Specification Based Testing – Part 2

Fuzz Testing

Ira A. Fulton Schools of Engineering
Arizona State University

Objective

Objective

Understand Fuzz Testing

Fuzz Testing

- **Approach to testing where invalid, random or unexpected inputs are automatically generated**
- **Often used by hackers to find vulnerability of the system**
- **Test oracle is not needed**
  - Only monitor for crashes or undesirable behavior
- **Fuzzing tool used to generate inputs**

Two Types of Test Generators

Mutation Based

Generation Based

Mutation Based Fuzzing

- **Generates test inputs by random modifications of valid test data**
- **Doesn't require knowledge of the inputs**
- **Modifications may be totally random or follow some pattern tied to frequent error types such as:**
  - Long or blank strings
  - Maximum or minimum values
  - Special characters
- **Some tools use "bit flipping" - corrupt input by changing random bits in input**

Generation Based Fuzzing

- Generates random test data based on specification of test input format
- Anomalies are added to each possible spot in the inputs
- Knowledge of protocol should give better results than random fuzzing

When to Stop Fuzz Testing?

- Utilize code coverage tools

Summary