

Projekt wdrożeniowy – Intel SIMICS fuzz testing w RISC-V

Tomasz Jaworski

<tomasz.jaworski@student.put.poznan.pl>

Piotr Kaszubski

<piotr.kaszubski@student.put.poznan.pl>

Karol Kiedrowski

<karol.kiedrowski@student.put.poznan.pl>

Mikołaj Załęski

<mikolaj.zaleski@student.put.poznan.pl>

kod źródłowy: <https://github.com/RoyalDonkey/put-intel-fuzzing>

Styczeń 2025

Contents

1	Opis problemu	3
2	Autorzy	5
3	Rozwiązanie – koncepcja	6
4	Rozwiązanie – implementacja	7
4.1	Linux	7
4.1.1	Sterownik	7
4.1.2	External Buildroot Toolchain	7
4.1.3	Modyfikacja Device-Tree	7
4.1.4	Overlay dla Buildroot	8
4.1.5	Budowanie systemu	8
4.1.6	Dodawanie systemu do SIMICS	8
4.2	SIMICS (i jego konfiguracja)	8
4.2.1	Dodawanie urządzenia	8
4.2.2	Skrypt inicjujący platformę	8
4.2.3	Python MAGIC hook	9
4.3	Kompilacja programu	9
4.4	Uruchomienie platformy (demonstracja działania)	9
5	Napotkane problemy	11
5.1	Wczesne podejście z LD_PRELOAD	11
5.2	Nadpisanie funkcji ze statycznie linkowanej biblioteki	11
5.2.1	Modyfikacja ELF	11
5.2.2	Trampolina	12
6	Kierunki Rozwoju	13
6.1	Bare-metal	13
6.2	Fuzzing	13

1 Opis problemu

Fuzzing Problem dotyczył fuzzingu, czyli metody testowania oprogramowania polegającej na celowym generowaniu niepoprawnych, lub pół-poprawnych danych wejściowych przez osobny program (tzw. fuzzer). Tak wygenerowane dane są następnie podawane do testowanego programu, w celu sprowokowania nieprawidłowego działania. Fuzzery są w zasadzie programami szukającym nowych danych do korpusu testowego.

Fuzzing jest gorącym tematem, który rozwija się prężnie od kilku dekad. Obecnie większość projektów i firm dużej skali takich jak jądro Linux, Microsoft, Google, etc. stosuje fuzzing z wielkim powodzeniem, ponieważ te narzędzia wykrywają błędy, które bardzo trudno jest zauważyć gołym okiem lub przy użyciu tradycyjnych metod takich jak testy jednostkowe.

Sanitizery Aby fuzzing był skuteczny do wdrożenia na dużą skalę, potrzebne są narzędzia do analizy poprawności stanu testowanego programu, aby umożliwić automatyczne wykrycie, kiedy fuzzer znalazł podatność. Jedną z klas takich narzędzi są sanitizery pamięci. Na potrzeby tego projektu istotny jest jeden konkretny sanitizer, czyli ASAN.

ASAN monitoruje stan pamięci testowanego programu w trakcie jego wykonywania i natychmiast zawiadamia o błędach (np. przepełnienie bufora), jeśli takowe wystąpią. Taka analiza jest możliwa, ponieważ instrukcje ASANa są bezpośrednio wkompilowane w testowany program (tak zwana “instrumentalizacja” programu). Testowany program funkcjonalnie pozostaje niezmieniony, ale na każdym kroku ma wbudowane dodatkowe sprawdzenia odczytów, zapisów, alokacji i zwalniania pamięci.

ASAN jest w sporej części po prostu biblioteką napisaną w C (libasan.so – na systemach Linux). W kompilatorze GCC, po instrumentalizacji testowanego programu, jest on zlinkowany dynamicznie z tą biblioteką. Zatem, aby uruchomić testowany program, system operacyjny musi znaleźć tę zależność.

Problem Istotą naszego zadania było znalezienie metody na przeprowadzenie fuzzingu programów na systemach wbudowanych bądź bare-metal, wewnątrz emulatora Intel SIMICS. Testowanie w takich warunkach jest z wielu powodów trudniejsze. W naszej pracy pomijamy element fuzzera i skupiamy się na sanitizerze.

Na szczególną uwagę zasługuje bare-metal, na którym jest zupełny brak systemu operacyjnego, więc nie ma możliwości nawet podejrzenia komunikatów printowanych przez ASANa. Aby umożliwić testowanie ASANem na bare-metal, konieczne jest utworzenie kanału komunikacji między nim a SIMICSem, tj. chcemy, aby każda wiadomość od ASANa, która klasycznie wylądowałaby na standardowym

wyjściu programu, była dostępna jako string w skrypcie SIMICSowym. Brzmi to abstrakcyjnie, bo takie jest. Zasadniczo, to jest największy problem projektu i cała nasza praca głównie sprowadziła się do tego zadania.

Dodatkowe założenia Dla uproszczenia, całą pracę wykonaliśmy w środowisku Linux na RISC-V (64-bit). Dołożyliśmy starań, aby nasze rozwiązanie było kompatybilne z ideą bare-metal, ale byliśmy zbyt ograniczeni czasowo, aby przeprowadzić na nim testy.

2 Autorzy

Piotr Kaszubski – Lider zespołu, organizacja repozytorium, przydzielanie zadań, zgłębianie teorii fuzzowania, dokumentacji ASANa i SIMICSa, znalezienie funkcji i pierwsza implementacja mechanizmu, eksperymenty z linkowaniem statycznym, pomysł i implementacja ostatecznej metody z łączeniem plików obiektowych, poprawki do tworzenia regionu pamięci w SIMICSie, modyfikacje sterownika dla urządzenia znakowego, kompilacja skrośna na RISC-V, finalna wersja, eksperymenty z w GCC, napisanie MAGIC hooka do SIMICSa, przeprowadzenie demo i prezentacji, dokumentacja.

Tomasz Jaworski – Tworzenie notatek z cotygodniowych spotkań, zaznajamianie się z dokumentacją SIMICS, stworzenie buforu pośredniczącego pomiędzy emulowanym systemem a emulatorem (przygotowanie sterownika dla urządzenia znakowego i modyfikacja device tree), dokumentacja.

Karol Kiedrowski – Zebranie informacji dotyczących działania sanitizera, przetestowanie jego działania, a także napisanie wstępnej logiki funkcji.

Mikołaj Załęski – Pierwsze badania nad przechwyceniem wyjścia z biblioteki ASAN, pomysł na mechanizm.

3 Rozwiązanie – koncepcja

Celem jest przesył wiadomości ASANa do SIMICSa.

Ogólny zamysł

- SIMICS utworzy dodatkowy region pamięci, który posłuży jako bufor do komunikacji. ASAN będzie tam wpisywał informacje, a SIMICS czytał.
- ASAN nie potrafi printować do osobnego pliku, logu, ani niczego podobnego. Musimy więc mieć sposób na odfiltrowanie jego wiadomości od pozostałych "śmieci", które potencjalnie może printować testowany program. W tym celu nadpiszemy jedną z funkcji w , która jest wywoływana w momencie printowania przez ASANa, i wstrzykniemy tam kod, który będzie pisał do regionu pamięci SIMICSa.
- SIMICS musi wiedzieć, kiedy powinien odczytać coś z pamięci i potraktować jako wiadomość. W tym celu użyjemy jego funkcji "MAGIC instructions". Nasz kod wstrzyknięty w ASANa skorzysta z MAGIC aby wysyłać powiadomienia do SIMICSa.

Szczegóły

- W przypadku Linuxa, potrzebna jest modyfikacja device tree, aby zawiadomić jądro o istnieniu dodatkowego regionu pamięci.
- Jeśli nasz testowany program przebywa w userspace, nie jest możliwe bezpośrednie pisanie do regionu pamięci. Konieczne jest napisanie modułu, który umożliwi interakcję z tym regionem. W naszym przypadku mamy moduł, który wystawia proste urządzenie znakowe.
- W SIMICSie, konieczne będzie napisanie hooka, który nasłuchuje MAGIC instructions i odczytuje pamięć.

4 Rozwiązanie – implementacja

Nasze rozwiązanie obejmuje platformę symulacyjną w SIMICS z systemem Linux oraz programem skompilowanym z sanitizерem. Do programu celowo wprowadziliśmy błędny dostęp do pamięci:

4.1 Linux

4.1.1 Sterownik

Napisaliśmy prosty sterownik (moduł jądra Linux) do obsługi bufora na wyjście sanitizera. Moduł ten pozwala nam na wpisywanie ciągów znaków do zdefiniowanego przez nas obszaru pamięci w celu ich późniejszego odczytania przez emulator SIMICS.

4.1.2 External Buildroot Toolchain

Stworzyliśmy external toolchain w Buildroot w celu budowania naszego modułu dla jądra Linuxa wraz z obrazem systemu. Nasz system dla SIMICSa jest zdefiniowany następującym defconfigiem:

4.1.3 Modyfikacja Device-Tree

Do drzewa urządzeń dodaliśmy własne urządzenie (`simics_shm`), które jest buforem pamięci. Adres `0x20000000` został dobrany ręcznie pod platformę SIMICSa, na której się opieraliśmy (brak kolizji z innymi regionami pamięci). Rozmiar `0x4000` odpowiada 4 KiB i został uznany jako wystarczająco duży, by pomieścić printy ASANa (największe, które zaobserwowaliśmy, miały około 1 KiB).

Następnie zmodyfikowane drzewo urządzeń budujemy do postaci binarnej, poleceniem

4.1.4 Overlay dla Buildroot

Overlay w Buildroot do dołączania programów lub plików do platformy docelowej do systemu plików. Wydał nam się najszybszym sposobem na statyczne osadzenie naszego programu w systemie. Głównie dlatego, że go już znaliśmy.

4.1.5 Budowanie systemu

Budowaliśmy system Linux, jak już wcześniej wspomniano korzystając z Buildroota i dodając mu odpowiednie flagi służące do obsługi externala oraz overlay'a.

4.1.6 Dodawanie systemu do SIMICS

Wgranie zbudowanego systemu do platformy emulowanej można wykonać poprzez (i tak to zrobiliśmy) linkowanie plików wynikowych z budowania systemów w Buildroot do folderu targets w platformie risc-v-simple w SIMICS, wykonaliśmy to poleceniem:

Dzięki temu nasza platforma po przebudowaniu będzie widoczna w aktualnej wersji z poziomu SIMICS, bez potrzeby ponownego kopiowania plików.

4.2 SIMICS (i jego konfiguracja)

4.2.1 Dodawanie urządzenia

Aby dodać urządzenie w emulatorze, aby adresy pamięci podane w naszym sterowniku były poprawnie interpretowane przez SIMICS i jądro Linuxa, stworzyliśmy każdorazowo obiekt:

4.2.2 Skrypt inicjujący platformę

Aby nie podawać za każdym razem kilku komend związanych z utworzeniem obiektu naszej pamięci oraz ładowania platformy, napisaliśmy skrypt:

4.2.3 Python MAGIC hook

Napisaliśmy też skrypt w języku python do uruchamiania w SIMICS, aby przechwytywać MAGIC instructions. Konwencjonalnie przyjęliśmy, że naszym będzie .

4.3 Kompilacja programu

ASAN wywołuje wewnętrznie funkcję za każdym razem, kiedy printuje informację dotyczącą błędów pamięciowych. Aby nadpisać tę funkcję, definiujemy ją po swojemu w :

Nasza wersja funkcji otwiera wpisuje do urządzenia znakowego, które tworzy `simics_shm`, a następnie emituje MAGIC instruction, dając SIMICSowi znak, że może odczytać zawartość.

Trik obiektowy Aby nadpisać funkcję bez ingerencji w kod źródłowy testowanego programu, kompilujemy testowany program do pliku obiektowego, kompilujemy do pliku obiektowego, następnie łączymy dwa pliki obiektowe w jeden, i dopiero ten wynikowy linkujemy z ASANem:

Dzięki tej kolejności, uniemożliwiamy ASANowi zdefiniowanie swojej wersji , ponieważ byłoby to powieleniem symbolu.

4.4 Uruchomienie platformy (demonstracja działania)

1. Budowanie systemu
2. Budowanie aplikacji z sanitizerek ()
3. Uruchomienie SIMICS, a w emulatorze:
 - (a) Ładujemy platformę ()
 - (b) Uruchamiamy system ()
 - (c) Uruchamiamy skrypt Python ()
 - (d) Tworzymy urządzenie znakowe ()

```

Edit View Settings
This frame has 1 object(s):
[ 602.552920] simics_shm: Device open!
[ 602.553220] simics_shm: Device write! (count=82, offset=0)
[ 602.553620] simics_shm: Device close!
[32, 52] 'a' (line 3) <== Memory access at offset 56 overflows this variable
602.554020] simics_shm: Device open!
[ 602.554320] simics_shm: Device write! (count=114, offset=0)
[ 602.554720] simics_shm: Device close!
HINT: this may be a false positive if your program uses some custom stack unwind
mechanism, swapcontext or vfork
[ 602.555420] simics_shm: Device write! (count=52, offset=0)
[ 602.555820] simics_shm: Device close!
SUMMARY: AddressSanitizer: stack-buffer-overflow src/bad.c:4 in main
Shadow bytes around the buggy address:
0x003fb41ffd00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb41ffe00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb41ffe80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb41fff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb41fff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x003fb4200000: f1 f1 f1 f1 00 00 04[f3]f3 f3 f3 00 00 00 00 00 00
0x003fb4200080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb4200100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb4200180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb4200200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x003fb4200280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
[ 602.562420] simics_shm: Device open!
[ 602.562820] simics_shm: Device write! (count=1390, offset=0)
[ 602.563320] simics_shm: Device close!
fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
[ 602.564420] simics_shm: Device open!
[ 602.564820] simics_shm: Device write! (count=17, offset=0)
[0m
Container[ 602.565320] simics_shm: Device close!
overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
==145==ABORTING
#

asan:
asan: #0 0xea6a0 in main src/bad.c:4
asan: #1 0x3fb5ec8ce (/lib64/libc.so.6+0x2b0ce)
asan: #2 0x3fb5ec9ba in __libc_start_main (/lib64/libc.so.6+0x2b9ba)
asan: #3 0x269f2 in _start (/root/bad+0x269f2)
asan:
asan: Address 0x003fb4200038 is located in stack of thread T0
asan: at offset 56 in frame
asan:
asan: #0 0xea560 in main src/bad.c:2
asan:
asan: This frame has 1 object(s):
asan:
asan: [32, 52] 'a' (line 3) <== Memory access at offset 56 overflows this variable
asan:
asan: HINT: this may be a false positive if your program uses some custom stack unwind
mechanism, swapcontext or vfork
asan:
asan: (longjmp and C++ exceptions *are* supported)
asan:
asan: SUMMARY: AddressSanitizer: stack-buffer-overflow src/bad.c:4 in main
asan:
asan: Shadow bytes around the buggy address:
asan: 0x003fb41ffd00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb41ffe00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb41ffe80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb41fff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb41fff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: =>0x003fb4200000: f1 f1 f1 f1 00 00 04[f3]f3 f3 f3 00 00 00 00 00 00
asan: 0x003fb4200080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb4200100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb4200180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb4200200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: 0x003fb4200280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
asan: Shadow byte legend (one shadow byte represents 8 application bytes):
asan: Addressable: 00
asan: Partially addressable: 01 02 03 04 05 06 07
asan: Heap left redzone: fa
asan: Freed heap region: fd
asan: Stack left redzone: f1
asan: Stack mid redzone: f2
asan: Stack right redzone: f3
asan: Stack after return: f5
asan: Stack use after scope: f8
asan: Global redzone: f9
asan: Global init order: f6
asan: Poisoned by user: f7
asan: Container overflow: fc
asan: Array cookie: ac
asan: Intra object redzone: bb
asan: ASan internal: fe
asan: Left alloca redzone: ca
asan: Right alloca redzone: cb
asan:
asan: ==145==ABORTING
asan:
running>

```

Figure 1: Końcowy rezultat projektu - uruchomiony SIMICS, w nim Linux i nasz program z sanitizerek. Widać, że print sanitizera udało się przenieść do terminala z emulatorem

(e) Uruchamiany program ()

(f) Obserwujemy wyniki (Figure 1)

5 Napotkane problemy

5.1 Wczesne podejście z LD_PRELOAD

Pierwszym pomysłem na nadpisanie funkcji było napisanie dynamicznej biblioteki definiującej tę funkcję, a następnie wywołanie testowanego programu ze zmienną

Ta metoda działa i jej największą zaletą jest to, że z , tak długo jak mamy program zlinkowany dynamicznie z , nie potrzebujemy dostępu ani do żadnych źródeł ani plików obiektowych. Niestety, są też wady, które dyskwalifikują to rozwiązanie:

1. Metoda jest uzależniona od mechanizmu systemu operacyjnego i nie działałaby na bare-metal.
2. Konieczne jest przeniesienie na platformę wraz z programem testowym oraz ustawienie , zatem potencjalnie musimy ingerować w skrypty uruchamiające program.
3. Metoda polega na dostępności na platformie. Na okrojonych instalacjach Linux, ta biblioteka najprawdopodobniej nie będzie istnieć, zatem pojawia się konieczność dostarczenia jej wraz z programem. Jest to szczególnie uciążliwe, jeśli platforma stoi na nietypowej architekturze, bo trzeba znaleźć odpowiednią wersję i mieć nadzieję, że nie będzie żadnych niekompatybilności między nią a dynamicznie zlinkowanym programem testowym (co nie jest oczywiste np. w przypadku różnic w wersjach kompilatora).

5.2 Nadpisanie funkcji ze statycznie linkowanej biblioteki

Zanim wpadliśmy na pomysł połączenia dwóch plików obiektowych w jeden przed linkowaniem, rozważaliśmy sposoby na nadpisanie funkcji **po** linkowaniu.

W grę wchodzi dwa fundamentalne podejścia: modyfikacja funkcji wewnątrz pliku binarnego (przyjmijmy ELF), lub nadpisanie adresu funkcji w trakcie wykonywania programu (tzw. "trampolina").

5.2.1 Modyfikacja ELF

W teorii, posiadając skompilowany plik binarny który nie został strip'owany, powinno być możliwe znalezienie miejsca, gdzie zapisane są instrukcje i podmiana ich na własną definicję. W praktyce, nie znaleźliśmy narzędzi, które w łatwy sposób umożliwiałyby zrobienie czegoś takiego. Co więcej, nawet gdyby

takie narzędzie istniało, zapewne byłoby bardzo specyficzne dla danej architektury lub formatu ELF i nie byłoby dostatecznie uniwersalne, aby umożliwić testowanie na wielu różnych platformach.

5.2.2 Trampolina

Nie ingerując w plik binarny, można rozważyć podejście dynamiczne: załadowanie do pamięci własnej implementacji, a następnie sprytna podmiana wszystkich skoków pamięci do oryginalnej wersji na nasz własny adres.

Takie metody się stosuje i można znaleźć nawet przykłady w internecie. Przeważnie polegają na napisaniu biblioteki dynamicznej z funkcją inicjalizacji (w GCC), która wykorzystuje `__builtin_offsetof` aby znaleźć adres funkcji, którą chcemy podmienić, a następnie wpisuje w odpowiednie miejsca (w pamięci) instrukcje assemblera do skoku pod inny adres.

Problem tych metod jest taki, że są bardzo mało uniwersalne, wymagają pisania kodu pod konkretną architekturę, przeważnie polegają na dynamicznym ładowaniu bibliotek (a zatem niekompatybilne z bare-metal) i nie należą do łatwych w implementacji. Dodatkowo mogłyby być blokowane przez zabezpieczenia sprzętowe typu NX bit.

6 Kierunki Rozwoju

Dalszą pracę, jaką można byłoby wykonać, można podzielić na dwa główne zadania.

6.1 Bare-metal

Jako pierwszy kierunek dalszego rozwoju projektu, należy wymienić zbudowanie programu i uruchomienie go bez systemu operacyjnego (czyli bare-metal). Wymagałoby to standardowych kroków dla takiej implementacji oprogramowania, a następnie, wykorzystując m.in. już wcześniej opisaną przez nas metodę kompilacji z sanitizmem programów statycznie, stworzenia pliku z kodem maszynowym, który mógłby wykonać procesor.

6.2 Fuzzing

Drugim kierunkiem niewątpliwie jest dodanie fuzzera do aplikacji, którą chcielibyśmy testować. Program ten powinien przyjmować jakieś wejście od użytkownika, a następnie przetwarzać je, aby możliwym było prześledzenie, czy program zachowuje się prawidłowo.