Static Analysis

- ITS4, RATS, FlawFinder
  - Treats source code as stream of tokens, and looks for matches in database of known vulnerabilities.
- Splint
  - Programmers add annotations to specify constraints on function calls, and Splint checks them via syntactic analysis based on parse tree.
- MOPS
  - Checks to see if paths in control flow graph end in states corresponding to security violations.

Static Analysis, cont.

- Static analysis can scan a lot of code (relatively) quickly, and help pinpoint trouble spots.
- ITS4, RATS, FlawFinder can only find known vulnerabilities from database.
- Splint, MOPS are only as good as the users' specifications.
- False-positive-prone.
- Static analysis gives little hint as to how to fix detected problems.

Dynamic Analysis

- Generate test cases and subject programs to them.
- ShareFuzz
  - Uses string inputs to try to find buffer overflows, format string vulnerabilities.
- ElectricFence
  - Stops programs on the exact instruction that overruns or underruns a malloc() buffer.
- MemWatch
  - Detects memory abuse such as double-free, use of freed memory, wild pointer writes.

Vulnerability Mitigation

- StackGuard
  - Uses canary value on stack to detect buffer overflow attacks.
- ProPolice
  - Uses StackGuard's canary idea, and also re-orders variables on stack so that buffers cannot over-flow other local variables or pointers.
- FormatGuard
  - Uses C preprocessor macros and runtime wrappers to detect format string attacks.

Vulnerability Mitigation, cont.

- Can provably secure targets and will produce no false positives.
- Known vulnerabilities only.
- Bugs still present in code; may not stop new attacks on same bugs.
- Most tools terminate execution upon detection of attack; this may lead to easy DoS attacks on services.
- Requires re-compilation of code.

Secure Language

- CCured
  - Inserts run-time checks into C source so that compiled program will halt before violating memory safety.
- Cyclone
  - Inserts run-time checks and annotations into C source to memory violations, dangling pointers, format string attacks.
- Spark
  - Annotated subset of Ada.
  - Built to facilitate fantastic static analysis, which can prove many properties on Spark programs.
  - Used in critical applications like avionics and weapon systems.