The Way Ahead for the Common Criteria-A Discussion Panel ICCC5 Berlin September 29, 2004

Stuart W. Katzke, Ph.D.
Senior Research Scientist
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive; Stop 8930
Gaithersburg, MD 20899
(301) 975-4768
skatzke@nist.gov

Handout at
Dec 2004 ISPAB

Presentation Contents

- My personal opinions on this topic are on record in proceedings of ICCC4 Stockholm—will not be repeated today
- Inform audience of studies/reports/activities on CC and NIAP that are on-going or completed in the U.S.
    - President Bush's *National Strategy to Secure Cyberspace*; Published February 2003
    - The NIAP Review; Task Order Oct. 2003; Started late Feb. 2004 (on-going)
    - *The Technical Standards and Common Criteria Task Force Recommendations Report*; Published April 2004
    - Cyber Security Industry Alliance (CSIA) Report: *NIAP Certification: Proposals by CSIA for strengthening security certification;* Published July 23, 2004.
    - *CC Users' Forum;* to be held October 6 & 7, 2004

Comments

- Bad News: Number of activities indicative of significant concerns with the CC & NIAP processes by many stakeholders
- Good News: My ICCC4 presentation & all studies/reports are intended to improve the CC and NIAP processes to achieve the promise of CC certification. None propose stopping use of CC or terminating/reducing scope of NIAP
- All comments/findings should be taken as "constructive"

National Strategy to Secure Cyberspace

- A/R 4-4: Additionally, the federal government will be conducting a comprehensive review of the National Information Assurance Partnership (NIAP), to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of products reviewed under NIAP or similar evaluation processes. (Feb. 2003)

NIAP Review

- DoD/Department of Homeland Security (DHS) issued task order in Oct. 03
- NIAP review started in late Feb. 04; on-going
- Review Objectives:
  - Characterize and document the past & current efficacy of NIAP and ***future expectations of a NIAP***
  - Identify and articulate the merit of options that improve the effectiveness of NIAP
  - Assess the cost and feasibility of implementing options
  - Recommend option(s) and an implementation road map

Technical Standards and Common Criteria Task Force (1)

- Established under the National Cyber Security Partnership
- National Cyber Security Partnership
  - Coalition of trade associations
    - US Chamber of Commerce
    - Information Technology Association of America (ITAA)
    - TechNet
    - Business Software Alliance
  - Sponsored the National Cyber Security Summit Dec. 2-3, 2003
  - Five Task Forces chartered to respond to *National Strategy to Secure Cyberspace.*
  - Technical Standards and Common Criteria Task Force

Technical Standards and Common Criteria Task Force (2)

- Industry-led coalition of security experts
- Public & private sectors
  - Trade associations
  - Non-profits
- Operates under guidance & coordination of National Cyber Security Partnership
- In CC area, focus on:
  - Developing recommendations to improve CC evaluation process and explore alternative mechanisms
  - To foster:
    - Effective industry usage & compliance
    - Enhanced government guidance & support

Technical Standards and Common Criteria Task Force (3)

- Leadership:
  - Mary Ann Davidson, Oracle
  - Chris Klaus, Internet Security System
  - Edward Roback, NIST
- – Established 5 Working Groups
  - Common Configuration (28 recommendations)
  - Research (3 recommendations)
  - Best Practices for Technical Standards (Compilation of Best Practices)
  - Equipment Deployment & Architecture Guidelines (4 recommendations)
  - CC, NIAP Review & Metrics (35 recommendations)

CC, NIAP Review & Metrics Working Group: Objectives

- Develop recommendations for how to:
  - Define better security metrics for consumers to:
    - Compare products against their requirements
    - Compare security claims among vendors
  - Develop a mechanism to express consensus-based requirements (expressed as PPs) for infrastructure components
  - Provide inputs to the "NIAP Review" to improve current processes based on past experiences

CC, NIAP Review & Metrics Working Group: Focus Areas

- Increase the NIAP scheme effectiveness
- Make government COTS procurement policies realistic
- Reduce the cost of CC evaluations
- Increase the demand for CC evaluated products
- Improve the use and utility of PPs
- Increase product security through CC specifications and evaluation

Cyber Security Industry Alliance (CSIA) Report: *NIAP Certification: Proposals by CSIA for strengthening security certification*

- CSIA formed in Feb. 2004
  - Advocacy Group to enhance cyber security through:
    - Public Policy Initiatives
    - Public sector partnerships
    - Corporate outreach
    - Academic programs
    - Alignment behind emerging industry technology standards and public education
  - Composed of software, hardware, & service vendors
- Report developed with knowledge of the NIAP Review (on going) & the Technical Standards and Common Criteria Task Force (completed?)

Cyber Security Industry Alliance (CSIA) Report: Issues

- NIAP Testing is too expensive & slow
- Government developed PPs need broader input
- NIAP testing process needs more uniformity & consistency
- Procurement policy (DoD) for evaluated products is misunderstood & its application is inconsistent
- Uneven acceptance of evaluated products
  - Government: only mandated by DoD
  - Commercial: hardly ever require
  - Commercial alternatives: BITS

Cyber Security Industry Alliance (CSIA) Report: Recommendations

- Sponsor a CC Users' Forum in conjunction with the National Cyber Security Partnership & other organizations, (Oct. 6 & 7, 2004)
  - Other sponsors are DHS & NIST
  - All stakeholders invited
- Recommendations for the Forum:
  - Discuss & develop practical means to improve the CC processes & standards
  - Provide open forum to discuss & resolve differences between the views of commercial entities and NIAP
  - Develop specific timelines and actions on recommendations from the NIAP Review & the Task Force Report
  - Share CC experiences to educate ourselves and foster widespread, cost-efficient use of NIAP testing

CC Users' Forum (CCUF)
October 6 & 7, 2004

- Steering Committee includes: NIST, NSA, DHS, CSIA, DoD, ISSA, BITS, ITAA, TechNet, Microsoft, Oracle, SAIC, Symantec, Internet Systems Security, Booze Allen Hamilton, BRT, BSA, Computer Associates, Merritt Group, Washington Mutual

CCUF Program (1)

- Oct. 6: Presentation Day
  - Technical Standards and Common Criteria Task Force Overview (Edward Roback/NIST; Task Force co-chair)
  - NSA
  - NIST
  - CC Testing Lab (SAIC)
  - Commercial Customer (Washington Mutual)
  - Vendor (Oracle)
  - Security product vendor (ISS)
  - NIAP Review Status (IDA)

CCUF Program (2)

- Oct. 7: Working Group Day
  - Panel: Broadening CC Application vs. Addressing CC Issues
  - Parallel Working Groups
    - Incentives for security & CC evaluations
    - Reducing the time & cost associated with CC evaluations
    - Security metrics relative to the CC
    - Setting requirements for commercial users
  - Open Discussion

URLs (May not be totally correct)

- *National Strategy to Secure Cyberspace*:

  http://www.whitehouse.gov/pcipb
- *Technical Standards & Common Criteria Task Force Report*, including the *CC, NIAP Review & Metrics Working Group Appendix E:*

  http://www.cyberpartnership.org/init-tech.html
- *NIAP Certification: Proposals by CSIA for strengthening security certification*

  http://www.csialliance.org/pdfs/CSIA_NIAP_Recommendations.pdf
- CCUF

  http://csrc.nist.gov (see current events on right side)