Getting a Buy-In to a Secure Development Process

andre.marien@inno.com
bart.dewin@cs.kuleuven.be
yo@johanpeeters.com

Development process for secure software and systems

- Goal: to demonstrably improve the security posture of a software system in a systematic and controlled manner
  - Security software vs. software security
  - Typically an add-on to existing processes

- Frontrunners
  - SDL
  - CLASP
  - Touchpoints
Software Security is … thinking white-hat and black-hat

- Two complementary views:
  - Constructive: design, defense and functionality
  - Destructive: attacks, exploits and breaking software
- Both views are valuable and necessary
- Examples:
  - Pen-testing vs. code review
  - Abuse cases

Software Security is … managing risk

- Address important threats
  - Requires prioritization via risk
- Risk management = analysis + mitigation
- Ideally, continuous control over residual risk
- Examples:
  - Threat modeling (e.g., Microsoft’s DREAD)
  - Security response planning (e.g., severity)
  - Attack surface reduction
Software security is …
knowing your security goals

• No security for the sake of security
  – What are the objectives?
• Identify and work towards acceptance criteria
  – Security objectives
  – Security policy
• Examples
  – The “bug bar” in MS SDL

Software security is …
based on engineering maturity

• Need for systematic method
• Symbiosis of construction and verification
  – Quality assurance
  – Possibility of cross-checking
  => Activity specific
• Metrics as a way to control improvement of
  – Product
  – Process
  Examples: attack surface, level of education, …
References


Questions for workgroups

- What are the biggest impediments to delivering secure software in your current way of working? (at most 3)
- What can you as a <role> do to improve this?
- How would you implement this?  
  – Methodology, tools, knowledge
- What do you need as input from the other groups to be successful?
Questions for appraisal

• What do they mean by ...?
• Are any of their measures related to my role? If so, do they sit well with what we (should) do?
• Is there a synergy between their proposals and ours?
• Would it be more optimal to move activities from one role to another?

Concluding

• What will you do differently on Monday as a result of the session?
• What are the impediments to improvement?
• Contact:
  andre.marien@inno.com
  bart.dewin@cs.kuleuven.be
  yo@johanpeeters.com
References


