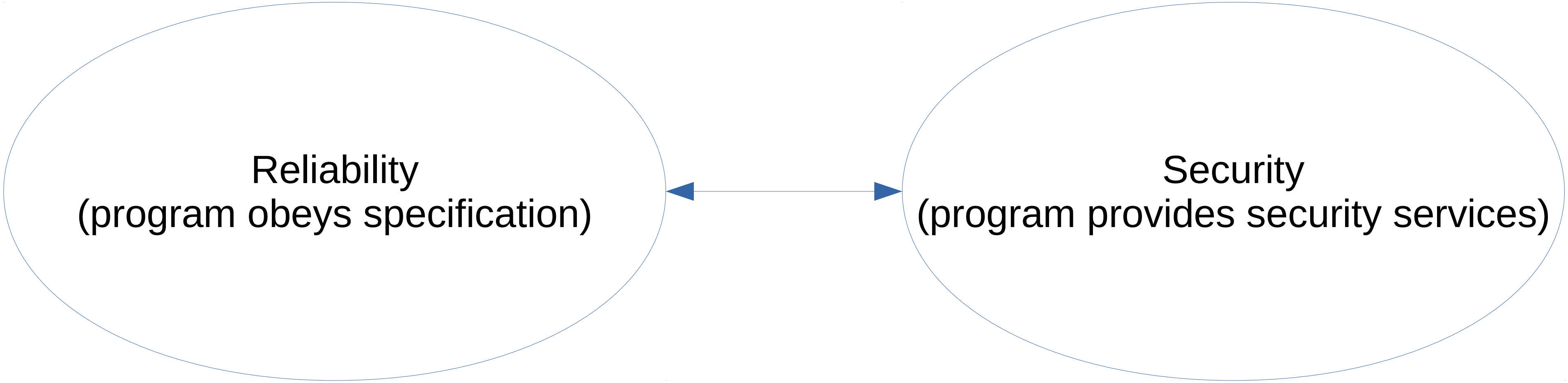
Secure Programming

Peter Chapin

Vermont Technical College

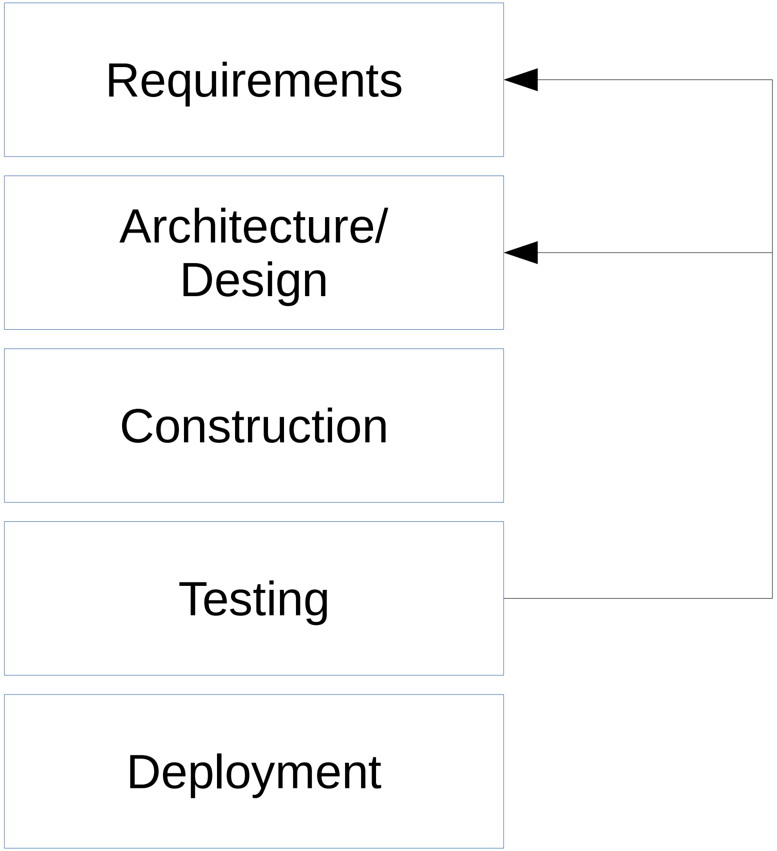
What is Secure Programming?



Reliability
(program obeys specification)

Security
(program provides security services)

Program Development Stack



Requirements

Architecture/ Design

Construction

Testing

Deployment

Validation: Are requirements met?

Verification: Is specification followed?

Reliability

- Reliability…
  - Program does what is specified and what is required (“it works”)
  - Program does not “crash”
    - True crash: e. g., program locks up, has an segment violation, etc… program exhibiting “undefined behavior.”
    - Unhandled exception: Program is still executing in a well defined way… just not what the user (or designer) wants to see.
  - Program does not exhibit unexpected (“odd”) behavior
    - e. g., outputs incorrect results, displays blank screens, misspelled error messages, etc.

Reliability

- A program is *unreliable* if…
  - … it produces undesirable results when used by users operating in good faith.
    - Trying to use the program as intended...
    - Not trying to cause issues...
    - … yet the program still doesn’t work

Security

- In contrast security is about…
  - … program behavior when users are operating in bad faith
  - Users are trying (on purpose) to create incorrect behavior
  - Users are trying (on purpose) to violate security properties (that may or may not be explicitly part of the program's requirements)
  - Users are trying (on purpose) to crash the program or otherwise prevent it from being used in a legitimate way
- "Malicious Intelligence"

Reliability & Security

- Reliability and Security are intertwined
  - Steps to improve reliability will tend to improve security
  - Steps to improve security will tend to improve reliability
  - “Every reliability issue is a potential security vulnerability”
  - “Every security vulnerability is a failure to satisfy implicit requirements and thus a reliability issue”

Security Services

- Services we (might) expect from a “secure” system:
  - Confidentiality: Sensitive data is not exposed improperly (read)
  - Data Integrity: Sensitive data is not modified improperly (write)
  - Authentication: Only legitimate users can use the system
    - “Who are you?”
  - Authorization: Legitimate users obey access restrictions
    - “What can you do?”
  - Availability: The system can be used when desired