Security testing

11 January 2017

What does security testing mean?

= test that system has desired *security objectives*

- confidentiality
- integrity
- authentication
- authorization
- availability
- non-repudiation

Security testing concepts

threat
a potential event with undesired consequences if it materializes into an *attack*

vulnerability: a weakness in the system (design or implementation)

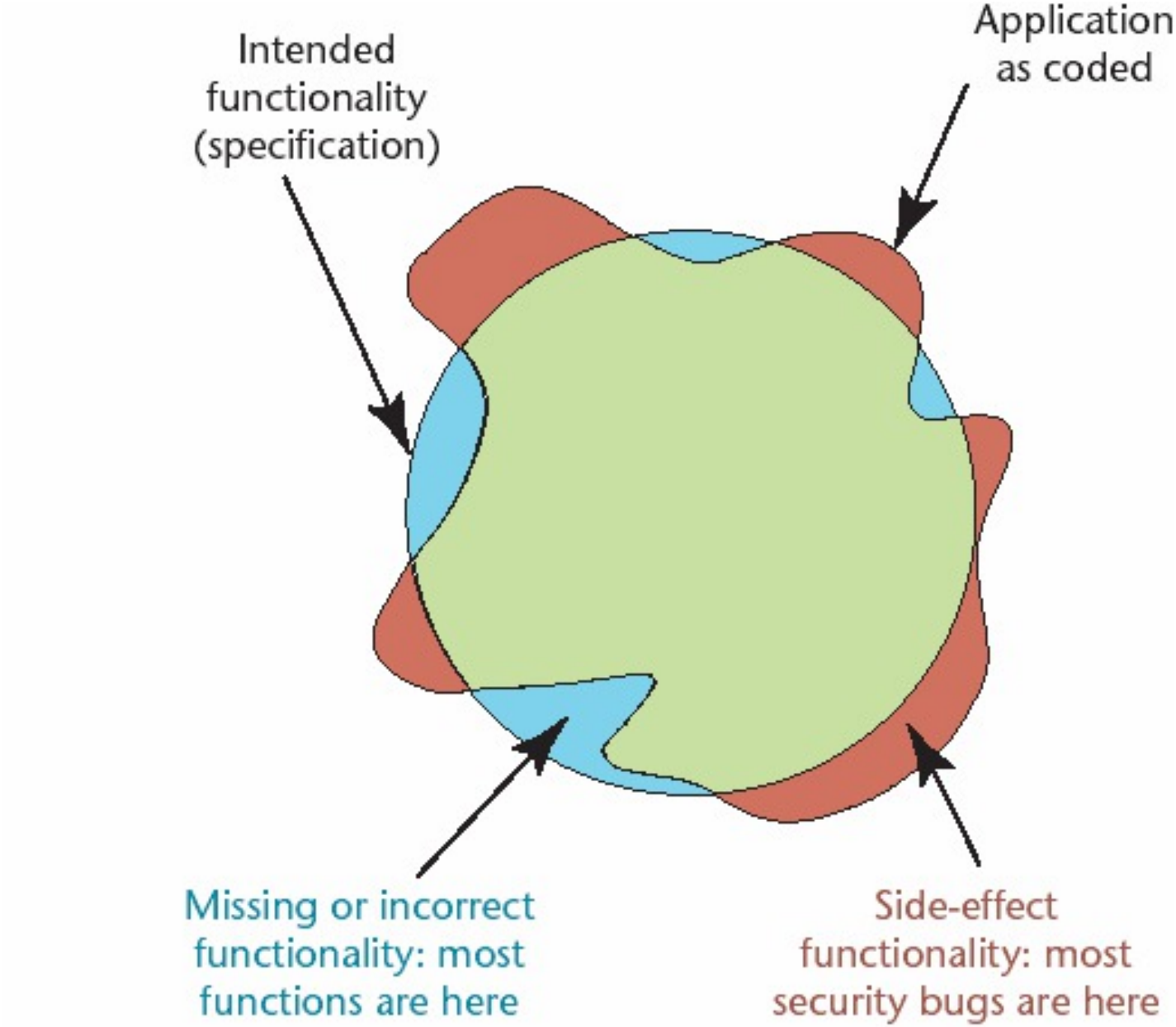
attack: action of an intruder which exploits a vulnerability, threatening an asset as effect

asset: *target* of an attack

Review: What is an error? [Patton, Software Testing]

1. does not do something required by specification
2. does something forbidden by specification
3. does something not mentioned by specification
4. does something not mentioned in specification, but which should be

Where do security vulnerabilities fall in?



H. Thompson, Why Security Testing Is Hard, IEEE S&P, 2003

What is vulnerable ?

Localization of security vulnerabilities (NIST, cf. Agarwal/McAfee)

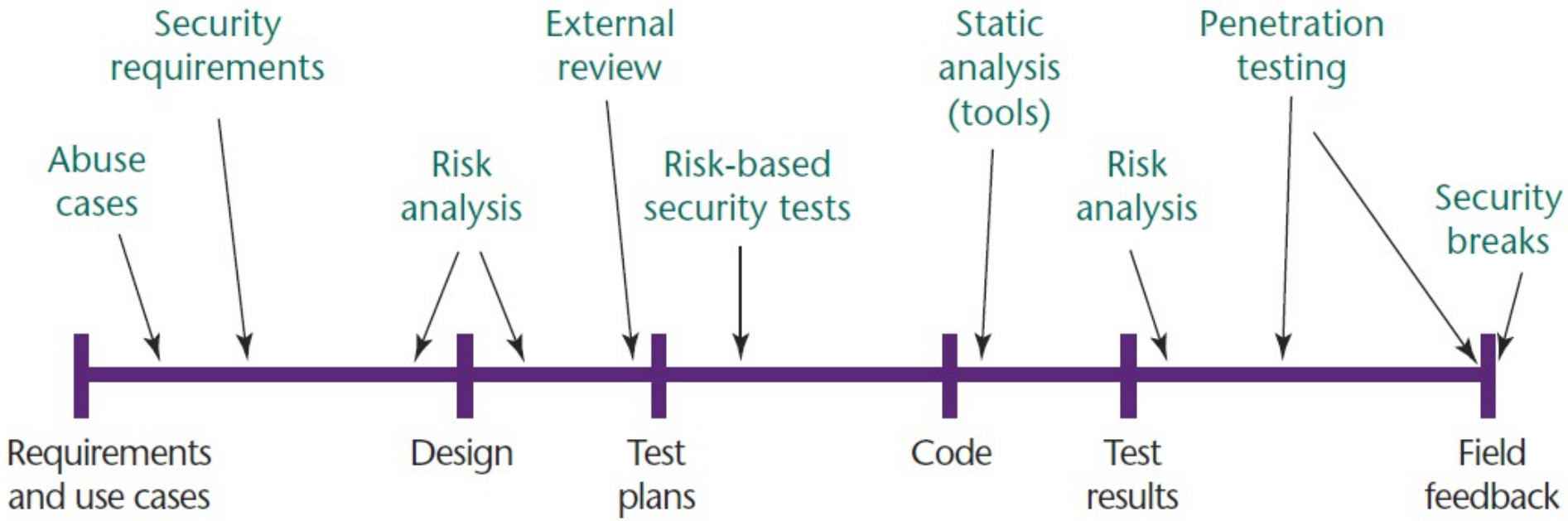
41% application code (server-side)

36% application code (non-server)

15% operating system

92% of vulnerabilities are in application not network

Security in product lifecycle



G. McGraw, Software Security, IEEE S&P, 2004

19 attack (categories) [SecurityInnovation]

http://web.securityinnovation.com/Portals/49125/docs/19AttacksforBreakingApplications.pdf