Testarea securității sistemelor

18 decembrie 2014

Ce înseamnă să testăm securitatea

= să testăm că sistemul satisface deziderateleele de securitate

- confidențialitate
- integritate
- autentificare
- autorizare
- disponibilitate
- non-repudiere

Noțiuni de testare a securității

amenințare (threat)
un eveniment posibil cu consecințe nedorite dacă se transformă în *atac*

vulnerabilitate: o slăbiciune în sistem (eroare de proiectare sau implementare)

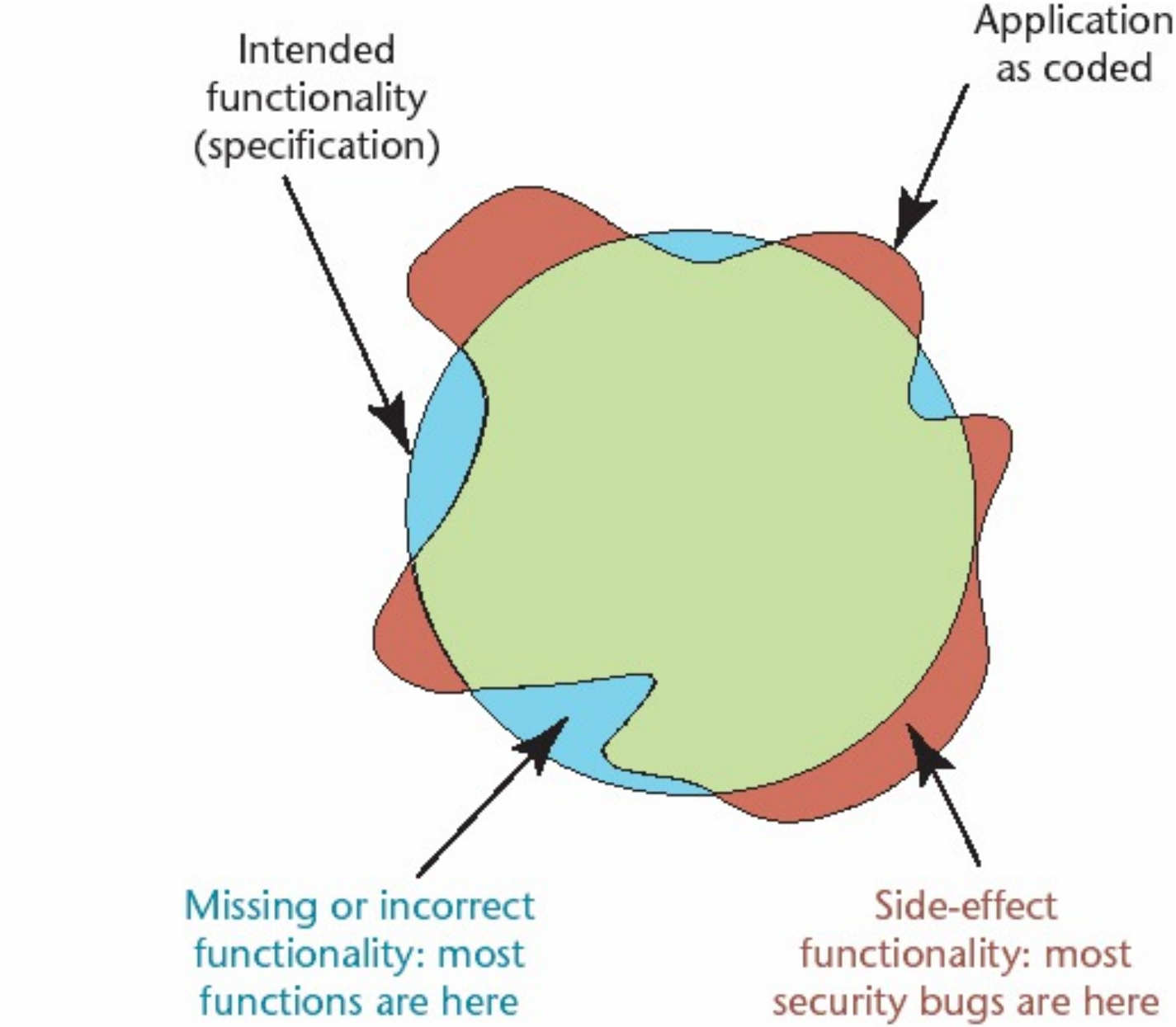
atac: acțiune a unui intrus (atacator) prin care exploatează o vulnerabilitate, cu efect (amenințare) a unei ținte (target, asset)

resursă: *ținta* unui atac

Recap: Ce e o eroare? [Patton, Software Testing]

1. nu face ceva prevăzut în specificație
2. face ceva interzis de specificație
3. face ceva care nu e menționat în specificație
4. nu face ceva care nu e menționat în specificație, dar ar trebui să fie

Unde se încadrează vulnerabilitătile de securitate?



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

Ce e vulnerabil ?

Localizarea vulnerabilităților (NIST, după Agarwal/McAfee)

41% cod aplicație (pe server)

36% cod aplicație (non-server)

15% sistem de operare

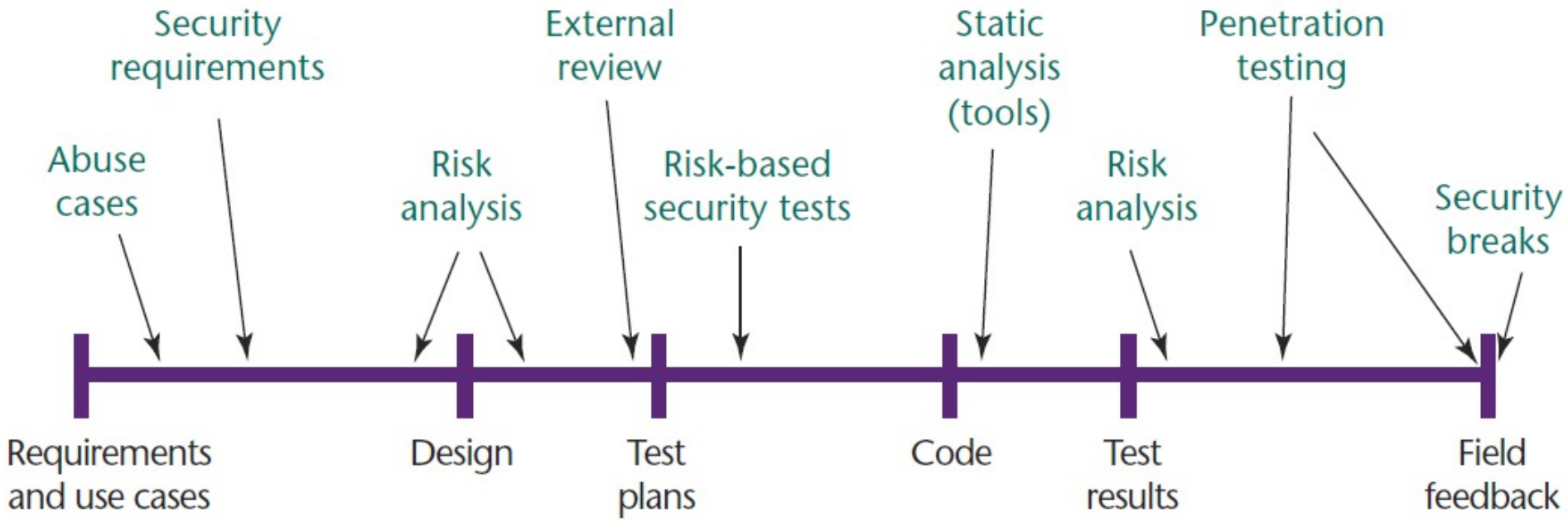
92% din vulnerabilități sunt în aplicație, nu rețele

Șapte mituri despre securitatea software

People Security / Coverity

`http://www.coverity.com/library/pdf/Coverity_Seven_Deadly_Myths.pdf`

Securitatea în ciclul de viață



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

19 (categorii) de atacuri [SecurityInnovation]

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