Vulnerability Detection

- **Static analysis (SAST)**
  Analyze source or binary without running it

- **Fuzzing**
  Automatically input generation to crash/trigger bugs

- **AI** (newest trend)
  Uses LLM to understand code behavior and identify vulnerabilities
  Aardvark (OpenAI) and Big Sleep (Google)

Using formal methods to verify a program

Static analysis - analyzing the code to detect security flaws

- Control flow - analyzing the sequence of instructions
- Data flow - analyzing how the date are accessed
- Data structure - analyzing how data are organized

➡ Abstract interpretation [Cousot]

✓ Verification of critical embedded software in Airbus aircrafts