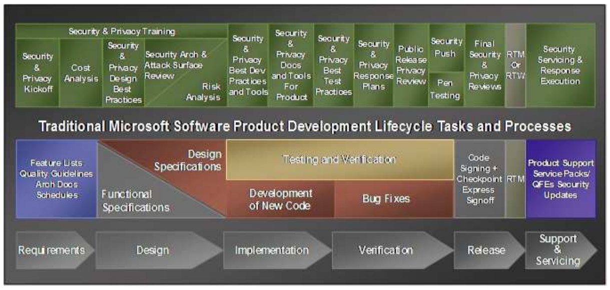
Getting a Buy-In to a Secure Development Process

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


Security & Privacy Training
Security & Privacy Kickoff
Cost Analysis
Security & Privacy Design Best Practices
Security Arch & Attack Surface Review
Risk Analysis
Security & Privacy Best Dev Practices and Tools
Security & Privacy Docs and Tools For Product
Security & Privacy Best Test Practices
Security & Privacy Response Plans
Public Release Privacy Review
Security Push
Pen Testing
Final Security & Privacy Reviews
RTM Or RTW
Security Servicing & Response Execution
Traditional Microsoft Software Product Development Lifecycle Tasks and Processes
Feature Lists Quality Guidelines Arch Docs Schedules
Design Specifications
Functional Specifications
Testing and Verification
Development of New Code
Bug Fixes
Code Signing + Checkpoint Express Signoff
RTM
Product Support Service Packs/ QFEs Security Updates
Requirements
Design
Implementation
Verification
Release
Support & Servicing

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

- M. Howard and S. Lipner. *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Microsoft Press, 2006.
- G. McGraw. *Software Security: Building Security In*. Addison Wesley, 2006.
- OWASP. *Comprehensive, lightweight application security process*. http://www.owasp.org, 2006.
- K. Buyens, J. Gregoire, B. De Win, R. Scandariato, and W. Joosen. *Similarities and differences between CLASP, SDL and Touchpoints: the activity-matrix*. Technical Report 501, Department of Computer Science, K.U.Leuven, 2007.

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

- M. Howard and S. Lipner. *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Microsoft Press, 2006.
- G. McGraw. *Software Security: Building Security In*. Addison Wesley, 2006.
- OWASP. *Comprehensive, lightweight application security process*. http://www.owasp.org, 2006.
- K. Buyens, J. Gregoire, B. De Win, R. Scandariato, and W. Joosen. *Similarities and differences between CLASP, SDL and Touchpoints: the activity-matrix*. Technical Report 501, Department of Computer Science, K.U.Leuven, 2007.