

Cybersecurity Dynamics in Software Development Environment: What system traps do exist?



1. Increasing hacking efforts

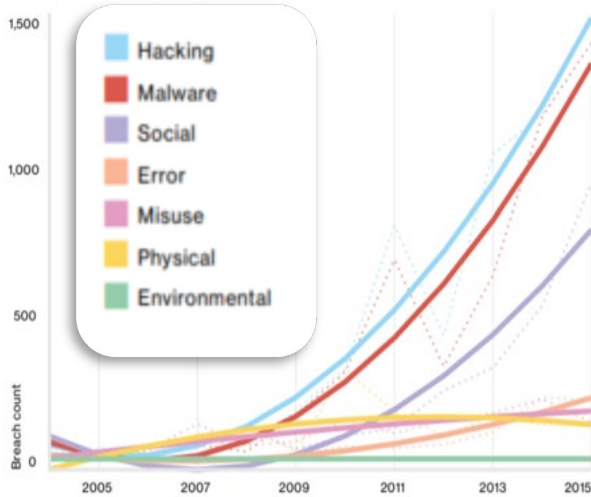


Figure 1. number of breaches per threat action category over time (source: Verizon 2016).

3. As the SDLC eco-system provide us five different system traps

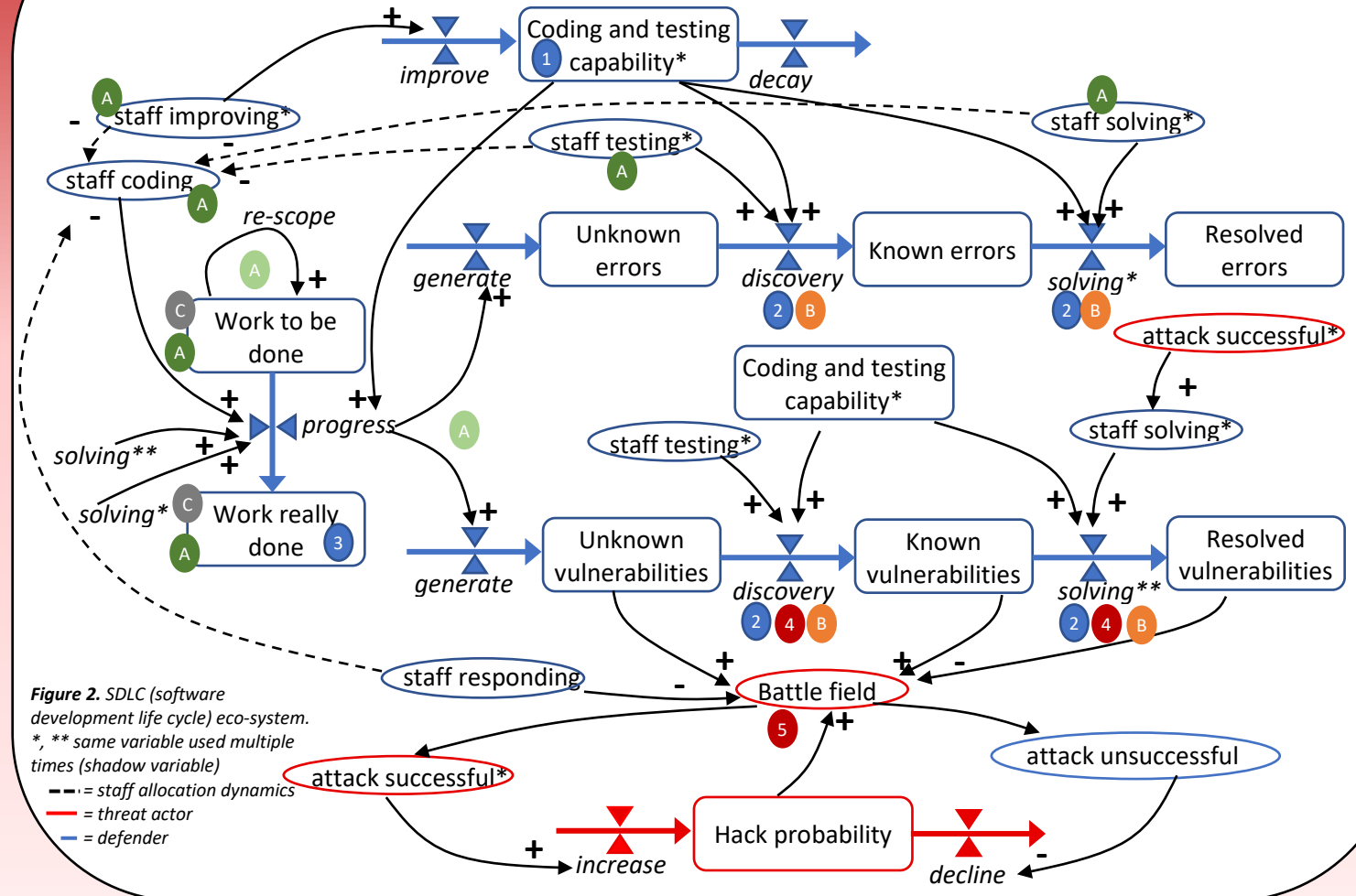


Figure 2. SDLC (software development life cycle) eco-system. *, ** same variable used multiple times (shadow variable)
 - - - = staff allocation dynamics
 - - = threat actor
 - = defender

2. Raise concerns about policies countering this effect

- A Delivery method:** Traditional vs Agile Project Method
- B Software delivery:** Minimal errors vs Fast delivery
- C Delivery priority:** Maximum reliability vs Minimal Viable Product
- **Managerial decision-making dilemma:** available software yield income while working on software generate costs

Trap details:

- 1 Adaptation trap: decay of coding and testing capability impacts future discovery and solving efforts.
- 2 Capability trap: low efforts on discovery and solving evoke future problems.
- 3 Decision trap: no overview on overall software base quality due to short term cycles evoke crappy software generation
- 4 Acceptance trap: mistakenly accept known vulnerabilities (no solving) evoke future successful hacks
- 5 Attacker defender interaction: arms race between attack and defender

Authors

Sander Zeijlemaker RA RE MSc SCF, PhD student Radboud University, IMR Faculty Nijmegen
 Prof. Dr. Michael von Kutzschenbach, University of Applied Sciences and Arts Northwestern Switzerland FHNW, Institute of Management