TYPESHIELD: Precise Protection of Forward Indirect Calls in Binaries

Your N. Here
Your Institution

Second Name
Second Institution

Abstract

High security, high performance and high availability applications are usually implemented in C/C++ for modularity, performance and compatibility to name just a few reasons. Virtual functions, which facilitate late binding, are a key ingredient in facilitating run-time polymorphism in C++ because it allows and object to use general (its own) or specific functions (inherited) contained in the class hierarchy. Despite the alarmingly high number of *vptr* corruption vulnerabilities, the *vptr* corruption problem has not been sufficiently addressed by researchers.

In this paper, we present *TypeShield*, a run-time *vptr* corruption detection tool. It is based on instrumentation of executables at load time and uses a novel run-time type and function parameter counter technique in order to overcome the limitations of current approaches and efficiently verify dynamic dispatching during runtime. In particular, *TypeShield* can be automatically and easily used in conjunction with legacy applications or where source code is missing. It achieves higher caller/caller matching (precision) and with reasonable run-time overhead. We have applied *TypeShield* to web servers, FTP servers and SPEC CPU2006 benchmark and were able to efficiently and with low performance overhead protect this applications from forward indirect edge *vptr* based corruptions. Our evaluation shows that our target reduction schema achieves an additional reduction of the possible call targets per call-site of up to 20% with an overall reduction of about 9% when comparing with other state-of-the-art parameter count based approaches.

1 Introduction

Motivation. Control-Flow Integrity (CFI) [5, 6] is one of the most used techniques to secure program execution flows against advanced Code-Reuse Attacks (CRAs). Advanced CRAs such as the recently published COOP [42] and its extension [18] or the attacks described by the Control Flow Bending paper [15] are able to bypass most traditional CFI solutions, as they focus on indirect call-sites, which are not as easy to determine at compile time.

Problem. This is a problem for applications written in C++, as one of its principle is inheritance and virtual functions. The concept of virtual functions allows the programmer to overwrite a virtual function of the base-class with his own implementation. While this allows for much more flexible code, this flexibility is the reason COOP actually works. The problem is that in order to implement virtual functions, the compiler needs to generate a table of all virtual functions for each class containing them and provide each instantiation of such a class with a pointer to said table. COOP now leverages a memory corruption to inject their own object with a fake virtual pointer, which basically gives him control over the whole program, while the control flow still looks genuine, as no code was replaced.

Current solutions. There exist several source code based solutions that either insert run-time checks during the compilation of the program like SafeDispatch [22], ShrinkWrap [21] or IFCC/VTV [44], which is the solution it is based on. Others modify and reorder the contents of the virtual table as their main aspect like the paper by Bounov et al. [11]. While the recently published Redactor++ [18] implements a combination of those ideas.

While this might seem that only C++ is vulnerable, while C is safe, this notion is wrong, as the Control Flow Bending paper [15] proposes attacks on nginx leveraging global function pointers, which are used to provide configurable behavior.

As previously mentioned, there exist many solutions when one tries to tackle this problem while access to the application in question is provided. However, when we are faced with proprietary third party binaries, which are provided as is and without the actual source code, the number of tools that can protect against COOP or similar attacks is rather low.

Limitations. TypeArmor [46] implements a fine grained forward edge CFI policy based on parameter count for binaries. It calculates invariants for call targets and indirect call sites based on the number of parameters they use by leveraging static analysis of the binary, which then is patched to enforce those invariants during run-time. The main shortcoming of TypeArmor is that even with high precision in the classification of call targets and call sites, one cannot exclude call targets with lower parameter number from call sites, for one due compatibility and also due to variadic functions, which are a special case in themselves. This basically means that

when a call site prepares 6 parameters, it is able to call all address taken functions. This generates a considerable attack surface due to the many situations in which this policy can be naturally circumvented.

In this paper, we present TYPESHIELD, a runtime illegitimate forward calls detection tool that can be seamlessly integrated with large scale applications such as web servers. It takes the binary of an program as input and it can automatically instrument the binary in order to detect illegitimate indirect calls at runtime. We implemented TYPESHIELD to demonstrate a possible remedy of this problem by introducing parameter types into the classification of call-sites and call-targets. We explore to what extent we can further narrow down the set of possible targets for indirect call sites and manage to stop the exploitation at the binary level w.r.t. TypeArmor. Our conclusion is that our tool can not stop all possible attacks since even solutions with access to source code are unable to protect against all possible attacks [9]. Nevertheless, we show that TYPESHIELD, our binary based tool can stop all COOP attacks published to date and significantly raises the bar for an adversary when compared our tool with TypeArmor and other similar tools. Moreover, TYPESHIELD provides strong mitigation for many types of code-reuse attacks (CRAs) for program binaries, without the need for source code.

Our Insight. TYPESHIELD is based on a forward-edge CFI policy that relies on a precise construction both the calle prototypes and callsite signatures and than uses this information to enforce that each callsite targets matching functions only. For example, TYPESHIELD disallows an indirect call that prepares fewer arguments than the target callee consumes and where the types of the arguments provided are not super types of the arguments expected at the target. Additionally, TYPESHIELD incorporates an improved protection policy which further reduces the possible target set of callees for each callsite. Our novel policy is based on the insight that if the binary adhere to the standard calling convention for indirect calls, undefined arguments at the callsite are not used by any callee by design. TYPESHIELD trashes these so-called spurious arguments and thus breaks all published COOP and improved COOP-like exploits. These exploits all chain virtual method calls that disrespect calling conventions to achieve convenient data flows between gadgets [13].

Current binary based techniques enforce imprecise forward-edge CFI plocies, often allowing controll transfers from any valid callsite to any valid referenced entry point [33], [34]. In the best case, existing policies only reduce the target set by removing all entry points of other modules unless they were explicitly exported or observed at runtime [24]. In contrast, TYPESHIELD matches up indirect callsites with a more precise target set in a considerably more precise many-to-many relationship than TypeArmor. It is based on a use-def analysis at all possible callees to approximated the function prototypes, and liveness analysis at indirect callsites to approximate callsite signatures. This efficiently leads to a more precise CFG of the binary progrma in question, which could be used by other systems in order to gain more a precise CFG on which to enforce their policies.

TYPESHIELD can protect only forward indirect edges at the binary level. Previous research has shown that, a backward-edge protection such as an shadow stack [14] or context-sensitive CFI [30] is still essential to ensure the integrity of return addresses at runtime [9], [18]. In this paper, we assume an ideal backward-edge protection mechanism such as a shadow stack with no design faults [12]. TYPESHIELD complements such backward-edge defenses by addressing attacks that take place without violating the integrity of the return path. Specifically, TYPESHIELD provides a precise protection against against COOP exploits as well as improved COOP derivations [18, 29, 1, 27].

TYPESHIELD is not more superior than source code based approaches such as IFCC/VTV [44]. IFCC/VTV are strong compiler based defenses which produce binaries which can resist control-flow hijacking attacks. It is well known that source-code based techniques are more precise when enforcing fine-grained policies based on program constructs (such as the C++ vtable hierarchy or generic data types) for mitigation purposes. However, there are still important reasons to study and improve binary-level defenses. First, the source code for many off-the-shelf programs is not always available. Second, real-world programs rely on a plethora of shared libraries and recompiling all shared libraries is not always possible. This is true even for purely open-source projects. Third, even if the source code of the libraries is available, recompiling big projects with dynamic dependencies is, again, a demanding task. Even state-of-the art defenses that enforce CFI policies at the source level such as Interleaving [ref] do not support dynamic libraries. Notice that mixing CFI-protected with non-protected code is impossible since applying CFI only on a part of the CFG would crash legitimate executions. In contrast, with a binary-level solution, we can offer strong protection even if the source code is not available or when recompilation is not feasible (or desirable).

Contributions. In summary, we make the following contributions:

- **Security analysis of forward indirect calls.** We analyzed the usage of illegitimate indirect forward calls in detail, thus providing security researchers and practitioners a better understanding of this emerging attack vector.
- **Illegitimate indirect calls detection tool.** We designed and implemented TYPESCHIELD, a general, automated, and easy to deploy tool that can be applied to C/C++ binaries in order to detect and mitigate illegitimate forward indirect calls during runtime. An open-source implementation of TYPESCHIELD is available at `https://github.com/tba/typeshield`.
- **Experiments.** We demonstrate trough extensive experiments that our precise binary-level CFI strategy can mitigate advanced code reuse attacks in absence of C++ semantics. For example TYPESCHIELD can protect against COOP [42] and its currently published variations [1, 18, 27, 29].

Outline. The rest of this paper is organized as follows. § 2 explains forbidden forward indirect calls issues and their security implications. § 3 contains a high level overview of TYPESHIELD. § 4 describes the theory used and decisions made during the design of TYPESHIELD. § 5 briefly presents the implementation details of TYPESHIELD. § 6 evaluates several properties of TYPESHIELD and § 7 surveys related work, respectively. § 8 contains the discussion, respectively while § 9 highlights future research venues. Finally, § 10 concludes this paper.

2 C++ Forbidden Forward Calls Exposed

Polymorphism in C++. Polymorphism along inheritance and encapsulation are the most used modern object-oriented concepts in C++. Polymorphism in C++ allows to access different types of objects through a common base class. A pointer of the type of the base object can be used to point to object(s) which are derived from the base class. In C++ there are several types of polymorphism: *a)* compile-time (or static, usually is implemented with templates), *b)* run-time (dynamic, is implemented with inheritance and virtual functions), *c)* ad-hoc (e.g., if the range of actual types that can be used is finite and the combinations must be individually specified prior to use), and *d)* parametric (e.g., if code is written without mention of any specific type and thus can be used transparently with any number of new types it is called parametric polymorphism). The first two are implemented through early and late binding, respectively. In C++, overloading concepts fall under the category of *c)* and Virtual functions; templates or parametric classes fall under the category of pure polymorphism. C++ provides polymorphism through: *i)* virtual functions, *ii)* function name overloading, and *iii)* operator overloading. In this paper, we will be concerned with dynamic polymorphism—based on virtual functions (10.3 and 11.5 in ISO/IEC N3690 [23])—because these can be exploited to call: *x)* illegitimate vTable entries not/-contained in the class hierarchy by varying or not the number of parameters and types, *y)* legitimate vTable entries not/contained in the class hierarchy by varying or not the number of parameters and types, *z)* fake vTables entries not contained in the class hierarchy by varying or not the number of parameters and types. By legitimate and illegitimate vTable entries we mean those vTable entries which for a single indirect call site lie in the vTable hierarchy. More precisely, a vTable entry is legitimate for a call site if from the call site to the vTable containing the entry there is an inheritance path (see [21]). Virtual functions have several uses and issues associated, but for the scope of this paper we will look at the indirect call sites which are exploiter by calling illegitimate vTable entries (functions) with varying number and type of parameters, *x)*. More precisely, *1)* load-time enforcement: as calling each indirect call site (callee) requires a fix number of parameters which are passed each time the caller is calling, we enforce a fine-grained CFI policy by statically determining the number and types of all function parameter that belong to an indirect call site. *2)* run-time verification: as

```
1  class nsMultiplexInputStream final
2   :public nsIMultiplexInputStream //A0
3   ,public nsISeekableStream //A1
4   ,public nsIIPCSerializableInputStream //A2
5   ,public nsICloneableInputStream{ //A3
6  nsTArray<nsCOMPtr<nsIInputStream>> mStreams;
7  NS_IMETHODIMP nsMultiplexInputStream::Close(){
8    MutexAutoLock lock(mLock);
9    mStatus = NS_BASE_STREAM_CLOSED;
10   //set NS_OK flag
11   nsresult rv = NS_OK;
12   //get array length
13   uint32_t len = mStreams.Length();
14   //array-based main loop gadget
15  for (uint32_t i = 0; i<len; ++i){
16   //(1) hijacked indirect call
17   nsresult rv2=mStreams[i]->Close();
18   if (NS_FAILED(rv2)) {
19       rv = rv2;
20   }
21  }
22   return rv;
23 }
```

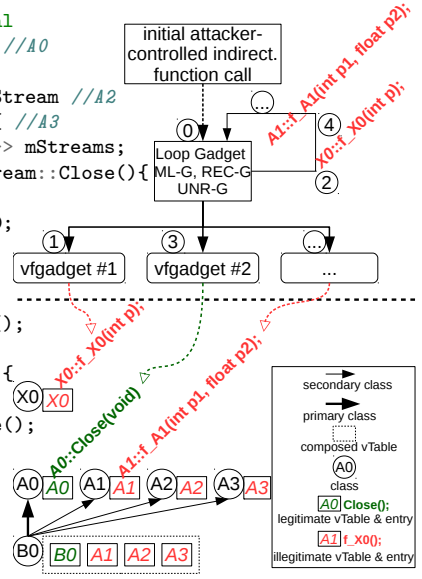

Figure 1: Code presenting how a COOP loop gadget works.

checking during run-time legitimate from illegitimate indirect caller/callee pairs requires parameter type (along parameter number), we check during run-rime before each indirect call-site if the caller matches to the callee based on the previously added checks.

Figure 1 depicts a C++ code example where it is illustrated how a COOP loop gadget (ML-G, REC-G, UNR-G, see [18]) works. (1) can be exploited in several ways, see *x), y) and z)*. The indirect call site (line 17) can be exploited to call by passing a varying number of parameters and types on each object contained in the array a different vTable entry contained in the: *1)* class hierarchy (overall, whole program), *2)* class hierarchy (partial, only legitimate for this call site), *3)* vTable hierarchy (overall, whole program), *4)* vTable hierarchy (partial, only legitimate for this call site), *5)* vTable hierarchy and/or class hierarchy (partial, only legitimate for this call site), and *6)* vTable hierarchy and/or class hierarchy (overall, whole program). There is no language semantics—such as cast checks—in C++ for vCall sites dispatch checking and as consequence the loop gadget indicated in Figure 1 can basically call all around in the class and vTable hierarchy by not being constrained by any build in check during run-time. The attacker corrupts an indirect function call, ①, next she invokes gadgets, ①, ③, through the calls, ②, ④, contained in the loop. As it can be observed in in Figure 1 she can invoke from the same call site legitimate functions residing in the vTable inheritance path (this type of information is usually very hard to recuperate from executables) for this particular call site, indicated with green color vTable entries. However, a real COOP attack invokes illegitimate vTable entries residing in the whole initial program hierarchy (or the extended one) with less or no relationship to the initial call site, indicated with red color vTable entries.

Checking Indirect Forward-Edge Calls in Practice. As far as we know, there is only the IFCC/VTV [44] tools (up to 8.7% performance overhead) deployed in practice which can be used to check legitimate from illegitimate in-

direct forward-edge calls during compile time. vPointers are checked based on the class hierarchy. ShrinkWrap [21] (as far as we know not deployed in practice) is a tool which further reduces the legitimate vTbles ranges for a given indirect call site through precise analysis of the program class hierarchy and vTable hierarchy. Evaluation results show similar performance overhead but more precision w.r.t. to legitimate vTables entries per call site. We noticed by analyzing the previous research results that the overhead incurred by these security checks can be very high due to the fact that for each call site many range checks have to be performed during runtime. Therefore, despite its security benefit these types of checks can not be applied in our opinion to high performance applications.

As alternative, there are other highly promising tools (not deployed in practice) that can be used to mitigate some of the drawbacks of the previous tools. Bounov et al [11] presented a tool ($\approx$ 1% runtime overhead) for indirect forward-edge call site checking based on vTable layout interleaving. The tool has better performance than VTV and better precision w.r.t. allowed vTables per indirect call site. Its precision (selecting legitimate vTables for each call site) compared to ShrinkWrap is lower since it does not consider vTable inheritance paths. vTrust [48] (average run-time overhead 2.2%) enforces two layers of defense (virtual function type enforcement and vTable pointer sanitization) against vTable corruption, injection and reuse. TypeArmor [46] ($\leq$ than 3 % runtime overhead) enforces an CFI policy based on runtime checking of caller/caller pairs based on function parameter count matching (coarse grained, parameter types and more than six parameters can be used as well). Important to notice is that there are no C++ language semantics which can be used to enforce type and parameter count matching for indirect call/callee pairs, this could be addresses with specifically intended language constructs in future.

Security Implications of Forbidden Indirect Calls. The C++ language standard (12.7 [23]) does not specify what happens when calling different vTable entries from an indirect call site. The standard says that we have have a virtual function related undefined behavior when: "a virtual function call uses an explicit class member access and the object expression refers to the complete object of x or one of that object's base class subobjects but not x or one of its base class subobjects". As undefined behavior is not a clearly defined concept we argue that in order to be able to deal with undefined behavior or unspecified behavior related to virtual function calls one needs to know how these language dependent concepts are implemented inside the used compilers.

Forbidden forward-edge indirect calls are the result of a vPointer corruption. A vPointer corruption is not a vulnerability but rather a capability which can be the result of a spatial or temporal memory corruption through: (1) bad-casting [28] of C++ objects, (2) buffer overflow in a buffer adjacent to a C++ object or a use-after-free condition [42]. A vPointer corruption can be exploited in several ways. A manipulated vPointer can be exploited by pointing it in any existing or added program vTable entry or into a fake vTable which was added by an attacker. For example in case a vPointer was corrupted than the attacker could highjack the control flow of the program and start a COOP attack [42].

vPointer corruptions are a real security threat which can be exploited if there is a memory corruption (e.g. buffer overflow) which is adjacent to the C++ object or a use-after-free condition. As a consequence each corruption which can reach an object (e.g. bad object casts) is a potential exploit vector for a vPointer corruption. Interestingly to notice in this context is that through: (1) memory layout analysis (through highly configurable compiler tool chains) of source code based locations which are highly prone to memory corruptions such as declarations and uses of buffers, integers or pointer deallocations one can obtain the internal machine code layout representation. (2) analysis of a code corruption which is adjacent (based on (1)) to a C++ object based on application class hierarchy, the vTble hierarchy and each location in source code where an object is declared and used (e.g., modern compiler tool chains can spill out this information for free), one can derive an analysis which can determine—up to a certain extent—if a memory corruption can influence (is adjacent) to a C++ object.

Finally, we notice that by building tools based on this two concepts (i.e., (1) and (2)) attackers (e.g., used to find new vulnerabilities) and for defenders which can harden the source code with checks only at the places which are most exposed to such vulnerabilities (i.e., we name this targeted security hardening).

Real COOP Attack Example. The given example depicted in Figure 2 is a proof of concept exploit extracted from [42] and used in order to perform a COOP attack on the Firefox browser. A buffer overflow bug was used in order to call into existing vTable entries by using the a main loop gadget. The attack concludes with opening of an Unix shell. A real-world bug, CVE-2014-3176, was exploited by Crane et al. [18] in order to perform another COOP attack on the Chromium browser. The details of the second attack are far to complex (i.e., involves not properly handled interaction of extensions, IPC, the sync API, and Google V8) and for this reason we briefly present the first documented COOP exploit on a Linux machine.

The C++ class `nsMultiplexInputStream` contains a main loop gadget inside the function `nsMultiplexInputStream::Close(void)` which is performing an indirect calls by dispatching indirect calls on the objects contained in the array. The objects contained in the array during normal execution are of type `nsInputStream` and each of the objects will call the `Close(void)` function in order to close each of the previously opened streams. In order to perform the COOP attack the attacker crafts a C++ program containing a array buffer holding six fake objects. Fake objects can call inside (and outside) the initial class and vTable hierarchies with no constraints. During the attack a buffer is created in order to hold the fake objects. The crafted buffer will be called in stead of the real code in order to call different functions available in the program code. For example the attacker calls a function contained in the

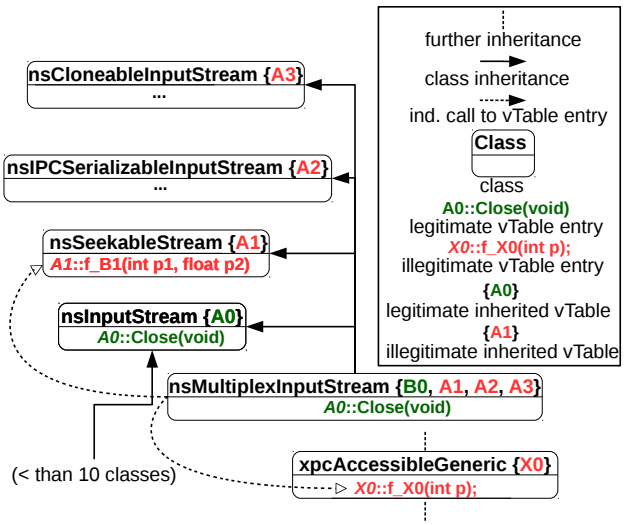

Figure 2: Class inheritance hierarchy of the classes involved in the COOP attack against the Firefox browser. Red letters indicate forbidden vTble entries and green letters indicate allowed vTable entries for the given indirect call site contained in the main loop gadget.

class `xpcAccessibleGeneric` which is not in the class hierarchy or vTable hierarchy of the initially intended type of objects used inside the array. Moreover, the header file of this class (`xpcAccessibleGeneric`) is not included in the class `nsMultiplexInputStream`. In total six fake objects are used to call into functions residing in not related class hierarchies with varying number of parameters and return types. The final goal of this attack is to prepare the program memory such that a Unix shell can be opened at the end of this attack.

This example illustrates why detecting vPointer corruptions is not trivial for real-world applications. As depicted in Figure 2 the class `nsInputStream` has 11 classes which inherit directly or indirectly from this class. The classes `nsSeekableStream`, `nsIPCSerializableInputStream` and `nsClonea-bleInputStream` provide additional inherited vTables which represent illegitimate call targets for the initial `nsInputStream` objects and legitimate call targets for the six fake objects which were added during the attack. Furthermore, declaration and usage of the objects can be wide spread in the source code. This makes detection of the object types (base class), range of vTables (longest vTable inheritance path for a particular call site) and parameter types of the vTable entries (functions) in which it is allowed to call a trivial task for source code (current research work is mostly concerned with performance issues) applications but a hard task in our opinion when one wants to apply similar security policies (e.g. which rely on parameter types of vTable entries) to executables.

3 Overview

Adversary Model and Assumptions. We largely use the same threat model and the same basic assumptions as described in the TypeArmor paper [46], meaning that our attacker has read and write access to the data sections of the attacked binary. We also assume that the protected binary does not contain self modifying code, handcrafted assembly or any kind of obfuscation. We also consider pages to be either writable or executable but not both at the same time. Furthermore we assume that our attacker has the ability to execute a memory corruption to hijack the programs control flow. We assume that a solution for backward CFI is in place.

Invariants for Targets and Callsites. Advanced code reuse attacks change the calltargets that are invoked within indirect call-sites. As standard CFI solutions can hardly restrict these, TypeArmor proposed using two base invariants:

1. Indirect call-sites provide a number of parameters (possibly overestimated compared to source)
2. Call-targets require a minimum number of parameters (possibly underestimated compared to source)

The idea is that a call-site might only call functions that do not require more parameters than provided by the call-site. To compute the necessary information, TypeArmor uses a modified version of forward liveness analysis for call-targets and backward reaching definitions analysis for call-sites.

TypeShield Impact on COOP. The problem with relying solely on the parameter count is that a call-site can use any call-target as long as the parameter count requirement is fulfilled, even if the parameter types do not match (imagine 8bit values provided but 64bit values required). Therefore we extend the classification schema to the parameter types:

1. Indirect call-sites provides a maximum wideness to each parameter (possibly overestimated compared to source)
2. Call-targets require a minimum wideness for each parameter(possibly underestimated compared to source)

The basic idea stays the same, the provision must be no lower than the rqeuirement. However, the approach is more fine-grained applying to the wideness of each parameter. The result is that we split the buckets of TypeArmor up into smaller ones, as shown in the limited example Figure 3. There we can see that while in a parameter-count oriented schema a call-site classified as (32,32) would be able to call functions classified as (64,0), however in our parameter wideness oriented schema that is not possible.

4 Design

In this section, we cover the design of TypeShield. We first present the details of the *count* policy in § 4.1—as introduced by [46]—and the new *type* policy in § 4.2. Then we describe

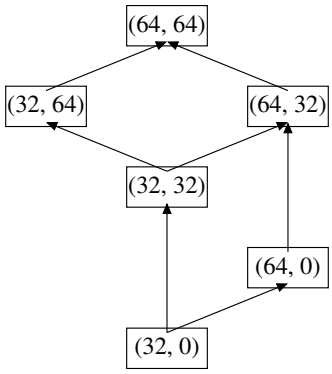

Figure 3: Example for the wideness based schema when only using a parameter wideness of 64, 32 and 0 bits and only two parameters.

general theory needed to transform set-based analysis to register based ones in § 4.3. We follow this up by presenting the theory needed implement the analysis for call-targets in § 4.4 and call-sites in § 4.5 for each policy. Finally, in § 4.6 we introduce a version of address taken analysis based on [51] to restrict the number of available call-targets even more.

4.1 *Count* Policy

What we call the *count* policy is essentially the policy introduced by TypeArmor [46]. The basic idea revolves around classifying call-targets by the number of parameters they provide and call-sites by the number of parameters they require. The schema to match those is that we have call-targets requiring parameters and the call-sites providing parameters as depicted in Figure 4.

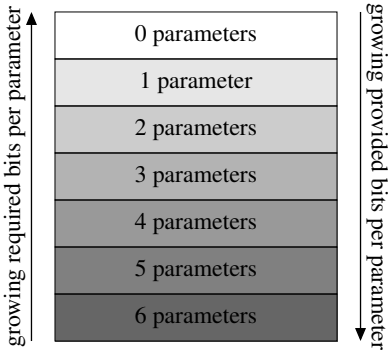

Figure 4: *Count* policy classification schema for call-sites and call-targets.

Furthermore, generating 100% precise measurements for such classification with binaries as the only source of information is rather difficult. Therefore over-estimations of parameter count for call-sites and underestimations of the parameter count for call-targets is deemed acceptable. This classification is based on the general purpose registers that the call convention of the current ABI—in this case the SystemV ABI—designates as parameter registers. Furthermore, we completely ignore floating point registers or multi-integer registers. The core of the *count* policy is now to allow any call-site *cs*, which provides c_{cs} parameters, to call any call-target *ct*, which requires c_{ct} parameters, iff $c_{ct} \leq c_{cs}$ holds. However, the main problem is that while there is a significant restriction of call-targets for the lower call-sites, the restriction capability drops rather rapidly when reaching higher parameter counts, with call-sites that use 6 or more parameters being able to call all possible call-targets: $\forall cs_1, cs_2.c_{cs_1} \leq c_{cs_2} \implies \|\{ct \in \mathscr{F} | c_{ct} \leq c_{cs_1}\}\| \leq \|\{ct \in \mathscr{F} | c_{ct} \leq c_{cs_2}\}\|$ One possible remedy would be the ability to introduce an upper bound for the classification deviation of parameter counts, however as of now, this does not seem feasible with current technology. Another possibility would be the overall reduction of call-sites, which can access the same set of call-targets, a route we will explore within this work.

4.2 *Type* Policy

What we call the *type* policy is the idea of not only relying on the parameter count but also on the type of a parameter. However due to complexity reasons, we are restricting ourselves to the general purpose registers, which the SystemV ABI designates as parameter registers. Furthermore we are not inferring the actual type of the data but the wideness of the data stored in the register. The schema again is that we have call-targets requiring wideness and the call-site providing wideness as depicted in Figure 5.

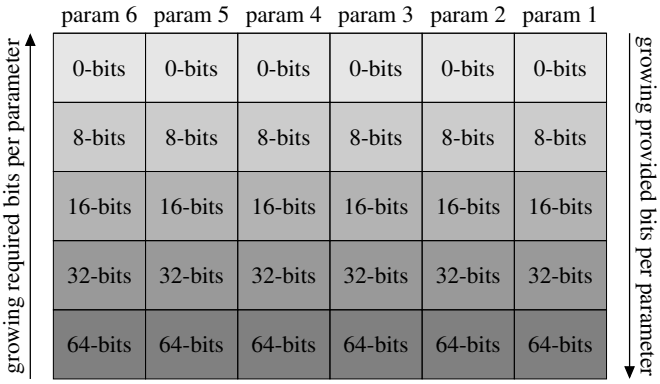

Figure 5: *Type* policy schema for call-sites and call-targets.

We are currently interested in x86-64 binaries, the registers we are looking at are 64-bit registers that can be accessed in four different ways: *1)* the whole 64-bits of the register, meaning a wideness of 64, *2)* the lower 32-bits of the register, meaning a wideness of 32, *3)* the lower 16-bits of the register, meaning a wideness of 16, and *4)* the lower 8-bits of the register, meaning a wideness of 8.

Four of those registers can also directly access the higher 8-bits of the lower 16-bits of the register. For our purpose we register this access as a 16-bit access. Based on this information, we can assign a register one of 5 possible types $\mathscr{T} = \{64, 32, 16, 8, 0\}$. We also included the type 0 to model the absence of data within a register. Similar to the *count*

policy, we allow overestimation of types in call-sites and underestimation of types in call-targets. However, the matching idea is different, because as can we depict in Figure 5, the type of a call-target and a call-site no longer depends solely on its parameter count, each call-site and call-target has its type from the set of $\mathscr{T}^6$, with the following comparison operator: $u \leq_{type} v :\Longleftrightarrow \forall_{i=0}^{5} u_i \leq v_i$, with $u, v \in \mathscr{T}^6$ Again we allow any call-site *cs* call any call-target *ct*, when it fulfills the requirement $ct \leq cs$. Meaning, just having an equal or lesser number of parameters than a call-site, does no longer allow a call-target being called there, thus restricting the number of call-targets per call-site even further. A function that requires 64-bit in its first parameter, and 0-bit in all other parameters, would have been callable by a call-site providing 8-bit in its first and second parameter when using the *count* policy, however in the *type* policy this is no longer possible. Thus it should decrease the number of targets per bucket.

4.3 Instruction Analysis

Usually data-flow analysis algorithms are based on set of variable or sets of definitions, which both are basically unbounded. However, we are analyzing the state of registers, which are baked into hardware and therefore their number is given, thus requiring us to adapt the data-flow theory to work on tuples.

The set $\mathscr{I}$ describes all possible instructions that can occur within the executable section of a binary. (in our case this is based on the instruction set for x86-64 processors)

An instruction $i \in \mathscr{I}$ can non-exclusively perform two kinds of operations on any number of existing registers:

1. Read *n*-bits from the register with $n \in \{64, 32, 16, 8\}$.
2. Write *n*-bits to the register with $n \in \{64, 32, 16, 8\}$.

Thus we describe the possible change that occurs in one register with the set $S = \{w64, w32, w16, w8, 0\} \times \{r64, r32, r16, r8, 0\}$. Note that 0 signals the absence of either a write or read access and $(0,0)$ signals the absence of both. Furthermore *wn* or *rn* with $n \in \{64, 32, 16, 8\}$ implies all *wm* or *rm* with $m \in \{64, 32, 16, 8\}$ and $m < n$ (e.g. *r*64 implies *r*32). Note that we exclude 0, as it means the absence of any access.

SystemV ABI specifies 16 general purpose integer registers, thus for our purpose we represent the change occurring at the processor level as $\mathscr{S} = S^{16}$.

At last we declare a function, which calculates the change occurring in the processor state, when executing an instruction from $\mathscr{I}$: $decode : \mathscr{I} \mapsto \mathscr{S}$

However, we do not go into detail how this function actually calculates this sate, because we rely on external libraries to perform this task. Implementing this function our self is out of scope due to the lengthy work required, as the x86-64 instruction set is quite large.

4.4 Call-target Analysis

For either *count* or *type* policy to work, we need to arrive at an underestimation of the required parameters by any function existing within the targeted binary. We will employ a modified version of liveness analysis that tracks registers instead of variables to generate the needed underestimation. As our algorithm will be customizable, we look at the required merge functions to implement *count* and *type* policy. Furthermore we need to eliminate the passing of variadic parameter lists from variadic functions, as this might cause our analysis to overestimate the required parameters.

Variable Liveness Analysis Theory. A variable is alive before the execution of an instruction, if at least one of the originating paths contains a read access before the variable is written to again. We employ liveness analysis, because we are looking for the parameters a function requires. This essentially requires read before write access, however global variables usually would also fall into this category, however these would not reside within parameter registers at the start of a function.

Khedker et al. [24] defines live variable analysis on blocks in the following manner:

$$In_n := (Out_n - Kill_n) \cup Gen_n \tag{1a}$$

$$Out_n := \begin{cases} Bl & \text{n is end block} \\ \bigcup\limits_{s \in succ(n)} In_s & \text{otherwise} \end{cases} \tag{1b}$$

Bl is the default state at the end of a path of execution and in our case reaching that state would mean that a variable has never been used (neither written nor read). The set $Kill_n$ describes all variables that are no longer live after the block *n*, meaning that a variable occurring within this set has been written to. The set Gen_n describes all variables that are alive due to the block *n*, meaning that a variable occurring within this set has been read before it was written to.

Function *analyze(block : BasicBlock) :* $\mathscr{S}^{\mathscr{L}}$ **is**
    state = Bl
    foreach *inst* $\in$ *block* **do**
        state' = analyze_instr(inst)
        state = merge_v(state, state')
    end
    states = { }
    blocks = succ(block)
    foreach *block'* $\in$ *blocks* **do**
        state' = analyse(block')
        states = states $\cup$ { state' }
    end
    state' = merge_h (states)
    return merge_v(state, state')
end

Figure 6: Algorithm to analyze the liveness of a Basic Block.

However, we cannot use variable liveness analysis as is, because the analysis is based on potentially unbound variable sets, while we are restricted to a finite number of registers and states. We also require an underestimation of live variables an not an overestimation as provided by standard liveness analysis. Furthermore we have to define how to interpret the changes occurring within one block based on the the change caused by its instructions. Considering this, we arrive at algorithm 6 to compute the liveness state at the start of a basic block.

This algorithm relies on various functions that can be used to configure its behavior. We need to define the function *merge_v*, which describes how to compound the state change of the current instruction and the current state, the function *merge_h*, which describes how to merge the states of several paths, the instruction analysis function *analyze_instr*. The function *succ*, which retrieves all possible successors of a block won't be implemented by us, because we rely on the DynInst instrumentation framework to achieve this.

$$merge\_v : \mathscr{S}^{\mathscr{L}} \times \mathscr{S}^{\mathscr{L}} \mapsto \mathscr{S}^{\mathscr{L}} \tag{2a}$$

$$merge\_h : \mathscr{P}(\mathscr{S}^{\mathscr{L}}) \mapsto \mathscr{S}^{\mathscr{L}} \tag{2b}$$

$$analyze\_instr : \mathscr{I} \mapsto \mathscr{S}^{\mathscr{L}} \tag{2c}$$

$$succ : \mathscr{I} \mapsto \mathscr{P}(\mathscr{I}) \tag{2d}$$

As the *analyze_instr* function calculates the effect of an instruction and is the heart of the analyze function. It will also handle non jump and non fall-through successors, as these are not handled by DynInst in our case. We essentially have four cases that we handle:

1. if the instruction is an indirect call or a direct call but we chose not follow calls, then return a state where all registers are considered written.

2. if the instruction is a direct call and we chose to follow calls, then we spawn a new analysis and return its result.

3. if the instruction is a constant write (e.g. xor of two registers) then we remove the read portion before we return the decoded state.

4. in all other cases we simply return the decoded state

This leaves us with the two merge functions remaining undefined and we will leave the implementation of these and the interpretation of the liveness state $\mathscr{S}^{\mathscr{L}}$ into parameters up to the following subsections.

Required Parameter Count. To implement the *count* policy, we only need a coarse representation of the state of one register, thus we are interested in the following three different exclusive informations:

1. Was the register written to before its value could be read ?
   We represent this with the state W.

$\bigsqcap^{\mathscr{L}}$	C	R	W
C	C	W	W
R	W	R	W
W	W	W	W

$\bigcap^{\mathscr{L}}$	C	R	W
C	C	C	W
R	C	R	W
W	W	W	W

$\bigcup^{\mathscr{L}}$	C	R	W
C	C	R	W
R	R	R	W
W	W	W	W

Table 1: Different mappings for combining two liveness state values in horizontal matching for the *count* policy.

2. Was the register read from before its value was overwritten ?
   We represent this with the state R.

3. Did neither read nor write access occur for the register ?
   We represent this with the state C.

This gives us the following register state $S^{\mathscr{L}} = \{C, R, W\}$ which translates to the register superstate $\mathscr{S}^{\mathscr{L}} = (S^{\mathscr{L}})^{16}$. Now, we assume that unless the instructions we are looking at does discard the value it is reading (`xor rax rax` would be such an instruction that we call const_write) that reading does precede the writing withing one instruction. Furthermore we are only interested in the first occurrence of a R or W within one path, as following reads or writes do not give us more information. Therefore, we can define our vertical merge function in the following way:

$$merge\_v^r(cur, delta) = \begin{cases} delta & cur = C \\ cur & otherwise \end{cases} \tag{3}$$

$$merge\_v(cur, delta) = (s'_0, ...s'_15) \text{ with } s'_j = merge\_v^r(cur_j, delta_j) \tag{4}$$

Our horizontal merge function is a simple pairwise combination of the given set of states:

$$merge\_h(\{s\}) = s \tag{5}$$

$$merge\_h(\{s\} \cup s') = s \circ merge\_h(s') \tag{6}$$

We have three viable possibilities for our combination operator $\circ$, depicted in Table 1, which all give priority to W:

$\bigsqcap^{\mathscr{L}}$ is what we call the destructive combination operator, as it returns W on any mismatch.

$\bigcap^{\mathscr{L}}$ is what we call the intersection operator, as it returns C, when combining C and R, similar to an intersection.

$\bigcup^{\mathscr{L}}$ is what we call the union operator, as it returns R, when combining C and R similar to a union.

We apply the liveness analysis for each function with the entry block of the function as start and the return blocks as end and after an analysis run for a function, the index of highest parameter register based on the used call convention that has the state R is considered to be the number of parameters a function at least requires to be prepared by a call-site.

Required Parameter Wideness. To implement the *type* policy, we need a finer representation of the state of one register, thus we are interested in the following three different not neccessarily exlusive informations:

1. Was the register written to before its value could be read ?
   We represent this with the state W.

2. How much was read from the register before its value was overwritten?
   We represent this with the states $\{r8, r16, r32, r64\}$ using R as a placeholder for arbitrary reads.

3. Did neither read nor write access occur for the register ?
   We represent this with the state C.

This gives us the following register state $S^{\mathscr{L}} = \{C, r8, r16, r32, r64, W\}$ which translates to the register superstate $\mathscr{S}^{\mathscr{L}} = (S^{\mathscr{L}})^{16}$. Now, we assume that unless the instructions we are looking at does discard the value it is reading (`xor rax rax` would be such an instruction that we call const_write) that reading does precede the writing withing one instruction.

As there could happen more than one read of a register before it is written, we might be interested in more than just the first occurrence of a write or read on a path. We arrive therefore at three possible vertical merge functions:

- The same vertical merge operator as used in the *count* policy, which only gives us the first non C state ($merge\_v^r$).
- A vertical merge operator that conceptually intersects all read accesses along a path until the first write occurs ($merge\_v^i$).
- A vertical merge operator that conceptually calculates the union of all read accesses along a path until the first write occurs ($merge\_v^u$).

Our horizontal merge function is a simple pairwise combination of the given set of states:

$$merge\_h(\{s\}) = s \tag{7}$$

$$merge\_h(\{s\} \cup s') = s \circ merge\_h(s') \tag{8}$$

The results of our experiments with the implementation of call-target classification gave presented us with essentially one possible candidate that we can base our horizontal merge function on, namely the union operator with an analysis function that follows into direct calls. The basic schema of the merging is depicted in 2 and it essentially behaves as if it was the union operator (when both states are set, the higher one is chosen). However, we have to account for W being used as an end marker, which is why we added mapping for RW, which is essentially that.

Variadic Functions. Variadic functions are special functions in C/C++ that have a basic set of parameters, which they always require and a variadic set of parameters, which as the name suggests may vary. A prominent example of this would be the *printf* function, which is used to output text to *stdout*.

The problem with these functions is that to allow for easier processing of parameters usually all potential variadic parameters are moved into a contiguous block of memory, as can be seen in the assembly in Figure 7. Our analysis interprets that as a read access on all parameters and we arrive at a problematic overestimation.

$\bigcup^{\mathscr{L}}$	C	R	W	RW
C	C	R	W	RW
R	R	$R^{\cup}$	W	$R^{\cup}W$
W	W	W	W	W
RW	RW	$R^{\cup}W$	W	RW

Table 2: The union mapping operator for liveness in the *type* policy.

```
00000000004222f0 <make_cmd>:
  4222f0:        push   %r15
  4222f2:        push   %r14
  4222f4:        push   %rbx
  4222f5:        sub    $0xd0,%rsp
  4222fc:        mov    %esi,%r15d
  4222ff:        mov    %rdi,%r14
  422302:        test   %al,%al
  422304:        je     42233d <make_cmd+0x4d>
  422306:        movaps %xmm0,0x50(%rsp)
  42230b:        movaps %xmm1,0x60(%rsp)
  422310:        movaps %xmm2,0x70(%rsp)
  422315:        movaps %xmm3,0x80(%rsp)
  42231d:        movaps %xmm4,0x90(%rsp)
  422325:        movaps %xmm5,0xa0(%rsp)
  42232d:        movaps %xmm6,0xb0(%rsp)
  422335:        movaps %xmm7,0xc0(%rsp)
  42233d:        mov    %r9,0x48(%rsp)
  422342:        mov    %r8,0x40(%rsp)
  422347:        mov    %rcx,0x38(%rsp)
  42234c:        mov    %rdx,0x30(%rsp)
  422351:        mov    $0x50,%esi
  422356:        mov    %r14,%rdi
  422359:        callq  409430 <pcalloc>
```

Figure 7: ASM code of the `make_cmd` function with optimize level O2, which has a variadic parameter list.

Our solution to this problem is to find these spurious reads and ignore them. A compiler will implement this type of operation very similar foll all cases, thus we can achieve this using the following steps:

- Look for what we call the xmm-passthrough block, which entierly consist of moving the values of registers `xmm0` to `xmm7` into contiguous memory (in our case basic block [`0x422306`, `0x42233d` [ ).
- Look at the predecessor of the xmm-passthrough block, which we call the entry block (in our case basic block [`0x4222f0`, `0x4222f2` [ ). Check if the successors of the entry block consist of the xmm-passthrough block and the successor of the xmm-passthrough block, which we call the param-passthrough block (in our case basic block [`0x42233d`, `0x42235e` [ ).
- Look at the param-passthrough block and set all instructions that move the value of a parameter register

into memory to be ignored (in our case the instructions `0x42233d`, `0x422342`, `0x422347` and `0x42234c`).

4.5 Call-site Analysis

For either *count* or *type* policy to work, we need to arrive at an overestimation of the provided parameters by any indirect call-site existing within the targeted binary. We will employ a modified version of reaching analysis that tracks registers instead of variables to generate the needed overestimation. As our algorithm will be customizable, we look at the required merge functions to implement *count* and *type* policy.

Reaching Definitions Theory. An assignment of a value to a variable is a reaching definition at the end of a block n, if that definition is present within at least one path from start to the end of the block n without being overwritten by another value assignment to the same variable. We employ reaching definitions analysis, because we are looking for the parameters a call-site provides. This essentially requires the last known set of definitions that reach the actual call instruction within the parameter registers.

The book [24] defines reaching definition analysis on blocks in the following manner:

$$In_n := \begin{cases} Bl & \text{n is start block} \\ \bigcup_{p \in pred(n)} Out_p & \text{otherwise} \end{cases} \tag{9a}$$

$$Out_n := (In_n - Kill_n) \cup Gen_n \tag{9b}$$

Bl is the default state at the start of a path of execution and in our case reaching that state would mean that we do not know whether a value has been provided for the variable and therefore we assume that one has been provided, reaching an overestimation. The set $Kill_n$ describes all definitions that are removed within this block, meaning that the value of a variable has been overwritten. The set Gen_n describes the new definitions that have been provided by the block n, meaning that the value of a variable has been assigned. Considering this, we can assume that $Gen_n \subseteq Kill_n$, as we can always create new definitions, but not simply remove definitions without assigning a new value to the variable.

However, we cannot use reaching definition analysis as is, because the analysis is again based on potentially unbound variable sets, while we are restricted to a finite number of registers and states. This time however the analysis provides us with an overestimation, we however want to get a result as close as possible so we again want to customize merge functions. Furthermore we have to define how to interpret the changes occuring withing one block based on the the change caused by its instructions. Considering this, w, we arrive at algorithm 8 to compute the liveness state at the start of a basic block.

This algorithm relies on various functions that can be used to configure its behavior. We need to define the function *merge_v*, which describes how to compound the state change of the current instruction and the current state, the function *merge_h*, which describes how to merge the states of several paths, the instruction analysis function *analyze_instr*. The function *pred*, which retrieves all possible predecessors of a block won't be implemented by us, because we rely on the DynInst instrumentation framework to achieve this.

```
Function analyze(block : BasicBlock) : 𝒮^ℛ is
    state = Bl
    foreach inst ∈ reversed(block) do
        state' = analyze_instr(inst)
        state = merge_v(state, state')
    end
    states = {}
    blocks = pred(block)
    foreach block' ∈ blocks do
        state' = analyse(block')
        states = states ∪ { state' }
    end
    state' = merge_h (states)
    return merge_v(state, state')
end
```

Figure 8: Algorithm to analyse the reaching definitions of a Basic Block.

$$merge\_v : \mathscr{S}^{\mathscr{R}} \times \mathscr{S}^{\mathscr{R}} \mapsto \mathscr{S}^{\mathscr{L}} \tag{10a}$$

$$merge\_h : \mathscr{P}(\mathscr{S}^{\mathscr{R}}) \mapsto \mathscr{S}^{\mathscr{R}} \tag{10b}$$

$$analyze\_instr : \mathscr{I} \mapsto \mathscr{S}^{\mathscr{R}} \tag{10c}$$

$$pred : \mathscr{I} \mapsto \mathscr{P}(\mathscr{I}) \tag{10d}$$

As the *analyze_instr* function calculates the effect of an instruction and is the heart of the analyze function. It will also handle non jump and non fall-through successors, as these are not handled by DynInst in our case. We essentially have three cases that we handle:

- if the instruction is an indirect call or a direct call but we chose not follow calls, then return a state where all trashed are considered written.
- if the instruction is a direct call and we chose to follow calls, then we spawn a new analysis and return its result.
- in all other cases we simply return the decoded state.

This leaves us with the two merge functions remaining undefined and we will leave the implementation of these and the interpretation of the liveness state $\mathscr{S}^{\mathscr{L}}$ into parameters up to the following subsections.

Provided Parameter Count. To implement the *count* policy, we only need a coarse representation of the state of one register, thus we are interested in the following three different exclusive informations:

- Was the register value trashed ?
  We represent this with the state T.
- Was the register written to ?
  We represent this with the state S.
- Was the register neither trashed nor written to ?
  We represent this with the state U.

$\sqcap^{\mathscr{R}}$	U	S	T
U	U	T	T
S	T	S	T
T	T	T	T

$\cap^{\mathscr{R}}$	U	S	T
U	U	U	T
S	U	S	T
T	T	T	T

$\cup^{\mathscr{R}}$	U	S	T
U	U	S	T
S	S	S	T
T	T	T	T

$\sqcup^{\mathscr{R}}$	U	S	T
U	U	S	T
S	S	S	S
T	T	T	T

Table 3: Different mappings for combining two reaching state values in horizontal matching for the *count* policy.

This gives us the following register state $S^{\mathscr{L}} = \{T, S, U\}$ which translates to the register superstate $\mathscr{S}^{\mathscr{R}} = (S^{\mathscr{R}})^{16}$. We are only interested in the first occurrence of a S or T within one path, as following reads or writes do not give us more information. Therefore, we can define our vertical merge function in the following way:

$$merge\_v^r(cur, delta) = \begin{cases} delta & cur = U \\ cur & otherwise \end{cases} \tag{11}$$

$$merge\_v(cur, delta) = (s'_0, ...s'_1 5) \text{ with } s'_j = merge\_v^r(cur_j, delta_j) \tag{12}$$

Our horizontal merge function is a simple pairwise combination of the given set of states:

$$merge\_h(\{s\}) = s \tag{13}$$

$$merge\_h(\{s\} \cup s') = s \circ merge\_h(s') \tag{14}$$

We have four viable possibilities for our combination operator $\circ$, depicted in table 3, which all (except one) give priority to T:

$\sqcap^{\mathscr{R}}$ is what we call the destructive combination operator, as it returns T on any mismatch.

$\cap^{\mathscr{R}}$ is what we call the intersection operator, as it returns U, when combining U and S, similar to an intersection.

$\cup^{\mathscr{R}}$ is what we call the union operator, as it returns S, when combining U and S similar to a union.

$\sqcup^{\mathscr{R}}$ is what we call the true union operator, as it gives S precedence over everything and returns T or U only when both sides are T or U being more inclusive than a union.

Provided Parameter Wideness. To implement the *type* policy, we need a finer representation of the state of one register, thus we are interested in the following three informations:

- Was the register value trashed ?
  We represent this with the state T.
- Was the register written to and how much ?
  We represent this with the states $\{s64, s32, s16, s8\}$ using S as a placeholder for arbitrary writes.
- Was the register neither trashed nor written to ?
  We represent this with the state U.

This gives us the following register state $S^{\mathscr{L}} = \{T, s64, s32, s16, s8, U\}$ which translates to the register superstate $\mathscr{S}^{\mathscr{R}} = (S^{\mathscr{R}})^{16}$. Again, we are only interested in the first occurrence of a state that is not U in a path, as following reads or writes do not give us more information.

$\cap^{\mathscr{R}}$	U	S	T
U	U	U	T
S	U	$S^{\cap}$	T
T	T	T	T

$\sqcap^{\mathscr{R}}$	U	S	T
U	U	U	T
S	U	$S^{\cup}$	T
T	T	T	T

$\cup^{\mathscr{R}}$	U	S	T
U	U	S	T
S	S	$S^{\cup}$	T
T	T	T	T

Table 4: Different mappings for combining two reaching state values in horizontal matching for the *type* policy.

Therefore we can use the same vertical merge function as for the *count* policy, which is essentially a pass-through until the first non U state.

Our horizontal merge function is again a simple pairwise combination of the given set of states:

$$merge\_h(\{s\}) = s \tag{15}$$

$$merge\_h(\{s\} \cup s') = s \circ merge\_h(s') \tag{16}$$

However, we have different possibilities regarding the merge operator. Experiments with our implementations for call-site classification in the *count* policy have given us the following results:

- The best candidate to minimize the problematic matches is the union operator without following direct calls.
- The best candidate to maximize precision is the intersection operator with following direct calls.

We therefore arrive at three viable possibilities for our combination operator $\circ$, depicted in table 4, which all (except one) give priority to T:

$\cap^{\mathscr{R}}$ is what we call the intersection operator, as it returns U, when combining U and S, similar to an intersection furthermore we also calculate the intersection of states when both states are set (the lower of the two is returned).

$\sqcap^{\mathscr{R}}$ is what we call the half intersection operator, as it returns U, when combining U and S, similar to an intersection but we calculate the union of states when both states are set (the higher of the two is returned).

$\cup^{\mathscr{R}}$ is what we call the union operator, as it returns S, when combining U and S similar to a union furthermore we calculate the union of states when both states are set (the higher of the two is returned).

Initial experiments with this implementation showed two problems regarding provided wideness detection. Parameter lists with "holes" and address wideness underestimation.

Parameter Lists with *Holes*. This refers to parameter lists that show one or more `void` parameters between start to the last actual parameter. These are not existant in actual code but our analysis has the possibility of generating them through the merge operations. An example would be the following: A

parameter list of $(64,0,64,0,0,0)$ is concluded, although the actual parameter list might be $(64,32,64,0,0,0)$. While the trailing 0es are what we expect, the 0 at the second parameter position will cause trouble, because it is an underestimation at the single parameter level, which we need to avoid. Our solution is to simply scan our reaching analysis result for these holes and replace them with the wideness 64, causing a (possible) overestimation.

Address Wideness Unterestimation. refers to the problem that while in the call-site a constant value of 32-bit is written to a register, however the call-target uses the whole 64-bit register. This can occur when pointers are passed from the call-site to the call-target. Specifically this happens when pointers to memory inside the ".bss", ".data" or ".rodata" section of the binary are passed. Our solution is to enhance our instruction analysis to watch out for constant writes. In case a 32-bit constant value write is detected, we check if the value is an address within the ".bss", ".data" or ".rodata" section of the binary. If this is the case, we simply return a write access of 64-bits instead of 32-bits. (This is not problematic, because we are looking for an overestimation of parameter wideness) It should be noted that the same problem can arise when a constant write causes the value 0 to be written to a 32-bit register. We use the same solution and set the wideness to 64-bits instead of 32-bits.

4.6 Address Taken Analysis

As of now, we use the maximum available set of call-targets—the set of all function entry basic blocks—as input for our algorithm. To restrict the number of call-targets per call-site even further, we explored the possibility of incorporating an address taken analysis into our application. We base our theory on the paper by Zhang et al. [51], which introduced various types of taken addresses. An address is considered to be taken, when it is loaded into memory or a register.

Address Taken Targets. Based on the notions of [51], which classified taken addresses into several types of indirect control flow targets, we only chose Code Pointer Constants (CK) and discarded the others:

- Code Pointer Constants (CK) are addresses that are calculated during the compilation of the binary and point within the possible range of addresses in the current module or to instruction boundaries. We are however only interested in addresses that directly point to an entry basic block of a function, as these are the only valid targets for any call-site.
- Computed code pointers (CC) are the result of simple pointer arithmetic, however these are only used for intra-procedural jumps. We rely on DynInst to resolve those and only focus on indirect call-sites, therefore these are of no interest to us.
- Exception handling addresses (EH) are used to handle exceptions within C++ functions and are modeled as jumps within the function. These are therefore within the normal control flow that we rely on DynInst to resolve for us.
- Exported function addresses (ES) are essentially functions that point outside of our current module (usually to dynamically linked libraries) and are implemented as jumps, which are of no concern to us, because our analysis is only concerned about the current object.
- Return addresses (RA), which are the addresses next to a call instruction, are also of no interest to us, because we only implement forward control flow integrity.

Binary Analysis. Our approach of identifying taken addresses consists of two steps: First, we iterate over the raw binary content of data sections. Second, we iterate over all functions within the disassembled binary. We rely on DynInst to provide us with the boundaries of the sections inside the binary and in case of shared libraries with the needed translation to current memory addresses:

- We look at three different data sections of the binary, which could possibly contain taken addresses: the .data, .rodata and .dynsym sections. As [51] proposed, we slide a four byte window over the data within those sections and look for addresses that point to function entry blocks. However, we are looking at x64 binaries therefore we additionally use an eight byte window. In case of shared libraries, we need to let DynInst translate the raw address, we extracted, so we can perform the function check.
- We specifically look for instructions that load a constant value into a register or memory, and again check whether the address points to the entry block of a function.

5 Implementation

We implemented TYPESHIELD as a module pass for the *dyninst* environment pass provided by the DynInst [9] instrumentation framework (v. 9.2.0). However, converting the pass to a standalone executable is also possible, as we do not rely on an extended set of DynInst features except for the pass abstraction.

We currently restricted our analysis and instrumentation to x86-64 bit elf binaries using the SystemV call convention, because the DynInst library does not yet support the Windows platform. However, there is currently work going on in order to allow DynInst to work with Windows binaries as well. We focused on the SystemV call convention as most C/C++ compilers on Linux implement this ABI, however we encapsulated most ABI dependent behavior, so it should be possible to implement other ABIs with relative ease. Therefore, we deem it possible to implement TYPESHIELD for the Windows platform in the near future, as we do not use any other platform-dependent API's.

We developed the core part of our pass in an instruction analyzer, which relies on the DynamoRIO [2] library (v. 6.6.1)

to decode single instructions and provide access to its information. The analyzer is then used to implement our version of the reaching and liveness analysis (similar to PathArmor [46]), which can be customized with relative ease, as we allow for arbitrary path merging functions. However, we implemented the three basic versions as follows: destructive, intersection and union. In order to accomplish this we patched the DynInst library in order to allow for local annotation of call-targets with arbitrary information, leveraging its relocation schema, which relies on the basic block abstraction.

We implemented a Clang/LLVM (v. 4.0.0, trunk 283889) pass used for collecting ground truth data in order to measure the quality and performance of our tool. The ground truth data is then used to verify the output of our tool for several test targets. This is accomplished with the help of our python based evaluation and test environment.

In total we implemented TYPESHIELD in 5123 source code lines (SLoC) of C++ code, our Clang/LLVM pass in 200 SLoC of C++ code and our test environment in 2674 SLoC of Python code.

6 Evaluation

We evaluated TYPESHIELD by instrumenting various open source applications and analyzing the results. We used the two ftp server applications vsftpd (version 1.1.0) and proftpd (version 1.3.3), the two http server applications postgresql (version 9.0.10) and mysql (5.1.65), the memory cache application memcached (version 1.4.20) and the node.js server application node (version 0.12.5). We chose these applications, which are a subset of the applications also used by the TypeAmor [46] to allow for later comparison. In our evaluation we addressed the following research questions:

- **RQ1:** How precise is TYPESHIELD in recovering parameter count and type information for call-sites and call-targets from a given binary?
- **RQ2:** What level of security does TYPESHIELD offer? We look at our implementation conceptually and assess qualitatievly whether our implementation can interfere with various classes of attacks.

Comparison Method. As we do not have access to the source code of TypeAmor, we implemented two modes in TYPESHIELD. The first mode of our tool is an approximate implementation of the *count* policy described by TypeArmor. The second mode is our implementation of the *type* policy on top of our *count* policy implementation.

6.1 RQ1: Precision of TYPESHIELD

To measure the precision of TYPESHIELD, we need to compare the classification of call-sites and call-targets as is given by our tool to some sort of ground truth for our test targets. We generate this ground truth by compiling our test targets using a custom compiled Clang/LLVM compiler (version 4.0.0 trunk 283889) with a MachineFunction pass inside the x86 code generation implementation of LLVM. We essentially collect three data points for each call-site/call-target from our LLVM-pass:

- The point of origination, which is either the name of the call-target or the name of the function the call-site resides in.
- The return type that is either expected by the call-site or provided by the call-target.
- The parameter list that is provided by the call-site or expected by the call-target, which discards the variadic argument list.

However, before we can proceed to measure the quality and precision of TYPESHIELD's classification of call-targets and call-sites using our ground truth, we need to evaluate the quality and applicability of the ground truth, we collected.

6.1.1 Quality and Applicability of Ground Truth

To assess the applicability of our collected ground truth, we essentially need to assess the structural compatibility of our two datasets. First, we take a look at the comparability of call-targets and second, we take a look at the compatibility of call-sites. The results are depcited in Table 5.

O2	**call-targets**			**call-sites**		
Target	match	Clang miss	tool miss	match	Clang miss	tool miss
proftpd	1015	0 (0.0%)	15 (1.45%)	155	0 (0.0%)	0 (0.0%)
vsftpd	318	0 (0.0%)	0 (0.0%)	14	0 (0.0%)	0 (0.0%)
lighttpd	290	0 (0.0%)	311 (51.74%)	66	0 (0.0%)	0 (0.0%)
nginx	921	0 (0.0%)	0 (0.0%)	266	0 (0.0%)	0 (0.0%)
mysqld	9742	13 (0.13%)	3690 (27.47%)	7923	24 (0.3%)	25 (0.31%)
postgres	6930	1 (0.01%)	1512 (17.91%)	687	1 (0.14%)	0 (0.0%)
memcached	133	0 (0.0%)	91 (40.62%)	48	1 (2.04%)	0 (0.0%)
node	20638	339 (1.61%)	620 (2.91%)	10965	29 (0.26%)	26 (0.23%)

Table 5: Table shows the quality of structural matching provided by our automated verify and test environment, regarding call-sites and call-targets when compiling with optimization level O2. The label Clang miss denotes elements not found in the data-set of the Clang/LLVM pass. The label tool miss denotes elements not found in the data-set of TYPESHIELD.

Call-targets. The obvious choice for structural comparison regarding call-targets is their name, as these are simply functions. First, we have to remove internal functions from our data-sets like the `_init` or `_fini` functions, which are of no consequence for us. Furthermore, while C functions can simply be matched by their name as they are unique through the binary, the same cannot be said about the language C++. One of the key differences between C and C++ is function overloading, which allows to define several functions with the same name, as long as they differ in namespace or parameter type. As LLVM does not know about either concept, the Clang compiler needs to generate unique names. The method used for unique name generation is called mangling and composes the actual name of the function, its the return type, its

name-space and the types of its parameter list. We therefore need to reverse this process and then compare the fully typed names. Table 5 shows three data points regarding call-targets for the optimization level O2:

- The number of comparable call-targets that are found in both datasets
- Clang miss: The number of call-targets that are found by TYPESHIELD but not by our Clang/LLVM pass
- tool miss: The number of call-targets that are found by our Clang/LLVM pass but not by TYPESHIELD

The problematic column is the Clang miss column, as these might indicate problems with TYPESHIELD. These numbers are relatively low (below 1%) with only node showing a significant higher value than the rest (around 1.6%). The column labeled tool miss lists higher numbers, however these are of no real concern to us, as our ground truth pass possibly collects more data: All source files used during the compilation of our test-targets are incorporated into our ground truth. The compilation might generate more than one binary and therefore not necessary all source files are used for our test-target.

Considering this, we can safely state that our structural matching between ground truth and TYPESHIELD regarding call-targets is nearly perfect (above 98%)

Call-sites. While our structural matching of call-targets is rather simple, the matter of matching callsites is more complex. Our tool can provide accurate addressing of call-sites within the binary. However, Clang/LLVM does not have such capabilities in its intermediate representation (IR). Furthermore the IR is not the final representation within the compiler, as the IR is transformed into a machine-based representation (MR), which is the again optimized. Although we can read information regarding paramters from the IR, it is not possible with the MR. Therefore we attach that data directly after the conversion from IR to MR and read that data at the end of the compilation. To not unneccessarily pollute our dataset, we only considered call-targets, which have been found in both datasets. The table 5 shows three data points regarding call-sites for the optimization level O2:

- The number of comparable call-sites that are found in both datasets.
- Clang miss: The number of call-sites that are discarded from the dataset of TYPESHIELD.
- tool miss: The number of call-sites that are discarded from the dataset of our Clang/LLVM pass.

Both columns (Clang miss and tool miss) show a relatively low number of problems (<0.5%), therefore we can also safely state that our structural matching between ground truth and TYPESHIELD regarding call-sites is also nearly perfect (above 99%)

6.1.2 Classification Precision (*count*)

We measured two data points per target, the number and ratio of perfect classifications and the number and ratio of problematic classifications, which in the case of calltargets refers to overestimations and in case of callsites refers to underestimations. The results are depicted in Table 6.

O2	Call-targets			Call-sites		
Target	#	perfect	problem	#	perfect	problem
proftpd	1015	903 (88.96%)	0 (0.0%)	155	131 (84.51%)	0 (0.0%)
vsftpd	318	273 (85.84%)	0 (0.0%)	14	14 (100.0%)	0 (0.0%)
lighttpd	290	278 (95.86%)	0 (0.0%)	66	48 (72.72%)	0 (0.0%)
nginx	921	762 (82.73%)	0 (0.0%)	266	129 (48.49%)	0 (0.0%)
mysqld	9742	7195 (73.85%)	1 (0.01%)	7923	5138 (64.84%)	0 (0.0%)
postgres	6930	6433 (92.82%)	0 (0.0%)	687	536 (78.02%)	0 (0.0%)
memcached	133	123 (92.48%)	0 (0.0%)	48	40 (83.33%)	0 (0.0%)
node	20638	17427 (84.44%)	1 (0.0%)	10965	6288 (57.34%)	1 (0.0%)
geomean	1413.94	1228.29 (86.86%)	0.0 (0.0%)	319.7	230.12 (71.97%)	0.0 (0.0%)

Table 6: The results for analysis using the *count* policy on the O2 optimization level.

Experiment Setup (Call-targets) Union combination operator with an *analyze* function that follows into occurring direct calls.

Results (Call-targets) The problem rate is under 0.01%, as there are only two testtargets, that exhibit a problematic classification. The rate of perfect classification is in general over 80% with mysql as an exception (73.85%) resulting in a geometric mean of 86.86%.

Experiment Setup (Call-sites) Union combination operator with an *analyze* function that does not follow into occurring direct calls while relying on a backward inter-procedural analysis.

Results (Call-sites) The problem rate is under 0.01%, as there is only one testtarget, that exhibit a problematic classification. The rate of perfect classification is in general over 60% with nginx (48.49%) and node (56.34%) as an exception resulting in a geometric mean of 71.97%.

6.1.3 Classification Precision (*type*)

We measured two data points per testtarget, the number and ratio of perfect classifications and the number and ratio of problematic classifications, which in the case of calltargets refers to overestimations and in case of callsites refers to underestimations. The results are depicted in Table 7.

O2	Call-targets			Call-sites		
Target	#	perfect	problem	#	perfect	problem
proftpd	1015	837 (82.46%)	10 (0.98%)	155	131 (84.51%)	0 (0.0%)
vsftpd	318	252 (79.24%)	3 (0.94%)	14	14 (100.0%)	0 (0.0%)
lighttpd	290	252 (86.89%)	1 (0.34%)	66	45 (68.18%)	1 (1.51%)
nginx	921	639 (69.38%)	0 (0.0%)	266	143 (53.75%)	8 (3.0%)
mysqld	9742	6154 (63.16%)	307 (3.15%)	7923	4391 (55.42%)	375 (4.73%)
postgres	6930	5691 (82.12%)	579 (8.35%)	687	476 (69.28%)	5 (0.72%)
memcached	133	109 (81.95%)	10 (7.51%)	48	43 (89.58%)	0 (0.0%)
node	20638	15483 (75.02%)	453 (2.19%)	10965	4909 (44.76%)	1038 (9.46%)
geomean	1413.94	1091.01 (77.15%)	22.0 (1.92%)	319.7	218.56 (68.35%)	7.97 (1.38%)

Table 7: The results for analysis using the *type* policy on the O2 optimization level.

Experiment Setup (Call-targets) Union combination operator with an *analyze* function that does follow into occurring direct calls and a vertical merge that intersects all reads until the first write.

Results (Call-targets) For half of the set, the problem rate is under 1% and for the other half it is not above 10%, resulting in a geomean of 1.92%. The rate of perfect classification is in general over 70% with nginx (69.38%) and mysql (63.16%) resulting in a geometric mean of 77.15%.

Experiment Setup (Call-sites) Union combination operator with an *analyze* function that does not follow into occurring direct calls while relying on a backward inter-procedural analysis.

Results (Call-sites) For two thirds of the set, the problem rate is under 2% and for last third it is not above 10%, resulting in a geomean of 1.38%. The rate of perfect classification is in general over 50% with node (44.76%) as an exception resulting in a geometric mean of 68.35%.

6.2 RQ2: Security Level of TYPESHIELD

We are now going to evaluate the effectiveness of TYPESHIELD leveraging the result of several experiment runs: First we are going to establish a baseline using the data collected from our Clang/LLVM pass, which are the theoretical limits our implementation can reach for both the *count* and the *type* schema. Second we are going to evaluate the effectiveness of our *count* policy and third we are going to evaluate the effectiveness of our *type* policy. For each series we collected three data points per test target, the average number of call-targets per call-site, the standard deviation σ and the median. The results are depicted in table 8.

6.2.1 Theoretical Limits.

We explore the theoretical limits regarding the effectiveness of the *count* and *type* policies by relying on the collected ground truth data, essentially assuming perfect classification.

Experiment Setup Based on the type information collected by our Clang/LLVM pass, we conducted two experiment series. We derived the available number of call-targets for each call-site based on the collected ground truth applying the *count* and *type* schema

Results:

- The theoretical limit of the *count** schema has a geometric mean of 233 possible call-targets, which is 16.48% of the geometric mean of total available call-targets.
- The theoretical limit of the *type** schema has a geometric mean of 210 possible call-targets, which is 14.86% of the geometric mean of total available call-targets.

When compared, the theoretical limit of the *type* policy allows about 10% less available call-targets in the geomean in O2 than the limit of the *count* policy.

6.2.2 TYPESHIELD implementation

Experiment Setup. We setup our two experiment series based on our previous evaluations regarding the classification precision for the *count* and the *type* policy.

Results.

- The *count* schema has a geometric mean of 315 possible call-targets, which is 22.29% of the geometric mean of total available call-targets. This is 35.19% more than the theoretical limit of available call-targets per call-site.
- The *type* schema has a geometric mean of 290 possible call-targets, which is 20.52% of the geometric mean of total available call-targets. This is 38.09% more than the theoretical limit of available call-targets per call-site.

When compared, our implementation of the *type* policy allows about 7.93% less available call-targets in the geomean in O2 than our implementation of the *type* policy.

O2	AT	*count**			*count*			*type**			*type*		
Target		limit (mean ± σ)		median	limit (mean ± σ)		median	limit (mean ± σ)		median	limit (mean ± σ)		median
proftpd	390	349.31 ± 53.13		369.0	370.0 ± 43.59		382.0	333.12 ± 63.21		312.0	359.4 ± 54.0		348.0
vsftpd	10	7.14 ± 1.8		6.0	7.14 ± 1.8		6.0	5.42 ± 0.9		6.0	5.42 ± 0.9		6.0
lighttpd	59	34.87 ± 14.75		21.0	45.27 ± 14.31		59.0	32.33 ± 13.28		21.0	42.58 ± 14.58		59.0
nginx	543	318.62 ± 151.56		266.0	461.88 ± 128.12		543.0	318.62 ± 151.56		266.0	447.54 ± 132.37		543.0
mysqld	5883	4140.22 ± 1067.55		3167.0	4987.34 ± 948.74		5513.0	3899.92 ± 963.58		3167.0	4739.99 ± 933.25		5564.0
postgres	2491	2094.82 ± 634.24		2286.0	2194.84 ± 590.4		2340.0	1939.74 ± 771.02		2286.0	2060.44 ± 710.43		2332.0
memcached	14	12.31 ± 2.34		14.0	13.35 ± 1.1		14.0	10.29 ± 0.95		11.0	10.64 ± 1.05		10.0
node	7527	5119.4 ± 1548.08		5536.0	6430.54 ± 1279.63		5909.0	4394.4 ± 1516.75		3589.0	5788.81 ± 1444.1		4578.0
geomean	350.0	256.0 ± 76.0		233.0	298.0 ± 65.0		315.0	231.0 ± 69.0		210.0	270.0 ± 66.0		290.0

Table 8: The results of comparing our implementation results with the theoretical limits for the different restriction policies combined with an address taken analysis for optimization level O2.

7 Related Work

Type-Inference on Executables. Recovering variable types from executable programs is very hard in general for several reasons. First, the quality of the disasembly can very much from used framework to another. TYPESHIELD is based on DynInst and the quality of the execuatble disasembly fits our needs. For a more comprehensive review on the capabilities of DynInst and other tools we advice the reader to have a look at [7]. Second, alias analysis in binares is undecidable in theory and intractable in practice [34]. There are several most promising tools such as: Rewards [30], BAP [12], SmartDec [20], and Divine [8]. These tools try with more or less success to recover type information from binary programs with different goals. Typical goals are: *i)* full program reconstruction (binary to code convertion, reversing), *ii)* checking for buffer overflows, *iii)* integer overflows and other types of memory corruptions. For a more exhaustive review of such tools we advice the reader to have a look at the review of Caballero et al. [14]. Intresting to notice is that the code from only a few of this tools is available.

While smartde seemed promising due to its simple type lattice that we wanted to leverage for our classification schema. Its integration into our DynInst based environment was not successful mostly for time constraints, as it was deemed to time consuming to extract the whole machinery and implemnt an interface to the DynInst disassembler. Therefore we finally implemented our own version of type analysis and only focused on the wideness of the types, resulting in a simpler lattice than we initially wanted.

Mitigation of Code-Reuse Attacks. In the last couple of years researchers have provided many versions of new Code Reuse Attacks (CRAs). These new attacks were possible since DEP [32] and ASLR [41] were successfully bypassed mostly based on Return Oriented Programming (ROP) [13, 25, 43] on one hand and on the other hand due to the discovery of new exploitable hardware and software primitives.

ROP started to present itself in the last couple of years in many faceted ways such as: Jump Oriented Programming (JOP) [10, 17, 19] which uses jumps in order to divert the control flow to the next gadget and Call Oriented Programming (COP) [16] which uses calls in order to chain gadgets together. CRAs have many manifestations and it is out of scope of this work to list them all.

On one hand, CRAs can be mitigated in general in the following ways: *(i)* binary instrumentation, *(ii)* source code recompilation and *(iii)* runtime application monitoring. On the other hand, there is a plethora of tools and techniques which try to enforce CFI based primitives in executables, source code and during runtime. Next we briefly present the solution landscape together with the approaches and the techniques on which these are based: *(a)* fine-grained CFI with hardware support, PathArmor [45], *(*(b)) coarse-grained CFI used for binary instrumentation, CCFIR [50], *(c)* coarse-grained CFI based on binary loader, CFCI [52] *(d)* fine-grained code randomization, O-CFI [33], *(e)* cryptografy with hardware support, CCFI [31], *(f)* ROP stack pivoting, PBlocker [40], *(g)* canary based protection, DynaGuard [38], *(h)* runtime and hardware support based on a combination of LBR, PMU and BTS registers CFIGuard [47], and *(i)* source code recompilation with CFI and/or randomization enforcement against JIT-ROP attacks, MCFI [35], RockJIT [36] and PiCFI [37].

The above list is not exhaustive and new protection techniques can be obtained by combining available techniques or by using newly available hardware features or software exploits. However, none of the above techniques and tools can mitigate against COOP attacks.

Mitigation of Forward-Edge based Attacks. Recur-sive-COOP [18], COOP [42] and Subversive-C [29]. are advanced CRAs since these attacks can not be addressed: *i)* with shadow stacks techniques (i.e., do not violate the caller/-calle convention), *ii)* coarse-grained Control-Flow Integrity (CFI) [5, 6] techniques are useless against these attacks, *iii)* hardware based approaches such as Intel CET [4] can not mitigate this attack for the same reason as in *i)*, and *iv)* with OS-based approaches such as Windows Control Flow Guard [3] since the precomputed CFG does not contain edges for indirect call sites which are explicitly exploited during the COOP attack. However, the following tools can protect against COOP attacks:

Source code based. Indirect call site targets are checked based on vTable integrity. Different types of CFI policies are used such as in the following tools: SafeDispatch [22], IFCC/VTV [44] LLVM and GCC compiler. Additionally, the Redactor++ [18] uses randomization vTrust [48] checks

call target function signatures, CPI [26] uses a memory safety technique in order to protect against the COOP attack.

There are several source code based tools which can successfully protect against the COOP attack. Such tools are: ShrinkWrap [21], IFCC/VTV [44], SafeDispatch [22], vTrust [48], Readactor++ [18], CPI [26] and the tool presented by Bounov et al. [11]. These tools profit from high precision since they have access to the full semantic context of the program though the scope of the compiler on which they are based. Because of this reason these tools target mostly other types of security problems than binary-based tools address. For example some last advancec in compile based protection against code reuse attacks address mainly performance issues. Currently, most of the above presented tools are only forward edge enforcers of fine-grained CFI policies with an overhead from 1% up to 15%.

We are aware that there is still a long research path to go until binary based techniques can recuperate program based semantic information from executable with the same precision as compiler based tools. These path could be even endless since compilers are optimized for speed and are designed to remove as much as possbile semantic information from an executable in order to make the program run as fast as possible. In light of this fact, TYPESHIELD is another attempt to recuperate just the needed semantic information (types and number of function parameters from indirect call sites) in order to be able to enforce a precise and with low overhead primitive against COOP attacks.

Rather than claiming that the invariants offered by TYPESHIELD are suffiecient to mitigate all versions of the COOP attack we take a more conservative path by claiming that TYPESHIELD further raises the bar w.r.t. what is possible when defending against COOP attacks on the binary level.

Binary based. vTable protection is addressed through binary instrumentation in tools such as: vfGuard [39], vTint [49]. However, none of these tools can help to mitigate against COOP. The only binary based tool which we are aware of that can mitigate protect against COOP is TypeArmor [46]. TypeArmor uses a fine-grained CFI policy based on caller (only indirect call sites)/callee matching which consists in checking during runtime if the number of provided and needed parameters match.

TYPESHIELD is most similar to TypeArmor [46] since we also enforce strong binary-level invariants on the number of function paramters. TYPESHIELD similarly to TypeArmor targets exclusive protection against advanced exploitation techniques which can bypass fine-grained CFI schemes and VTable protections at the binary level.

However, TYPESHIELD offers a better restriction of call targets to call sites, since we not only restrict based on the number of parameters but also on the wideness of their types. This results in much smaller buckets that in turn can only target a smaller subset of all address taken functions. However, we rely for that on the variety of parameter types and when there is none, we will degrade into a parameter count policy.

Runtime based. "There is something available out there but I can not use it" *Anonymous*. Long story short conclusion: There are several promising runtime-based line of defenses against advanced CRAs but none of them can successfully protect against the COOP attack.

IntelCET [4] is based on, `ENDBRANCH`, a new CPU instruction which can be used to enforce an efficient shadow stack mechanism. The shadow stack can be used to check during program execution if caller/return pairs match. Since the COOP attack reuses whole functions as gadgets and does not violate the caller/return convention than the new feature provided by intel is useless in the face of this attack. Nevertheless other highly notorious CRAs may not be possible after this feature will be implemented main stream in OSs and compilers.

Windows Control Flow Guard [3] is based on a user-space and kernel-space components which by working closely together can enforce an efficient fine-grained CFI policy based on a precomputed CFG. These new feature available in Windows 10 can considerably rise the bar for future attacks but in our opinion advanced CRAs such as COOP are still possible due the typical characteristics of COOP.

PathArmor [45] is yet another tool which is based on a precomputed CFG and on the LBR register which can give a string of 16 up to 32 pairs of from/to addressed of different types of indirect instructions such as `call`, `ret`, and `jump`. Because of the sporadic query of the LBR register (only during invocation of certain function calls) and because of the sheer amount of data which passes through the LBR register this approach has in our opinion a fair potential to catch different types of CRAs but we think that against COOP this tool can not be used. First, because of the fact that the precomputed CFG does not contain edges for all possible indirect call sites which are accessed during runtime and second, the LBR buffer can be easily triked by adding legitimate indirect call sites during the COOP attack.

8 Discussion

Comparison with TypeArmor. We are looking at two sets of results. First of all, we compare the overall precision of our implementation of the COUNT policy with the results from TypeArmor to set the perspective for the precision of our TYPE policy. We cannot compare data regarding overestimations of call targets or underestimations of call sites, as TypeArmor did not provide sufficient data. The second point of comparison is the reduction of call targets per call site, however, this comparison is rather crude, as we most surely do not have the same measuring environment and not sufficient data to infer its quality.

Precision of Classification. TypeArmor reports a geometric mean of 83.26% for the perfect classification of call targets regarding parameter count in optimization level O2, which compares rather well to our result of 82.24%. Regarding the perfect classification of call sites we report a geometric mean of 81.6% perfect classification regarding parameter count, while TypeArmor reports a geometric mean of 79.19%. However we also have a geometric mean of about 7% regarding underestimations in the call site classification with an upper

bound of 16%, while TypeArmor reports that it does not incur underestimations in their call sites. Now, for our type based classification we incur the cost for two error sources. First, the error from the parameter count classification, which we base our type analysis on and second for the type analysis itself. The numbers for the perfect classification of call targets regarding parameter types we report a 72.25% geometric mean of perfect classification, which is 87.85% of our precision regarding parameter counts. However we report a geometric mean of 57.36% for perfect classification of call sites, which although seemingly low, is still 69.74% of our precision regarding parameter counts.

Reduction of Available Call Targets While our count based precision focused implementation achieves a reduction in the same ballpark as TypeArmor regarding our test targets, lets us believe that our implementation of their classification schema is a sufficient approximation to compare against. However, we cannot safely compare those numbers, as the information regarding their test environment are rather sparse and the only data available is the median, which in our opinion does discard valuable information from the actual result set. This is the main reason we implemented an approximation, because we needed more metrics to compare TYPESHIELD and TypeArmor regarding call targets. Using average and sigma, we can report that our precision focused type based classification can reduce the number of call targets, by up to 20% more than parameter number based classification with an overall reduction of about 9%.

TypeArmor Discrepancies. As we have no access to source code of TypeArmor, we implemented an approximation of TypeArmor. Using this approximation we found some discrepancies between the data that we collected and data that was presented in the TypeArmor paper. A minor discrepancy between our results and the results of TypeArmor is that, while they basically implemented what we call a destructive merge operator for the liveness analysis. However, our data suggests that this operator is marginally inferior to the union path merge operator, when we compared them in our implementation. A major concern is the classification of call targets, while we were able to reduce the number of overestimations of call targets regarding parameter counts to essentially 0, the number of underestimations of call target did stay at a geometric mean of 7%. This error rate is rather large when compared to the reported 0% underestimation of TypeArmor, however we are not entirely sure what has caused this discrepancy. A possibility is the differing test environments, or a bug within our implementation that we are not aware of, or simply reaching definitions analysis alone is not the best possible algorithm for this particular problem.

Improving TYPESHIELD. To improve our type analysis, we see at least two possibilities. Incorporating refined data flow analysis and expanding the scope to also include memory. The main point of improvement is not the precision but for now more importantly the reduction of underestimations in the call site analysis.

To refine the data flow analysis, we propose the actual tracking of data values and simple operations, as these can be used to better differentiate the actual wideness stored within the current register. The highest gain, we see here would be the establishment of upper and lower bounds regarding values within the register, which would allow for more sophisticated call site and call target invariants. Essentially we would have to resort to symbolic execution or some other sort of precise abstract interpretation.

Expanding the scope to also include memory, is another possible way of improving the type analysis, as it would allow us to distinguish normal 32 or 64 bit values and pointer addresses. Although we already have a limited approach of that in our reaching implementation, we still see room for improvement, as we only check whether a value is within one of three binary sections or 0.

Limitations of TYPESHIELD. First of all, we are limited by the capabilities of the DynInst instrumentation environment, the main problem, we are facing here is that non returning functions like exit are not detected reliably in some cases, which is why we were not able to test the Pure-FTP server, as it heavily relies on these functions. The problem is that those non returning functions usually appear as a second branch within a function that occurs after the normal control flow, causing basic blocks from the following function to be attributed to the current function. This results in a malformed control flow graph and erroneous attribution of call sites and problematic miss classifications for both call targets and call sites.

Another limitation of TYPESHIELD is it reliance on variety within the binary, in particular we rely on the fact that functions use more than only 64-bit values or pointers within their parameter list. Should this scenario occur, our analysis has nothing to work with and essentially degrades into a parameter count based implementation. Thankfully this occurrence is quite rare, as we experienced within our experiments. When working based on source level information, we could not detect a difference between our TYPE and a COUNT policies. However when leveraging our tool, we were able to detect differences, which reinforces the fact, that we do not rely on declaration of parameters but usage of those.

9 Future Work

Structural matching capability. Improving the structural matching capability is in our opinion the most important further venue of research, as we need a reliable way to match a ground truth against the resulting binary. This is important, because it is a prerequisite to the ability to generate reliable measurements and reduces the current uncertainy (we rely on the number of calltargets per callsite to match callsites and furthermore assume that the order within ground truth and binary is the same).

Better callsite analysis. Finding a better suited callsite analysis would present itself as another important possibility, as we still have a relatively high—up to16%—number of underestimated callsites. However, this venue should only be attempted after significant improvements to the structural matching of callsites.

Better patching schema. Devising a patching schema that is based on Dyninst functionality, which allows annotation of calltargets so they can hold at least 4 bytes of arbitrary data. This is required to hold the type data that we generate using our classification. Keeping the runtime overhead of said patching schema low should be the second goal of this venue after satisfying stability.

Expanding to return values. Expanding our schema to return values is another viable venue of further work, as we were not able to reliably reduce the number of problematic classification regarding the return values of functions to managable levels. Should one attempt this, it should be noted that the responsibilities of callsites and calltargets are reversed in this case: The callsite requires return value wideness, while the calltarget needs to provide it.

Using pointer/memory analysis. Introducing pointer/memory analysis to distinguish simple 32/64bit values and actual addresses to even further restrict the possible number of calltargets per callsite. This would require more precise dataflow analysis, as in calculating value possibilities for registers at each instruction.

10 Conclusion

The family of forward indirect call based attacks which can manifest due to a series of factors such as a memory corruption, binary layout leackage and presence of useful gadgets in sufficiently large executables is a serious security threat. We have developed TYPESHIELD, a runtime based fine-grained CFI enforcing tool which can precissely filter legitimate from illegitimate indirect forward calls in binaries. It uses a novel run-time type checking technique based on function parameter type checking and parameter counting in order to efficiently filter-out legitimate and illegitimate forward edges. TYPESHIELD provides a more precise analysis than existing approaches with a comparable performance overhead. We have implemented TYPESHIELD and applied it to real software such as: web servers, and FTP servers. We demonstrated through extensive experiments and comparisons with related software that TYPESHIELD has higher precision and comparable performance overhead than the existing state-of-the-art tools. To date, we were able to provide a more precise technique than parameter count based techniques by reducing the average target count of up to 20%. This results in a more precise analysis and a considerably reduced attack surface.

References

[1] BlueLotus Team, Bctf challenge: bypass vtable read-only checks. `https://github.com/ctfs/write-ups-2015/tree/master/bctf-2015/exploit/zhongguancun`.

[2] DynamoRIO. `http://dynamorio.org/home.html`.

[3] Windows Control Flow Guard. `http://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx`.

[4] Intel Control-flow Enforcement Technology (CET). `http://blogs.intel.com/evangelists/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks/`.

[5] ABADI, M., BUDIU, M., ERLINGSSON, Ú., AND LIGATTI, J. Control Flow Integrity. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS),* (2005).

[6] ABADI, M., BUDIU, M., ERLINGSSON, Ú., AND LIGATTI, J. Control Flow Integrity Principles, Implementations, and Applications. In *ACM Transactions on Information and System Security (TISSEC),* (2009).

[7] ANDRIESSE, D., CHEN, X., VEEN, V. V. D., SLOWINSKA, A., AND BOS, H. An In-Depth Analysis of Disassembly on Full-Scale x86/x64 Binaries. In *Proceedings of the USENIX Conference on Security (USENIX SEC),* (2016).

[8] BALAKRISHNAN, G., AND REPS, T. DIVINE: Discovering Variables in Executables. In *International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI),* (2007).

[9] BERNAT, A. R., AND MILLER, B. P. Anywhere, Any-Time Binary Instrumentation. In *Proceedings of the 10th ACM SIGPLAN-SIGSOFT workshop on Program analysis for software tools, (PASTE),* (2011).

[10] BLETSCH, T., JIANG, X., FREEH, V. W., AND LIANG, Z. Jump-Oriented Programming: A New Class of Code-Reuse Attack. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS),* (2011).

[11] BOUNOV, D., GÖKHAN KICI, R., AND LERNER, S. Protecting C++ Dynamic Dispatch Through VTable Interleaving. In *Symposium on aravindNetwork and Distributed System Security (NDSS),* (2016).

[12] BRUMLEY, D., JAGER, I., AVGERINOS, T., AND SCHWARTZ, E. J. BAP: A Binary Analysis Platform. In *Proceedings of Computer AidedVTint: Protecting Virtual Function Tab Verification (CAV),* (2011).

[13] BUCHANAN, E., ROEMER, R., SHACHAM, H., AND SAVAGE, S. When Good Instructions Go Bad: Generalizing Return-oriented Programming to RISC. In *ACM Conference on Computer and Communications Security (CCS),* (2008).

[14] CABALLERO, J., AND LIN, Z. Type Inference on Executables. In *ACM Computing Surveys (CSUR),* (2016).

[15] CARLINI, N., BARRESI, A., PAYER, M., WAGNER, D., AND GROSS, T. R. Control-Flow Bending: On the Effectiveness of Control-Flow Integrity. In *Proceedings of the USENIX conference on Security (USENIX SEC),* (2015).

[16] CARLINI, N., AND WAGNER, D. ROP is still dangerous: Breaking Modern Defenses. In *Proceedings of the USENIX conference on Security (USENIX SEC),* (2014).

[17] CHECKOWAY, S., DAVI, L., DMITRIENKO, A., SADEGHI, A.-R., SHACHAM, H., AND WINANDY, M. Return-oriented Programming Without Returns. In *ACM Conference on Computer and Communications Security (CCS),* (2010).

[18] CRANE, S., VOLCKAERT, S., SCHUSTER, F., LIEBCHEN, C., LARSEN, P., DAVI, L., SADEGHI, A.-R., HOLZ, T., DE SUTTER, B., AND FRANZ, M. It's a TRaP: Table Randomization and Protection against Function-Reuse Attacks. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS),* (2015).

[19] DAVI, L., DMITRIENKO, A., SADEGHI, A.-R., AND WINANDY, M. Return-Oriented Programming without Returns on ARM. In *Technical report, Technical Report HGI-TR-2010-002, Ruhr-University Bochum,* (2010).

[20] FOKIN, A., DEREVENETS, Y., CHERNOV, A., AND TROSHINA, K. SmartDec: Approaching C++ decompilation. In *Working Conference on Reverse Engineering (WCRE),* (2011).

[21] HALLER, I., GOKTAS, E., ATHANASOPOULOS, E., PORTOKALIDIS, G., AND BOS, H. ShrinkWrap: VTable Protection Without Loose Ends. In *Annual Computer Security Applications Conference (ACSAC),* (2015).

[22] JANG, D., TATLOCK, T., AND LERNER, S. SafeDispatch: Securing C++ Virtual Calls from Memory Corruption Attacks. In *Symposium on Network and Distributed System Security (NDSS),* (2014).

[23] JTC1/SC22WG21, I. ISO/IEC 14882:2013 Programming Language C++ (N3690). `https://isocpp.org/files/papers/N3690.pdf`.

[24] KHEDKER, U., SANYAL, A., AND SATHE, B. *Data flow analysis: Theory and Practice*. CRC Press, 2009.

[25] KORNAU, T. Return-Oriented Programming for the ARM Architecture. `http://www.zynamics.com/downloads/kornau-tim--diplomarbeit--rop.pdf`.

[26] KUZNETSOV, V., SZEKERES, L., PAYER, M., CANDEA, G., SEKAR, R., AND SONG, D. Code-Pointer Integrity. In *Proceedings of the USENIX Symposium on Operating Systems Design and Implementation (OSDI)* (2014).

[27] LAN, B., LI, Y., SUN, H., SU, C., LIU, Y., AND ZENG, Q. Loop-Oriented Programming: A New Code Reuse Attack to Bypass Modern Defenses. In *IEEE Trustcom/BigDataSE/ISPA* (2015).

[28] LEE, B., SONG, C., KIM, T., AND LEE, W. Type Casting Verification: Stopping an Emerging Attack Vector. In *Proceedings of the USENIX Conference on Security (USENIX SEC),* (2015).

[29] LETTNER, J., KOLLENDA, B., HOMESCU, A., LARSEN, P., SCHUSTER, F., DAVI, L., SADEGHI, A.-R., HOLZ, T., AND FRANZ, M. Subversive-C: Abusing and Protecting Dynamic Message Dispatch. In *USENIX Annual Technical Conference (USENIX ATC),* (2016).

[30] LIN, Z., ZHANG, X., AND XU, D. Automatic Reverse Engineering of Data Structures from Binary Execution. In *Symposium on Network and Distributed System Security (NDSS),* (2010).

[31] MASHTIZADEH, A. J., BITTAU, A., BONEH, D., AND MAZIÈRES, D. CCFI: Cryptograhically Enforced Control Flow Integrity. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS),* (2015).

[32] MICROSOFT, C. T. F. I. M. W. X. S. P. . `https://technet.microsoft.com/en-us/library/bb457151.aspx`.

[33] MOHAN, V., LARSEN, P., BRUNTHALER, S., HAMLEN, K. W., AND FRANZ, M. Opaque Control-Flow Integrity. In *Symposium on Network and Distributed System Security (NDSS),* (2015).

[34] MYCROFT, A. Lecture Notes. `https://www.cl.cam.ac.uk/~am21/papers/sas07slides.pdf`.

[35] NIU, B., AND TAN, G. Modular Control-Flow VTint: Protecting Virtual Function TabIntegrity. In *ACM Conferece on Programming Language Design and Implementation (PLDI),* (2014).

[36] NIU, B., AND TAN, G. RockJIT: Securing Just-In-Time Compilation Using Modular Control-Flow Inegrity. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS),* (2014).

[37] NIU, B., AND TAN, G. Per-Input Control-Flow Integrity. In *Proceedings the ACM Conference on Computer and Communications Security (CCS),* (2015).

[38] PETSIOS, T., KEMERLIS, V. P., POLYCHRONAKIS, M., AND KEROMYTIS, A. D. DynaGuard: Armoring Canary-based Protections against Brute-force Attacks. In *Annual Computer Security Applications Conference (ACSAC),* (2015).

[39] PRAKASH, A., HU, X., AND YIN, H. Strict Protection for Virtual Function Calls in COTS C++ Binaries. In *Symposium on Network and Distributed System Security (NDSS),* (2015).

[40] PRAKASH, A., AND YIN, H. Defeating ROP Through Denial of Stack Pivot. In *Annual Computer Security Applications Conference (ACSAC),* (2015).

[41] RANDOMIZATION, P. T. A. S. L. `https://pax.grsecurity.net/docs/aslr.txt`.

[42] SCHUSTER, F., TENDYCK, T., LIEBCHEN, C., DAVI, L., SADEGHI, A.-R., AND HOLZ, T. Counterfeit Object-Oriented Programming. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P),* (2015).

[43] SHACHAM, H. The Geometry of Innocent Flesh on the Bone: Return-into-Libc without Function Calls (On the x86). In *ACM Conference on Computer and Communications Security (CCS),* (2007).

[44] TICE, C., ROEDER, T., COLLINGBOURNE, P., CHECKOWAY, S., ERLINGSSON, Ú., LOZANO, L., AND PIKE, G. Enforcing Forward-Edge Control-Flow Integrity in GCC and LLVM. In *Proceedings of the USENIX conference on Security (USENIX SEC)* (2014).

[45] VEEN, V. V. D., ANDRIESSE, D., GÖKTAS, E., GRAS, B., SAMBUC, L., SLOWINSKA, A., BOS, H., AND GIUFFRIDA, C. Practical Context-Sensiticve CFI. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS),* (2015).

[46] VEEN, V. V. D., GOKTAS, E., CONTAG, M., PAWLOWSKI, A., CHEN, X., RAWAT, S., BOS, H., HOLZ, T., ATHANASOPOULOS, E., AND GIUFFRIDA, C. A Tough call: Mitigating Advanced Code-Reuse Attacks At The Binary Level. In *Proceedings oaravindf the IEEE Symposium on Security and Privacy (S&P)* (2016).

[47] YUAN, P., ZENG, Q., AND DING, X. Hardware-Assisted Fine-Grained Code-Reuse Attack Detection. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID),* (2015).

[48] ZHANG, C., CARR, S. A., LI, T., DING, Y., SONG, C., PAYER, M., AND SONG, D. VTrust: Regaining Trust on Virtual Calls. In *Symposium on Network and Distributed System Security (NDSS),* (2016).

[49] ZHANG, C., SONG, C., ZHIJIE, K. C., CHEN, Z., AND SONG, D. VTint: Protecting Virtual Function TablesÍntegrity. In *Proceedings of the Symposium on Network and Distributed System Security (NDSS),* (2015).

[50] ZHANG, C., WEI, T., CHEN, Z., DUAN, L., SZEKERES, L., MCCAMANT, S., SONG, D., AND ZOU, W. Practical Control Flow Integrity & Randomization for Binary Executables. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P),* (2013).

[51] ZHANG, M., AND SEKAR, R. Control Flow Integrity for COTS Binaries. In *Proceedings of the USENIX conference on Security (USENIX SEC),* (2013).

[52] ZHANG, M., AND SEKAR, R. Control Flow and Code Integrity for COTS binaries: An Effective Defense Against Real-ROP Attcks. In *Annual Computer Security Applications Conference (ACSAC),* (2015).