

Examples of Code Roaches

First Draft List

Cem Kaner

September 11, 2005

Why a Potential-Bug List?

- **Given a potential error, you can develop a method to test for it**
- **Foundation for**
 - **Code inspections**
 - **Glass box tests**
 - **Glass box test tools**
 - **Test tool evaluation**
- **What is a test technique?**
 - **A heuristic for exposing a bug of a specific kind**
- **Every type of bug can have one or more techniques optimized to expose it**
- **A list of potential bugs is a list of requirements for test techniques.**

Example: How Should You Test a Loop?

It Helps to Consider Loop Types

- **Index variable**
- **Initialization expression**
- **Continuation expression**
- **Update expression**

```
for ( init_expr;  
      continue_expr;  
      update_expr )  
      statement;
```

```
while ( continue_expr )  
      statement;
```

```
do  
      statement  
      while (continue_expr);
```

```
Break;
```

Risks

- **Associated with the index variable or expressions**

- **Associated with the statements being iterated**

So How Can a Loop Fail?

Associated with index or expressions

- *Overflow yields unexpected value*
- *Divide by zero*
- *Continue condition off by 1*

for (init; continue; update) statement;

- *Index reset in loop, never terminates*
- *Index reset inside loop, causing error in calculations based on loop iterations*
- *Index never meets continue condition:*
 - *Condition is equality, index skips past it*
 - *Condition rounds to not-quite-equal*
- *What if initialization fails the continuation expression?*
 - *Loop never runs, is that a problem?*

while (continue_expr) statement;

- *Loop might never execute*
- *Loop might never terminate*

do statement while (continue_expr);

- *Loop might never terminate*

Associated with statements iterated

- *Memory leak triggered by the iteration*
- *Stack overflow triggered by the iteration*
- *Variable intended to be in synch with the index goes out of synch*

break;

Now, What Tests Should You Run?

Data Declaration

- **Referenced variable not yet declared**
- **Variable declared but never used**

Data Reference

- **Reference the wrong variable**
 - two variables differ only in capitalization
 - two variables have same name, defined and used in different places
- **Read an outdated copy of the variable**
- **Reference outside the bounds of the array**
 - causes runtime error
 - causes runtime extension of the array
- **problems associated with non-integer array indexes**
- **off-by-one reference**
 - e.g. expect first array element to be [0] when it is really [1] or [1] when it is really [0]

Data Setting

- **Set the value of the wrong variable**
 - two variables differ only in capitalization
 - two variables have same name, defined and used in different places
- **Method fails to update a variable before returning**
 - Calculates but doesn't update
- **Method sets variable to a constant (relic of junit passing test) and returns**
- **Attempt to set to/with wrong type**
 - aliases to same block of storage, with different data types
 - result variable has lower precision than variables in the calculated expression:
 - rounding error or truncation on conversion

Data Setting (2)

- **Doesn't validate against user supplied filters**
 - **Doesn't validate the user supplied filters**
 - **Inappropriately reconciles user and system filters**
 - **Doesn't read the full set of filters**
 - **unexpectedly long list**
 - **Parameter inconsistency**
- **Fails to notice it is copying a value that overflow/underflowed**
- **Wrong mask in bit field**

Data Value

- **Initial state**
 - Sets to outdated constant
 - Not initialized to zero
 - Not initialized to empty
 - Supposed to be initialized elsewhere
 - Other method / process
 - Compiler
 - initialized elsewhere unexpectedly (scope broader than you realize)
- **Updated state**
 - User input values
 - Accepts invalid input
 - Accepts inconsistent input
 - Accepts unlikely input without confirmation
 - updated elsewhere unexpectedly (scope broader than you realize)
 - updated by method that doesn't obviously operate on this variable

Data Value (2)

- **Out of range**
 - **String too long**
 - **File name too long**
 - **Too long for buffer**
 - **Overwrites other data**
 - **Integer overflow**
 - **Float exponent overflow**
 - **Float mantissa overflow**
 - **Not in the enumerated list**
 - **Too many**
 - **array overflow**
 - **stack overflow**
- **Edited string visually appears to have data deleted but data are overwritten**
- **Creates/displays new instance rather than modify or replace old instance**
- **Persistent data**
 - **lose value unexpectedly**
 - **retain value (don't realize this is persistent)**

Message passing

- **Parameter lists**
 - **Correct sequence (number and types)**
 - **Plausible values**
 - **Correct values**
- **Processing results**
 - **Does wrong thing in response to proper command**
 - **Does less than expected in response to proper command**

Message passing (2)

- **Feedback**
 - **Success feedback**
 - needs results
 - needs success flag
 - **Message rejection**
 - **Requested task attempted but failed**
 - **No feedback expected**
 - **Unexpected response**
 - response to nonexistent message
 - Nth response when N-1 are expected
 - **Expected response at unexpected time**
 - **Unreadable response**
 - **Response with inappropriate content**
- **Message sent to wrong process or port**
- **Message sent to N of N+1 proper recipients**
- **units (e.g. cm versus inches) don't match for sender / recipient**

Pointers

- **pointer to unallocated area of memory**
 - wasn't ever allocated
 - allocated but then freed up
- **pointer into wrong place in the data structure**
 - miscalculate length of record
 - miscalculate position in record (e.g. which element in the array)
- **pointer into wrong data structure**
 - past end of referenced data structure
 - wrong address

Data Use

Data Interpretation

- **misunderstood contents of memory (e.g. interpret integer data as string)**

Data Storage

- **Save at an unexpected time, overwriting data**
- **Fail to save at the expected time, doesn't update data**
- **Problems with undo buffer or stack**
- **Saves record in slightly wrong format (e.g. 1-character too long, misaligns next record)**

Memory management

Device Operations

- **Doesn't handle device nonresponse**
- **Doesn't handle device error messages (such as)**
 - **printer not ready**
 - **out of memory**
 - **wants data resent**
 - **invalid command**
 - **invalid data**

Device Operations (2)

- **Input device (keyboard/mouse/etc)**
 - **misunderstands state of device (e.g. language settings modify interpretation of keys)**
 - **conflicting demands from parallel devices**
 - **Drops characters or clicks**
 - **Queues characters or clicks unexpectedly**
 - **Queues characters or clicks inconsistently or in wrong sequence**
- **Sound**
 - **Plays wrong sound**
 - **Plays sound through wrong device**
 - **Too loud or too soft (i.e. louder or softer than the parameters require)**
 - **Incomplete sound**

File operations

- **No such file**
- **Full (on write)**
- **Almost full on write**
- **Illegal characters**
- **Premature terminator character/string**
 - **end of file embedded in string being stored**
- **fails to recognize end of file when attempting to read/write data**
- **Interrupted while writing**
- **Interrupted while reading**
- **Wrong record structure**
- **No error message**
- **Fails to interpret error message**
- **Wrong error message**
- **insufficient memory to hold the file**
- **attempt to read/write a file before opening it**
- **attempt to read/write a file after closing it**
- **failure to close a file after changing it**

Display

- **Write to wrong screen position**
- **Message too large for display field**
- **Message oriented incorrectly**
- **Message has wrong attributes**
 - **color**
 - **size**
 - **font**
 - **blink**

Display (2)

- **Cursor**
 - not displayed
 - doubled
 - not blinking
 - wrong shape or color
 - moves to wrong place
- **Pointer**
 - not displayed
 - doubled
 - not blinking
 - wrong shape or color
 - moves to wrong place

Performance

- **Nested loop unnecessarily repeats an operation**
- **Long time-out delays**
- **Unnecessary time-out delay (error message or other redundant state info available)**
- **garbage collection creates unexpected delay**
- **Synchronization (A1 through AN must all happen, then we can do B) includes too many Ai's or is too variable**

Exception handling

Log

- **Error log**
 - **Fails to log**
 - **Logs wrong data**
 - **Mostly correct, some data outdated**
 - **Mostly correct, some data mis-set or miscalculated**
 - **Wrong error / conditions (i.e. packs the wrong message overall)**
 - **Logs in wrong sequence**
 - **Log in wrong format**
 - **Incorrect termination of log entry**
 - **Incorrect header**
- **Transaction log**
- **Monitored event log**

Control Flow

- Unreachable code
- Does too much before exiting on error
- Will not exit on invalid state / data
- Comes from unexpected place
- Jump through data rather than address
- Returns to wrong place
 - Corrupt stack
 - Goto
- Interrupt at unexpected time
- Fails to restore or update interrupt vector
- Loop starts with wrong initial value
- Loop doesn't terminate
 - Never reaches terminal comparison
 - Terminates when $\text{index} = N$, but skips N
 - Terminates when $\text{index} = N$, but rounding error creates not-quite- N
 - Index reset in body of loop
- Loop control variable changed unexpectedly
- Variable intended to be in synch with loop control goes out of synch

Control Flow (2)

- Assume incorrectly that X has finished before beginning Y
- Assume that X cannot happen in the short time needed to process Y
- exits before setting (resetting) a key variable
- loop never executes (but subsequent code assumes that it did)
- drops through to an inappropriate default case
- no default case
- off-by-one error in number of iterations
- incorrect assumptions associated with multiple entry points into same segment of code

Table-driven control Flow

- **Index to wrong table entry**
- **Unreachable table entry**
- **Invalid address in table**
- **Incorrect address in table**

Comparison

- **Test floating point for equality fails to allow for rounding error**
- **compare signed instead of absolute values**
- **compare absolute values instead of signed**
- **Wrong inequalities**
 - **< versus <=**
 - **= and not-equal when there's a third meaningful case**

Calculation

- **Unexpected precision**
 - high
 - low
- **Rounds rather than truncates**
- **Truncates rather than rounds**
- **Sequence of operations costs precision**
- **Erroneous algorithm**
- **wrong result from 3rd party library**
- **Allegedly equivalent operations/methods are not**

Calculation (2)

- **Alternate calculations depending on a parameter (e.g. algorithm1 for small N, algorithm2 for large N)**
 - **wrong calculation selected**
 - **wrong boundary (on N) specified**
 - **Error because only one of the calculations was tested**
- **Order of operations**
 - **Error because parentheses needed**
 - **Error because of precedence rules**
- **mixed-mode arithmetic yields unexpected results**
 - **order of operations may yield different effects**
- **integer overflow**
- **integer division has unexpected results**

Boolean Expressions

- confuse inclusive and exclusive OR
- negated expression
- precedence error
- missing parentheses
 - invalid expression
 - valid but wrong
- complex expression fails to consider some of the cases
- wrong default
- overlapping cases that should have both operations done to them not just one

Comments

Syntax