Reading 1: PREfix and Metal

17-654/17-754: Analysis of Software Artifacts
Jonathan Aldrich (jonathan.aldrich@cs.cmu.edu)

Due: Thursday, February 16, 2006 (5:00 pm)

20 points

Turn in a file named <username>-17654-R1.{txt,doc,pdf}, where username is your Andrew id. At the top of the document, state your name and Andrew id.

Readings:

- William Bush, Jonathan Pincus, and David Sielaff. A Static Analyzer for Finding Dynamic Programming Errors. Software–Practice and Experience 30(7):775-802, June 2000.
- Dawson Engler, Benjamin Chelf, Andy Chou, and Seth Hallem. Checking System Rules using System-Specific, Programmer-Written Compiler Extensions. Proceedings Operating System Design and Implementation, 2000.

Note: When answering these reading assignment questions be concise. It is expected that each question set can be answered adequately in a page of text or less. Rambling answers with irrelevant detail will not be received warmly. On the other hand, answers should contain enough detail to understand clearly what you are saying. Good English grammar and syntax is important, as always.

Reading Objectives:

- To understand two industrially important approaches to static analysis, along with their relative merits: PREfix, which finds memory errors on large programs through interprocedural, path-sensitive analysis, and Metal, which identifies system specific errors through intraprocedural analysis.

Questions:

- Thus far in class, we have not discussed how to analyze function calls. One obvious technique is to simply inline the function (i.e. copy the body of the function to the call site) and analyze the resulting code as if it were in the caller function. PREfix does *not* use this technique. Briefly summarize what PREfix does do to analyze function calls, and name at least one advantage this might have over the naive technique described above.

- Like many static analyses, Metal can yield both false positives (warning messages that do not represent real errors) and false negatives (real errors that the tool does not warn about). Explain at least one reason why an analysis written in Metal might yield a false positive, and one reason why it might yield a false negative.