

# Common Criteria: Meeting the Needs of a Global Market?

Steve Lipner  
SLipner@microsoft.com  
Senior Director  
Security Engineering Strategy  
Microsoft Corporation



# Some Questions to Ponder

- > How successful is CC in the global market?
- > Why does CC appeal to a global audience?
- > What could CC do better?
- > What should CCDB do?

# Common Criteria and the Global Market

- > Users are trained to ask for CC
  - Even if they don't "require" evaluation at all
  - Even if they don't know what it means for the product they are seeking
- > Vendors worldwide seek CC evaluations
- > Non-CCRA countries pay attention to CC
- > A few commercial customers ask about CC

# Common Criteria and the Global Market

- Mutual recognition is the “jewel in the crown”
  - Evaluation is expensive
  - Vendors and customers benefit from widely accepted evaluations
  - Avoiding national variants is desirable
    - Nation specific PPs or SDs
    - Alternate evaluation schemes
- CC is a mixed picture, but better than predecessors
- But is CCRA starting to fragment?
  - Rumors are discouraging

***We must all hang together, or most assuredly we shall all hang separately – Benjamin Franklin***

# Effectiveness for the Global Market

- > Product size, complexity, and feature-richness determine potential level of security
  - Smart card
  - Minimal “security kernel” or standalone device
  - Modern operating system or DBMS
- > One size of evaluation does not fit all
  - An EAL4 smart card is not “the same” as an EAL4 operating system
  - But many customers (still) do not understand this

# Effectiveness for the Global Market

- > Customers expect secure systems to resist attack
- > What can CC say about resistance to attack?
  - Documentation-centered approach (still) ineffective and inconsistent with commercial development practices for large feature-rich products
- > CCv4 hoped to solve problem of resistance to attack
  - Approach depended on specific evaluator talents
  - Pilots proved infeasible for large (i.e. real) products
- > CCv4 pilots demonstrated importance of developer's process to effective security—

# Effectiveness for the Global Market

- > Focus on CWE weaknesses a promising approach
  - Imperfect
  - Practical
  - Better than review of CC “design documentation”
- > Customers expect secure systems to be evaluated in realistic scenarios
  - No unrealistic configurations
  - Evaluation needs to cover product as deployed
  - Independent evaluation of application and OS at best “a convenient fiction”

# Efficiency for the Global Market

- > The definition of “security relevant” is outdated
  - Many products without security features are relevant
  - Many products open documents and run code...
- > A vendor perspective:
  - We *need* security for *more* products
  - We *need* products that can *resist attack*
  - We *need* to focus on *pragmatic and effective* measures
- > How can evaluation help meet this goal without unacceptable cost?
  - Basic mitigations
  - Appropriate use of underlying platform

# Efficiency for the Global Market

- > Can we evaluate more products at acceptable cost?
- > Evaluate what matters
  - The OS
  - Mitigations
  - Use of OS
  - Presence of features
- > Improve confidence in mutual recognition
  - Apply objective criteria
    - > Replace subtle interpretation with clear “yes-no” decisions

# The Role of Vendors

- Smart card community is the example of successful vendor involvement in Common Criteria
- Some promising recent steps
  - BSI operating system protection profile
  - NIAP firewall protection profile
- More vendor involvement will benefit Common Criteria and customers
  - More realistic functional and assurance requirements
- Scheme commitment and vendor engagement more important than formal structure

# The Way Ahead

- > We *all* need mutual recognition
- > Customers seek assurance of the commercial products they use
- > Focus on what will benefit customers
  - Common protection profiles
  - Basic feature validation
  - Use of operating system services
  - Mitigating common attacks
- Bring vendors and schemes together to identify realistic requirements

# The Way Ahead

- > Approach will require
  - Big change by schemes, labs, and vendors
  - ***Clear communication to users who seek or expect evaluated products***
  - Extra effort from OS vendors – like Microsoft
- > Improved security for customers and meaningful certification process justify the change and investment

*Microsoft*<sup>®</sup>

# ICCC 2010

