Outline

Overview

Program understanding

Program verification and property checking

Bug finding

Summary
Recap

We’re looking at

► principles and tools

for ensuring software security.

This lecture looks at:

► further example uses of static analysis
► some hints about how static analysis works
Advanced static analysis jobs

Static analysis is used for a range of tasks that are useful for ensuring secure code.

Basic tasks include **type checking** and **style checking**, described last lecture.

More advanced tasks are:

- **Program understanding**: inferring meaning
- **Property checking**: ensuring no bad behaviour
- **Program verification**: ensuring correct behaviour
- **Bug finding**: detecting likely errors
Outline

Overview

Program understanding

Program verification and property checking

Bug finding

Summary
Program understanding tools

Help developers understand and manipulate large codebases.

- Navigation swiftly inside the code
  - finding definition of a constant
  - finding call graph for a method

- Support *refactoring* operations
  - re-naming functions or constants
  - move functions from one module to another
  - needs internal model of whole code base

- Inferring *design from code*
  - Reverse engineer or check informal design

**Outlook:** may become increasingly used for security review, with dedicated tools. Close relation to tools used for malware analysis (reverse engineering).
Commercial example: Structure101
Research example: Fujaba and Reclipse
How Reclipse works

We’ll explain some of these processes later.

See Fujaba project at University of Paderborn
Outline

Overview

Program understanding

Program verification and property checking

Bug finding

Summary
Program verification

- The gold standard, best guarantee
- Uses **formal methods**
  - theorem proving
  - model checking
- Drawback: needs precise **formal specification**
- Drawback: expensive to industry
  - time consuming, needs experts (logic/maths)
  - ... but investment up front may pay off
- Currently mainly used in safety critical domains
  - e.g., railway, nuclear, aeronautics
  - emerging: automobile, security

Example tools: **SPARK, Event-B**. General purpose **Interactive Theorem Provers** such as **Coq** and **Isabelle/HOL** are also used to verify code.
Property checking

**Lightweight formal methods**

- Make specifications be *standard* and *generic*
- this program cannot raise NullPointerException
- all database connections are closed after use

**Static checking** (not verification)

- Prevent many violations of specification, not all
- May produce *counterexamples* to explain violations
- Chain preconditions *(requires)* - postconditions *(ensures)*
  - allows *inter-procedural* analysis

Examples: Code Contracts, Splint, JML, Grammatech CodeSonar, PolySpace, ThreadSafe, Facebook Infer.
Assertion checking

Many languages have support for *assertions*. These are dynamic (runtime) checks that can be used to test properties the programmer expects to be true.

```plaintext
assert(exp)
```

- fails if `exp` evaluates to false
- assertion tests **usually disabled**
  - treated as comments
  - may be enabled for testing during development
  - or when running unit tests

**Question.** What could happen if tests are run only with assertions enabled?
Private static int addHeights(int ah, int bh) {
    assert ah > 0 && bh > 0 : "parameters should be positive";
    return ah+bh;
}

Notice above method is private.

- API (public) functions should *always* test constraints
  - throw exceptions if not met
  - eliminate clients (or attackers) who break API contract
- Internal functions may rely on local properties
  - if maintained in same class, easier to check/ensure
Assertions for security

We could use assertions as safety checks for functions that are at risk of being used in a buggy way.

```c
assert(alloc_size(dest) > strlen(src));
strcpy(dest, src);
```

alloc_size() is not a standard C function, but GCC, for example, has support for trying to track the size of allocated functions with function attributes.
From dynamic to static

With static analysis, we *may* be able to automatically determine whether assertions (if enabled) will:

1. always succeed
2. may sometimes fail (unknown)
3. will always fail

Easy cases:

1. `assert(true);`
2. `x=readint(); assert(x>0);`
3. `assert(false);`

The perfect case would be showing that assertions in a program can only succeed: thus they do not need to be checked dynamically.

**Question.** what troubles can you see with case 2?
Programming with contracts

This can be useful to increase confidence in programs, or use a contract based programming approach, where pre- and post-conditions are explicitly described by the programmer.

Some static analysis tools use assertions (entirely) internally; others allow an interface using annotations.
Design by Contract (TM) aims to build a system as a set of components whose interaction is governed by mutual obligations, or contract.

The idea was promoted by Bertrand Meyer in his design of the Eiffel OOP language (1986).

It adapts and extends ideas from Hoare Logic used for program verification, in particular, the use of pre-conditions and post-conditions.

\( \{P\}C\{Q\} \)
### Example contract for insertion into dictionary

<table>
<thead>
<tr>
<th></th>
<th>Obligations</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client</strong></td>
<td>Table isn’t full, key is non-empty string</td>
<td>Get updated table with element added for given key</td>
</tr>
<tr>
<td><strong>Supplier</strong></td>
<td>Record given element in table associated with given key</td>
<td>No need to check for full table or empty key</td>
</tr>
</tbody>
</table>

**Question.** What are the preconditions and postconditions for the code here?
Specification in Eiffel

```
put (x: ELEMENT; key: STRING) is
   -- Insert x so that it will be retrievable through key.
   require
      count <= capacity
      not key.empty
   do
      ... Some insertion algorithm ...
   ensure
      has (x)
      item (key) = x
      count = old count + 1
   end
```

As well as pre and post conditions, other contract features include *class invariants* which must be established when an object is created and maintained whenever it is modified.
Relationship to defensive programming

“Defensive programming” adds checks to code to ensure that pre-conditions are met (coding assertions explicitly).

```plaintext
put (x: ELEMENT; key: STRING) is
  do
    if key.empty then
      error "Empty key supplied"
    ...
  end
```

With contracts these checks are not added: they are replaced by contract checking.

Contract checking may use static verification, or dynamic checking (or some combination).

Besides products sold by Eiffel Software, there is an open source free Eiffel tool chain developed by the Gobo Eiffel Project.
Contracts in Java

The **Java Modeling Language** allows specifications in the same way as Design by Contract.

```java
/* requires 0 < n;
   assignable elems;
   ensures elems.length == n; */
public BoundedStack(int n) {
  elems = new Object[n];
}
```

The **OpenJML project** implements a contract checking tool for JML.

**Exercise.** Play around with the example program on the OpenJML home page, using its web-based checking tool to fix the error.
Splint: Secure Programming Lint

Allows annotations to be added by programmer, specifically for a static analysis tool to check.

```c
void *strcpy(char *s1, char *s2)
  /*modifies *s1 */
  /*requires maxSet(s1) >= maxRead(s2) */
  /*ensures maxRead(s1) == maxRead (s2) */;
```

- maxSet(x): greatest offset (index) that may be written to in x
- maxRead(y): greatest that may be read from in y

Splint was introduced in 2001, it has a Github repo but isn’t in active development by original academic authors.
strncat

strncat(dest, src, num): appends the first num characters of source to destination, plus a terminating null character. If the length of the C string in src is less than num, only the content up to the terminating null-character is copied.

char *strncat (char *s1, char *s2, size_t n)
    /*requires maxSet(s1) >= maxRead(s1) + n*/

void f(char *str){
    char buffer[256];
    strncat(buffer, str, sizeof(buffer) - 1);
    return;
}
Splint warning messages

```c
char *strncat (char *s1, char *s2, size_t n)
    /*requires maxSet(s1) >=maxRead(s1) + n*/

void f(char *str){
    char buffer[256];
    strncat(buffer, str, sizeof(buffer) - 1);
    return;
}
```

strncat.c:4:21: Possible out-of-bounds store:
    strncat(buffer, str, sizeof((buffer)) - 1);
Unable to resolve constraint:
    requires maxRead (buffer strncat.c:4:29) <= 0
needed to satisfy precondition:
    requires maxSet (buffer strncat.c:4:29)
        >= maxRead (buffer strncat.c:4:29) + 255
derived from strncat precondition:
    requires maxSet (<parameter 1>)
        >= maxRead (<parameter1>) + <parameter 3>
Reasoning with assertions

How does a static analyser reason?

Computations about assertions can be chained through the program, using a program logic inside the tool.

E.g., build up a set of facts known before each statement:

```cpp
x = 1;    // { } (nothing known)
y = 1;    // { x = 1 }
assert (x < y);  // { x = 1, y = 1 }
```
Symbolic evaluation

This can work also with variables, whose value is not known statically:

```plaintext
x = z; // { } (nothing known)
y = z+1; // { x = z }
assert (x < y); // { x = z, y = z+1 }
```

// SUCCEED (provided z<MAXINT)
Conditionals and loops

These make static analysis *much* harder, of course.

```plaintext
x = v;    // {} (nothing known)
if (x < y) // {x=v}
  y = v;   // {x=v, x<y}
assert (x < y) // Either: {x=v,y=v}: FAIL
              // Or: {x=v,¬(x<y)}: FAIL
```

For conditionals, we need to either

- explore every path
- merge information at *join-points*

For loops, we need to either

- unroll for a finite number of iterations
- capture variation using logical *invariants*
Using logical (or other) reasoning techniques, there are various different types of assertions that are useful for security checking, for example:

- **Bounds and range analysis**
- **Tainted data analysis**
- **Type state** and **Resource** tracking

**Exercise.** What kinds of security issues can these assertions help with? What kinds of security issues would need other assertions?
Bound/range Analysis

```plaintext
alloc_size(dest) > strlen(src)
array_size(a) > n before a[n] access

- Check integers are in required ranges
```
Taintedness

tainted(mypageinput)
untainted(newkey)

- Tracks whether data can be affected by adversary.
- Tainted input shouldn’t be used for security sensitive choices
- and should be sanitized before being output
- Taint analysis approximates information flow
  - information may be leaked indirectly as well as directly
Type State (Resource) Tracking

- `isnull(ptr), nonull(ptr)`
- `isopen_for_read(handle), isclosed(handle)`
- `uninitialized(buffer), terminatedstring(buffer)`

- Tracks status of data value held by a variable
- Helps enforce API usage contracts to avoid errors
  - e.g., DoS
- Usage/lifecycle may be expressed with automaton
Example: avoiding double-free errors

start → initial state → free(x) → freed → free(x) → error

(other operations) → (other operations)
Not all null pointer analyses are equal! Some compilers spot only "obvious" null pointer risks, others perform deeper analysis like CodeSonar. IDE analysis may be in between.
We’ll see examples of contracts further on in this lecture.
Outline

Overview

Program understanding

Program verification and property checking

Bug finding

Summary
Bug finding tools look for suspicious patterns in code. 

FindBugs is an example:

- Finds possible Java bugs according to rules
  - rules are suspicious patterns in code
  - designed by experience of buggy programs
  - ... collected from real world and student(!) code

- Warnings are categorized by
  - **severity**: how serious in general the problem is
  - **confidence**: tool’s belief of true problem
Example bugs

Common accidents

An error found in Sun’s JDK 1.6:

```java
public String foundType() {
    return this.foundType();
}
```

Misunderstood APIs

```java
public String makeUserId(String s) {
    s.toLowerCase();
    return s;
}
```
if (this.fitz == null) {
    synchronized (mylock) {
        if (this.fitz == null) {
            this.fitz = new Fitzer();
        }
    }
}

[dice]da: findbugs Fitz.class
M M DC: Possible doublecheck on Fizz.fitz in Fitz.getFitz()
    At Fitz.java:[lines 1-3]
## Findbugs GUI

### Package | Priority | Category | Bug Kind | Bug Pattern | Severity | Issue Message
--- | --- | --- | --- | --- | --- | ---
edu.umd.cs.findbugs.config | (3) | | | | | Method may fail to close stream
edu.umd.cs.findbugs.filter | (1) | | | | | Stream not closed on all paths
edu.umd.cs.findbugs.util | (1) | | | | | Method may fail to close stream
edu.umd.cs.findbugs.visclass | (1) | | | | | Stream not closed on all paths
edu.umd.cs.findbugs.workflow | (2) | | | | | Stream not closed on all paths
java.util | (2) | | | | | Stream not closed on all paths

### Error Message

**edu.umd.cs.findbugs.util.Util.getXMLType(InputStream) may fail to close stream**

At Util.java (line 108)

In method edu.umd.cs.findbugs.util.Util.getXMLType(InputStream) [Lines 102 - 123]

Need to close java.io.Reader

**Method may fail to close stream**

The method creates an IO stream object, does not assign it to any fields, pass it to other methods that might close it, or return it, and does not appear to close the stream on all paths out of the method. This may result in a file descriptor leak. It is generally a good idea to use a finally block to ensure that streams are closed.

[Findbugs SourceForge](http://findbugs.sourceforge.net/)

[University of Maryland](http://www.umd.edu)
Clang Static Analyser

An open source tool for C, C++, Objective-C included in XCode.
Clang Static Analyser HTML reports

openssl-1.0.0 - scan-build results

<table>
<thead>
<tr>
<th>User:</th>
<th>user@localhost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Directory:</td>
<td>/home/user/Exercise-4/openssl-1.0.0</td>
</tr>
<tr>
<td>Command Line:</td>
<td>make</td>
</tr>
<tr>
<td>Clang Version:</td>
<td>clang version 3.4 (tags/RELEASE_34/final)</td>
</tr>
<tr>
<td>Date:</td>
<td>Fri Jan 17 12:03:31 2014</td>
</tr>
</tbody>
</table>

Bug Summary

<table>
<thead>
<tr>
<th>Bug Type</th>
<th>Quantity</th>
<th>Display?</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Bugs</td>
<td>269</td>
<td>✓</td>
</tr>
<tr>
<td><strong>API</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argument with 'nonnull' attribute passed null</td>
<td>7</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Dead store</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dead assignment</td>
<td>203</td>
<td>✓</td>
</tr>
<tr>
<td>Dead increment</td>
<td>11</td>
<td>✓</td>
</tr>
<tr>
<td>Dead initialization</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Logic error</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assigned value is garbage or undefined</td>
<td>3</td>
<td>✓</td>
</tr>
<tr>
<td>Branch condition evaluates to a garbage value</td>
<td>1</td>
<td>✓</td>
</tr>
<tr>
<td>Dereference of null pointer</td>
<td>30</td>
<td>✓</td>
</tr>
<tr>
<td>Division by zero</td>
<td>1</td>
<td>✓</td>
</tr>
<tr>
<td>Result of operation is garbage or undefined</td>
<td>7</td>
<td>✓</td>
</tr>
<tr>
<td>Uninitialized argument value</td>
<td>4</td>
<td>✓</td>
</tr>
</tbody>
</table>

Reports

<table>
<thead>
<tr>
<th>Bug Group</th>
<th>Bug Type</th>
<th>File</th>
<th>Line</th>
<th>Path Length</th>
<th>View Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Argument with 'nonnull' attribute passed null</td>
<td>ssl/d1_both.c</td>
<td>1015</td>
<td>9</td>
<td><a href="#">View Report</a></td>
</tr>
<tr>
<td>API</td>
<td>Argument with 'nonnull' attribute passed null</td>
<td>ssl/d1_srv.c</td>
<td>1184</td>
<td>10</td>
<td><a href="#">View Report</a></td>
</tr>
<tr>
<td>API</td>
<td>Argument with 'nonnull' attribute passed null</td>
<td>ssl/s3_srv.c</td>
<td>1725</td>
<td>10</td>
<td><a href="#">View Report</a></td>
</tr>
<tr>
<td>API</td>
<td>Argument with 'nonnull' attribute passed null</td>
<td>crypto/asn1/a_bytes.c</td>
<td>295</td>
<td>21</td>
<td><a href="#">View Report</a></td>
</tr>
</tbody>
</table>
Outline

Overview

Program understanding

Program verification and property checking

Bug finding

Summary
Take away points

Program analysis tools can help find security flaws.

- static: examine millions of lines, repeatedly
- dynamic: equip code with *self-checking*

Some tools are generic bug finding, built into IDE.
Others are specific to security, may include:

- risk analysis, including impact/likelihood
- issue/requirements tracking, metrics

Expect these to become mainstream

- current frequency of security errors unacceptable
- incentives will eventually affect priorities
Some of this lecture is based Chapters 2-4 of

- *Secure Programming With Static Analysis* by Brian Chess and Jacob West, Addison-Wesley 2007.

Recommended reading: