Lightweight Modeling of Java Virtual Machine
Security Constraints using Alloy

Mark C. Reynolds
Boston University Department of Computer Science

May 11, 2008

Introduction

This paper will describe an analysis tool for verifying security constraints within Java bytecodes. This investigation was motivated by the continued appearance of malicious Java code that violates the security constraints imposed by the Java compiler, the Java Bytecode Verifier and the Java runtime. The analysis approach is based on the lightweight modeling language Alloy [AL, DJ]. This paper will describe the security verification approach taken by the Java Virtual Machine (JVM), and briefly enumerate some of the ways that it has been circumvented. A review of the top level goals of this work will then be presented, followed by a hierarchical description of the design of the analysis tool and its implementation. Results will then be presented in detail. Finally, a path toward future work on the analysis tool will be described.

The analysis tool has, in fact, proven to be a powerful approach to analyzing JVM security constraints. To the author’s knowledge, the approach of applying lightweight modeling as a means to check JVM security constraints is a new approach. It is therefore believed that the results presented in this paper are novel.

Background

The Java programming language has been touted as “secure by design” since its inception. However, attacks against Java security have been promulgated from the earliest days of Java. Felten discovered several weaknesses in the Java security model almost immediately, and his work on Java [FE] contains an extensive list of early exploits. The development of Java malware has continued unabated up to the present. The Common Vulnerabilities and Exposures project [CV] lists numerous Java bugs that can lead to privilege escalation, sensitive data exfiltration, denial of service and other malicious outcomes. Of particular note is the “BlackBox” malicious Java applet [BB, LS]. This applet exploits a number of Java security weaknesses, and was widely deployed, infecting thousands of machines. The BlackBox applet not only breaks out of the supposedly invulnerable sandbox that the Java applet runtime imposes, it also manages to escalate its privilege to the highest possible level (since BlackBox is specific to the Windows operating system, this is the SYSTEM privilege, equivalent to root on a Unix/Linux machine). The BlackBox applet can be easily customized to download any program to the infected machine and then run it. This applet is thus not only an exploit in itself; it is also a delivery vehicle for an arbitrary malicious payload.

In order to understand how these security failures come about, and also to understand the motivations for developing the analysis tool described in this paper, it is first necessary to briefly review the Java security model. Java security is enforced in three ways. The Java compiler has a large number of rules that it enforces in order to ensure that the syntax and semantics of the Java language are satisfied, but also to prohibit certain actions that are known to be associated with malicious code. For example, the Java compiler will refuse to compile any program that contains a method that makes use of an uninitialized variable. The output of the Java compiler is a binary file known as a classfile. In order for a Java application or applet to use the methods provided by a class, it must load it into the process or thread that is utilizing those methods. Loading is accomplished by a Java classloader. Every Java classloader will implicitly invoke the Java Bytecode Verifier. The Bytecode Verifier checks that the contents of the classfile conform to the classfile format. More importantly, the Bytecode Verifier verifies a large number of security constraints before it will allow the classloader to succeed. The final part of Java security enforcement is
handled by the Java runtime, which performs array bounds checking, runtime type conversion checking and a number of other tests.

Almost all Java exploits to date have used weaknesses in the Bytecode Verifier. The Bytecode Verifier is a part of the JVM, and the rules that it checks when analyzing a classfile are described in great detail in the JVM specification [JV]. The Bytecode Verifier uses a constraint based approach in performing its analysis. For example it checks that all local variables are written before being read, that each instruction receives precisely the set of operands that it is expecting, that the stack has the same depth at each program point regardless of execution path used to reach that program point, and many other constraints.

Our approach uses Alloy to perform constraint analysis on Java bytecodes. It attempts to emulate the constraint checking that is ostensibly being performed by the Bytecode Verifier. In Alloy it is very easy to express constraints in terms of formulas involving relations, and therefore the author has found it to be a rich environment for checking Java security constraints. Some efforts have been made to apply formal methods to Java bytecodes [XU], but these efforts have used a more heavyweight model checking approach that attempts to prove soundness, as opposed to Alloy’s lightweight constraint based approach that converts assertions into Boolean formulas and then searches for satisfaction assignments or the existence of counterexamples.

**Project Goals**

This project has two goals: (1) to provide an extensible framework for modeling security constraints imposed by the JVM’s Bytecode Verifier; and (2) to provide a concrete model for as many security constraints as possible, and to demonstrate that the analysis tool does check them correctly.

It would be straightforward to use Alloy to create a model for a specific block of Java code. While this might serve as the demonstration of the applicable power of Alloy to security analysis of the JVM, in the author’s opinion this would have little value in analyzing compliance with the JVM security constraints as a whole. Therefore it is desirable to have an extensible model. In this context “extensible” means that the model must have the ability to be applied to any block of JVM code and to perform analysis on that code against a specified set of constraints. In the Design section it will be shown how this goal was realized.

In the Background section several of the security constraints imposed by the JVM were mentioned. As indicated there, the JVM checks against a substantial number of such constraints. In general, most constraints are independent of one another, although there are some functional overlaps, as will be demonstrated below. Given the time constraints of the project, it was deemed necessary to select a realistic subset of the total set of JVM security constraints and model those. In developing the model for this initial set of constraints, with the extensibility goal in mind, a general framework for code analysis was created such that adding additional constraints would involve only incremental modifications, and not a complete restructuring of the model code. The current implementation concretely models three security constraints. While certain technical challenges, such as modeling exception handling, have not yet been addressed, the author believes that the current implementation can be readily adapted to additional constraints. A survey of next steps is given in the Future Work section of this paper.

**Design**

Alloy is a lightweight modeling language that uses first order logic. In Alloy the concept of a “relation” is central. Alloy is capable of analyzing assertions for satisfiability and also for the existence of counterexamples. A key observation is that the security constraints imposed by the JVM can be modeled as invariants, and thus can be analyzed by the Alloy Analyzer. Alloy is not a proof system, so the failure to find a counterexample to a constraint is not a proof that that constraint is satisfied, only that the constraint is satisfied with the search space specified. If a counterexample is found, however, that does indicate that the invariant has been violated, and the Alloy Analyzer conveniently provides a graphical representation of that counterexample.
In light of the extensibility goal described in the previous section, the initial design problem was to find an implementation of the Alloy model that would capture the invariants of interest abstractly, independent of any actual JVM code, but would then permit the model to be run against any concrete realization of JVM code. Initial experimentation with Alloy suggested two possible approaches: automatically generate Alloy functions, facts or predicates based on the JVM code to be analyzed, or automatically generate Alloy statements that initialized relations based on the JVM code to be analyzed. In order to realize a classical code/data separation, it was decided to use the latter approach. Thus, the Alloy model would be realized as a template, containing a fixed set of relations, functions, facts, predicates and assertions. This model would then be supplemented by relation initializers that would be derived from particular JVM code. In this approach, the template portion of the Alloy model would be completely independent of any choice of Java bytecodes, while the initializers would depend only weakly on the detailed implementation of the template. Specifically, the initializers being generated would only depend on the set of relations being initialized, and not on any specifics of the way in which the constraints were realized in the model template. This decoupling between the “data” portion of the model and the “code” portion of the model is the means by which the stated extensibility goal is achieved.

Further requirements analysis revealed that these two top level components, the model template and the initializers, could be further refined into four components: (1) the relation definitions; (2) the relation initializers; (3) the execution engine; and (4) the constraint assertions. The relation definitions, execution engine and constraint assertions are all part of the Alloy model template. The relation definitions are Alloy definitions of the top level signatures, which are atoms which contain relations, as well as the definitions of the relations themselves. As will be seen in the Implementation section, these relation definitions capture the static properties of individual JVM instructions, as well as capturing the JVM state as the execution engine executes. All other components of the Alloy model are logically dependent on the relation definitions.

The relation initializers are the initial values of the Alloy relations. They are generated from specific JVM code, and vary from one invocation of the model to the next. An initial design decision was made to capture JVM code at the method level. This, of course, is a tradeoff between performance and granularity. It would certainly be possible to model multiple methods within a single model. However, the time that Alloy takes to analyze a particular model is strongly dependent on the number of (program execution) states, which, in turn is strongly dependent on the size of the relation initializers. As will be seen below, the actual Alloy model template is quite suited to analyzing code blocks within a method, and could be extended (with some effort) to handle multiple methods. Relation initializers need to be generated from specific Java methods. Therefore, there needs to be an automatic way of converting the Java bytecodes in a method into these relation initializers. To this end, a Java classfile parser was created to perform this conversion. The parser takes a Java classfile as input and produces an Alloy model fragment as output. When the model fragment is combined with the Alloy template, a complete Alloy model is produced, as is shown in Figure 1 below.

![Diagram](https://via.placeholder.com/150)

**Figure 1:** Constructing a complete Alloy model using the classfile parser
The relation definitions and their initializers form a static representation of a set of properties of the Java method being analyzed. In order to observe dynamic behavior, this static representation needed to be extended with model actions that would mimic the execution of the JVM itself, at least to the extent that the JVM’s Bytecode Verifier would synthetically execute method code in order to perform its own constraint checking. Thus, an execution engine was needed. This execution engine would represent the flow of execution through the medium of stateful relations. Alloy’s “ordering” utility is used for representing this state. Execution could not be unbounded, of course, since Alloy only performs analysis over a finite set of states. It would have been possible to simply let Alloy “fall off the end” of execution, which is to say to allow the analyzer to perform an exhaustive analysis of all possible states in the state space. For both performance and structural reasons this was deemed to be an unacceptable solution. Therefore, the execution engine was designed such that certain JVM instructions are designated as terminal instructions. The execution engine was then designed to recognize this condition and act on it in such a way as to create no further unique states. Of course, this models the actual execution of the JVM itself. Certain instructions within a method are, in fact, terminal, in that they cause the method to be exited. One obvious question is the manner in which iterative constructs are handled by the execution engine. Would it provide better model fidelity to have the execution engine attempt to exactly mimic runtime execution, or would this lead to unacceptable performance penalties? In fact, the execution engine does not attempt to perform any branch prediction analysis in the model. The precise way in which this was handled, and its implications, will be explained in the Implementation section.

Finally, the model must provide for a way in which each JVM security constraint is actually checked by Alloy. Formulating the security constraints as Alloy assertions proved to be straightforward once the model had been constructed to accurately reflect the static and dynamic properties of the method code.

**Implementation**

The implementation of the JVM security constraints analyzer will be described in third subsections. In the first subsection, the three components of the model template, namely the relation definitions, the execution engine, and the security constraint assertions, will be described. In the second subsection, the implementation of the Class2Alloy classfile parser which is used to generate the relation initializers will be discussed. In the third section a concrete example will be dissected, including a description of the parser invocation and subsequent model analysis. The complete source code for the model template and the parser will be found on the author’s website [MR].

**Model Template**

The model template employs two top level signatures, an “Instruction” signature and a “State” signature. The Instruction signature is made abstract in order that each of the individual instructions that make up a method can be defined as concrete, atomic extensions of this abstract signature. Intuitively, this is reasonable because the properties (relations) of instructions vary from instruction to instruction, but are still static for any particular instruction. For example, the length of a given instruction in bytes is fixed for all time once the instruction is specified, but obviously varies between instructions. The “State” signature is derived from Alloy’s ordering utility, which predefines certain relations such as “first”, “next” and “last”. The State signature is dynamic, and the values of its relations are updated by the execution engine as it executes during analysis. The Alloy definition of these two signatures is shown below.

```alloy
abstract sig Instruction { map: Int,
    term: lone Int,
    r: set Int,
    w: set Int,
    ubt: lone Int,
    cbt: lone Int,
    smod: Int,
    len: Int }
```
An Alloy model is defined by its relations, so a careful description of each of the relations shown above will serve to illuminate the rest of the implementation. In the Instruction signature the map relation defines the byte offset of the instruction from the beginning of the method (or other block of code) being analyzed. The value of the map relation is an integer. The term relation is a set of integers that is either empty, or contains a single value. If the set is non-empty and contains the value 1, then the instruction is a terminal instruction – it causes the execution engine to cease creating new states. Note that it would have been entirely acceptable to model this relation as a Boolean taking the values 0 or 1. This implementation would have lead to more cluttered Alloy code, however, as most instructions are not terminal, while the chosen implementation allows the relation initializers to refrain from mentioning those relations for which the value is the empty set. The \( r \) and \( w \) relations model the sets of local variables read or written by the instruction, respectively. It is quite possible for an instruction to access more than one local variable, so these relations must be modeled as sets of integers. (The JVM itself also describes local variables in terms of integers.) The ubt relation names a possible unconditional branch target for the instruction. Most instructions do not have such a target, so the value of this relation is usually the empty set. An instruction can have at most one such target. If such a target exists, it is specified as a byte offset from the beginning of the method or code block, which is identical to the manner in which it is encoded in a classfile. The cbt relation names a possible conditional branch target. Conditional branch targets occur with conditional instructions, as will be seen in the example below. An unconditional branch target represents a transfer of control that must be executed, while a conditional branch target represents one that might be executed. Note that in the JVM it is possible for a conditional branch instruction to have multiple targets, but for simplicity this is not currently modeled. The smod relation models the number of bytes that the instruction modifies the method stack. This can be a positive integer (item(s) are pushed onto the stack), a negative integer (item(s) are popped off the stack) or zero. Finally, the len relation models the length of the instruction in bytes. Note that len and map contain redundant information, in that it should be the case that next->map = current->map + current->len. This redundancy was introduced deliberately as an additional way of validating the internal consistency of the model, as will be further described shortly.

The State signature represents the dynamic execution state. Its prog relation models the current instruction being executed; its readers and writers relations model the current set of local variables that have been read or written up to the current program point, respectively, and its depth relation models the current depth of the stack up to the current program point. As the execution engine processes the instruction initializers, it effectively creates new State atoms presenting the execution state after the effects of the current instruction have been applied. The current model encompasses three constraints that are being checked. These three constraints are checked by imposing assertions on the values of readers, writers and depth for some or all possible States.

The execution engine contains the Alloy code associated with State initialization, State sequencing, and execution termination. State initialization code is fixed within the model template and is not subject to being generated as part of relation initialization. The State initialization code creates an initial state \( s_0 \), sets the readers and writers relations of \( s_0 \) to be empty, sets the depth relation of \( s_0 \) to be zero, and sets the prog relation of \( s_0 \) to be the special “startup” instruction. There is no JVM instruction named “startup.” However, when the JVM invokes a method it performs certain very specific startup actions (the so-called method prologue) before the first instruction of that method in executed. The pseudo-instruction startup captures these actions. Specifically, when the JVM enters a method it will set the value of the local variable 0 to be “this.” If the method has arguments, these arguments are placed in local variables starting at index 1. Thus, the startup instruction will always have a non-empty value for its \( r \) relation. This will vary depending on the method signature, however, so that the initializer for the startup instruction must be generated by the classfile parser. By convention, the startup instruction is located at a map value of -1, and has length 1.
State transitions and also execution termination are handled by an Alloy fact known as stateTransition:

```alloy
fact stateTransition {
    all s: State - ord/last |
    let s' = ord/next[s] |
    ( some t: s.prog.term | t = 1 ) =>
        sameState/s, s' else
        nextState/s, s' }
```

This Alloy code makes use of the ordering utility. The model of execution is that for all States s, other than the last State, a new State s’ is constructed. If this new State corresponds to an Instruction with a non-empty term relation with value 1, then the execution engine ceases to create further new states. Otherwise, it executes the nextState predicate with the current and next States as its arguments. The nextState predicate is shown below. This predicate is responsible for updating the execution state relations (readers, writers and depth) and advancing the instruction state. This predicate first calls the nextInstruction predicate, which is responsible for updating the execution state relations (readers, writers and depth) and advancing the instruction state. This predicate first calls the nextInstruction predicate, which is updates the value of the current instruction for s’. It then updates the reader and writer relations for the new State s’ by calling predicates that take the unions of the corresponding r and w sets from the current instruction s.prog with the values of readers and writers from the current state s, respectively. Finally, it updates the depth relation for s’ by adding the smod value of the current instruction to the depth in the current State s. Thus, nextState is responsible for advancing to the next instruction, and also updating all the relations of the State that will be subsequently checked against the security constraints.

```alloy
pred nextState[s, s': State] {
    nextInstruction[s.prog, s'.prog] &&
    nextReader[s.prog, s.readers, s'.readers] &&
    nextWriter[s.prog, s.writers, s'.writers] &&
    (s'.depth = add[s.depth, s.prog.smod])
}
```

The nextInstruction calculates the next instruction for the state s’ as follows. If the current instruction has an unconditional branch target, as evinced by the fact that the current instruction’s ubt relation is non-empty, then the unconditional branch is taken. The next instruction is the one whose map value (byte offset) matches the value of the ubt for the current instruction. This raises the interesting possibility that the JVM bytecodes were sufficiently damaged that the ubt relation pointed to a map value that was not represented by any instruction, e.g. that the ubt pointed to the middle of an instruction, or outside the method entirely. This internal consistency constraint is checked by the solve predicate described below.

If there was no unconditional branch target, but there was a conditional branch target, then Alloy can choose to take that branch, and synthesize a new State based on that choice, or it can instead simply go to the next instruction in the map by adding the current value of the map relation to the length of the current instruction. It will also perform this latter action in case there are no branches of either type.

```alloy
pred nextInstruction[from, to: Instruction] {
    some from.ubt =>
    ( to.map = from.ubt ) else
    ( ( to.map = add[from.map, from.len] ) ||
        some bt: from.cbt { to.map = bt } )
}
```

The Alloy model template captures three JVM security constraints as Alloy assertions. The three security constraints being checked are the local variable constraint, the stack depth invariance constraint and the stack guard constraint. The local variable constraint states that no local variable can be read until it has first been written. The purpose of this constraint is to avoid accessing uninitialized local variables. The Java compiler enforces this constraint at the source code level for any variable (not just those that end up being stored in JVM local variables), and the Bytecode Verifier checks it at the classfile level. The stack depth invariance constraint states that the depth of the stack will always be the same at any program point, no matter how that program point was reached. The stack guard constraint states that the depth of the stack
will never become negative. This is a critical constraint for the JVM architecture. Unlike the architectures of many real machines, the JVM does not use the stack to pass parameters or return values; local variables are always used for both. Thus, the state of the stack (empty) should be the same on exit as on entry, for every method. Each of the constraints corresponds to a single Alloy assertion. There is also a special predicate that performs consistency checks on the model. These three assertions and the special predicate are:

```alloy
assert checkit {
  all s: State | s.readers in s.writers }
assert checkit1 {
  all s, s': State | (s.prog.map = s'.prog.map) =>
    (s.depth = s'.depth) }
assert checkit2 {
  all s: State | gte[s.depth, 0] }
pred solve {
  some finalState: State | finalState.prog.term = 1 }
```

These three assertions show the expressive power of Alloy. Each of the three constraints is expressible in a single Alloy statement. The local variable constraint, checkit, asserts that for all States, the set of integers in the readers relation must be a subset of the set of integers in the writers relation. Since a State has a 1-1 correspondence with a program point (except for the special State that has “startup” as its Instruction) this exactly expresses the local variable constraint. The stack depth invariance constraint, checkit1, asserts that for any pair of States s and s’ that have the same program point (s.prog.map = s’.prog.map) the depth of the stack must be the same (s.depth = s’.depth). The stack guard constraint, checkit2, asserts that for all States the corresponding stack depth must be greater than or equal to zero. These three constraints are positive constraints: if Alloy finds a counterexample this demonstrates that the constraint has been violated. A violation of the constraint then indicates that the corresponding JVM code does not conform to the classfile standard, and contains buggy or potentially malicious bytecode.

The “solve” predicate bears closer examination, since it relates to the handling of looping constructs and also internal consistency checking. This predicate asserts that there is some State with an Instruction that is terminal. In effect, this predicate asserts that execution terminates for some set of branch choices. When faced with a conditional branch choice, Alloy will choose a possibility. Thus, if there is any path to the terminal instruction, it will be reached by some set of choices by Alloy (provided the search space is large enough). What conditions could case this predicate to fail? One case would be the case of an unconditional branch whose target is an earlier program point. This could correspond to JVM code that contained an unambiguous infinite loop, such as one with a “while ( true )” test. Another situation that would cause this predicate to fail is if the map and len relations are not internally consistent. Examination of the nextInstruction predicate shows that if there are no branches the Instruction in the next State is calculated from the Instruction in the current state by adding the length of the current Instruction (the len relation) to the byte offset of the current Instruction (the map relation). Alloy must then find a matching Instruction whose map relation is equal to this sum. If no such Instruction exists, then the nextInstruction predicate will return false and the solve predicate will never be satisfied. The solve predicate therefore also provides a test of the internal consistency of the map and len relations.

**Class2Alloy Classfile Parser**

The model template is not a complete Alloy model, in that it does not encode any property information of an actual JVM method. That encoding is handled by the relation initializers, which must initialize all the Instruction relations based on the bytecodes of a specified method. The initialization must also handle the creation of concrete signatures that extend the abstract Instruction signature. Again, these concrete instruction signatures are based on exactly those instructions that are in the specified method.
A classfile parser, known as Class2Alloy, was written to generate these Alloy relation initializers given a Java classfile and also a method name. Class2Alloy was implemented in Java using the BCEL [BC], the Byte Code Engineering Library. BCEL is an extremely powerful classfile analysis library that provides ready access to the instruction stream in Java classes. BCEL makes it straightforward to extract the requisite properties for each instruction under consideration.

Class2Alloy is implemented in two Java files, Class2Alloy.java and AlloyString.java. Class2Alloy contains the main analysis routines, while AlloyString is a utility class that handles the specific Alloy syntax needed to generate syntactically correct relation initializers. The operation of the parser is as follows. The main() method receives three arguments: the name of a classfile, which must be in the classpath, the name of a method, and the name of an output file. The main() method creates a Class2Alloy instance; the Class2Alloy constructor creates a set of empty AlloyStrings, one for each relation to be initialized, along with an empty AlloyString that will hold the instruction signature information. The main() method then calls the doInput() method with the first two command line arguments. The doInput() method uses BCEL to load the classfile, enumerate its methods, and then searches for the named method in the array of methods present. If it fails to find a method with that name, an exception is thrown. On success doInput() returns a Method object, Method being a BCEL data type. The main() method then checks to see if the Method is abstract; if so, it prints an error message and exits. If not, it calls the main analysis method, doAnalyzeMethod(). The doAnalyzeMethod() method parses the Method object to obtain a list of instructions contained within the method. For each instruction, it then queries that instruction for those properties that need to be initialized in the Alloy model, namely its byte offset from the beginning of the method, its byte length, the sets of local variables that it reads or writes, the set of possible conditional or unconditional branches that it can take, and also the number of bytes that it adds or removes from the stack. The doAnalyzeMethod() method then calls utility methods to update the AlloyString objects with the information just obtained. When the doAnalyzeMethod() method returns the output file is then opened, and each AlloyString object is asked to print itself to that output file. This, of course, causes an invocation of the toString() method in the AlloyString class. The toString() method handles the gory details of generating syntactically correct Alloy output for each of the relation initializers, as well as generating the appropriate Instruction extension signatures for each instruction in the method being analyzed.

Once this output file is combined with the model template, a complete model specialized for the method under analysis is obtained. The Alloy analyzer is then be run on that model, and each of the three constraint assertions, as well as the solve consistency predicate, is then invoked to determine the presence of counterexamples or a failure to converge to a terminal state. The example shown in the next subsection should serve to clarify the entire process.

Example Model Generation and Analysis

Consider the following extremely simple Java method:

```java
public int fred(int input) {
    int tmp;
    if ( input < 10 )
        tmp = input*5;
    else
        tmp = input;
    return tmp;
}
```

In this method, the variable “tmp” is initialized in each path within the method. Indeed, if one were to replace one the assignments to “tmp” with other code that failed to give it some value, the Java compiler would complain vigorously, and would refuse to compile the class containing fred(). This method was used as the initial test case for constraint checking. When compiled and then passed through the Class2Alloy classfile parser, a set of relation values is obtained. Table 1 shows these relation values.
Table 1: Instruction relation initializers for the “fred()” method

<table>
<thead>
<tr>
<th>Instruction</th>
<th>map</th>
<th>len</th>
<th>r</th>
<th>w</th>
<th>term</th>
<th>ubt</th>
<th>cbt</th>
<th>smod</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>iload_1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>bipush 10</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>icmpge 13</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-2</td>
</tr>
<tr>
<td>iload_1</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>iconst_5</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>imul</td>
<td>8</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>istore_2</td>
<td>9</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td>-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>goto 15</td>
<td>10</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>iload_1</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>istore_2</td>
<td>14</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td>-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iload_2</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ireturn</td>
<td>16</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-1</td>
</tr>
</tbody>
</table>

The classfile parser is invoked on a classfile test.class containing the fred() method with the following command line:

```
java Class2Alloy.class test.class fred output.txt
```

(Note that the BCEL jar file must be in the classpath.) The actual output of Class2Alloy is a set of eight initializers for each of the eight Instruction relations, as well as the Instruction signature extension string. The Instruction signature extension string and the first of the eight relations are shown below:

```
one sig startup, iload_1_1, bipush_2, if_icmpge_3, iload_1_4, iconst_5_5, imul_6, istore_2_7, goto_8, iload_1_9, istore_2_10, iload_2_11, ireturn_12 extends Instruction {}

fact maps {
  map = startup->(-1) + iload_1_1->0 + bipush_2->1 + if_icmpge_3->3 + iload_1_4->6 + iconst_5_5->7 + imul_6->8 + istore_2_7->9 + goto_8->10 + iload_1_9->13 + istore_2_10->14 + iload_2_11->15 + ireturn_12->16 }
```

Observe that each instruction signature that extends Instruction is declared to be unique, using the “one” keyword. Observe also that in order to enable each occurrence of an instruction to be distinguishable, each instruction signature has a unique serial number _1, _2, etc appended to it. Thus, the three occurrences of the iload_1 instruction are uniquely identified, since each has a different suffix (_1, _5 and _9).

The output of the classfile parser can be validated in two ways. First, one can manually examine its output against that obtained by a high quality Java disassembler, such as DJ [DI]. Second, one can reconstitute the bytecodes for the fred() method by taking the Class2Alloy output, constructing the Java assembly language from which it came, and then assembling that using a JVM assembler such as Jasmin [JA]. While neither of these approaches constitutes proof that the parser output is correct, repeated applications of these processes, together with the existence of a large user community for BCEL, gives high confidence that the parser output obtained is indeed correct.

If one analyzes the resulting model for fred(), all three constraints are satisfied and the solve predicate converges. Examination of the Alloy solutions for the solve predicate reveals that in some of the solutions...
the if_icmpge branch is taken, and in others it is not taken. It is straightforward to modify the Alloy code for this method in order to deliberately introduce constraint violations. For example, if one replaces the istore_2_7 instruction, which writes into local variable 2, with a nop instruction which does not perform the local variable write, a counterexample to the checkit assertion is obtained immediately. If one turns off the terminal relation on the ireturn_12 instruction, the solve predicate will fail to converge. In total, almost a hundred methods were examined using this analysis process; expected results were obtained in all cases.

In summary, JVM security constraint analysis using Alloy has proven to be an extremely powerful tool for examining Java bytecodes. Even at this early stage of development, where only three constraints are tested, meaningful results have been obtained. Extensions to this work, as described next, are ongoing with the goal of increase the scope of constraint checking and further refining and improving the analysis process.

Future Work

There are several areas in which the JVM security analysis approach described in this paper can be extended and improved. The most obvious, and certainly the most important, is to add constraint checking for additional constraints. The opcode argument constraint, which states that each JVM instruction is invoked with the correct number of type-conformant arguments, is of particular importance. In addition, extending the current consistency checking of the map and len properties is also a worthwhile step, since the current model does not distinguish the two possible cases in which the solve predicate does not converge, namely infinite loops and an inconsistent set of map and len relation values. The latter should be checked explicitly.

The current model does not handle exceptions. Since exploitation of exception handling by the Bytecode Verifier has been the basis of at least one widespread piece of malware, adding exception handling to the model has high priority. Naively, one might say that every instruction in that portion of a Java method that is protected by an exception handler has a conditional branch target equal to the first instruction of the handler code. It is necessary to fix up the stack depth as well, because when an exception is thrown an object that has a type which is a subtype of Exception is placed on the stack. The challenge for this implementation is handling multiple exception handlers within the same method. This is an ongoing area of development.

The cbt relation currently permits at most one conditional branch target. This means that any Java method that contains an instruction with multiple conditional branch targets, such as the tableswitch instruction, will not be handled properly by the current model. This must be addressed by a more complete model, since most Java compilers will generate a tableswitch bytecode for “switch” statements that appear in the Java source.

Finally, the current analysis tool would benefit significantly from increased automation. Since Alloy itself is written in Java, the Class2Alloy class could be modified to create an Alloy model in memory, using the template and its current relation analysis code, and could then invoke the Alloy analyzer directly on that in-memory representation of the model. Once this modification was made it would then be straightforward to analyze all methods in a classfile, or all methods in all classes in a jar file.

Acknowledgements

The author wishes to extend special thanks to Professor Assaf Kfoury of the Computer Science Department of Boston University for suggesting this line of inquiry, and for his continued support and encouragement.
References

AL: http://alloy.mit.edu
BC: http://jakarta.apache.org/bcel
CV: http://cve.mitre.org
DI: http://members.fortunecity.com/neshkov/dj.html
JA: http://jasmin.sourceforge.net
MR: http://cs-people.bu.edu/markrey