U. S. Department of
Health and Human Services

Center for Devices and
Radiological Health

The FDA Forensics Lab, New Tools and Capabilities

Symposium on Static Code Analysis and Complex Medical Devices

University of Minnesota

July 23, 2009

Static Analysis

Center for Devices and
Radiological Health

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- Safety-critical systems
- Pre-market approval or clearance
- Post-market
  - Recalls

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- Performing a post-market investigation, however, is not an easy task.
- This is particularly true in the case of software, where the execution is often user-driven and system-specific.
- To further complicate matters, device software is usually event-driven, resulting in failures that are often unpredictable and may not be easily reproducible.
- In such cases, the only way to trace the software flaws has historically been to manually review the source code itself.

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- Given the complexity of modern medical-device software, this is a very difficult and time-consuming task for a third-party investigator with no prior knowledge of the software.

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- We use static analysis for the postmarket review of commercial medical devices
- The aim of our analysis is:
  - to determine all possible potential causes for failure in the software that can be identified with the SA tools, and
  - to assess compliance to established software and quality control standards

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- Assay
- Definition:
  - Examination and determination as to characteristics (as weight, measure, or quality)
  - analysis (as of an ore or drug) to determine the presence, absence, or quantity of one or more components ; *also* **:** a test used in this analysis software
- Filthy, putrid

FDA Use of Static Analysis Tools

Center for Devices and Radiological Health

- Multiple SA tools
  - CodeSonar (Grammatech)
  - PolySpace (Mathworks)
  - Coverity
  - LDRA
  - Soon
    - Klocwork
    - Parasoft
- Languages
  - C/C++, C#, Java

Steps

Center for Devices and Radiological Health

- Obtain source code, include files, make files, etc. Description of the development environment.
- A mock environment is created based on the documentation accompanying the source code. The result of this is a makefile that could be used to emulate the original compilation environment.
  - Embedded systems / I/O

Steps

Center for Devices and Radiological Health

- In addition, several configuration parameters are changed from the default in order to improve the precision of the analysis. This includes:
  - Increasing the number of paths being searched in each procedure
  - Maximizing the path finding effort
  - Setting the lower bound for the null pointer threshold to 1 to indicate that all address values (except NULL) could be dereferenced safely.

Steps

Center for Devices and Radiological Health

- Engineering Bill of Materials
- Script developed to recurse the source code and pull the dependencies out from the source code.

Effort

Center for Devices and Radiological Health

- In one case there were 736 warnings of which 127 were found to be of concern. They either reflected poor quality control or had the potential to cause the device to malfunction.
- These warnings were submitted as part of a report to the compliance group to take further action as necessary.
- Reference: Using Static Analysis to Evaluate Software in Medical Devices http://www.parsintl.com/18521.pdf

Example warnings

Center for Devices and Radiological Health

Warning class	Warnings reported	Actual problems
Buffer overrun	6	
Buffer underrun	9	
Cast alters value	116	29
Ignored return value	14	
Division by zero	1	
Leak	25	
Missing return statement	13	1
Null pointer dereference	62	28
Redundant condition	139	4
Shift amount exceeds bit width	2	
Type overrun	3	
Type underrun	2	
Uninitialized variable	169	36
Unreachable code	34	20
Unused value	23	
Useless assignment	118	9

- Warnings reported by CodeSonar (Grammatech)

Effort

Center for Devices and Radiological Health

- The total effort expended during the post-market analysis was 210 person hours.
- A majority of the effort was expended in configuring the build for the application and manual analysis of the results.
- While 210 person-hours is still a significant amount in terms of the effort required for the analysis, it is considerably less than what would have been required for a purely manual analysis.
- Also, the static analysis method provides for a much more reliable means for tracing errors in the software as opposed to the manual process.

Effort

Center for Devices and Radiological Health

- Big Bang Approach!
- Not recommended – easier if implemented early and used as part of the development effort.

Valuable Tool

Center for Devices and Radiological Health

- Static analysis is a valuable tool for postmarket investigation. By reasoning about potential run-time errors in the software, static analysis provides an independent, standardized, and repeatable inspection of a medical device's software, as part of a broader scientific analysis of the device.

Valuable Tool

Center for Devices and Radiological Health

- Further, providing the precise location of the failure and a corresponding execution trace enables the investigator to trace the root cause of failure to its origin in the source code.
- This ability not only helps reduce time and effort involved in post-market investigation, but also leads to a more accurate means for post-market analysis, as opposed to manual inspection.
- Most importantly, the use of static analysis allows the post-market investigator to evaluate the product, in this case the software, and not just the processes involved in developing it.

Device Manufacturers

Center for Devices and Radiological Health

- Much as static analysis helps the FDA, it can be leveraged to even greater effect by medical-device manufacturers in the premarket.

- Hazard Analysis
- Reviewers potential additional information questions

Device Manufacturers

Center for Devices and Radiological Health

- The manufacturers can use static analysis to help find flaws early in the development cycle.
- Static analysis lends itself readily to verification and validation activities and can easily be incorporated as part of the manufacturers' software-development processes.
- Doing so facilitates a deeper assessment of the code before releasing it to market and helps establish conformance to good programming practices.

NIST

Center for Devices and Radiological Health

- SAMATE - Software Assurance Metrics And Tool Evaluation
- http://samate.nist.gov/index.php/Main_Page.html
- The objective of part 3, Technology (Tools and Requirements) is the identification, enhancement and development of software assurance tools. NIST is leading in (A) testing software evaluation tools, (B) measuring the effectiveness of tools, and (C) identifying gaps in tools and methods.

Future SA Tools

Center for Devices and Radiological Health

- Model Checking x86 Executables with CodeSurfer/x86 and WPDS++
- G. Balakrishnan[1], T. Reps[1,2], N. Kidd[1], A. Lal[1], J. Lim[1], D. Melski[2], R. Gruian[2], S. Yong[2], C.-H. Chen[2],and T. Teitelbaum[2,3]
  - [1]University of Wisconsin
  - [2]GrammaTech, Inc.
  - [3]Cornell University

Future SA Tools

Center for Devices and Radiological Health

- Relies on the executable binary
- Why the executable?
  - Reveals platform-specific choices made by compiler
    - What you see is what you get
  - Some source-level issues go away
  - Better platform for finding security vulnerabilities
    - Source-code tools: Lack of fidelity can allow vulnerabilities to escape detection
  - Compiler validation especially for optimizing compilers

Future SA Tools

Center for Devices and
Radiological Health

- Service-oriented Architecture
  - Parasoft
  - Check if interfaces coherent