The Keyhole Problem

Scott Meyers

www.aristeia.com
Topics

- What are “keyholes?”
- Why are they important?
- How can we eliminate or avoid them?
  - In some cases, elimination (from current software) isn’t worth it, but avoidance (for future software) is.
  - Due to time restrictions, I’ll treat this aspect superficially.

Almost everything that follows is something I experienced personally.

- I don’t seek out keyholes.
- They’re unavoidable.
Visible Keyholes
(GUI Components)
The Vertical ListBox/ComboBox Keyhole

From Adobe’s FrameMaker 6:

To test for the existence of a value in a sorted range, use binary_search. Unlike binary_search in the standard C++ library (and hence also in the standard C library), binary_search returns only a bool whether the value was found. binary_search answers the question, “Is it there?” and its answer is either yes or no. If you need more information than that, you need a different algorithm.

Here’s an example of binary_search applied to a sorted vector:

```cpp
vector<Widget> vw;  // create vector, put...
sort(vw.begin(), vw.end());  // data into it, sort the...
Widget vw;  // value to search for...
if (binary_search(vw.begin(), vw.end(), w)) {
    // w is in vw...
} else {
    // it’s not...
}
```

If you have a sorted range and your question is, “Is it there?” and it’s somewhere in it? you want equal_range, but you may think you want lower_bound. I’ll discuss equal_range shortly, but first, let’s examine lower_bound as a way of locating values in a range.

When you ask lower_bound to look for a value, it returns an iterator pointing to either the first copy of that value (if it’s found) or to the proper insertion location for that value if it’s not. lower_bound thus answers the question, “Is it there?” If so, where is the first copy, and if it’s not, where would it go? As with find, the result of lower_bound must be tested to see if it’s pointing to the value you’re looking for. Unlike find, you can’t just test lower_bound’s return value against the lead iterator. Instead, you must test the object lower_bound identifies to see if that’s the value you want.

Many programmers use lower_bound like this:

```cpp
vector<Widget> iterator = lower_bound(vw.begin(), vw.end(), w);  // make sure points to an object...
if (*iterator == w) {  // make sure the object has the...
    // correct value; this has a bug...
    // found the value; points to the...
    // first object with that value...
} else {  // not found...
}
```
Microsoft’s Windows 2000 demonstrates that keyholes lead to inconsistency:
The Off-By-One ListBox/ComboBox Keyhole

Murphy strikes United Airlines’ and Microsoft’s web sites:
It Doesn’t Have to be This Way
The Horizontal ListBox/ComboBox Keyhole

From Microsoft’s web site for an older version of Windows Media Player:

- “Burn your own au” makes me nervous.
The Fixed Size Window Keyhole

Popular during program installation. From Real Networks and Rose City Software:
The Fixed Size Window Keyhole

Application windows can also be fixed in size. From PC Tools’ Registry Mechanic:

- This window is fixed at 800x600. This allows 5 of 457 problems to be shown.
The Fixed Size Window Keyhole

Web sites like fixed-sized windows, too. From Ameritrade’s web site:
The Fixed Size Window Keyhole

An interesting twist: an unscrollable window from Photo Imaging News’ web site:
CNN’s web site has no trouble offering scroll bars:

- Interestingly, the window size is fixed in Internet Explorer, but not in Firefox.
The Fixed Size Window Keyhole

Microsoft’s Office Update web site has trouble only when...can you guess?
Intuit’s Quicken Premier 2006 offers a curious variation:

![Quicken window](image)

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Transactions</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charles Schwab &amp; Co.</td>
<td>50</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
<tr>
<td>Managed Joint Account</td>
<td>17</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
<tr>
<td>Managed MPPP</td>
<td>198</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
<tr>
<td>Managed SEP</td>
<td>16</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
<tr>
<td>Nancy’s Account</td>
<td>16</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
<tr>
<td>Primary Schwab One</td>
<td>398</td>
<td>8/18/2006 5:00:00 PM</td>
</tr>
</tbody>
</table>
The **Fixed Size Dialog Keyhole**

When long paths collide with narrow dialogs. From ACD Systems’ ACDSee 7:
The Fixed Size Dialog Keyhole

Open source, closed source, it doesn’t matter. From Mozilla’s Firefox:
Microsoft’s Windows 2000 Dial-Up Networking defines irony:

**The Fixed Size Dialog Keyhole**

To enable operator-assisted calls or manual dialing

1. Open **Network and Dial-up Connections**.
2. On the **Advanced** menu, click **Operator-Assisted Dialing**.
3. Double-click the connection you want to dial.
4. Pick up the telephone handset, and then dial the number or ask the operator to dial it for you.

The number assigned to the entry is displayed in the dialog box for easy reference.

5. Immediately after you have finished dialing, click **Dial**.
6. Hang up the handset only when the call is typically signaled with a click.

It is always safe to replace the handset before the call begins verifying your user. The computer will remind you of this.

**Notes**

- To open Network and Dial-up Connections, open Control Panel and double-click on **Network and Dial-up Connections**.

---

Operator Assisted or Manual Dial

Pick up the handset and dial (or ask the operator to dial). Press OK immediately after dialing, then replace the handset.

Phone Number: 008008888000, ....503638602845
The Fixed Size Dialog Keyhole

When many tabs collide with narrow dialogs. From Microsoft’s Visual Studio 6:
Microsoft's Visual Studio .NET replaces one keyhole with another:
The Fixed Width Edit Control Keyhole

From Microsoft’s Internet Explorer 6:
The Fixed Width Edit Control Keyhole

From OneSuite.com’s web site (account setup):

<table>
<thead>
<tr>
<th>STEP 2: Account Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Re-Enter Password</td>
</tr>
<tr>
<td>Secret Question</td>
</tr>
<tr>
<td>Secret Answer</td>
</tr>
<tr>
<td>E-Mail Address</td>
</tr>
</tbody>
</table>

This question and answer are used if you lose your password. The answer to your secret question. Account information is sent to this e-mail address.

From OneSuite.com’s web site (account maintenance):

Secret Question: What is your favorite color?
Answer:
Save  Reset
From SourceForge’s web site:

It's my understanding that text similar or identical to the following is standard in various places at SourceForge:

- Below is a list of all files released by this project. Before downloading, you may want to read Release Notes and ChangeLog (accessible by clicking an release version).
- I visit SourceForge only rarely, and in trying to evaluate my download options for the Boost C++ Libraries, I found this text confusing. I suggest changing the parenthetical phrase to:
  - (accessible by clicking on the release version number)
- In particular, I clicked on "[show only this release]" next to the version number, expecting to see further links to Release Notes and the ChangeLog, but no such links were present.
The Fixed Width Edit Control Keyhole

For web pages, fixing the problem is trivial.

- Add this to each `input` and `textarea` tag: `style="width:100%"`
The **Lying Fixed Width Edit Control Keyhole**

From Marriott’s web site:

```
Check-in Date: April, 2002 17
Check-out Date: April, 2002 18
Number of Guests: 1

Enter your Marriott Rewards number to earn points or miles at participating Marriott Rewards hotels.

Marriott Rewards Number: 777 555 4
```

![Marriott Rewards Card Image]
The Lying Fixed Width Edit Control Keyhole

From Symantec’s Winfax Pro 10:
The Fixed-Width Web Page Keyhole

Examples on the bottom employ children’s “reduced vegetable density” strategy.

Scott Meyers, Software Development Consultant
http://www.aristeia.com/
Inconsistency manifestation I: from Ebay’s web site:
Inconsistency manifestation II: from IBM’s web site:

Performance Testing C++ Code

By Neil Hunt, 1996

A popular maxim in software engineering is: “make it run first, then make it run fast.” The reason is that it is better to make a clean, simple implementation that works, and then add the optimizations later, only after the bugs are eliminated.

Unfortunately, two things often happen. First, the time taken to make it work and get rid of the bugs always expands, compressing any time that might have been scheduled for performance tuning later in the schedule.

Second, the simple, well-organized implementation with which you started out gradually grows more spaghetti-like as the code evolves in response to fixes, changes in the specification or requirements, or new features added. This makes it much harder to do any kind of optimization late in the cycle.

Both of these problems often lead to shipping programs after doing little or no performance optimization.

The result is too often code that behaves sluggishly and is frustrating to use. Is this a bug? The code runs correctly, so it cannot be a bug, right?

If software is slow enough that users label it "unusable," you have the same result as a crashing application: customers cannot get work done.

The good news is that a product’s poor performance might lose more customers than outright crashes or malfunctions! At least a user can report a crash with tangible symptoms, and expect a fixed version of the code. Users can often avoid buggy features and still get use from the rest of the product. On the other hand, if the program runs too slowly, or hogs too much memory or disc, they may well have the perception that any problem report will be ignored.

How many updated versions of software have you ever seen where performance did not degrade at least a little in favor of new features?

View the full document (.pdf, 234 KB)
The Massachusetts Convention Center Authority’s web site is formatted to look good only on a PDA:
The Fixed-Width Web Page Keyhole

Addison-Wesley fixes content width, then adds embedded scroll bars for too-long lines!
Artima is one of many sites that let browsers do what they are designed to do—determine line lengths dynamically:
The Fixed-Height Web Page Keyhole

From Semantic Designs’ web site:

- The keyhole is present under Firefox 1.07, absent under Internet Explorer 6.
Invisible Keyholes
(Non-GUI Components)

Important: Invisible ≠ Undetectable!
The Too Few Bits Keyhole

From Roxio’s web site (but the software is due to Adaptec):

If you have Easy CD Creator 4.00 and have more than 8Gb of free space, please create TEMP directories and fill up space in these until less than 8Gb of free space remains.

8GB is 33 bits...
Naviscope’s Naviscope status report:

Naviscope: Active, 10 Prefetched, -4116 Ads Blocked
A phrase to index using Adobe’s FrameMaker 6:

Prefer iterator to const_iterator, reverse_iterator, and const_reverse_iterator.

I want several different index entries:

iterator: vs. other iterator types
const_iterator: vs. other iterator types
reverse_iterator: vs. other iterator types
const_reverse_iterator: vs. other iterator types
iterators: choosing among types
containers: choosing among iterator types

With markup, here’s the index entry I want to make:

<$startrange><c>iterator<d>: vs. other iterator types;
<c>const_iterator<d>: vs. other iterator types; <c>reverse_iterator<d>: vs.
other iterator types; <c>const_reverse_iterator<d>: vs. other iterator
types; iterators: choosing among types; containers: choosing among iterator types
The Restricted Field Size Keyhole

FrameMaker makes me type it into this lovely keyhole,

![Diagram of FrameMaker interface with a keyhole]

but when I try to add it to the document...

![Error message in FrameMaker: Marker text is too long. Marker text is limited to 255 characters.]

Scott Meyers, Software Development Consultant
http://www.aristeia.com/
Microsoft’s Excel 2002 has a similar limitation:
Adobe’s Acrobat 6 limits the number of open files — without saying what it is. (It’s 20):
The Restricted Field Size Keyhole

From Microsoft’s Visual C++ 6:

Compiler Warning C4786

The debugger cannot debug code with symbols longer than 255 characters.

From Microsoft’s Visual Studio .NET Readme:

Setup fails if any path and file name combination exceeds 260 characters. The maximum length of a path in Visual Studio is 221 characters; accordingly, you should copy files to a path with less than 70 characters.

If you create a network share for a network image, the UNC path to the root install location should contain fewer than 39 characters.

Annotations in Adobe Acrobat 6 are limited to 5000 characters.

Nostalgia:

- Local phone numbers will never have more than 7 digits.
- Two digits will always suffice to identify the year.
The **Restricted Domain Keyhole**

Unbelievably common for user IDs and passwords, often in conjunction with field size keyholes. From **Ameritrade**:

Your PIN...

1. Must be a 4-digit number
2. Cannot begin with a zero
3. Cannot include letters or symbols
The Restricted Domain Keyhole

Linksys’s WRT54G router software combines a keyhole with linguistic incompetence:

- But my existing Linksys router *has* a space in the password!
The Restricted Domain Keyhole

Rifco’s DC SmartFTP’s keyhole actually keeps the program from working!

- Most sites I FTP to have passwords with spaces in them!
The Restricted Domain Keyhole

From 1800flowers.com’s web site:

Enter a Card Message

There is a 150 character limit for your message due to the size of the card. **Note:** please do not use any special symbols like "&".

At a loss for words? We can help you express your sentiments. [Click here to view](http://www.aristeia.com/).
Keyholes by Induction

If 1 is good, n must be better.
Keyholes Everywhere

Here’s my environment (PATH is highlighted):

```bash
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CommonProgramFiles=C:\Program Files\Common Files
COM_MSC_INCLUDE=D:\Apps\Programming\Visual Studio\VC98\Include
COMPUTERNAME=ATLANTA
Common\%SystemRoot%\system32\cmd.exe
CWFD\der=d:\apps\programming\MW6\MW
HOME=D:\HOMEPATH\INCLUDE=:\Apps\Programming\Visual Studio\Framework\SDK\include;D:\Apps\Programming\Visual Studio\VC98\at\include;D:\Apps\Programming\Visual Studio\VC98\mfc\include;D:\Apps\Programming\Visual Studio\VC98\include;D:\C++\boost\boost_1_27_0\LIB=:\Apps\Programming\Visual Studio\Framework\SDK\Lib;D:\Apps\Programming\Visual Studio\VC98\mfc\lib;D:\Apps\Programming\Visual Studio\VC98\lib
LM_LICENSE_FILE=d:\apps\programming\MW6\license.etc
LOGONSERVER=\ATLANTA
MSDevDir=D:\apps\programming\Visual Studio\Common\MSDev98
MSC_INCLUDE=d:\apps\programming\MW6\MSL\MSL_C++\MSL_Common\Include;d:\apps\programming\MW6\MSL\MSL_Common\Inc
CLUDE;d:\apps\programming\MW6\MSL\MSL_Common\Win32\Include;d:\apps\programming\MW6\Win32\x86\Support\Headers\Win32\SDK;d:\apps\programming\MW6\MSL\MSL_Common\X86\d:\C++\boost\boost_1_27_0
MW_APP=:\apps\programming\MW6\GAME;\id=d:\apps\programming\MW6\Win32\x86\Support\Libraries
MSL\LIBRARY_FILES=\ED232.lib;\user32.lib;\kernel32.lib;\ansic86.lib;\ansicpp.lib;\MFCRT.lib
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
OS21LibPath=C:\WINNT\system32\os2\dll:
Path=d:\network\perl\bin;C:\WINNT\system32;C:\\WINNT;C:\WINNT\System32\wbem;C:\PROGRAM FILES\THINKPAD\UTILITIES;D:\Networ
ge\Borland 5.5\Bin;C:\Program Files\Microsoft SQL Server\80\Tools\Binn;d:\apps\programming\MW6\Bin;\d:\apps\programming\MW6\Other Metroworks Tools\Command Line Tools;D:\Apps\Programming\Visual Studio\Common\Tools\WinNT;D:\Apps\Programming\Visual Studio\Common\Tools\WinNT;D:\Apps\Programming\Visual Studio\VC98\Bin;D:\Apps\Programming\CommaC++\Bin;\\\Netware\g++\Bin;D:\Netware\Emacs\GnuServe\D:\Netware\Emacs\emacs-20.7\bin;D:\bin
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 8 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=080a
ProgramFiles=C:\Program Files
PROMPT=$PS
SystemDrive=C:\
SystemRoot=C:\WINNT
TEMP=C:\WINNT\TEMP
TMP=C:\WINNT\TEMP
USERDOMAIN=ATLANTA
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
VSCOMMTOLS=D:\Apps\Programming\Visual Studio\Common\Tools"
windir=C:\WINNT
```
Keyholes Everywhere

Here is Microsoft’s Windows 2000’s interface for editing it:
Keyholes Everywhere

From Crucial Technology's web site:

[Image of Crucial Technology's web page with information about motherboard specifications and shipping rates.]
Beyond Inconvenience

What happens when the log exceeds 65.535" in width?

“It was a very serious bug. It really could have killed someone.”
Beyond Inconvenience

Fixed-size buffers + programmer incompetence or oversight = Hackers’ Delight.

- Code Red and Code Red II worms

A quick Google search yields reported buffer overrun vulnerabilities all over the place:

- gzip under Linux
- xdat under AIX
- count.cgi everywhere
- MIT’s Kerberos
- SGI df, pset, and eject under IRIX
- HP’s Openview Network Node Manager Alarm Service
- Microsoft Clip Art Gallery
- Microsoft Index Server 2.0 under Windows NT.
- rpc.espd daemon under IRIX
- xterm under OpenBSD
- statd under Unix
- talkd under HPUX
- NTP under NetBSD
- AOL Instant Messenger under Windows
- Microsoft Windows Media player
- Microsoft HyperTerminal
- Microsoft SQL Server
- Microsoft Internet Explorer under MacOS
- Microsoft IIS
- TalentSoft’s Web+
- CDE’s dtspcd daemon under Unix
- login under System-V-derived Unix
- Microsoft’s C Runtime Library
- Apple’s sudo under MacOS
Beyond Inconvenience

San Francisco, November 5, 2004:

Unexpectedly high voter turnout caused vote-counting software to crash.

- Cause: the amount of data exceeded a pre-set limit.
- The vendor later determined that the limit was not necessary.
Beyond Inconvenience

The stakes can be high...

- March 1979: TMI-2 comes within 30 minutes of total meltdown
- Contributing factor: A steam temperature readout is programmed never to display values over 280°F
Topics Revisited

What are “keyholes?”

- Primarily *gratuitous* restrictions on what a user can see or express.
  - Not all restrictions are gratuitous.
  - Length restrictions on usernames are typically justifiable, on passwords typically not.

- Often:
  - **Use of a constant where a variable would be better.**
  - **Imposition of a constraint where none is warranted.**

- Missing features are typically *not* due to keyholes:
  - Keyholes generally keep you from seeing everything at once.
  - Missing features are not visible at all.

- Not all usability problems are due to keyholes.

- Not all keyholes lead to what are usually considered “usability issues.”
Topics Revisited

Why are keyholes important?

- They typically degrade a system’s usability.
  - Users can’t see what they want to see.
  - Users can’t express what they want to express.
  - Users must cope with inconsistent behavior.
  - Such users are often frustrated, unhappy, and “unloyal” to a product or system.

- They often make systems brittle in the face of change:
  - Constants that are “obviously appropriate” become inappropriate (e.g., PDA meets SXGA)
  - Limits that are “obviously big enough” become too small (e.g., Warning C4786)

- They can lead to serious security and safety vulnerabilities.
Topics Revisited

How can we eliminate or avoid keyholes?

- **Give them “a seat at the table”**
  - Along with functionality, schedule, performance, etc.

- During design and development, avoid imposing gratuitous restrictions.
  - Determine things dynamically instead of statically.
  - If constraints must be imposed, make them as lax as possible.
  - Reject components that impose keyholes.

- During web site design and implementation:
  - Follow the advice above.
  - When in doubt, copy Amazon.
  - When not in doubt, check Amazon anyway.

- Before putting something somewhere, make sure it will fit!
But, But...

But programming with keyholes is faster and easier than programming without them:

- **Often false for GUIs.** Standard components/techniques offer better behavior:
  - Fixed-width web pages are easily eliminated (cf. Amazon)
  - Ditto fixed-size windows (cf. most Windows apps)
  - Ditto windows with a maximum size.
  - Ditto fixed-width edit controls (cf. Windows search)
  - Ditto lying fixed-width edit controls.

- **Also often false for invisible keyholes:**
  - Use of unsigned or 64-bit ints typically trivial.
  - Use of variable-sized fields typically trivial.
  - Use of unrestricted value domains typically *easier* (when it makes sense).

- **Even when true, a lousy argument:**
  - Write non-keyhole components once, then use them all over.
  - You have to write some infrastructure anyway.

But everybody uses keyholes:

- **Listen to your mother:**
  - “If everybody jumped off a cliff, would you jump, too?”
More on Keyholes

  - Draft chapters of the book I’m supposed to be working on.
  - Information on a mailing list on keyholes.
Please Note

Scott Meyers offers consulting services in all aspects of the design and implementation of software systems. For details, visit his web site:

http://www.aristeia.com/

Scott also offers a mailing list to keep you up to date on his professional publications and activities. Read about the mailing list at:

http://www.aristeia.com/MailingList/