

Security testing

13 January 2016

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)

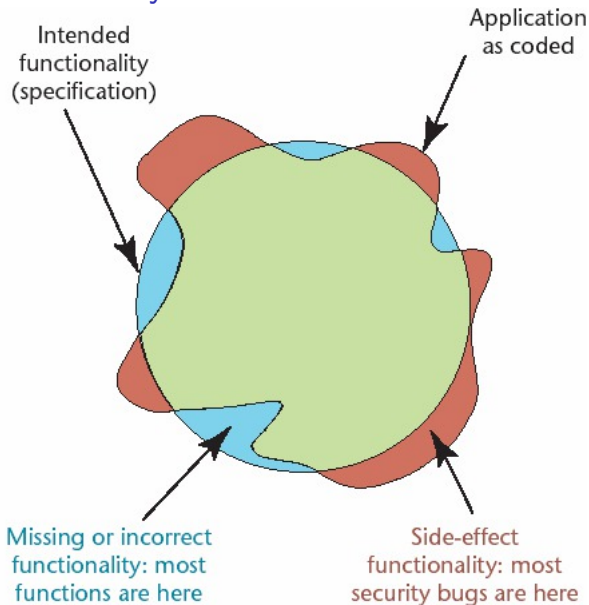
attack: action of an intruder which exploits a vulnerability, threatening an asset as effect

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?



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

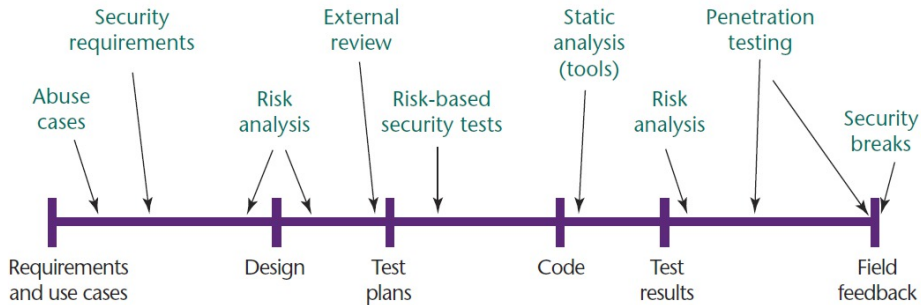
Seven Myths of Software Security

People Security / Coverity

http:

[//www.coverity.com/library/pdf/Coverity_Seven_Deadly_Myths.pdf](http://www.coverity.com/library/pdf/Coverity_Seven_Deadly_Myths.pdf)

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