The Common Criteria (CC) Years (1993-2008): Looking Back and Ahead

Stuart Katzke, Ph.D.
Senior Research Scientist
National Institute for Standards and Technology

Preliminary Remarks

- Opinions are mine, not NIST's or NIAP's
- CC Paradigm
  - Use of CC for expression of requirements
  - Use of CC & CEM for evaluation
- I have devoted significant portion of my career to promotion of the CC paradigm
- Believe in CC paradigm; want to see it succeed
- Constructive suggestions for continued success
- Remarks do not take into consideration CC-related activities since last ICCC
- Some minor changes made to original slides—contact me for update

Briefing Contents

- Introduction: Where we are today
- Stakeholder perspectives
- Long-Term survival of the CC: Obstacles, Barriers, & Trouble Indicators
- Recommendations/Conclusions
- Questions to ponder

Introduction: Where we are today

- CC Project initiated June 1993
- CC published May 1998
- CC Recognition Arrangement (CCRA) signed October 1998
  - 17 current members of CCRA
  - Japan & others in progress
  - 6 CC schemes
  - Over 30 CLEFS
  - Hundreds of certificates issued
  - Many other countries interested in joining
- ISO/IEC SC 27
  - WG 3 established to focus on CC-related work items
  - ISO/IEC Standard 15408 December 1999

Introduction (cont.)

- National & International Policy/Regulation
  - United States (US):
    - National Security Policy 11 & related policy/guidance
    - On-going consideration of extending to rest of government
    - Government recommended technology area protection profiles (PPs)
  - France: Regulation recommending the use of CC evaluations for public administration
  - European Union:
    - Resolution on information and network security
    - Electronic signature
    - European central bank.
  - NATO: CC is the standard
  - Germany: CC evaluations required in digital signature legislation

Introduction (cont.)

- User communities are using the CC to develop PPs & functional packages
  - US Government
  - Smartcard community
  - Financial Services Roundtable/BITS
  - Healthcare community
  - Process control community
  - IEEE/NIST
- New uses of the CC: research & application
  - Composite evaluations
  - Composite PPs
  - System evaluations
  - Technology-specific applications of the CC
- ICCC 1-4

One Might Conclude:

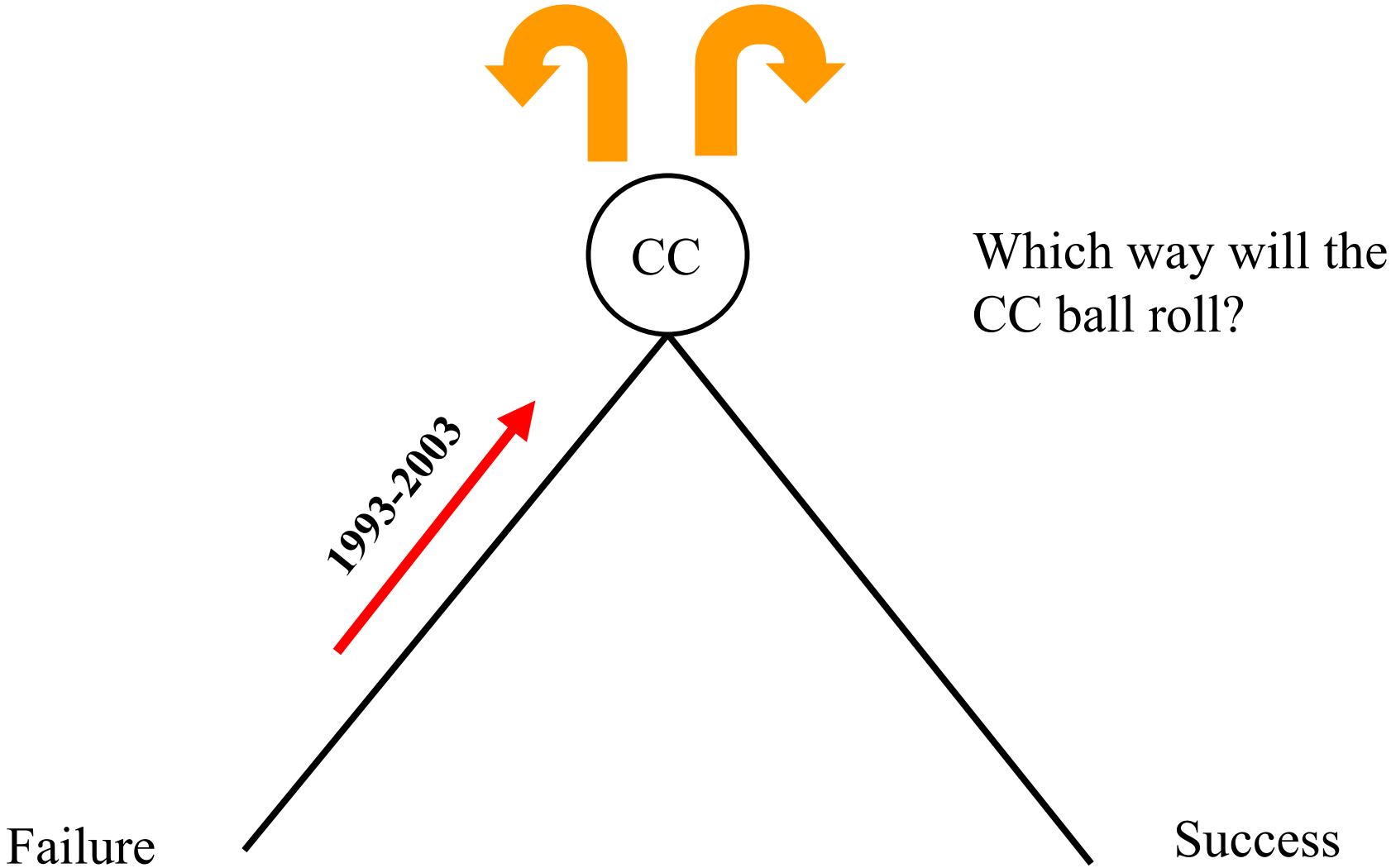
CC paradigm

Use of CC for expression of requirements
Use of CC & CEM for evaluation purposes

appears to be successful!

But

- What about long term survival?
- What obstacles/barriers remain?
- What are the trouble indicators?
- What must be done about these?



Which way will the CC ball roll?

Stakeholder Perspectives

- CCRA government members
- Vendors
- Informed/concerned users & user communities
  - Emphasis on “Informed/concerned” because:
    - Some/many users do not care about evaluations (This should be a big “Red Flag”)
    - Others only want a “mark” of approval but do not care about what “mark” really represents/means (Another big “Red Flag”)
    - Not addressing uninformed/unconcerned users in this presentation

Perspective of CCRA Government Members

- Desire a rich variety of evaluated products for use in government systems
  - Multiple technology areas
  - Variety of assurance levels
- Why? Belief that:
  - Evaluated products provide better protection than unevaluated products
  - Evaluated products improve/contribute to overall system security when integrated into systems

Perspective of CCRA Government Members (cont.)

- In context of CCRA, recognize need for comparability of evaluations, both intra-scheme & inter-scheme
- Recognize that variations/differences exist in national Certification Bodies (CBs) evaluation processes that complicate comparability
  - Common Evaluation Methodology (CEM) at high level of abstraction
  - CEM allows considerable evaluation latitude/interpretation
  - Lack of common evaluator/validator competency requirements
- Current methods for assuring comparability of evaluations include:
  - Voluntary Periodic Assessments
    - Initially, unverified trust
  - Shadowing of new members
  - CCIMB international agreements on new material & Ris
  - Scheme technical meetings
  - Supporting Documents

Perspective of Vendors

- Evaluations are expensive and take too long
- Can not afford to meet evaluation requirements

for:

  - Multiple CBs
  - Multiple customers

- For better/acceptable return on investment (ROI)
  - Need to amortize evaluation costs over a large market
  - Want one evaluation accepted everywhere

Perspective of Vendors (cont.)

- CCRA partially resolves these concerns
  - One evaluation accepted by all CCRA government member nations
  - Commercial customers may require more stringent/different:
    - Test methods
    - Demonstration of lab competence
  - Vendor's product may still be subjected to multiple different testing requirements if all customers do not accept a CC evaluation
    - Vendor pays for each customer-unique testing
    - Customer pays for tests it requires

Perspective of Vendors (cont)

- Mutual recognition of evaluations by CCRA government members does not guarantee use by those governments. Use is a:
  - Requirements issue
  - National security issue

Perspective of Informed/Concerned Users & Communities

- PPs & security targets (STs) can be used to communicate security requirements
  - ST: vendor to user
  - PP: user community to vendor
    - Smart cards
    - Healthcare
    - Process control
    - BITS
    - IEEE Basic Operating System Security (BOSS)
- Want assurance of comparability of evaluations, both intra-scheme & inter-scheme
- Want more visibility into & influence over evaluation processes, including lab accreditation/competence
- Communities can work with CBs to develop technology-specific applications of the CC & CEM (e.g., CCRA smart card supporting documents)

`

Long Term Survival of the CC Paradigm: Obstacles, Barriers, & Trouble Indicators

Obstacles, Barriers, & Trouble Indicators

- Technical & economic
- Organizational, administrative, promotional

Obstacles, Barriers, & Trouble Indicators

Technical & Economic

- Lack of wide-spread government sector adoption of the CC paradigm (i.e, use of evaluated products & of PP mechanism)
- Lack of wide-spread commercial sector adoption of the CC paradigm
- Lack of a solid business case demonstrating the economic value of an evaluation
- Lack of specific metrics & data demonstrating the security value-added of an evaluation

Obstacles, Barriers, & Trouble Indicators

Technical & Economic (cont.)

- High cost of obtaining significant assurance
- Imbalance in CC paradigm use
- Lack of significant improvements in testing & test methods
- Ability of CC & CEM to evolve/change to meet stakeholders' needs
- Conflicting goals of international harmonization vs. protecting national scheme interests/investments
- Concern about comparability & competency of evaluations

Obstacles, Barriers, & Trouble Indicators

Organizational, Administrative, & Promotional

- CCRA growing pains: Ability of CCRA to grow from "small group" to "international organization"
- No organized aggressive promotion of the CC paradigm to encourage government & commercial sector use of the CC

Obstacles, Barriers, & Trouble Indicators:

Technical & Economic

Lack of wide-spread government sector adoption of the CC paradigm (i.e, use of evaluated products & of PP mechanism)

- No wide-spread adoption/use by any CCRA government
  - No examples of mandatory acquisition/use of evaluated products by all agencies/departments within any government
- Primary government participants are those that:
  - Developed the CC & CEM
  - Established the national CB
  - Exceptions noted in introductory slides
- Most aggressive approach being taken in US DoD/national security community
  - National Security Policy 11
  - DoD 8500 Policy requirement to use government recommended PPs
  - Consideration of extension to whole government

Lack of wide-spread commercial sector adoption of the CC paradigm

- Adoption only by governments (even full adoption) is not sufficient for success
  - Small percent of market
  - CIP commercial systems
- Government sector not setting good example
- Smartcard/IC community only major commercial sector to adopt the CC paradigm
- Adoption of CC paradigm by commercial sector communities depends very much on their expectations, requirements, and prior testing experiences

Lack of wide-spread commercial sector adoption of the CC paradigm (cont.)

- Using the smart card community as an example:
  - Participation/adoption by European stakeholders a "good sign"
    - Established group consisting of CBs, labs, vendors, users, other stakeholders
    - Developed smartcard-specific application of the CC
      - Attack potential
      - Integrated Circuits
      - Composite evaluations
      - Evaluation Technical Reports
    - Adopted by 3 CBs (France, Germany, UK)
    - Accepted as CCRA supporting documents

Lack of wide-spread commercial sector adoption of the CC paradigm (cont.)

- Smart Card Security Users Group (SCSUG) abandonment of CC paradigm a “bad sign”
  - Bank card issuers (e.g., Visa, Mastercard, Europay, AmEx)
  - Compared CC-evaluations to their testing approach
  - Evaluations take too long & cost to much
  - Lacked confidence in:
    - Testing results
    - Competence of testers/labs
    - Comparability of testing results (among labs, to their results)
    - Ability of labs to keep up with newly discovered smartcard attacks and vulnerabilities
  - Expectations of more interaction between SCSUG & CCIMB/CCRA members

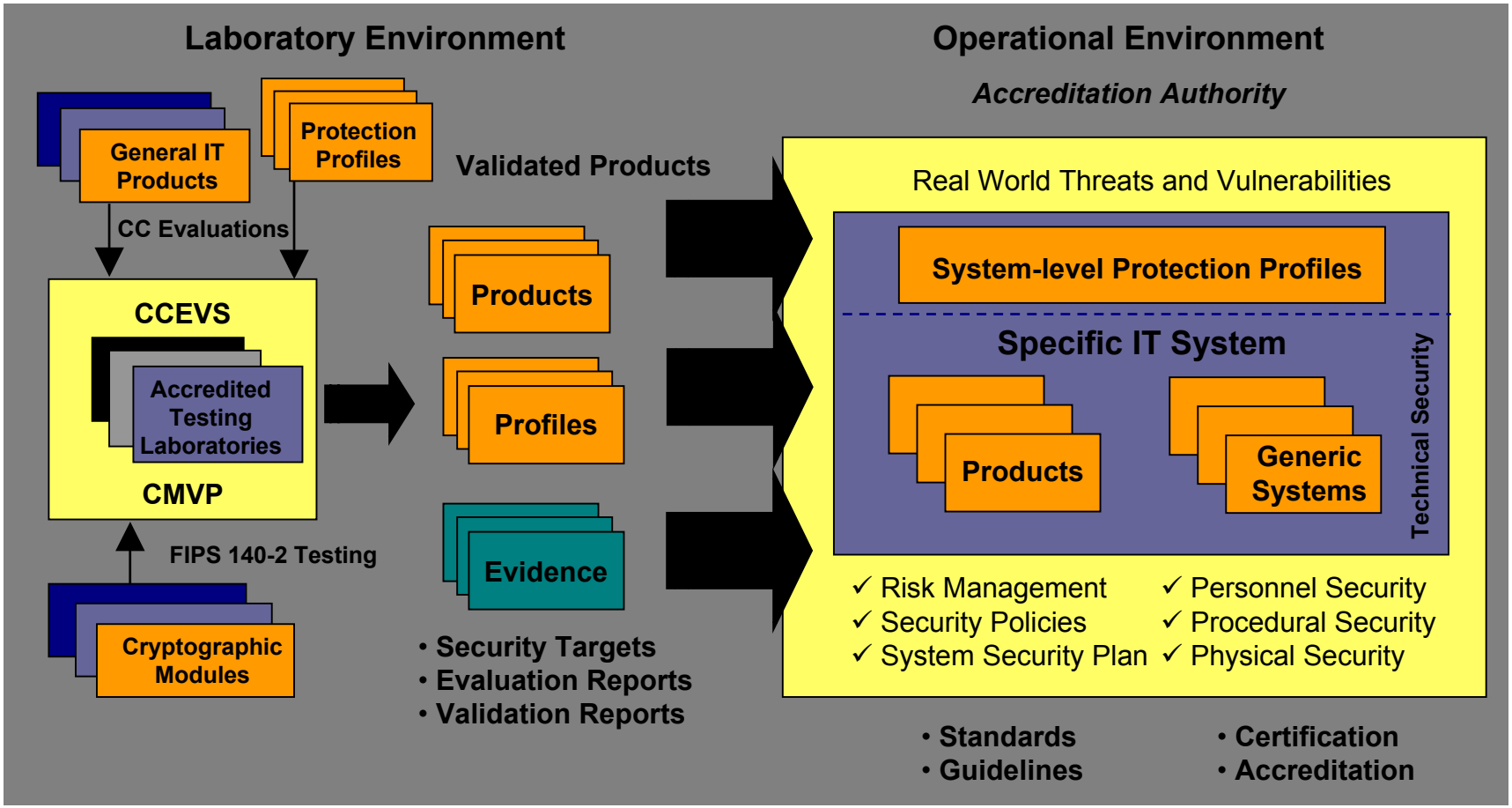
Lack of wide-spread commercial sector adoption of the CC paradigm (cont.)

- BITS: The Technology Group for The Financial Services Roundtable: http://www.bitsinfo.org/index.html
  - Partially adopted CC
  - Developed requirements as CC functional packages
  - Will accept CC evaluations of products that demonstrate conformance to their functional packages
    - Vendors will get both a CC certificate and BITS mark
  - But also established their own testing lab for vendors that only want a BITS mark (i.e., do not want a CC evaluation)
  - See: http://www.bitsinfo.org/sltesting.html
- Lack of other major commercial adoption

Lack of a solid business case demonstrating the economic value of an evaluation

- Value/contribution of an evaluated product insignificant/minor in the context of an information system (IS)

How Component Evaluations Contribute to IS Assurance



Lack of a solid business case demonstrating the security value of an evaluation (cont.)

- No data/metrics for determining how much an evaluated product contributes to overall system security
- Without such data, not possible to assess the security benefit of an evaluated product
- One has to question the value of integrating "gold bricks" into a structure (i.e.,system) that has many other vulnerabilities.
- As with security controls in general, one should not spend more on an evaluation than the improved protection provided by the evaluated product—but we can not measure this so don't know the value
- Only solid economic value is to vendors when they can amortize the evaluation cost across large market

Lack of specific metrics & data demonstrating the security value-added of an evaluation

- Little evidence/metrics that demonstrate an evaluated product provides more/better security than if the product had not been evaluated
- At EAL 4 & below, evaluations do not improve the quality of products: the quality is built in prior to evaluation & is not changed by the evaluation
- Only limited vulnerability analysis is performed at low assurance levels
- For identified vulnerabilities, vendors have option to change ST rather than repair vulnerability
- No guarantee product is free from malicious code
- Developmental high assurance requirements (e.g., design, modularity) do improve quality of product-but still lack metrics

High cost of obtaining significant assurance

- Low assurance (EAL 1-2) provides little protection—but is affordable (some what)
- High assurance (EAL 6-7) provides significantly improved protection and quality -- at significant increase in cost/effort to developer
- Need to look closer at cost-benefit values of EAL 4-5 evaluations
- Beware of false sense of security in reducing costs of high assurance evaluations
  - At some point, security assurance reduces as costs reduce
  - You get what you pay for
  - Cheaper is not always better
- User ambivalence about high assurance products
  - Very few consumers demand/desire it

High cost of obtaining significant assurance (cont.)

- Tendency not to stray from EALs
  - EALs provide a comparison “cocoon”
  - EALs may have requirements not needed or desired
- Selecting only desired assurance requirements could be advantageous
  - Need better guidance on how to select assurance requirements
  - Uncomfortable to be out of comparison “cocoon”

High cost of obtaining significant assurance (cont.)

- Suggest that high assurance in long term may actually be very cost effective taking into consideration all factors
  - Improved product quality
  - Improved reliability
  - Improved protection
    - Reduced vulnerabilities
    - More attack resistant
  - Easier to maintain/change over time
  - Requires experienced, careful systems engineering/design
  - Needs further study/assessment

Imbalance in CC paradigm use

- CC paradigm
  - Use of CC for expression of requirements
  - Use of CC & CEM for evaluation purposes
- CC least used for expressing requirements
  - Definition of STs, PPs, & functional packages
  - Evaluation of STs & PPs
  - Useful even if no product evaluation performed
    - A product ST is a very informative, useful document in a system integration context
    - Full evaluation at EAL4 & below provides questionable additional value based on prior “metrics”, “security value-added” & “high assurance” slides
    - Perhaps only evaluate enough to:
      - Obtain a general sense of trustworthiness
      - Use the product wisely in the system context

Lack of significant improvements in testing & test methods

- Still done much as before
- Not high research priority
- Little automation
- At higher assurance levels (> EAL 4) still:
  - More art than science
  - More subjective than objective
  - Very labor intensive
  - Very costly
  - Can not really measure “security improvement”

Ability of CC & CEM to evolve/change

- Stakeholders include:
  - Founding fathers
  - CB's and their labs
  - CCIMB
  - CCRA members
  - Standards groups (e.g., ISO/IEC SC27 WG 3)
  - Vendors
  - User communities
- CC & CEM must evolve/change in ways that are useful to all stakeholders--otherwise it will not be used
  - Example: how to incorporate/reference national/international standards and how to reuse external (i.e., non-CC) conformance tests against those standards in a CC evaluation

Ability of CC & CEM to evolve/change (cont.)

- Constant tension between “growth/change” stakeholders and CCRA/CBs
- Rapid change not in best interest of CBs
  - Changes in CC & CEM cause serious perturbations to schemes & labs operations
- Change without cooperation of CBs is ineffective & unproductive: CBs are the only “evaluation game in town”
- Evolution will most likely result in two versions of the CC & CEM: ISO & CCRA “implemented version”
- Need to find a realistic evolution pattern acceptable to all stakeholders

Conflicting goals of international harmonization vs. protecting national scheme interests/investments

- National CB interests, investments, and philosophical differences often preclude rapid CCRA convergence on:
  - Request for interpretation (RIs)
  - Development of new material for CC & CEM
  - For example: Assurance maintenance supplement
- CCIMB deliberations & deliverables reflects this situation
- Inability to reach compromise is not in the best interests of the CC community

Concern about comparability & competency of evaluations

- Evaluation acceptance/use based on:
  - Technical quality and competence of labs/evaluators/validators
  - Comparability (inter & intra-schemes)
  - Cost
  - Time
  - Other factors
- Comparability & competency issues raised by
  - ECMA TC 36
  - SCSUG

Concern about comparability & competency of evaluations (cont.)

- Desire visibility into & influence over evaluation processes, including lab accreditation/competence
- Communities can work with CBs to develop technology-specific applications of the CC & CEM (e.g., CCRA smartcard supporting documents)

Obstacles, Barriers, & Trouble Indicators:

Organizational, Administrative, & Promotional

CCRA growing pains: ability of CCRA to grow from “small group” to “international organization”

- Similar growing pains in going from small business to medium size business
- Mode of operation must change.
  - Need better administration & management processes
  - Need devoted staff to manage CCRA
  - Need long-term planning & budget process
  - Need accountability for meeting goals/milestones/deliverables

No organized aggressive promotion of the CC paradigm to encourage commercial sector use of the CC

- Primary focus of the CCRA is certificate recognition and other scheme-related issues, including:
  - Technical quality & comparability of evaluations/labs
  - Administering the CCRA
  - Acceptance of new members
  - Voluntary periodic assessments
  - International resolution of problems/interpretations
  - Maintaining CCRA versions of the CC & CEM
  - Cooperation with ISO
- CC paradigm needs to be promoted in both the government & commercial sectors

No organized aggressive promotion of the CC paradigm to encourage commercial sector use of the CC (cont.)

- Active & aggressive promotion of CC & CEM is outside of CCRA. Promotion includes:
  - Education & awareness
  - Advice & assistance
  - Joint projects
- Communities need to be encouraged/courted to work with CBs to develop technology-specific applications of the CC & CEM (e.g., CCRA smart card supporting documents)
- Where is/who has that responsibility?
- Issue recognized by CCRA members: solutions being explored

Recommendations

- The CCRA should:
  - Transition organizationally/administratively to become a “mature” international organization
  - Resolve internal impediments to rapid convergence on technical issues (e.g., RIs & new material)
  - Improve public confidence in comparability and competence of evaluations
  - Work toward improving efficiency of evaluations without sacrificing quality & security

Recommendations (cont.)

- National CB's/Schemes jointly should:
  - Develop a solid business case demonstrating the security & economic value of an evaluation in a system context
  - Develop metrics & data demonstrating the security value-added of an evaluation
  - Invest in R&D of test methods/approaches that reduce evaluation subjectivity and increase its objectivity

Recommendations (cont.)

- An outreach organization should be established to aggressively promote use of CC in communities-of-interest for
  - Requirements definition
  - Acquisition of evaluated products
- Communities-of-interest should use the established (smartcard) model for developing technology-specific applications of the CC & CEM
  - Use of CC for expression of requirements
  - Use of CC & CEM for evaluation purposes

Recommendations (cont.)

- Investigate why government & commercial sectors have not embraced the CC paradigm
  - Lack confidence in result?
  - Do not believe/understand how result helps in system integration/assessment?
  - Do not believe/understand how use improves security?
  - Want latest versions of products?

Conclusion

- CC foundation is in place
- Considerable and significant energy being expended
  - CCRA members & CBs
  - New CCRA members
  - Vendor evaluations
  - New labs
  - R & D efforts
  - International standardization
- CC foundation is internationally recognized
- Parts of some governments have “bought in”
- There are significant examples of commercial sector adoption—but very few.

Questions to Ponder about the CC & CC Paradigm

- Why the CC paradigm has not been universally adopted for improving the security of systems?
- Under what conditions are evaluations cost-beneficial?
- Is the technical quality of the result credible?
- Why we can not make a credible/convincing case for adoption—with metrics; not words?
- Is there a CC-use latency factor until momentum builds?
- If so, will it survive until acceptance/usage builds?
- Will there be an ICCC 9 in 2008?
- I sincerely hope so -- but not unless we recognize the trouble signs and remove the barriers

Contact Information

Stuart Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards & Technology
100 Bureau Drive; Stop 8930
Gaithersburg, MD 20899
(301) 975-4768
skatzke@nist.gov
fax: (301) 975-4964