instead of the default Int32 type. This activation is consistent and does not vary over time or with environmental factors.

Error Propagation: The error propagation is stable and consistent. It does not change its behavior over time or with changes in the system environment.

Failure Occurrence: The occurrence of the issue is predictable and reproducible under specific conditions. It does not exhibit variability in behavior or timing.

Given these characteristics, the issue aligns with the definition of a Bohrbug.

Project/Repository: Apache

Issue 68661 - Memory leak in load_install_path() in jlibtool.c [9]

Classification: ARB-MEM

Justification:

Bug Activation: The bug is triggered by the execution of the load_install_path() function in jlibtool.c. Specifically, it involves a memory leak within this function, indicating that the bug's activation is associated with memory management processes rather than environmental conditions or specific sequences of actions.

Error Propagation: The error likely propagates within the load_install_path() function and potentially affects other memory-related operations within the codebase. Memory leaks typically propagate as the program executes, consuming memory resources and potentially leading to system instability or crashes.

Failure Occurrence: The failure occurs gradually over time as the load_install_path() function is repeatedly executed without proper memory deallocation. This gradual accumulation of memory leaks may lead to system instability or performance degradation, depending on the frequency and intensity of function execution.

Given that the bug's activation is related to memory management processes, its error propagation involves the gradual accumulation of memory leaks within the function and potentially throughout the codebase, and its failure occurrence is characterized by gradual system degradation over time, it aligns with the ARB-MEM classification. This classification indicates that the bug is aging-related and primarily affects memory management within the system.

Issue 63666 - Should take the OS buffers into account when timing lingering [10]

Classification: NAM-TIM

Justification:

Bug Activation: The bug is triggered by the timing mechanism concerning the lingering of connections, specifically concerning the consideration of OS buffers. This indicates that the bug's activation is associated with timing aspects rather than environmental conditions or sequential actions. Therefore, it aligns with the NAM-TIM classification.

Error Propagation: The error propagates as a result of incorrect timing calculations related to lingering connections, specifically due to the failure to consider OS buffers. This implies that the bug's error propagation is tied to timing intricacies within the system rather than environmental dependencies or sequential events.

Failure Occurrence: The failure occurs due to incorrect timing calculations regarding connection lingering, particularly the lack of consideration for OS buffers. This failure pattern is indicative of a timing-related issue rather than one stemming from environmental constraints or specific sequences of actions. Hence, it supports the classification of NAM-TIM, emphasizing the timing aspect of the bug's manifestation and propagation.

Issue 63716 - mod_proxy_uwsgi: No support for UNIX sockets [11]

Classification: BOH

Justification:

Bug Activation: The bug involves the absence of support for UNIX sockets in mod_proxy_uwsgi. This indicates that the bug is not related to timing issues, environmental conditions, or specific sequences of actions. Instead, it is a fundamental limitation in the functionality of the module.

Error Propagation: The error is likely confined to the functionality of mod_proxy_uwsgi itself. There is no indication that this issue propagates errors to other parts of the system or affects the behavior of other modules or components.

Failure Occurrence: The failure occurs consistently whenever users attempt to use UNIX sockets with `mod_proxy_uwsgi`. This indicates that the bug's manifestation is predictable and not sporadic.

Given that the bug is not related to timing, environmental conditions, or complex error propagation patterns, and its occurrence is consistent and not sporadic, it aligns with the characteristics of a Bohrbug (BOH). This classification indicates that the issue is a fundamental flaw in the system rather than being related to aging, complexity, or environmental dependencies.

Issue 39725 - `mod_rewrite`'s RewriteMap directive does not expand back-references in lookup keys [12]

Classification: NAM-SEQ

Justification:

Bug Activation: The bug is triggered when using `mod_rewrite`'s RewriteMap directive without the expansion of back-references in lookup keys. This indicates that the bug's activation is related to the sequence of actions performed when utilizing the RewriteMap directive without proper expansion of back-references.

Error Propagation: The error likely propagates within the `mod_rewrite` module, affecting the lookup process in RewriteMap directives. It does not seem to spread beyond the scope of `mod_rewrite` or affect other components in the system.

Failure Occurrence: The failure occurs consistently when attempting to use RewriteMap directives without expanding back-references in lookup keys. This indicates that the bug's manifestation is predictable and reproducible.

Given that the bug's activation is associated with the specific sequence of actions performed when using `mod_rewrite`'s RewriteMap directive, its error propagation seems contained within the module, and its occurrence is consistent and reproducible, it aligns with the NAM-SEQ classification. This classification indicates that the bug's behavior is influenced by the sequence of actions performed rather than environmental conditions or timing issues.

Reference:

- [1] https://bugzilla.kernel.org/show_bug.cgi?id=218173
- [2] https://bugzilla.kernel.org/show_bug.cgi?id=89611
- [3] https://bugzilla.kernel.org/show_bug.cgi?id=53031
- [4] https://bugzilla.kernel.org/show_bug.cgi?id=218530
- [5] <https://bugs.mysql.com/bug.php?id=71204>
- [6] <https://bugs.mysql.com/bug.php?id=2261>
- [7] <https://bugs.mysql.com/bug.php?id=107991>
- [8] <https://bugs.mysql.com/bug.php?id=86043>
- [9] https://bz.apache.org/bugzilla/show_bug.cgi?id=68661
- [10] https://bz.apache.org/bugzilla/show_bug.cgi?id=63666
- [11] https://bz.apache.org/bugzilla/show_bug.cgi?id=63716
- [12] https://bz.apache.org/bugzilla/show_bug.cgi?id=39725