What are you trying to do?

- Develop a unique single security mechanism that can defend against memory corruption exploits
- Provide mechanisms for remediation, including diagnostics, recovery and repair.
- Make generalized defense practical by keeping run-time performance penalties small and making protections easily portable and scalable.

Milestones/Schedule

- Demonstrate ability to identify critical data and untrusted operations in binaries (Nov 2007)
- Demonstrate coarse-grained defense using output of analysis phase (Jan 2008)
- Demonstrate fine-grained defense (May 2008)
- Adaptive feedback scheme (July 2008)
- Final prototype including remediation and supporting documentation (September 2008)

Progress Since Last Review

- Designed and implemented Prototypes 3-4, extending the coarse-grained memory defense of Prototypes 1-2 to a fine-grained defense
- Developed a dynamic profiler tool to assist other tools
- Implemented adaptive feedback design and several run-time recovery policies
- Significant reduction in run time overhead