Lessons Learned in Market Adoption of the Common Criteria

Steven B. Lipner
Senior Director
Security Engineering Strategy
Security Technology Unit
Microsoft Corporation
SLipner@microsoft.com

Overview

- Microsoft experience with product evaluation
- Achieving Common Criteria compliance for COTS software
- Customer demand
- At the crossroads
  - Common Criteria version 3
  - Alternative paths to assurance
- Summary

Microsoft Experience with Product Evaluation

- Commitment to evaluation goes back to earliest days of Windows NT
  - NT originally targeted for Orange Book class B2
- Long track record of completed evaluations
  - NT 3.51, NT 4.0, SQL Server 2000 at Orange Book C2
  - NT 4.0 under ITSEC
  - Windows 2000, ISA Server under Common Criteria
- Commitment to evaluation continues
  - Windows XP, Windows Server 2003, ISA Server, many others under Common Criteria
- Microsoft is serious about evaluation, and has committed serious resources

Achieving Common Criteria Compliance for COTS Products

- While Microsoft is serious about evaluation, Microsoft must ship functional software on a timely basis
- Microsoft development process is spiral (not waterfall) and not documentation-heavy
- Achieving Common Criteria compliance involves
  - Ensuring that features are consistent with protection profiles (during design/development)
  - Producing Common Criteria documentation and tests after design/code is stable (late in development/after software ships)
  - Completing evaluation process with aid of consultant who works with evaluation laboratory
- Major parts of Common Criteria are “outside” of development process

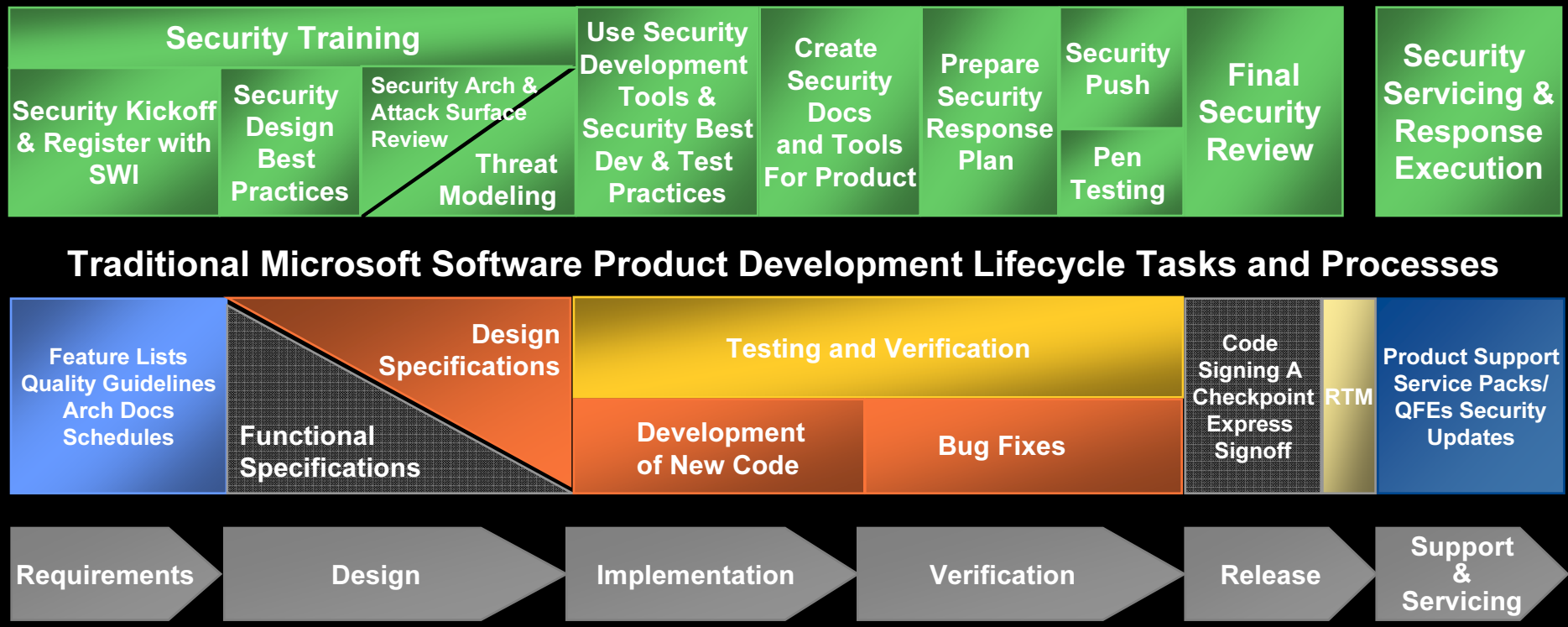
Customer Demand

- Today, essentially all Microsoft customers require (more) secure software
  - Reduced vulnerability rates
  - Fewer successful attacks by worms, viruses, malware, etc.
  - Reduced vulnerability to web site defacements, etc.
  - Improved control over authorized users
- Customers do not express requirement for more secure software in terms of Common Criteria compliance
- Only (some) government agencies require Common Criteria compliance, and they appear to treat it as a procurement requirement unrelated to security and vulnerabilities

Customer Demand (continued)

- In response to customer demand, Microsoft has developed the Security Development Lifecycle (SDL)
  - Discussed at ICCC 2004
  - Focused on adding steps that reduce vulnerability rates during development
    - Engineer training
    - Threat modeling
    - Coding standards, code reviews
    - Use of static analysis tools
    - Fuzz testing
    - Independent “Final Security Reviews”
- SDL has proven effective at reducing vulnerability rates
  - SDL versions of Microsoft software better than pre-SDL versions
  - SDL versions of Microsoft software fare better than competitors – even Common Criteria evaluated competitors

Security Deployment Lifecycle Tasks and Processes



At the Crossroads

- Common Criteria v3
  - Assumed waterfall model inconsistent with COTS development processes
  - Common Criteria v3 document is inconsistent
    - Potential to retrofit compliance up to EAL4
    - Extensive documentation requirements at EAL3 and above
      - Requirements expanded to include non-security relevant information
  - Increased documentation requirements will
    - Raise vendor costs for consultants
    - Increase delays until software evaluated
    - Raise costs most for most functional targets of evaluation
  - No reason to expect improved security in terms that users would value
    - Evaluators as document checkers, not security assessors

At the Crossroads (continued)

- Alternative paths to assurance: update Common Criteria to reflect processes such as the SDL that improve security as users see it
  - Dialog proposed at ICCC 2004
  - Integration of SDL-like processes would result in
    - Reduced vulnerability rates
    - Availability of evaluated versions soon after release
  - A way to keep Common Criteria relevant?
  - We are eager to work with CC community as a whole or with individual CC agencies

Summary

- Common Criteria and evaluations at a crossroads
- Adding documentation (as v3) will increase costs and delays but not security
- Changing requirements to mandate improved security will increase value of evaluations

Microsoft®