Defect Analysis

CPRE 556: Lecture 4
Summary: Types of Defects

• Last time we listed the following types of defects:
  – Memory leaks
  – Dangling pointers
  – Uninitialized pointers
  – Segmentation faults
  – Floating point problems such as division by zero
  – Segmentation fault (e.g. an array index goes beyond the array bound)
  – Deadlocks
  – Race conditions
Our Goal

• Defect analysis strategies that will work with large software.
• We want to get insights into the thinking process behind designing such strategies – ability to design new strategies to address new defect scenarios.
• Qualifying the strategies – how scalable, sound and complete are the strategies?
• Experience of applying the strategies to real-world software.
Starting with an example

• I have selected a routine called dswrite from the Xinu operating system. The routine has a getbuf() call that allocates memory.

• We want to know if there is a memory leak in this case, i.e., is the allocated memory released later.

• Our discussion will be:
  – What code should we examine? Why?
Homework

• The first homework is posted on the web.
• Type the answer and send the answer to me by next Thursday (1/26), 2 pm.
• Mail a PDF or MS Word document to: kothari@iastate.edu