BinComp: A Stratified Approach to Compiler Provenance Attribution

Ashkan Rahimian, Paria Shirani, Saed Aliraei, Lingyu Wang, Mourad Debbabi

Computer Security Laboratory, Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada

Abstract

Compiler provenance comprises numerous pieces of information, such as the compiler family, compiler version, optimization level, and compiler-related functions. The extraction of information is imperative for various binary analysis applications, such as function fingerprinting, clone detection, and authorship attribution. It is thus important to develop an efficient and automated approach for extracting compiler provenance. In this study, we present BinComp, a practical approach which, analyzes the syntax, structure, and semantics of disassembled functions to extract compiler provenance. BinComp has a stratified architecture with three layers. The first layer applies a supervised compilation process to a set of known programs to model the default code transformation of compilers. The second layer employs an intersection process that disassembles functions across compiled binaries to extract statistical features (e.g., numerical values) from common compiler/linker-inserted functions. This layer labels the compiler-related functions. The third layer extracts semantic features from the labeled compiler-related functions to identify the compiler version and the optimization level. Our experimental results demonstrate that BinComp is efficient in terms of both computational resources and time.

Keywords:
Compiler Provenance, Reverse Engineering, Binary Program Analysis, Digital Forensics

Introduction

Program binaries are often the focus of forensic investigations, covering numerous issues ranging from copyright infringement to malware analysis. Program binary analysis can be extremely challenging due to the absence of high level information, which is found in source code, and the myriad variations in compilers, versions, and optimization levels [3]. The term compiler provenance refers to information about the compiler family, compiler version, optimization level, and compiler-related functions. Extracting compiler provenance is important in digital forensics, as it provides crucial information about the process by which a malware binary is produced.

Few studies have been conducted on extracting compiler provenance [10, 13, 14]. The existing body of work can be considered as a series of pioneering efforts, beginning with labeling functions in stripped binaries [10], followed by identifying the source compiler of program binaries [13], and culminating in recovering the toolchain provenance of binary code [14]. Inspired by such efforts, we provide improvements by addressing the following issues: 1) the features used in the aforementioned works follow generic templates, which may not always provide meaningful information about compilers; 2) large data sets are usually necessary for the training phase; and 3) significant computational power and time are often needed to rank the features. More recently, the compiler was identified in [18] based on a hidden Markov model that is intended for malware detection. However, it does not extract information regarding the compiler version or optimization level. Furthermore, there are certain tools that are capable of identifying compilers (e.g., IDA Pro [21], PEID [19], and RDG [20]); however, these tools typically suffer from various drawbacks. For instance, most of these tools apply an exact matching algorithm, which may fail when even a slight difference between signatures is present.

Motivation

Our motivation is twofold:

- Existing techniques [13, 14] rely on generic feature templates and feature ranking. This usually leads to large amounts of irrelevant features and consequently results in prohibitive time and computational complexity. Moreover, top-ranked features are not necessarily related to the structure or semantics of compiler-related functions. In contrast, BinComp uses syntactic, semantic, and structural features to extract compiler provenance in a more efficient manner.

- Existing techniques [13, 14] do not explicitly label compiler-related functions, which provides vital help to various tasks in binary analysis, such as authorship
attribute [1, 15], function recognition [2, 16, 17], and clone detection [4, 5], in which filtering out compiler-related functions is a critical pre-processing step for reducing false positives. In contrast, BinComp allows labeling compiler-related functions.

We propose BinComp, a practical approach based on the hypothesis that compiler-helper functions are preserved throughout the compilation process. These functions can be used to identify the source compiler of the binary. The stratified architecture of BinComp consists of three layers. The first layer extracts syntax features, namely, Compiler Transformation Profile (CTP), and compiler tags (CT). The second layer extracts Compiler Function (CF) features, which are represented as symbolic and numerical feature vectors used to label the compiler-related functions. This layer provides a list of compiler-helper functions. The third layer extracts semantic features, namely, the Compiler Transformer Terminator (CCT) graph and the Annotated Control Flow Graph (ACFG). This layer identifies the version and the optimization level from the helper functions. The architecture of BinComp is illustrated in Figure 1. Each layer relies on a different detection technique: Layer 1 employs signatures to perform exact matching; Layer 2 uses the distances between the numerical vectors to label compiler-related functions; and Layer 3 extracts semantic graphs that are represented as feature vectors, after which hashing is applied to control the granularity level over the program components.

The novelty of the proposed approach is that it combines prior knowledge of compiler code transformations with an incremental learning component. This serves to adjust source compiler features as well as to update them when compiler-related functions undergo changes due to new versions or updates. Our experimental results show that BinComp identifies compiler families effectively, and that the approach is efficient in terms of both time and computational resources. This makes BinComp a practical approach for binary analysis.

**Contribution**

Our paper makes following contributions:

- BinComp is a stratified approach which simultaneously achieves several goals, including compiler identification, compiler-related function labeling, compiler version detection, and optimization level recognition.

- The signatures used in most tools depend on metadata or other details of program headers. This can be problematic as such information might be unavailable in stripped binaries or might be easily altered. However, the signature used in BinComp relies on the characteristics of the binary, which are available even in stripped binaries.

- We evaluate BinComp on a large set of real-world binaries across several compiler families, versions, and optimization levels. Our results show that compiler provenance can be extracted with high accuracy: BinComp identifies the compiler with an accuracy that is above 0.90, the version an average accuracy of 0.86 and the optimization level with accuracy that is over 0.90.

The remainder of this paper is organized as follows: Section Motivating Example provides a motivating example. Section Evaluation of the ECP Approach introduces the re-evaluation of the technique used by Rosenblum et al. Section BinComp Approach details the main methodology. Section Evaluation evaluates the proposed approach and provides comparisons against existing work. Section Conclusion presents some concluding remarks on this work together with a discussion of future research.

**Motivating Example**

Consider the simple program shown in Listing 1. We compile this program with Visual Studio 2010 under release mode, and we obtain 34 functions after disassembling the binary. These functions include one user function (e.g., the main function), five library functions (e.g., iostream), and 28 compiler-related functions. Subsequently, we compile the same example with Visual Studio 2012. Upon disassembling the binary, we find 73 functions: three user functions, 18 library functions, and 52 compiler-related functions. By checking the compiler-related functions, we find that 25 functions remain the same. In addition, we conduct the same simple experiment with a slightly complex program, and we find the same set of 25 compiler-related functions. To obtain the exact list of these functions, we intersect the sets of disassembled compiled binaries. However, we cannot rely merely on the names of the functions, as in most cases functions are given generic names (e.g., sub-xxx) by the disassembler. Therefore, after listing the helper functions (common compiler-related functions), two feature vectors are created for each function, as detailed in BinComp Approach Section. These feature vectors are used to ascribe a profile to each compiler.

Listing 1: Do Nothing C++ Program

```cpp
#include <stdio.h>
```
In addition, we extract the compiler effect (compiler transformation profile) from the user functions, since different compilers may generate distinct binary representations for analogous source code. Several parameters, such as compiler families, mapping profiles of operations to instructions, conditional/loop structures, optimization options, etc., govern the way compilers transform code from high-level source to low-level machine code. Listing 2 shows a simple C program consisting of a single function call to printf. Listings 3, 4, and 5 display the compiled versions with MSVC (Windows), GCC (Linux), and Clang (OS X), respectively. It is evident that each compiler generates a different sequence of instructions for the source program. Given a list of assembly functions (similar to listings 3, 4, and 5) from a target disassembly, we will show how to identify the most likely compiler with which the binary is built.

Listing 2: A Simple C Program
```
#include <stdio.h>
int main(){
    printf("Minimal, Program, \n");
    return 0x1234;
}
```

Listing 3: Compilation with MSVC on Windows
```
main
push ebp
mov ebp, esp
push offset aMinimalProg
call ds_:imp__printf
add esp, 4
mov eax, 1234h
pop ebp
ret
```

Listing 4: Compilation with GCC on Linux
```
main
lea 0x4(esp), ecx
and $0xfffffffff0, esp
push -0x4(ecx)
push ebp
mov esp,ebp
push ecx
sub $0x4, esp
mov $0x8048460, (esp)
call S048224 <puts@plt>
mov $0x1234, eax
add $0x4, esp
pop ecx
pop ebp
lea -0x4(ecx), esp
ret nesp
```

Listing 5: Compilation with XCode on OS X
```
main
push ebp
mov esp,ebp
push ebx
sub $0x14, esp
call 0x00001fd6
pop ebx
lea 0x0000001a(ebx), eax
mov eax,(esp)
call 0x0000300S
mov $0x00001234, eax
add $0x14, esp
pop ebx
leave ret
```

Evaluation of the ECP Approach

ECP models compiler identification as a structured classification problem and labels each byte of the binaries with the information whether it is compiled with one or two compilers (statically linked code). The authors use wildcards idiom features, which are defined as short sequences of instructions that neglect details such as literal arguments and memory offsets. After extracting the features from a large number of binaries, redundant features can be found, which are related to the user functions or the architecture. Therefore, the authors consider top-ranked features based on the results of mutual information computation between the features and compiler classes. The proposed technique is performed on three sets of binaries containing code from three compilers: GNU C Compiler (GCC), Intel C Compiler (ICC), and Visual Studio (VS). The data set is collected for GCC and VS on Linux and Microsoft Windows workstations, respectively. In addition, they have compiled various open-source software packages with the ICC compiler.

Most of these data sets are not publicly available. We have collected different source files from various years of the Google Code Jam (referred to as the G data set) [22] (2008-2014). We have also gathered several source code samples from our university (referred to as the U data set). Our experimental corpus comprises three sets of binaries: GNU C Compiler (GCC), Intel C Compiler (ICC), and Visual Studio compiler (VS). We disassemble each program binary using IDA Pro [21] disassembler. Furthermore, we test their approach with an additional compiler, Clang (XCode).

ECP Evaluation Results

We generate our data set after considering all applicable combinations of compilers, various data set combinations, and different optimization levels. In what follows, we discuss our results based on a specific process of validation. First, we split the training data into ten sets, reserving one set as a testing set. We then train a classifier on the remaining sets and evaluate its accuracy on the testing set. In addition, we perform various experiments, as shown in Figure 2: (i) changing the number of files; (ii) modifying the threshold value of the ranked features; and (iii) mixing various percentages of data sets to observe the effect.
of data set diversity. Finally, we measure the time efficiency by showing the relationship between the number of features and the total elapsed time.

The ECP approach can attain relatively high accuracy, as shown in Figure 2 (a), where the accuracy for the G data set is between 0.89 and 0.98. This is higher than the accuracy obtained using the U data set (min = 0.82, max = 0.95). By analyzing the source code, we find out that the user contribution in the U data set is greater than that of the G data set. The U data set is also more complex than the G data set, as it consists of classes, methods, etc. In addition, we study how changing the threshold value for the number of top-ranked features affects accuracy. We find out that the accuracy of their method may depend on the choice of the threshold value, as shown in Figure 2 (b). For instance, the best threshold values for GCC and XCode compilers are 16,000 and 18,000, respectively. In practice, finding the best threshold for a given compiler and data set combination may be a task that is both time-consuming and prone to errors.

Finally, we perform an experiment to study the effects of data set diversity on accuracy, as illustrated in Figure 2 (c). We consider different percentages of mixed data sets (e.g., 100% G data set, and 20% G - 80% U data sets). As shown, the accuracy decreases when the diversity of the data set increases, especially when the percentage of university projects increases, since the user contribution in the U data set is higher than that of the G data set. We measure the time efficiency of the ECP approach by calculating the total required time for feature extraction and feature ranking. Figure 2 (d) shows the total time versus the number of features for different experiments.

**Discussion and Limitation**

The ECP approach represents pioneering effort on compiler identification and may attain relatively high accuracy. This approach can also identify the compilers of binaries containing a mixture of code from multiple compilers, such as statically linked library code. However, a few limitations could be observed. First, as the number of features increases, the running time may increase even more rapidly. Second, the features of specific compilers may only become apparent after examining a large number of binaries. Third, the accuracy may depend on both the data set and the choice of threshold.

**BinComp Approach**

We present hereafter the different layers of our BinComp approach.

**First Layer: Compiler Identification**

The aim in this layer is to derive unique signatures for compilers by collecting a set of known source code and observing the compiled outputs. We tailor BinComp to C-family compilers due to their popularity and widespread adoption, especially in the development of malicious programs [11]. The steps used in this layer are displayed in Figure 3. As can be seen, we use the artifacts of each compilation step to generate specific types of features.

**Figure 3: Compilation Steps**

1. **Pre-processing**: The input of this step is the original source code (SRC), and the output is a pre-processed source file that includes the contents of header files imported into the source code. The symbolic constants are replaced with their values as a result of this process. To support the signature generation process, we extract the values of constants and the list of source-level functions along with their prototypes.

2. **Compilation**: The expanded source file generated in Step 1 is fed into the compilation step, which results in a platform-dependent assembler file (IAS). In support of the signature generation process, the list of assembly functions is extracted.
3. **Assembly**: We use the disassembled version of the object file (OBJ) — the output of this step — to extract the relevant features. To support the signature generation process, we match each assembly-level function with the corresponding source-level function obtained from Step 1. At this point, we are able to establish a mapping between assembly code profiles (sequences) and the source code. This mapping provides us with clues about the compiler code transformation process and syntactic styles (compiler transformation profile, as described later in BinComp Approach Section).

4. **Linking**: The linking step deals with the integration of the library object code (LIB) with the user object code (OBJ) built in Step 3 to produce the final binary file (BIN).

5. **Disassembly**: We utilize the disassembled version of the binary file to extract compiler tags (compiler tags are described later in BinComp Approach Section).

First Layer: Feature Description

**Compiler Transformation Profile (CTP)**

CTP is a syntactic feature that highlights how certain syntactic source-level data and control structures (such as conditional/unconditional jumps, loops, arrays, structs, etc.) are reflected in the assembly output of compilers. The compiler transformation profile captures the code transformation process and maps the chosen source-level statements to a sequence of assembly-level instructions in order to profile the code transformation for each compiler. For instance, the assembly code translation of a simple `if/else` construct involves a comparison instruction followed by a conditional jump at the assembly level, which can be stated as `if/else: cmp or test, then jcc, in binaries compiled by VS.

**Compiler Tags (CT)**

Compilers may embed in output binaries certain tags in the form of strings or constants. For instance, GCC-compiled binaries carry a tag that survives even after the symbol stripping process. Similarly, programs compiled with VS have an XOR-encoded value in the file header section that indicates the compiler version. These values can therefore be considered as compiler indicators. We apply a file parsing mechanism (PE/COFF/ELF) to obtain such values.

First Layer: Detection method

All extracted features in this layer are recorded as strings and used for exact matching. The features in this layer, including the compiler transformation profile and compiler tags, captures the behavior of the compiler to access primitive and composite data structures and code structures (e.g., control statements, loop structures, register utilization, and memory access). We combine them into a single signature entity $Sig_{ct}$ that is used to identify the compiler $c_i$.

Second Layer: Compiler Functions Labeling

The aim in this layer is to label compiler-related functions. To support our goal, we select a pair of source programs $P_1$ and $P_2$ and direct them through the supervised compilation process using the compiler $c_i$. The outcome of this process includes two sets of disassembled functions $F_{P_1}$ and $F_{P_2}$ as well as their corresponding symbolic $V_S$ and numeric $V_n$ feature vectors for each function. We perform a similarity measurement based on the numerical values of feature vectors. We use a standard clustering algorithm (k-means) [6] to group functions with similar attributes $(v_{n1}, \ldots, v_{ni})$ into $k$ clusters $S = S_1, \ldots, S_k$ and $(k \leq |F_{P_1}| + |F_{P_2}|)$ to minimize the intra-cluster sum of squares. In the following equation, $\mu_i$ denotes the mean of the numerical feature values of each cluster.

$$\arg\min_{S} \sum_{i=1}^{k} \sum_{v_j \in S_i} \|v_j - \mu_i\|^2$$

The parameter $k$ may be estimated either by following standard practices in k-means clustering [6], or by beginning with one cluster and continually dividing the clusters until the points assigned to each cluster have a Gaussian distribution as described in [7]. If function names are available in symbolic vectors (which is the case for debug binaries), we would have the option to intersect functions based on their symbolic names. In this case, we compute $\text{list}(\text{set}(V_{P_1}.\text{names}()) \cap \text{set}(V_{P_2}.\text{names}()))$, where the $\text{list}()$ function returns the list of commonly disassembled functions and the $\text{names}()$ method returns the property name of each function.

Table 1: Instruction Categories

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTR</td>
<td>Data Transfer</td>
<td>TNA</td>
<td>Indirect Near Address</td>
</tr>
<tr>
<td>INO</td>
<td>Input / Output</td>
<td>DTO</td>
<td>Data Transfer Object</td>
</tr>
<tr>
<td>FLT</td>
<td>Float Point</td>
<td>FLO</td>
<td>Flag Manipulation</td>
</tr>
<tr>
<td>REG</td>
<td>Registers</td>
<td>LGC</td>
<td>Logical Instructions</td>
</tr>
<tr>
<td>MEM</td>
<td>Memory</td>
<td>CTI</td>
<td>Control Instructions</td>
</tr>
<tr>
<td>IMM</td>
<td>Immediate Value</td>
<td>IFA</td>
<td>Indirect Far Address</td>
</tr>
<tr>
<td>INT</td>
<td>Interrupt / System</td>
<td>ATH</td>
<td>Arithmetic Instructions</td>
</tr>
</tbody>
</table>

Second Layer: Feature Description

**Compiler Functions (CF)**

Compiler function features are extracted in two steps: i) intersect a set of disassembled files, and ii) extract symbolic and numerical vectors for each compiler function. Given a target binary $B$ (with unknown compiler) and its set of disassembled functions $F_B = \{f_1, \ldots, f_m\}$, which are classified into two groups of functions (compiler-related functions and user-related functions), we extract symbolic feature vectors $V_S = \{V_{s1}, V_{s2}, \ldots, V_{sn}\}$ and numerical feature vectors $V_n = \{V_{n1}, V_{n2}, \ldots, V_{nn}\}$ from each disassembled compiler/linker-related function $f_i \in F_B$. We group
the instructions according to the instruction categories as shown in Table 1. The numerical vectors are generated using a function fingerprinting technique [12], which encodes and quantifies the syntactic and structural features of binary functions. Table 2 shows an example of numerical vectors.

**Second Layer: Detection method**

We introduce a function fingerprinting approach for the generation and detection of abstract representations of assembly functions. We consider a program \( P \) to be comprised of a set of functions \( F = \{ f_1, \ldots, f_m \} \). A feature extraction function \( X : F \rightarrow S \) maps each function \( f_i \in F \) to a set of features \( s_i \in S \), where \( F \) is the set of compiler/linker-related functions and \( S \) is the set of all possible features:

\[
s_i = X(f_i)
\]  

We define \( G : S \rightarrow T \) as a fingerprint computation function that takes the set of features to generate the fingerprints. Each fingerprint \( t_i \in T \) represents the encoded characteristics of function \( f_i \):

\[
t_i = G(s_i) = G(X(f_i))
\]

At a different level of abstraction, this function is similar to a hash function since it generates a fixed length output for an arbitrary length assembly function and compresses the information. However, this function computes the output based on a normalized form of assembly instructions. This function can be interpreted as a semantic hash function, which builds a bit vector of length \( m \) from the subset of features \( S \) that appear in \( f_i \). The mechanics of the hash function can be balanced according to the required level of strength [number of feature bits] and the size of the feature space.

\[
t_i \in \text{domain}(S) \rightarrow \{0, 1\}^m
\]

For function fingerprinting, we calculate the similarity between pairs of functions. It is also necessary to determine the similarity between a target function and a group of functions (e.g., incremental clustering). The similarity function \( M \) assigns a score to a pair of candidate fingerprints using a similarity metric. The similarity score can be computed at the level of features (i.e., \( M' : F \times F \rightarrow \mathbb{R}^+ \)) or at the level of fingerprints (i.e., \( M : T \times T \rightarrow \mathbb{R}^+ \)). There are various metrics for the computation of vector similarity scores (e.g., Jaccard similarity). Let \( t_i \) and \( t_j \) be two fingerprint vectors generated from the candidate function pairs \( \{f_i, f_j\} \), respectively. The Jaccard similarity can be calculated using the following equation [9]:

\[
d_j(t_i, t_j) = \frac{S(t_i \land t_j)}{S(t_i \lor t_j)}
\]  

where the \( S() \) function counts the number of ones in the fingerprint bit vector.

**Third Layer: Version and Optimization Recognition**

The aim in this layer is to detect the version and the optimization level of the binary code. During the training phase, we observe that two features are slightly distinct: the annotated control flow graph (ACFG) and the compiler constructor terminator (CCT) graph. In such cases, we use neighborhood hashing [9] to provide a level of granularity over the program components and features used that is more refined than graph encoding.

**Third Layer: Feature Description**

**Annotated Control Flow Graph (ACFG)**

We present a new scheme, the Annotated Control Flow Graph (ACFG), to efficiently detect the version and optimization levels. It is an abstracted version of the CFG, which generalizes specific types of CFG features according to multiple criteria. We build an annotated control flow graph for each disassembled compiler-related function according to the type of operations that take place in each basic block. Each node in this graph represents a basic block, and each edge connects basic block \( B_1 \) to basic block \( B_2 \) if basic block \( B_2 \) can directly follow basic block \( B_1 \) in execution. The method for extracting an ACFG can be summarized in the following steps: First, we consider a CFG as an input and compute the frequency of opcodes across instruction groups. Second, each assembly instruction can be categorized according to the mnemonic groups and types of operands. As one category, the x86 instructions can be classified into six groups, as shown in Table 3. Third, we treat the ACFG as a structural feature and complement it with subgraph encoding values.

**Definition 1**. An Annotated Control Flow Graph \( ACFG = (N, E, \zeta, \gamma) \) is an attributed graph where \( N \) is a set of nodes each representing a basic block, \( E \subseteq (N \times N) \) is a set of edges which represents a control flow statement, \( \gamma \) is a function that groups the instructions, and \( \zeta \) is a function which colors nodes according to the type of operations that take place.
Table 3: Patterns for Annotation

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTR &amp; STK</td>
<td>Data Transfer and Stack</td>
<td>push, mov, etc</td>
</tr>
<tr>
<td>ATH &amp; LGC</td>
<td>Arithmetic and Logical</td>
<td>add, xor, etc</td>
</tr>
<tr>
<td>CAL &amp; TST</td>
<td>Call and Test</td>
<td>call, cmp, etc</td>
</tr>
<tr>
<td>REG &amp; MEM</td>
<td>Register and Memory</td>
<td>esi, esp+4</td>
</tr>
<tr>
<td>REG &amp; CONST</td>
<td>Register and Constant</td>
<td>esi, 30</td>
</tr>
<tr>
<td>MSC</td>
<td>Milestones</td>
<td>MEM and Const</td>
</tr>
</tbody>
</table>

ACFG Construction

We use one compiler function (e.g., setprecision) to illustrate the steps involved in translating CFG to ACFG, as shown in Figure 4. The first part on the left side represents the standard control flow graph. As illustrated in the middle part, we convert each basic block in accordance with Table 3. Finally, function $\zeta$ converts these values to a specific color.

Consider the last basic block in Figure 4 which contains the two instructions pop esi and ret. Function $\gamma$ groups the two operators to STK and MSC, and the esi operand to REG. To color the nodes, $\zeta$ intersects the opcode and operands according to Table 3. For instance, DTR & STK $= 0 \land 1 = 0$, while MSC $= 1$. Each basic block ends up with a six-bit value (e.g., 000001) which will be represented in a new graph by a decimal value equivalent to its binary. The ACFG captures the control flow semantics of a program, which contains more information and hence provides more accuracy than a CFG. An ACFG can convert equivalent compiler functions to a similar ACFG because the compiler functions are semantically similar. In contrast, a CFG deals only with the structure of the function; since different functions may have the same structure, this fact makes compiler function identification more difficult.

Compiler Constructor Terminator (CCT)

One important application of call graphs and control flow graphs is in the recognition of compiler-related call sequences. Each compiler exhibits a relatively unique signature for initialization, startup, and termination code. In both the initialization and termination part of the program, there are compiler functions that call other functions or are called by other functions. The order of these functions, number of nodes, flow, and other characteristics are some of the signatures that we use for the compiler constructor terminator (CCT) feature.

![Figure 4: ACFG construction](image)

During the execution of the system, the call graph of the application is traversed until it reaches the main function. Every sequence of function calls taking place before and after the main function (initialization and terminators) is recorded in the compiler constructor terminator (CCT) of each compiler. Figure 5 shows an example of a GCC compiler constructor terminator.

Third Layer: Detection method

In certain applications, it may be necessary to match subsets of multiple graphs. For instance, we consider the initialization part of a call graph as a startup signature for compiler identification (compiler constructor terminator profile). In such cases, neighborhood hashing provides a more refined level of granularity compared to graph encoding. In order to fingerprint adjacent nodes, a neighbor hash graph kernel (NHGK) can be applied to subsets of the call graph [9]. The function $G$ maps the set of annotated graphs $AG$ to a bit vector of length $m$.

$$G : AG \to \{0, 1\}^m$$  \hspace{1cm} (6)

The neighborhood hash value $h$ for a function $f_i$ and its set of neighbor functions $N_{f_i}$ can be computed using the following formula [8]:

$$h(f_i) = shr_1(G(f_i)) \oplus (\oplus_{f_j \in N_{f_i}} G(f_j))$$  \hspace{1cm} (7)

where $shr_1$ denotes a one-bit shift right operation and $\oplus$ indicates the XOR function.

Evaluations

Data set

Gathering a data corpus for the evaluation of compiler provenance extraction is challenging. For example, despite
the fact that collecting code from open-source projects may be attractive, the source files usually have numerous dependencies which complicates the compilation process. Nonetheless, we choose four free open-source projects and use them to test BinComp. In addition, we have gathered programs written for the Google Code Jam [22] as well as university projects from a programming course at our university. All of our data sets are publicly accessible in [23].

We generate the binaries that make up our data set by compiling the source code with all applicable combinations of compiler versions and optimization levels (O0 and O2), as shown in Table 4. Our data set consists of 1177 files, 232 of which belong to the Google Code Jam data set, 933 of which belong to the Students Code Projects, and 12 of which belong to the Open Source Projects.

Table 4: Data set compilation settings

<table>
<thead>
<tr>
<th>Compiler</th>
<th>Version</th>
<th>Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCC</td>
<td>3.4</td>
<td>O0</td>
</tr>
<tr>
<td></td>
<td>4.4</td>
<td>O2</td>
</tr>
<tr>
<td>ICC</td>
<td>10</td>
<td>O0</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>O2</td>
</tr>
<tr>
<td>VS</td>
<td>2010</td>
<td>O0</td>
</tr>
<tr>
<td></td>
<td>2012</td>
<td>O2</td>
</tr>
<tr>
<td>XCODE</td>
<td>6.1</td>
<td>O0</td>
</tr>
<tr>
<td></td>
<td>6.1</td>
<td>O2</td>
</tr>
</tbody>
</table>

Evaluation Results

We evaluate our compiler provenance approach using the aforementioned data sets. We split the training data into ten sets, reserving one set as a testing set, and using nine sets as training sets to evaluate our approach; we repeat this process numerous times. To evaluation our approach, we use precision (P) and recall (R) as follows.

\[
P = \frac{TP}{TP + FP} \tag{8}
\]

\[
R = \frac{TP}{TP + FN} \tag{9}
\]

Since our application domain is much more sensitive to false positives than false negatives, we use the F-measure as follows.

\[
F_{0.5} = 1.25 \cdot \frac{PR}{0.25P + R} \tag{10}
\]

Our results of \(F_{0.5}\) measure is summarized in Table 5.

Table 5: \(F_{0.5}\) results

<table>
<thead>
<tr>
<th>Feature</th>
<th>(F_{0.5}) (data set = 500 files)</th>
<th>(F_{0.5}) (data set = 1000 files)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idioms</td>
<td>0.780</td>
<td>0.812</td>
</tr>
<tr>
<td>Graphlet</td>
<td>0.602</td>
<td>0.62</td>
</tr>
<tr>
<td>CF</td>
<td>0.72</td>
<td>0.745</td>
</tr>
<tr>
<td>CTP</td>
<td>0.694</td>
<td>0.708</td>
</tr>
<tr>
<td>CCT</td>
<td>0.807</td>
<td>0.877</td>
</tr>
<tr>
<td>CT</td>
<td>0.680</td>
<td>0.70</td>
</tr>
<tr>
<td>ACFG</td>
<td>0.634</td>
<td>0.671</td>
</tr>
</tbody>
</table>

As depicted separately in Figure 6 (a-d), BinComp can detect the VS compiler with an average accuracy of 0.97, while ECP average accuracy is 0.93. The main explanation for this difference lies in the type of features used in the technique; BinComp uses different kind of features (syntactical, structural, and semantical), whereas ECP uses only syntactical features. In addition, we record the overall run time and compare BinComp and ECP approaches in terms of time complexity, as shown in Figure 7.
We test BinComp using different variations of compiler versions and optimization levels, as shown in Table 6 and Table 7. Table 6 indicates that identifying the version of compiler is significantly more difficult than recognizing the compiler and optimization levels. For instance, the accuracy to identify the version of XCode compiler is below 0.80. In addition, we observe that the features of VS and XCode compilers are slightly different when we change either the version or the optimization level, which makes the detection process more challenging. However, the GCC and ICC compilers produce more various code amongst versions compared to the VS and XCode compilers.

<table>
<thead>
<tr>
<th>Compiler</th>
<th>Version</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCC</td>
<td>3.4.x</td>
<td>80%</td>
</tr>
<tr>
<td></td>
<td>4.4.x</td>
<td>89%</td>
</tr>
<tr>
<td>ICC</td>
<td>10.x</td>
<td>83%</td>
</tr>
<tr>
<td></td>
<td>11.x</td>
<td>90%</td>
</tr>
<tr>
<td>VS</td>
<td>2010</td>
<td>70%</td>
</tr>
<tr>
<td></td>
<td>2012</td>
<td>71%</td>
</tr>
<tr>
<td>XCode</td>
<td>5.x</td>
<td>78%</td>
</tr>
<tr>
<td></td>
<td>6.1</td>
<td>74%</td>
</tr>
</tbody>
</table>

We find that up to 75% of the functions in our data set are identical when generated by Visual Studio 2010 or 2012 with the same optimization level. In other words, the code generator in Visual Studio has remained relatively stable between these versions, which offers an explanation for the low accuracy for VS version detection. On the other hand, we found that up to 85% of the functions of XCode are identical among two versions. However, we have observed changes in our proposed features for the GCC and ICC compilers which allow us to detect the version and optimization level by measuring the differences in the features.

<table>
<thead>
<tr>
<th>Compiler</th>
<th>Optimization</th>
<th>Average Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCC</td>
<td>00, 02</td>
<td>91%</td>
</tr>
<tr>
<td>ICC</td>
<td>00, 02</td>
<td>89%</td>
</tr>
<tr>
<td>VS</td>
<td>00, 02</td>
<td>95%</td>
</tr>
</tbody>
</table>

A comparison between BinComp, ECP, and IDA Pro based on four open source projects named SQLite, libpng, zlib, and OpenSSL are illustrated in Figure 8. We compile SQLite and zlib with VS 2010 (02), and the compiler is successfully identified by these three approaches; whereas libpng and OpenSSL are compiled with GCC (02), which IDA Pro is not able to identify the source compiler of these binaries. BinComp and ECP provide more accurate results in identifying the VS compiler, while IDA cannot identify the GCC compiler.

<table>
<thead>
<tr>
<th>Features</th>
<th>Inst.</th>
<th>Control flow</th>
<th>Ext.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idioms</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphlet</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>CP</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTP</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCT</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CT</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACFG</td>
<td>*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Discussion and Limitations

We evaluate compiler provenance recovery on different data sets across several compiler families, versions, and optimization levels. We check the applicability of the features used in BinComp and the features used in the existing techniques (e.g., Idioms, Graphlet) to identify the compiler, version, and optimization level based on our observations during the experiments. For instance, CT has the same pattern in the binaries that are compiled with the same compiler. Furthermore, we formulate a template called compiler transformation profile (CTP) that maps the instructions underlying a binary according to the most likely compiler family by which it was generated. We use such features as a unique signature (fingerprint) to identify a binary source compiler. We use other features (e.g., ACFG, and CCT) to identify the version and optimization level. The variations in compiler provenance lead to variations in the structure of the binary code. We introduce features that capture detailed provenance at function-level granularity, allowing us to recover the optimization levels used to produce binary code. We design ACFG and compiler constructor terminator (CCT) features to explicitly capture such changes and identify the version.

BinComp uses different features that cover various aspects of the binary. Each feature captures one or more of the code instruction-level (inst), control flow, or external library (ext) interaction properties, as shown in Table 8. The features used in BinComp cover all aspects of compiler transformations and behaviors.

Table 8: Feature abstraction levels: instruction-level (inst), control flow, and external library (ext) interaction properties level.

<table>
<thead>
<tr>
<th>Features</th>
<th>Inst.</th>
<th>Control flow</th>
<th>Ext.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idioms</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphlet</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>CP</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTP</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCT</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CT</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACFG</td>
<td>*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9
BinComp still suffers from some limitations. For instance, like most existing methods, BinComp works under the assumption that the binary code is already de-obfuscated. In practice, the de-obfuscation of malware can be very demanding. How to extract compiler provenance directly over obfuscated code is an important but very challenging future avenue of research. BinComp also assumes the binary code is not stripped. In addition, for this work, only Intel x86/x86-64 architecture is considered, and we evaluate BinComp only over compiled C++ programs.

Conclusion

We have presented a technique called BinComp for accurately and automatically recovering the compiler provenance of program binaries using syntactical, semantical, and structural features to capture the compiler behavior. BinComp extracted specific features from program binaries, which enabled us to build representative and meaningful features to describe each compiler characteristics better. Our results show that compiler provenance can be extracted accurately. Moreover, the results indicate that the approach was efficient in terms of computational resources and time requirements, and could thus be considered as a practical approach for real-world binary analysis.

Acknowledgments

The authors thank the anonymous reviewers for their valuable comments. They are also thankful to Dr. Vassil Roussev for his constructive comments. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsoring organizations.

References


