

# Bypassing memory safety mechanisms through speculative control flow hijacks

Andrea Mambretti<sup>1,2</sup>, Alexandra Sandulescu<sup>1</sup>, Alessandro Sorniotti<sup>1</sup>,  
William Robertson<sup>2</sup>, Engin Kirda<sup>2</sup>, and Anil Kurmus<sup>1</sup>

<sup>1</sup>IBM Research – Zurich, Rüschlikon, Switzerland  
{asa, aso, kur}@zurich.ibm.com

<sup>2</sup>Northeastern University, Boston, USA  
{mbr,ek,wkr}@ccs.neu.edu

## Abstract

The prevalence of memory corruption bugs in the past decades resulted in numerous defenses, such as stack canaries, control flow integrity (CFI), and memory safe languages. These defenses can prevent entire classes of vulnerabilities, and help increase the security posture of a program. In this paper, we show that memory corruption defenses can be bypassed using speculative execution attacks. We study the cases of stack protectors, CFI, and bounds checks in Go, demonstrating under which conditions they can be bypassed by a form of speculative control flow hijack, relying on speculative or architectural overwrites of control flow data. Information is leaked by redirecting the speculative control flow of the victim to a gadget accessing secret data and acting as a side channel send. We also demonstrate, for the first time, that this can be achieved by stitching together multiple gadgets, in a speculative return-oriented programming attack. We discuss and implement software mitigations, showing moderate performance impact.

## 1 Introduction

Memory corruption vulnerabilities have plagued the computer security field for more than 30 years. Multiple ways of exploiting memory bugs have surfaced, requiring controls to be placed at different levels in the software stack: mechanisms such as stack canaries and control flow integrity have been designed and deployed as a mitigation in existing software, while new languages were designed with memory safety to close this class of bugs in new programs [26, 29].

Meanwhile, a new class of attacks, transient execution attacks [6], and more specifically speculative execution attacks [5, 14, 16, 17, 20, 22, 25] have been the subject of intense scrutiny. The ensuing vulnerabilities appear difficult to mitigate without considerable performance trade-offs, leading to the conclusion that speculative execution attacks will remain a problem for the foreseeable future, and therefore a possibly fruitful area of research [23].

A natural question to ask is whether the advent of transient execution attacks has changed the security stance of modern computing systems against memory corruption attacks: does the security of memory safety mechanisms, such as stack smashing protection (SSP), control flow integrity (CFI), and those embedded in memory safe languages, hold in the post-spectre threat model?

In this paper, we show that multiple memory safety mechanisms that would otherwise successfully prevent exploitation of vulnerabilities can be speculatively bypassed to perform arbitrary memory reads. Because these attacks require a combination of techniques, we show that they do not apply to all memory safety mechanisms and a careful, case-by-case analysis is necessary.

At a high level, these attacks work by overwriting, either architecturally or speculatively, a backwards or forward edge, followed by the use of speculative code reuse attacks to leak data. In all cases this overwrite achieves a speculative control flow hijack, i.e., a redirection of the speculative control flow to an attacker-chosen arbitrary address. One case of such an attack is the *speculative buffer overflow* discovered by Kiriansky and Waldspurger [14], where a return address is speculatively overwritten.

We demonstrate that SSP, GCC’s vtable verification (VTV), and Go’s runtime memory safety checks are all vulnerable. In particular, we develop an end-to-end proof-of-concept attack in the case of SSP, where the mitigations against a stack-based buffer overflow in `libpng` can be speculatively bypassed to read arbitrary bytes from the victim program. This attack additionally leverages a last level cache (LLC) eviction attack to extend the speculative execution window, and a speculative return-oriented programming (ROP) attack to achieve a Flush+Reload side channel by reusing 5 gadgets from the victim program. Both components of the attack are not specific to SSP and generalise beyond our selected use case. Our results show that, while such end-to-end attacks are not trivial to mount, they still represent a viable attack vector. For this reason we evaluate countermeasures for each attack scenario, showing how mitigations can be both effective and viable

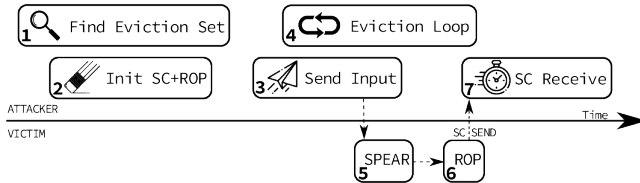
from a performance standpoint.

This paper makes the following contributions:

- Demonstration of PoC attacks against SSP-based buffer overflow mitigations, GCC VTable Verification (VTV) and against Go’s array bounds checks.
- Demonstration of an LLC eviction attack without knowledge of physical addresses.
- Demonstration of the use of multiple ROP gadgets (and the necessary condition for such attacks) for exploiting speculative control flow hijacks.
- Proposals of improved mitigations, withstanding speculative execution attacks, together with a performance evaluation.

## 2 Speculative execution attacks on memory safety mechanisms

In this section we describe end-to-end speculative execution attacks on abstracted memory safety mechanisms. We begin with a high level overview of the various components necessary to perform such an end-to-end attack. We then proceed to analyse the class of speculative control flow hijacks which is at the heart of the attack; we refer to this general category of attacks as SPEculative ARchitectural control flow hijacks, or SPEAR, and detail them in Section 2.1. Furthermore, we analyse the eviction mechanism in Section 2.2, and the speculative ROP in Section 2.3.



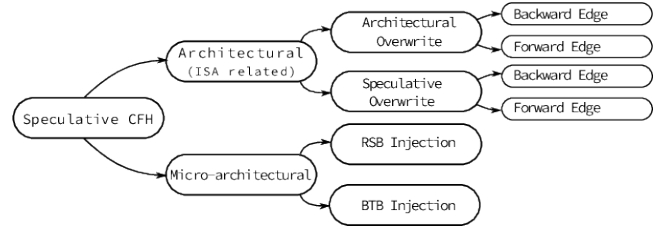
**Figure 1:** Overview of speculative attack against memory safety mechanisms.

Figure 1 shows an overview of the steps required to perform an end-to-end attack. The attack has a preparation phase (steps 1 and 2), where eviction sets (to ensure the existence of a suitably long speculation window) are identified, memory used by the side channel is created and initialised, and ROP gadgets are primed in the instruction cache. The attacker then submits an input to the victim in step 3, crafted to trigger a violation of a memory safety property. We assume that traditional exploitation of the violation is prevented by a suitable memory safety mechanism. However, the attacker uses a speculative execution attack to bypass the mechanism by overwriting (architecturally or speculatively) control-flow data, and obtaining a speculative control flow hijack (step 5). As a result, the victim is tricked into executing a side-channel

send of attacker-chosen memory in step 6: this is achieved with the ROP component, which reuses code snippets from the victim program, appropriately selected and primed in the initialisation phase. The attacker can then execute the corresponding side-channel receive in step 7. The success rate of the attack is increased by concurrently executing an eviction loop to lengthen the speculation window (step 4) by carefully finding eviction sets for selected data.

### 2.1 SPEAR attacks

A SPEAR-vulnerable code sequence is a code sequence that results in a speculative control flow hijack. A speculative control flow hijack allows an attacker to gain control of the target program’s speculatively-executed code. This is a powerful primitive: an attacker can follow such an attack with a speculative ROP sequence to speculatively execute code sequences that access a secret and send it to the attacker via a side channel.



**Figure 2:** Overview of various Speculative control flow hijacking attacks

Figure 2 shows a breakdown of the various instances in the SPEAR attack class in the context of different variants of speculative control flow hijacks. Classic speculative control flow hijack attacks can be performed through micro-architectural components such as the Branch Target Buffer (BTB) and Return Stack Buffer (RSB) [16, 17, 20]. At the same time, the speculative control flow can also be influenced by instruction sequences that only affect architectural components, such as registers or memory: we refer to these as SPEAR attacks. For instance, executing the `call %rbx x86` instruction speculatively, when the value of `%rbx` is available at execution time will result in speculative execution continuing at the address in the `%rbx` register. Therefore, if the `%rbx` register can be controlled by the attacker, a speculative control flow hijack can occur. This control by the attacker can either be architectural or speculative, as we will see next.

Similarly, a `push %rbx; ret` instruction sequence with the register value available would also simply continue execution at the provided address, with no need to predict where speculative execution continues via the RSB. Hence, SPEAR-vulnerable code patterns can concern both forward edges (`jmp` and `call`) and backward edges (`ret`).

The SPEAR categorisation offers us a convenient way to reason on attacks triggered by a control flow data overwrite.

The classification covers all attack scenarios studied in this paper, namely, speculative bypass of memory safety mechanisms; the classification also covers other known attacks, such as the speculative overwrite of a backward edge [14], and the speculative bypass of manually-inserted array bounds checks in C/C++ [8].

### 2.1.1 Architectural overwrite

The case where an attacker controls the control-flow-influencing register architecturally, i.e., via the Instruction Set Architecture (ISA), is closely related to traditional memory corruption attacks. These attacks can nowadays be mitigated by mechanisms such as stack smashing protection (SSP) and, in general, CFI implementations that check the validity of control flow metadata before control flow is transferred, thus detecting and preventing outcomes induced by attacker-controlled overwrites. SPEAR architectural overwrite attacks focus on the opportunity that the attacker has to speculatively bypass the checks introduced by these mitigations.

```

1 ;Copy of RET Value
2 mov rax,[rsp]
3 mov [stored_ret], rax
4
5 ;Architectural Overwrite
6 ; (Attacker Controlled)
7 mov rax, [target]
8 mov [rsp], rax
9
10 ;Evict RET Value Copy
11 clflush [stored_ret]
12 lfence
13
14 ;Backward Edge Integrity Check
15 ; (Speculation Trigger)
16 mov rax, [rsp]
17 cmp rax, [stored_ret]
18 jne my_exit
19
20 ;Backward Edge Hijack
21 ret

```

Listing 1: Architectural backward edge overwrite

We provide in Listing 1 and Listing 2 two snippets of code that illustrate the forward and backward edge cases for architectural overwrites. The structure of both cases is similar: the original value of the edge (line 3) is preserved in a safe location, after which, we assume that the architectural overwrite is performed (line 8) with an attacker-controlled value (e.g. through a buffer overflow). Afterwards, the program executes an integrity check on the forward or backward edge (line 17) before performing the control flow transfer (e.g. SSP or CFI check). To increase the success rate of the attack we try to maximize the speculation window caused by the integrity check, for instance by causing the eviction of its reference value – in the snippet, this step is captured by a `clflush` instruction (line 11). If the CPU mispredicts the outcome of the check, it might execute either a `ret` (backward

Family	Architectural		Speculative	
	Fwd	Bwd	Fwd	Bwd
Intel Broadwell	99.5	94.9	99.5	98.7
Intel Skylake	97.6	98.3	98.2	92.1
Intel Coffee Lake	99.8	98.1	99.7	99.4
Intel Kabylake	99.5	95.9	100	99.5
AMD Ryzen	100	100	100	100

**Table 1:** Success rate (in percentage) for architectural or speculative overwrites of backward and forward edges performed on various architectures families

edge) or a `call` (forward edge) which will transfer the control towards the attacker-controlled value used in the architectural overwrite (line 21).

```

1 ;Copy of Target Value
2 mov rax, [orig_target]
3 mov QWORD[stored_target], rax
4
5 ;Architectural Overwrite
6 ; (Attacker Controlled)
7 mov rax, [hijacked_target]
8 mov QWORD[target], rax
9
10 ;Evict Target Value Copy
11 clflush [stored_target]
12 lfence
13
14 ;Forward Edge Integrity Check
15 ; (Speculation Trigger)
16 mov rax, QWORD[target]
17 cmp rax, QWORD[stored_target]
18 jne my_exit
19
20 ;Forward Edge Hijack
21 call QWORD[target]

```

Listing 2: Architectural forward edge overwrite

We follow the methodology of Mambretti et al. [21] and test the snippet using the Speculator tool [9], which aids the detection of speculative control flow transfers by using performance monitor counters (PMC) and *speculation markers*. Results show that on every CPU tested, control flow is indeed speculatively transferred to the overwritten location, thereby bypassing the checks during speculative execution. As shown in Table 1, speculative control flow hijacks are observed at least 95% of the time for Listing 1 and 97% of the time for Listing 2 on all tested architectures. We thus conclude that SPEAR attacks with architectural overwrites can result in speculative control flow hijacks. In Section 3.1 and Section 3.2, we further analyze SPEAR architectural overwrites of backwards edges (for stack canaries) and forward edges (for CFI).

### 2.1.2 Speculative overwrite

Alternatively, the attacker may control the control-flow-influencing register speculatively. This means that in a first

phase, speculative execution is triggered (for example by a conditional branch). In a second phase, the attacker speculatively influences the control flow edge, thus hijacking speculative control flow. The control-flow-influencing value may be the result of a load from an address that is generated during the speculative execution phase, or it may be loaded from a location that is speculatively overwritten by a preceding store operation, resulting in speculative store-to-load forwarding.

We provide in Listing 3 and Listing 4 the two snippets of code that illustrate the backward and forward edge cases for speculative overwrites. Both cases share the same structure. First speculative execution is triggered by a condition (line 2). Then, the speculative overwrite is performed through some instruction within the speculated part of the code. Here, the value used for the overwrite is under the control of the attacker (line 7). Finally, the overwritten value is used for control flow transfer allowing the attacker to hijack the speculative control flow (line 10).

Similarly to the architectural overwrite case, experiment results in Table 1 show that for the backward edge case the success rate is at least 92% while it is at least 98% for the forward edge case: speculative overwrites are feasible and lead to speculative control flow hijack provided that a sufficiently large speculation window exist during which the edge is overwritten, and later dereferenced.

```

1 ;Speculative execution trigger
2 ...
3
4 ;Speculative Overwrite
5 ; (Attacker Controlled)
6     mov rax, QWORD[target]
7     mov QWORD[rsp], rax
8
9 ;Backward Edge Hijack
10    ret

```

Listing 3: Speculative backward edge overwrite

```

1 ;Speculative execution trigger
2 ...
3
4 ;Speculative Overwrite
5 ; (Attacker Controlled)
6     mov rax, [hijacked_target]
7     mov QWORD[target], rax
8
9 ;Forward Edge Hijack
10    call QWORD[target]

```

Listing 4: Speculative forward edge overwrite

## 2.2 Speculative window and eviction

We now focus on an important requirement for SPEAR attacks: the existence of a speculation window to permit the execution of the control flow transfer and the side channel send operation, a common requirement for all speculative execution attacks. This requires a speculative execution trigger, i.e., an instruction that causes a wide-enough window

of dependent instructions that are executed but not retired, awaiting the retirement of the initial instruction. This is usually achieved when the process accesses uncached data: the speculative window then corresponds to the time for the access to main memory to complete. In Listing 2 for example, this is achieved by the `clflush` instruction. To verify this, we re-run the snippet without `clflush` in the Speculator tool and verify that indeed the control flow hijack only takes place in about one run out of 1000. When it does, the window is only a couple of instructions wide. We therefore conclude that without eviction, or other similar approaches to lengthen the speculative window, SPEAR attacks are unlikely to be practical.

In all snippets referenced by this section, the speculation window is artificially lengthened by flushing one of the memory operands to the compare instruction. This may not be realistic, as it imposes a strong requirement on the victim code to include a flush (or comparable) instruction. Instead, because the last level cache (LLC) is shared and often inclusive, the same effect can be accomplished more realistically by an external attacker thread computing an *eviction set* and performing a small number of accesses to addresses in this set. An LLC eviction set competes for the same LLC slice and cache set as the target address to be evicted. Existing techniques for performing such attacks typically assume knowledge of the targeted physical address, as the LLC is physically indexed. As a consequence of rowhammer attacks, this is no longer realistic, as most OSes have removed access to physical mappings for unprivileged users.

We demonstrate here that such eviction attacks can still be performed without knowledge of the physical address. To this end, we perform the eviction in two steps. The first step consists of the identification of an eviction set for a cache line in a page under the attacker’s control, by following the approach of Liu et al [19]. The second step consists in releasing this page to the OS, and executing the victim process such that it reuses the previously-created page. This permits the reuse of the eviction set constructed and verified to be working in the first step. We show details of such a practical attack in Section 3.1.2 for SSP.

## 2.3 Speculative ROP

To perform a complete speculative execution attack, the speculative control flow hijack must be followed by a *side channel send* gadget with a secret input. Unfortunately, Spectre v1-type Flush+Reload side channel send gadgets are known to be difficult to find [16, 31]. As in classical control flow hijacks [24] however, a speculative code reuse attack can be performed by concatenating the execution of speculative gadgets to construct a Flush+Reload side channel send sequence. To chain the gadget sequences, we observe that we can conveniently make use of a speculative overwrite of backward edges SPEAR variant, making such attacks very similar to

existing code reuse attacks. A similar approach and analogy exists with forward edges for code reuse.

The requirements for performing speculative code reuse are the following: *i)* limited number of gadgets can fit into the speculation window; *ii)* all code pages where gadgets are used must be present and mapped in the victim process. The first requirement is a consequence of the behavior of speculative execution. Using Speculator, we concluded that the maximum number of empty gadgets that fit in the largest speculation window is 20. The second requirement is explained by page misses causing speculative execution to stop. We show in Section 3.1.3 that this can be achieved for a practical use case.

### 3 Case studies

In this section we analyze different case studies where memory safety mechanisms can be bypassed with SPEAR attacks. In particular, in Section 3.1 we use a proof-of-concept attack that speculatively bypasses SSP leveraging architectural overwrites of backward edges. Section 3.2 analyses architectural overwrites of forward edges, targeting two prominent CFI frameworks, GCC VTV and LLVM CFI. In the case of the former, we show how the integrity check of the forward edge can be used to performed a speculative control flow hijack. For the latter we report the constraints that this type of implementation presents and detail the conditions under which the checks may be bypassed. Finally, in Section 3.3 we demonstrate two types of speculative bounds check bypasses in the Go language using speculative overwrites of a forward edge. We show how the attacker may influence the control flow target through both a load whose address value is attacker controlled and a load of a value that was speculatively overwritten by the attacker.

**Threat model.** The general threat model for all attacks in this paper is a local unprivileged attacker, targeting privileged processes. The threat model for attacks based on architectural overwrite of a backward or forward edge assumes a local attacker able to provoke a memory safety violation, but unable to exploit it traditionally due to hardening mechanisms being in place. In addition, we assume that the victim program can either be executed multiple times by the attacker or that the program automatically restarts, given that each attack run leaks one byte at a time and likely leads to program termination afterwards. Although mitigations against repeated execution exist, they are not commonly employed and therefore this threat model remains realistic. For the speculative overwrite of a forward edge, demonstrated in the Go use case, the threat model assumes a victim program with a specific code sequence, and a local attacker able to provide input that exercises this code sequence. We do not assume that the attacker is able to inject code in the victim program. In all cases, we assume the attacker has access to the victim program code and is able to bypass ASLR, or that ASLR is not present, as in the case of Go. The goal of the attacker is,

as in all transient execution attacks, to leak secrets from the target program.

#### 3.1 Attacking Stack Canaries

Stack canaries are one of the earliest mitigations against buffer overflows [26], and are widely used to this day. Among the most broadly adopted implementations are LLVM’s and GCC’s Stack Smashing Protection (SSP) and Microsoft’s /GS. At a high level, stack canaries work by inserting a value (the *canary*) between stack buffers and control-flow influencing data on the stack, in particular the saved return value. The integrity of the canary is then checked prior to using the saved return value. Local stack variables are reordered such that buffers, likely to be overflowed, reside adjacent to the canary while code pointers remain further away. This way, contiguous overflows of local stack buffers can be detected by the integrity check. The chosen canary value is randomly generated once during process execution start, and stored in a safe location.

Each compiler performs the instrumentation differently but in essence the mechanics are identical with respect to SPEAR attacks; we therefore focus on the example of LLVM on Linux x86\_64. Implementations consist of two distinct *instrumentation atoms*. The instrumentation atoms on our target system are shown in Listing 5. The first, the prologue SSP atom, is placed after the function prologue and local variable allocation, and is responsible for storing the canary value on the current stack frame. The second, the epilogue SSP atom, is placed before local variable deallocation and the function epilogue. It compares for equality between the global and local canary values; if the values differ, the `__stack_chk_fail` function is called, terminating the program. If the local canary value was not modified during function execution, the function returns normally. We show next that this particular comparison can be the target of a SPEAR attack.

```

1  func:
2      prologue
3
4      ; Store canary on the stack
5      mov rbp, QWORD[fs:0x28]
6      mov QWORD[stack_canary], rbp
7      ...
8      body
9      ...
10     ; Check for corrupted canary, if yes fail
11     mov rbp, QWORD[stack_canary]
12     xor QWORD[fs:0x28], rbp
13     je exit
14     call __stack_chk_fail
15 exit:
16     epilogue
17     ret

```

Listing 5: Stack canary check instrumentation example

### 3.1.1 SPEAR attack on LLVM-SSP

The pattern of the SSP instrumentation closely resembles that of Listing 1. Under our threat model, an attacker with a buffer overflow against a function protected by SSP can perform a SPEAR architectural overwrite attack of the return value of that function. We describe an end-to-end proof of concept of an attack targeting a version of `libpng` with a reported buffer overflow (CVE-2004-0597): the bug is not exploitable in the traditional way owing to the fact that the function is compiled with SSP. We show how a speculative adversary can exploit the SPEAR architectural overwrite to leak arbitrary secrets from the victim.

The attack proceeds as follows: in the first step, the attacker overwrites the saved return address of a victim function, e.g., through a classical buffer overflow. In the second step, the attacker leverages a misprediction in the conditional jump of the canary integrity check, thus transiently executing a return to the previously overwritten return address. This PHT-based misprediction can be forced by the attacker in a way similar to Spectre v1, by executing the canary integrity check with an intact local canary sufficiently many times. As discussed in Section 2.2, another requirement is that a sufficiently long speculation window exist. We achieve this by evicting the global canary from the LLC, as we show in Section 3.1.2. The attacker is then able to perform a side-channel send operation by constructing a speculative ROP chain to access a secret and perform a side channel send, as we show in Section 3.1.3.

### 3.1.2 LLC eviction of the global canary

We apply the two-step method described in Section 2.2 for the eviction of the global canary from LLC, and thus from all cache levels by the property of inclusiveness of caches on the target platform. The global canary value is always stored at a fixed offset in a page: we use this property to find eviction sets for this particular offset, following the approach of Liu et al. [19], which works without knowledge of physical addresses.

The attacker process first identifies a page with a known eviction set and then unmaps it to be reused by the victim to store its canary. This is achieved with two processes under attacker control, as follows. At first, one of them maps a hugepage and enters a loop in which it brings an eviction set into cache and waits for feedback from the second attacker process. The latter in turn probes its own stack canary and reports back a success as soon as the canary is no longer cached.

Once the eviction set is identified, the second attacker process releases the page hosting its canary by `exec`'ing the victim. During `exec`, the virtual memory of the process is released, thus pushing frames to the internal kernel freelist. Then `exec` creates mappings for the new process. Each subsequent memory access by the victim results in a page fault which is resolved by popping frames from the internal freelist.

The objective of the attacker at this point is to make sure that the page for which it holds the eviction set is allocated by the kernel for the victim to host its canary. The chances of this happening can be maximised by knowing the memory layout of the attacker and the victim and the (deterministic) way in which the kernel releases and allocates pages during an `exec`. With this method, we obtain an overall success rate of  $66.6\% \pm 0.96$  for LLC canary eviction. We report the mean over 100 runs with 95% confidence level.

### 3.1.3 Speculative ROP

We now focus on building and using a speculative ROP chain that accesses a secret and leaks it through a side channel. We use the Flush+Reload cache side channel initially used by Kocher et al. [16], although other side channels can be used similarly [5, 22, 25].

In Section 2.3, we have identified two major constraints on the attack: *i*) a limited number of instructions can fit into the speculation window; and, *ii*) all code pages where gadgets are used must be present and mapped with corresponding TLB entries. In addition to these requirements, we note that gadget code, as well as any data accessed by gadgets, must be available in cache during speculative execution. Typically, this is not an issue in speculative execution attacks because the attacker can use the first speculative execution attack as a warm up phase which brings the required data in the cache, whereas this attack is *single shot*: the process terminates after each attempt and this is an additional requirement.

Concerning the first requirement, the Flush+Reload side-channel send gadget only requires a few instructions: there are sufficiently short gadgets available, and length is therefore not an issue in practice. For the second requirement instead, we create a tool to search for gadgets in code that was recently accessed by the victim program, for which pages are present and mapped in the victim process. The tool traces the victim process and collects all executed shared (library) code pages, which are then fed into an existing ROP gadget search tool, ROPgadget [1]. We ran the tool on the victim program and found 26 mapped code pages within the 4 different modules used by the victim: `libc`, `libpng`, `libz` and `ld`. In total, the tool discovered 2096 gadgets. Finally, to ensure that all gadget sequences are in cache, a hyperthread-colocated attacker performs a ROP chain warm up phase by executing the chain in close temporal proximity with the SPEAR attack.

```
1  mov rax, secret
2  shl rax, 8
3  add rax, shared_array
4  mov rax, [rax]
```

Listing 6: Example of Flush+Reload gadget

We build a 5-gadget ROP chain using the ROP gadgets found by our gadget search tool. The chain is functionally equivalent to the Flush+Reload gadget shown in Listing 6. The chain accesses a target address computed using a secret

byte value, as in the initial Spectre attacks [16]. Because Flush+Reload requires shared memory, we choose the target address to reside in such a shared memory area between attacker and victim, the first 16 readable and executable pages of the `libpthread` library. To leak one byte we use an array size of 256. To avoid prefetching effects during side-channel receive, we choose the element size to be 256, i.e., four cache lines. The total array size equals  $256 \times 256$  bytes, 16 pages.

The ROP chain that we find and use in the attack is shown in Listing 7. By splitting them in small sequences of instructions, we easily find the required gadgets within the constraints of the attack. This chain pops the addresses (controlled by the attacker) of the start of the 16 pages and of the targeted secret from the stack. Next the secret value is loaded at line 8. The next speculative gadgets multiply the secret value by 256 and compute the target address. The last speculative gadget dereferences the target address, resulting in a load being issued during speculative execution. This eventually brings the value into the cache to be measured by the attacker. The whole chain therefore allows the attacker to implement a universal read primitive over the victim process speculatively, using a Flush+Reload attack and the attacker’s control over the stack.

```

1  libpng.so.3.1.2.5 : 0x7960
2      pop rdx
3      ret
4  libpng.so.3.1.2.5: 0x7f0a
5      pop rsi
6      ret
7  libpng.so.3.1.2.5 : 0x128ec
8      mov eax, dword ptr [rsi]
9      mov byte ptr [rdi + 6a], al
10     ret
11 libpng.so.3.1.2.5 : 0x9f4b
12     shl rax, 8
13     add rax, rdx
14     ret
15 libpng.so.3.1.2.5 : 0x9fde
16     add eax, dword ptr [rax]
17     add byte ptr [rdi], cl
18     xchg eax, ebp
19     ret

```

Listing 7: Flush+Reload gadget ROP chain

### 3.1.4 Attack evaluation and results

In our PoC, we target the `libpng` 1.2.5 code in Listing 8 which is vulnerable to CVE-2004-0597 [2].

CVE-2004-0597 is a stack buffer overflow which allows the attacker to read `length` bytes in `readbuf`. Due to improper sanitization of `length`, a read larger than `PNG_MAX_PALETTE_LENGTH` is allowed in a stack buffer. Our victim target is a program which receives a `.png` file and parses the file using an unpatched `libpng` 1.2.5. When building the victim target with stack canaries enabled, the compiler will instrument `png_handle_tRNS` with the corresponding prologue and epilogue SSP atoms. As expected, SSP protects `png_handle_tRNS` from exploitation by stopping execution

before the function returns. However, using a SPEAR architectural overwrite attack, we can perform a speculative control flow hijack. During the SPEAR attack, the attacker feeds `.png` files of the legitimate length to train the pattern history table. Then, the attacker provides a `length` larger than `PNG_MAX_PALETTE_LENGTH` that overwrites the value of the return address to trigger the speculative ROP attack.

We run the attack on an Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz. The machine runs Ubuntu 16.04.6, kernel version 4.15.0. As described in Section 2, the attack has an initialisation phase where eviction sets are identified, the ROP sequence is primed and memory used for the side channel is allocated. Concurrently with the submission of the malicious payload, the attacker also runs the eviction loop to lengthen the speculation window by causing the eviction of the stack canary in the victim.

```

1  void /* PRIVATE */
2  png_handle_tRNS(png_structp png_ptr,
3                  png_info_ptr info_ptr, png_uint_32 length)
4  {
5      ...
6      png_byte readbuf[PNG_MAX_PALETTE_LENGTH];
7      ...
8      if (png_ptr->color_type ==
9          PNG_COLOR_TYPE_PALETTE) {
10         if (!(png_ptr->mode & PNG_HAVE_PLTE))
11         {
12             /* Should be an error, but we can cope
13              * with it */
14             png_warning(png_ptr, "Missing PLTE
15              before tRNS");
16         }
17         ...
18         png_crc_read(png_ptr, readbuf, (
19             png_size_t)length);
20         png_ptr->num_trans = (png_uint_16)
21             length;
22     }
23     ...
24 }

```

Listing 8: `libpng` vulnerable snippet related to CVE-2004-0597

We measure the attack success rate as the number of times the attacker is able to correctly guess a secret byte from the victim memory space, per total number of runs. Canary eviction has a significant impact on the attack success rate. We therefore also show the attack success rate when successful eviction of the stack canary is detectable by the attacker, which could be achieved through a side channel, depending on the victim program. In both cases we measure how many victim secret bytes are leaked per second. We report means over 100 runs with 95% confidence level. We measure a success rate of  $7.19\% \pm 0.62$  for cases where the global stack canary is successfully evicted, and of  $4.78\% \pm 0.41$  assuming the attacker cannot detect a successful eviction of the global canary, the most generic case. This results in an end-to-end leakage rate of victim bytes of 0.3 and 0.2 bits per second respectively.

## 3.2 Attacking CFI

Control Flow Integrity (CFI) of forward edges aims to protect the integrity of code pointers used in indirect calls and jumps. CFI implementations contain two main parts: instrumenting all indirect control transfers to check their validity at runtime, and classifying valid control flow transfers (typically using static analysis at build time). We analyze here two prominent cases: the GCC Virtual Table Verification (VTV) [27] mechanism to prevent `c++` virtual table corruption, as well as LLVM-CFI [18], a publicly available, low overhead, forward-edge CFI implementation. In the GCC VTV, we prove that a SPEAR attack is possible, while in the LLVM-CFI case we conclude that eviction-related considerations result in the speculation window being too short for practical exploitation. In particular, this case study demonstrates that we cannot conclude that SPEAR attacks apply equally to all implementations of memory safety-related defenses, and case-by-case analysis is necessary.

### 3.2.1 GCC VTV

In the GCC VTV implementation, for every call to a virtual function in the program, the compiler inserts a check to make sure that the pointer used for the indirect call belongs to the virtual table of the object. Such check is represented by a call to the function `__VLTVerifyVtablePointer` implemented in `libvttv.so` library. Within this function, the pointer is looked up from the table; if found, the function simply returns to the program which will perform the call, otherwise, it gracefully fails. If an attacker can successfully evict the cache line related to the variable the pointer is tested against, speculative execution is triggered during the evaluation of the check. In that case, the indirect call to the virtual function is speculatively executed and the code at the corrupted pointer is executed. At this point, the attacker has performed speculative control flow hijack and can mount a data exfiltration attack as described in Section 3.1.

In our proof-of-concept implementation of this attack, we artificially evict from all cache levels the variable related to the vtable of the object within the `libvttv.so` code. Then, we create a `c++` program that defines two different classes each containing one virtual method. The first class is our target for the forward edge overwrite. To verify whether speculative control flow hijack takes place, we instrument the program to read performance monitor counters and set the speculative control flow hijack target to contain a *speculation marker*. We use the second class to instantiate the object that is later corrupted.

After object initialization, we perform a vtable pointer overwrite in our victim object making it point to the vtable of the first class. Finally, we perform the virtual call for the control flow transfer which is instrumented by GCC VTV with a call to the integrity check inside the `libvttv.so` library. During normal execution, this overwrite is detected by the library

which reports the corruption and prevents the control flow transfer by terminating the application. With a SPEAR attack as described here, we verify that control flow hijacking occurs in 85% of runs, demonstrating that a SPEAR architectural forward-edge attack is viable against GCC VTV. We note also that the redirection is performed to a vtable of a completely unrelated class, a case which should be prevented by VTV. A real-world attack would additionally require evicting the compare variable, for example by using the same method as in Section 3.1.2, as well as a way of achieving a side-channel send for the attacker, as in Section 3.1.3.

### 3.2.2 LLVM CFI

The CFI solution implemented in LLVM uses function types as *equivalence classes*: an indirect call to a function of a different type than the one specified by the programmer is forbidden by the CFI instrumentation. This is achieved by placing functions of an equivalence class in a jump table, thereby having as many jump tables (whose addresses are carefully chosen) as equivalence classes. The instrumentation for indirect calls then consist in simply checking that the address of the target fall within the range of the jump table, and at the right alignment.

This range check can be seen as a check against a compile-provided constant value, using the address of the provided target. Both of these components are by design available and cached while performing this check: evicting the code that contains the range check would result in speculative execution stopping, and evicting the address of the target would result in the iBTB being used for speculative execution. In either case, a SPEAR attack would fail. The attack may be triggered without any attempt to artificially extend the speculation window, but, as demonstrated experimentally in Section 2.2, the resulting speculation window is rare and short, making such attacks unlikely to be practical. We conclude that LLVM CFI is in practice not vulnerable to SPEAR attacks.

## 3.3 Attacking memory safe languages

Most modern languages are designed to ensure memory safety. Instrumental to achieving this property are bounds checks for load and store operations into arrays. In this section we show how bounds checks may be speculatively bypassed, allowing the transient execution of out-of-bounds load and store operations. We show under which conditions this leads to a SPEAR attack.

We focus in this case study on the popular Go programming language, runtime and compiler. We present two variants, one where data that influences a forward control flow edge is architecturally overwritten and one where a forward edge is speculatively overwritten. In either case, the attacker is able to achieve a speculative control flow hijack. We prototype both variants and show the conditions under which the attack



succeeds at a rate exceeding 80%.

```
1 type slice struct {
2     array unsafe.Pointer
3     len    int
4     cap    int
5 }
```

Listing 9: Arrays in Go

Before detailing the two attacks, we give a brief introduction to the way the Go compiler manages arrays and bounds checks. Arrays in Go are represented in memory as the `struct` shown in Listing 9. The address of the contiguous chunk of virtual memory backing the array is stored in `array`. The number of elements that `array` can hold (and implicitly the size of the memory chunk since Go is statically typed and the size of the elements is always known) is stored in `cap`. The current number of elements that have been stored in the array is stored in `len`.

Whenever an array access is performed in Go, the compiler will add appropriate bounds checks. This is achieved in the course of the compiler pass to translate the abstract syntax tree (AST) into the static single assignment (SSA) intermediate representation by adding an `IsInBounds` meta-operation before every array load or store. `IsInBounds` takes two arguments, the index of the current access and the length of the array, and drives a conditional jump either to the basic block that performs the array access if the index is between zero and length minus one, or a jump to a function that raises a panic otherwise.

```
1 mov rcx, [rip+0xd0121]      #<array>
2 cmp [rip+0xd0121], rax      #<array+0x8>
3 jbe 486a66 <main.main+0xa6>
4 mov rax, [rcx+rax*8]
```

Listing 10: Bounds check in Go

`IsInBounds` is translated by later passes into a sequence of instructions similar to the one shown in Listing 10. The snippet shows a load from an array of integers: at first `rcx` is loaded with the address of the memory array, a compare instruction is issued between the index in `rax` and the array length at `main.array+8`. If the index is negative or not strictly less than the length, the code jumps to a call to the `runtime.panicindex` function. Otherwise the array access is performed.

The conditional jump generated by the `IsInBounds` meta-operation may speculatively execute the wrong jump target and perform a transient load or store operation out of bounds. We show two distinct code patterns, one leveraging a load and one a store, that may lead to speculative control flow hijack.

```
1 array[index].function()
```

Listing 11: Load-based speculative control flow hijack code pattern

### 3.3.1 Load-based SPEAR speculative attack

The first pattern is shown in Listing 11. It represents an instance of a SPEAR-speculative attack and consists of an interface function call, where the interface is stored into an array of interfaces `array`, dereferenced at position `index`. Note that the array must be an array of interfaces so that calling the function is achieved by an indirect call. For the attack to be successful, we need `index` to be attacker-controlled and the attacker must be able to store the value of two pointers in the memory space of the target process at a known location. The first condition is met whenever a process accesses an array using an index that is received as an external input. The second condition is very commonly met since programs store user-provided input for processing. Knowledge of the location of the stored pointers depends on the memory area being used, and is aided by the deterministic nature of the Go allocator.

```
1 type iface struct {
2     tab *itab
3     data unsafe.Pointer
4 }
5
6 type itab struct {
7     inter *interfacetype
8     _type *_type
9     hash  uint32
10    _      [4]byte
11    fun    [1]uintptr
12 }
```

Listing 12: Structs used by interface calls

Without loss of generality, we describe the case where function is the first function defined by the interface. Exploitation proceeds as follows: first, the attacker prepares the memory structures that are used when an interface call is performed. The structures are shown in Listing 12, and are used by dereferencing the `tab` pointer from the `iface` struct and then calling into the `fun` array.

```
1 0x561000: 0x562000
2 0x561008: 0x0000000000000000
3 ...
4 0x562000: 0x0000000000000000
5 0x562008: 0x0000000000000000
6 0x562010: 0x0000000000000000
7 0x562018: 0x563000
8 ...
9 0x563000: <CFH target here>
```

Listing 13: Memory layout in preparation for the exploitation of load-based speculative control flow hijack

In preparation for exploitation, the attacker ensures that the memory layout of the target program contains a pattern similar to that shown in Listing 13. Assuming that the attacker wants to speculatively redirect the control flow to address `0x563000`, the attacker creates a fake `itab` structure (in the example at `0x562000`) such that the first entry in the `fun` pointer array points to the desired target. Then the attacker creates a fake

`iface` structure (in the example at `0x561000`) such that the `tab` pointer points to the aforementioned `itab` structure. With the memory thus prepared, the attacker supplies the index into the array such that the resulting address (the base address plus index multiplied by the size of an `iface` structure) equals the fake `iface` structure (`0x561000` in our example). With the index thus set the program will call the `runtime.panicindex` function; however if the conditional jump of the bounds check is mispredicted, the dereference and subsequent indirect call will take place transiently. Note that, contrary to the case studies in Section 3.1 and Section 3.2, the attack is not necessarily “single shot”: if the program calls `recover`, the attacker might be able to execute the vulnerable sequence multiple times.

We prototype the attack to evaluate its effectiveness in a proof of concept. The proof of concept only aims to establish the feasibility of the attack: in particular we do not integrate into an end-to-end attack and refer to Section 3.1.4 for cache eviction and speculative ROP. The PoC contains the pattern of Listing 11 called in a loop to train the pattern history table and ensure that the bounds check conditional jump as strongly non-taken. The index used to access the array in the loop is in bounds during the training phase and is then set to the target index computed as described above in the last iteration.

To verify whether speculative control flow hijack takes place we instrument the program to read PMCs during the execution of the loop, and set the speculative control flow hijack target to contain a speculation marker. The `runtime.panicindex` function is modified to read and persist PMC values for each execution.

This instrumentation permits us to verify that speculative control flow hijack indeed takes place. The success rate is influenced by several factors that we review here. The most relevant factor is the size of the speculation window, which is influenced by how quickly the correct jump target is determined. The speculation window is maximised if the variables used in the compare instruction that drives the jump – especially the array length – are not present in any of the levels of the cache. In order to get empirical evidence of this fact we instrument the program with a `clflush` instruction right before the array dereference to ensure that the array length is not cached. In practice, an attacker may achieve the same result by performing cache eviction code sequences. However flushing the cache alone does not ensure a high success rate: this is because the array length is stored right after the base address of the array, whose address is loaded into memory as the first instruction of the dereference sequence. We verify that if the two memory locations belong to different cache lines, the speculation window is maximised. Another factor that influences the success rate is whether the target of the speculative control flow hijack is already in the instruction cache. We make sure that this be the case by inserting a call to the marker function in the warm up phase before the loop. We report success rates exceeding 80% when the array length is flushed and is in a separate cache line as the base address

on multiple platforms (Xeon CPU E5-2640, Core i7-8650U, Core i7-6700K) and different versions of the Go runtime (1.13.4, 1.12, 1.10.4).

### 3.3.2 Store-based SPEAR speculative attack

The second pattern is shown in Listing 14.

```
1 array[index] = value
2 ...
3 interface.function()
```

Listing 14: Store-based speculative control flow hijack code pattern

The pattern consists of a store operation of an attacker-controlled value at an attacker-controlled location into an array. The elements stored in the array must permit storage of a pointer. Smaller sizes would permit partial control over the speculative control flow hijack target. The pattern requires that the array store be followed by an interface call. The interface call does not need to be related to the array. It only needs to be in close proximity of the store operation so that it may still be speculatively executed. This pattern does not require any ability to perform preparatory store operations in the memory space of the target program. The pattern makes use of store-to-load forwarding, since the store in the array is used to (speculatively) overwrite a function pointer which is later (speculatively) loaded and called. This corresponds to the “speculative overwrite of forward edge” variant of a SPEAR attack.

The store part of the pattern consists of a speculative version of a “write-what-where” condition. It may be exploited in several ways to hijack the interface call: the most basic one would be to overwrite the `tab` pointer in the `iface` struct (see Listing 12). However this would either require the attacker to perform a set of preparatory stores identical to those discussed in Section 3.3.1, or it would restrict the freedom of the attacker to choose a target out of the existing interface pointers. Another strategy would be for the attacker to overwrite the `fun` pointer in the `itab` structure directly. These structures are stored in a non-writable virtual memory region. However, given that the store takes place speculatively, the attacker is able to bypass the write restrictions and overwrite the pointer. We therefore chose to prototype this simpler and more effective variant.

Exploitation proceeds as follows: at first the attacker speculatively overwrites the `fun` pointer in the `itab` of the interface that is later dereferenced. This is achieved, as the attacker controls value and index. The former is set to the address of the desired speculative control flow hijack target; the latter is set such that base array and index multiplied by the size of the array elements add up to the address of the `fun` pointer to be overwritten. As in the previous section, with the index thus set the program will panic; however if the bounds check is mispredicted, the store-to-load forwarding and subsequent

indirect call will take place, achieving speculative control flow hijack.

We prototype the attack to evaluate its effectiveness employing a similar instrumentation as the previous section, with PMCs and speculation markers employed to identify successful runs, and a loop to set the predictor state. The success rate is similarly influenced by ensuring that the variables driving the conditional branch are not cached, and that the speculative control flow hijack target is in cache. Under these conditions, we report success rates exceeding 80% on the same platforms listed in the previous section.

## 4 Mitigations

In this section, we implement and analyze serializing-based (lfence) and masking-based mitigations for SPEAR-architectural attacks (SSP) and SPEAR-speculative ones (Go). We show that in both cases that the masking-based solution results in a low overhead.

### 4.1 Mitigations for SSP

We investigate two possible mitigations for the SPEAR-architectural attack against SSP. A serializing instruction such as lfence can be inserted after loading the canary in the epilogue instrumentation, thereby ensuring that the comparison can only lead to a short enough speculation window. Alternatively, the return value can be masked architecturally with a generated value that is set to 0 when the check fails (the canary is corrupted), and all ones when it passes, as shown in Listing 15.

```
1 mov rax, QWORD[fs:0x28]
2 mov rcx, QWORD[stack_canary]
3 xor rdx, rdx
4 cmp rax, rcx
5 setne dl
6 add rdx, 0xffffffffffffffff
7 and QWORD[rsp + 8], rdx
```

Listing 15: Masking mitigation sequence; rax contains global canary value and rcx contains the stack canary; rsp + 8 points to the return address

We implement both mitigations as compiler passes in clang+llvm. SSP is architecture specific, thus our solution is built for x86\_64 Linux systems. We run the SSP mitigations benchmarking on Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz. We measure the normalized runtime of both *return address masking* and lfence on SPECint CPU 2006 Figure 3a. The normalized runtime is computed as runtime over the baseline runtime constituted by execution with SSP Disabled. For reference, we additionally plot the normalized runtime for all existing SSP implementations, SSP Loose (-fstack-protector flag), SSP Strong (-fstack-protector-strong flag), and SSP All (-fstack-protector-all flag).

The lfence mitigation shows a high overhead in 9 out of 12 benchmarks, the highest being 100%, in the SSP All case with xalancbmk. Return address masking incurs a significantly lower, albeit still significant performance penalty, reaching a maximum of 13% for the same benchmark.

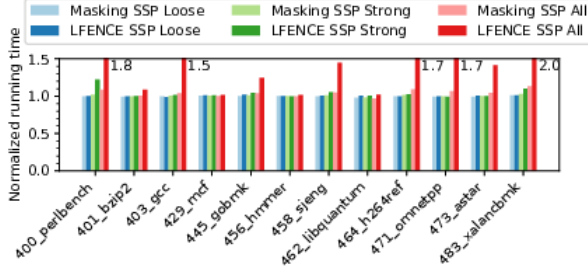
Based on this evaluation, we find the return address masking mitigation to be viable and superior to the lfence mitigation: the overhead of vanilla SSP (shown in Figure 3b on SPECint CPU 2006 is at most 9%, in the case of SSP All on xalancbmk). In addition, we note that most Linux distributions either use the SSP Loose or SSP Strong options, both of which incur a low overhead on all SSP benchmarks: we record a maximum of 2.1% overhead over the SSP Disabled baseline. With return address masking, the maximum overhead becomes 2.7% over the SSP Disabled baseline. We conclude that return address masking does not impose a significant overhead with the most commonly used SSP compiler options.

### 4.2 Mitigations for the Go compiler

We investigate possible mitigations for the SPEAR-speculative attack on Go. The mitigations consist of two different compiler passes that ensure that the vulnerability is no longer exploitable. The first is based on lfence, whereas the second is based on branchless index masking sequences. As part of responsible disclosure we have notified the Go team, who have implemented index masking as an optional compiler switch. The feature is planned for Go 1.15.

The first mitigation consists of adding an lfence instruction after the cmp instruction in the sequence that implements the IsInBounds metaoperation. With reference to Listing 10, the lfence instruction is inserted after the cmp on line 2. The insertion ensures that all prior instructions have completed, which means that there will be no misprediction of the branch target and any out-of-bound access will result in a panic with no transient execution. The instruction is added explicitly in the pass that translates the AST into SSA form by defining a new Lfence meta-operation and adding it after each IsInBounds operation. We ensure that the operation is neither reordered nor eliminated.

The second mitigation we investigate entails the addition of an appropriate masking sequence that ensures that the index is set to a “safe” value in case of out-of-bounds accesses. The masking sequence amounts to a no-op in case the access is in bounds by performing an and operation on the index with a sign extended -1 mask. If the access is not in bounds, in our implementation, the masking operation forces an access of the element at index 0 in the array by performing an and operation on the index with a 0 mask. We can see the masking sequence in Listing 16: after the usual cmp and jmp instructions, length and index and subtracted in order to set the carry flag. Then, the sbb instruction is used to set a register to -1 in case of an in-bounds access or 0 otherwise. The array is



(a) SSP with speculative bypass mitigations



(b) Vanilla SSP

Figure 3: Overhead computed as normalized runtime over SSP Disabled baseline.

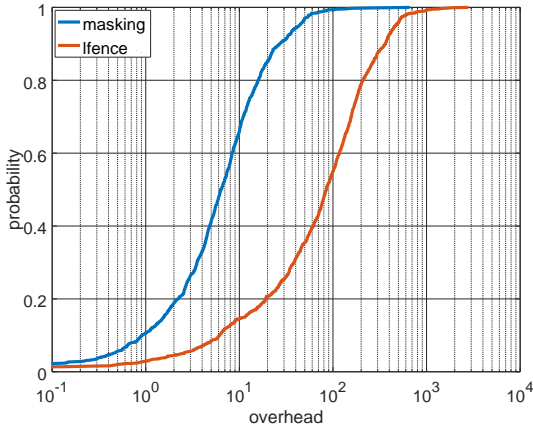


Figure 4: Empirical CDF of the logarithm of the overhead percentage for the considered mitigations. Overhead data is gathered by running the full set of benchmarks of the go runtime version 1.12.0.

subsequently accessed after performing an `and` operation on the index with the mask thus obtained. The pattern might be further optimised by using the `cmp` instruction of the bounds check to set the carry flag. This, however, is not always possible since the compiler will use a compare instruction with an immediate whenever possible. The immediate can only be the second source operand, forcing the direction of the comparison instruction. For the sake of simplicity we therefore rely on an extra subtraction operation. The masking instruction sequence is added by defining three new meta-operations – `OpMaskStep1`, `OpMaskStep2` and `OpMaskStep3` – which are later lowered into a `sub`, `sbb` and `and` instruction, respectively.

We measure the overhead of both mitigations by building the Go runtime version 1.12.0 and running the full benchmark suite. We run the experiments on a 40-core Xeon E5-2640 machine with 64 GiB of RAM. Figure 4 displays the empirical cumulative distribution function of the overhead of each of the two mitigation strategies. We can see how the `lfence`-based approach incurs a high overhead (143% mean and 84% median) due to the fact that `lfence` will terminate

any speculative execution and thus severely curtail the instruction throughput. On the other hand, the masking approach shows a much lighter overhead (12% mean and 6% median) since the instructions involved are simple and do not cause any memory-related operation.

```

1  cmp    rcx, rdx
2  jae    <raise-panic-code>
3  mov    rbx, rdx
4  sub    rdx, rcx
5  sbb    rcx, rcx
6  and    rcx, rbx
7  shl    rcx, 0x4
8  mov    rax, [rax+rcx*1]

```

Listing 16: Masking mitigation sequence; `rdx` contains the index and `rcx` contains the length of the array and `rax` contains the base address of the array

## 5 Related Work

### 5.1 Speculative execution attacks

Transient execution attacks can be subdivided into two main categories: fault-based and speculation-based attacks [6]. The speculation-based, or Spectre-family, attacks comprise those leveraging microarchitectural components such as the Pattern History Table (PHT) for Spectre v1 [16], the Branch Target Buffer for Spectre v2, the Return Stack Buffer (RSB) for Ret2Spec [20] and Spectre returns [17]. Both BTB and RSB attacks are cases of speculative control flow hijacks, i.e., they provide the ability for an attacker to steer speculative execution to an arbitrary location. Varied and powerful attacks leveraging the BTB for speculative control flow hijacks have been demonstrated, in combination with port contention-based, instruction cache-based, or BTB-based side channels [5, 22]. In contrast, this paper focuses on SPEAR attacks. Although the start of speculative execution always requires a speculative trigger, based on a microarchitectural component, the speculative control flow hijack step is based on architecturally visible control-flow influencing instructions in SPEAR attacks. Among the four subtypes of SPEAR attacks, in Spectre

v1.1 [14], Kiriansky and Waldspurger identify that speculative overwrites can lead to speculative control flow hijacks, whereas we identify three new types. We also demonstrate practical use cases on Go memory safety, GCC VTV and GCC SSP with a full working attack chain.

The idea of chaining speculative gadgets in a way similar to ROP was suggested shortly after the first publication of Spectre attacks [10, 16]. While some publications have referred to the same idea [14, 22], this paper presents the first demonstrated case of chaining multiple speculative gadgets to form a cache side-channel send gadget. In addition, this chaining is performed using a speculative overwrite of the return address, and not by poisoning the RSB or BTB.

## 5.2 Mitigations

Since the first speculative execution attacks have been disclosed in early 2018, different mitigations have been proposed to prevent each variant. Some mitigations are introduced at hardware level meanwhile others are software-based. Many of these mitigations target Spectre v2 type of attacks, meanwhile no complete mitigation has been introduced for Spectre v1.

The only available Spectre v1 mitigations are software-based and consists in either deploying barrier (e.g `lfence`) around each sensitive bounds check or, alternatively, masking the index used for accessing arrays [7, 14, 15, 30].

While `lfence` is an effective mitigation, it incurs huge performance penalties if widely applied. Static analysis tools have been proposed to search for sensitive code patterns. One example is the Linux kernel where vulnerable code is instrumented on a case by case basis either through manual audit or automatic tools (e.g., `smatch` [3]) detection [4]. The drawback of current available tools is that they target Spectre v1 code patterns only and therefore are not useful to detect edges overwrites.

For Spectre v2 instead, there are software and hardware mitigations. The software mitigation currently available is Retpoline [28]. This mitigation targets indirect calls and indirect jumps and prevents them from being speculatively executed by trapping speculation within a loop. As in the barrier cases for Spectre v1, Retpoline requires code modification and therefore each program has to be recompiled to enforce such mechanism. While this has been done inside the Linux kernel, user-space programs have not yet been using this mechanism.

On the hardware side, Intel published three major protections: *i*) IBRS [12], which prevents speculation of indirect branches using target values computed using lower privileged predictor modes, *ii*) STIBP [13], which prevents BTB poisoning from sibling threads, and *iii*) IBPB [11], which ensures that code before a barrier does not influence the behavior of the code after. IBRS and IBPB are meant to protect higher privileged code from lower privileged code [22]. The only mitigation that provides protection within the same privilege level is STIBP, which is not enabled by default for perfor-

mance reasons.

Finally, Intel announced as part of its Control Flow Enforcement (CET) extension, the future introduction of a new mitigation that will constrain the target of near indirect jumps and calls to only `ENDBRANCH` instructions. With this mitigation there is a reduction of possible gadgets where speculative execution can be redirect to during branch target injection attacks. In the context of SPEAR, this mitigation applies only for the forward edge overwrite case and not to the backward edge.

## 6 Discussion

**Applicability to other use cases.** Beyond the highlighted use-cases, SPEAR attacks may be employed against other targets. For example, other memory-safe languages may be targeted with SPEAR attacks to speculatively bypass bounds checks as we showed for the Go programming language. Preliminary investigation suggests that this is likely to be possible, since instruction sequences for bounds checks similar to those detailed in Section 3.3 are also present in `Rust` and `Java` (for JITted blocks). Similarly, heap hardening mechanisms such as the checks inserted in recent versions of the `libc` allocator might also become the target of SPEAR attacks: they introduce conditional branches which verify properties of heap pointers (e.g. the value and size) and may terminate the program before the control flow returns to the application. A SPEAR attack might speculatively bypass that check, leading the application to possibly use corrupted pointers as part of a control flow decision. Theoretically, any security check that directly or indirectly gates a control flow transfer may be turned into a speculative control flow hijack attack. However, as demonstrated in the LLVM CFI case, a case-by-case analysis is necessary to establish whether SPEAR attacks are applicable.

**General applicability of speculative ROP.** The speculative ROP and LLC eviction techniques are demonstrated as part of the SSP, SPEAR-architectural overwrite of a backward edge, use case. Nevertheless these techniques are generally applicable for the exploitation of other SPEAR use cases, with exploitability always depending on the scenario at hand. For the general forward edge cases, we note that this requires, as in classical ROP attacks, a technique known as a stack pivot, which consists in the attacker setting up a fake return stack somewhere under its control in memory, and having the first control flow hijack point to an instruction setting the stack pointer to that address (for instance, the `push rax; pop rsp; ret stack pivot gadget`). We have verified using the Speculator tool that such stack pivots do work for SPEAR-architectural as well as SPEAR-speculative attacks.

## 7 Conclusion

In this paper, we investigate variants of speculative control flow hijacking attacks, called SPEAR, that exploit and bypass current mitigations against classic memory corruption vulnerabilities to leak information from local processes. With SPEAR, we show that Spectre-like vulnerabilities drastically increase attack vectors for local attackers. Therefore, they force not only the creation of new mitigations but also the re-design of previously deployed protections. In this work, we present attacks against stack canaries, CFI and memory-safe languages. We provide proof-of-concepts implementations against SSP buffer overflow mitigations, GCC VTV and Go's runtime. We show the use of multiple ROP gadgets and details on how to use LLC eviction without knowledge of physical addresses in the context of SPEAR attacks. Finally, we discuss how SPEAR attacks can be mitigated and report our performance results.

## Disclosure

We submitted the PoC exploits and our findings to the Go security team on November 22nd, 2019. As a result of our notification, the Go security team is considering deploying hardening measures (index masking and retpoline) for the next release cycle (Go 1.15 due for August 2020).

## Acknowledgement

We would like to thank Russ Cox and Matthias Neugschwandtner for their helpful comments on an earlier draft of this paper.

## References

- [1] ROPgadget. <http://shell-storm.org/project/ROPgadget>.
- [2] CVE-2004-0597. <https://nvd.nist.gov/vuln/detail/CVE-2004-0597>, 2004.
- [3] <https://repo.or.cz/w/smash.git>, 2018.
- [4] The Linux Kernel user's and administrator's guide. <https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/spectre.html>, 2019.
- [5] Atri Bhattacharyya, Alexandra Sandulescu, Matthias Neugschwandtner, Alessandro Sorniotti, Babak Falsafi, Mathias Payer, and Anil Kurmus. Smotherspectre: Exploiting speculative execution through port contention. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, pages 785–800, 2019.
- [6] Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtvyushkin, and Daniel Gruss. A systematic evaluation of transient execution attacks and defenses. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 249–266, Santa Clara, CA, August 2019. USENIX Association.
- [7] Chandler Carruth. Speculative load hardening. <https://l1vm.org/docs/SpeculativeLoadHardening.html>, 2018.
- [8] Colin Robertson et al. C++ developer guidance for speculative execution side channels. <https://docs.microsoft.com/en-us/cpp/security/developer-guidance-speculative-execution>, 2018.
- [9] Mambretti et al. Speculator. <https://github.com/ibm-research/speculator/wiki>, 2019.
- [10] Richard Grisenthwaite. ARM Whitepaper: Cache Speculation Side-channels, 2018.
- [11] Intel. Deep dive: Indirect branch predictor barrier. <https://software.intel.com/security-software-guidance/insights/deep-dive-indirect-branch-predictor-barrier>, 2018.
- [12] Intel. Deep dive: Indirect branch restricted speculation. <https://software.intel.com/security-software-guidance/insights/deep-dive-indirect-branch-restricted-speculation>, 2018.
- [13] Intel. Deep dive: Single thread indirect branch predictors. <https://software.intel.com/security-software-guidance/insights/deep-dive-single-thread-indirect-branch-predictors>, 2018.
- [14] Vladimir Kiriansky and Carl Waldspurger. Speculative Buffer Overflows: Attacks and Defenses. <https://people.csail.mit.edu/vlk/spectre11.pdf>, 2018.
- [15] Paul Kocher. <https://www.paulkocher.com/doc/MicrosoftCompilerSpectreMitigation.html>, 2018.
- [16] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *IEEE Symposium on Security and Privacy*, 2018.
- [17] Esmaeil Mohammadian Koruyeh, Khaled N. Khasawneh, Chengyu Song, and Nael Abu-Ghazaleh. Spectre returns! speculation attacks using the return stack

- buffer. In *USENIX Workshop On Offensive Technologies*, 2018.
- [18] Volodymyr Kuznetsov, Laszlo Szekeres, Mathias Payer, George Candea, R. Sekar, and Dawn Song. Code-pointer integrity. In *11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14)*, pages 147–163, Broomfield, CO, October 2014. USENIX Association.
- [19] Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee. Last-level cache side-channel attacks are practical. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, SP ’15, pages 605–622, Washington, DC, USA, 2015. IEEE Computer Society.
- [20] Giorgi Maisuradze and Christian Rossow. Ret2spec: Speculative execution using return stack buffers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS ’18*, pages 2109–2122, New York, NY, USA, 2018. ACM.
- [21] Andrea Mambretti, Matthias Neugschwandtner, Alessandro Sorniotti, Engin Kirda, William Robertson, and Anil Kurmus. Speculator: A tool to analyze speculative execution attacks and mitigations. In *To appear in proceedings of the 35th Annual Computer Applications Conference ACSAC*, San Juan, PR, USA, December 2019. ACS Association.
- [22] Andrea Mambretti, Alexandra Sandulescu, Matthias Neugschwandtner, Alessandro Sorniotti, and Anil Kurmus. Two methods for exploiting speculative control flow hijacks. In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, August 2019. USENIX Association.
- [23] Ross McIlroy, Jaroslav Sevcik, Tobias Tebbi, Ben L. Titzer, and Toon Verwaest. Spectre is here to stay: An analysis of side-channels and speculative execution, 2019.
- [24] Ryan Roemer, Erik Buchanan, Hovav Shacham, and Stefan Savage. Return-oriented programming: Systems, languages, and applications. *ACM Trans. Inf. Syst. Secur.*, 15(1):2:1–2:34, March 2012.
- [25] Michael Schwarz, Martin Schwarzl, Moritz Lipp, Jon Masters, and Daniel Gruss. Netspectre: Read arbitrary memory over network. In Kazuo Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *Computer Security – ESORICS 2019*, pages 279–299, Cham, 2019. Springer International Publishing.
- [26] Laszlo Szekeres, Mathias Payer, Tao Wei, and Dawn Song. SoK: Eternal War in Memory. In *IEEE Symposium on Security and Privacy*, 2013.
- [27] Caroline Tice, Google Inc, Tom Roeder, Google Inc, Peter Collingbourne, Google Inc, Stephen Checkoway, Úlfar Erlingsson, Google Inc, Luis Lozano, Google Inc, and Geoff Pike. Enforcing forward-edge control-flow integrity. In *in GCC & LLVM. In 23rd USENIX Security Symposium (USENIX Security 14) (Aug. 2014)*, USENIX Association, pages 941–955, 2014.
- [28] Paul Turner. Retpoline: a software construct for preventing branch-target-injection. <https://support.google.com/faqs/answer/7625886>, 2018.
- [29] Victor van der Veen, Nitish dutt Sharma, Lorenzo Cavallaro, and Herbert Bos. Memory errors: The past, the present, and the future. In *Proceedings of the 15th International Conference on Research in Attacks, Intrusions, and Defenses, RAID’12*, pages 86–106, Berlin, Heidelberg, 2012. Springer-Verlag.
- [30] Dan Williams. Sanitize speculative array dereferences. <https://lore.kernel.org/patchwork/patch/874621/>, 2018.
- [31] Google Project Zero. Reading privileged memory with a side-channel. <https://googleprojectzero.blogspot.ch/2018/01/reading-privileged-memory-with-side.html>, 2018.