



Ground Station Architectures Workshop 2002

Harmonizing the Certification and Accreditation Process With Modern Security Evaluation Standards

March 15, 2001

Stuart Schaeffer
stuart@aero.org

Charles Lavine
lavine@aero.org

Trusted
Computer
Systems
Department



Introduction

- C&A = determination of level of risk of putting a system into service.
- Evaluation = rigorous determination of whether a product meets security requirements.
- Traditional C&A has not taken advantage of evaluation methods.

Introduction ➔

Why Do We Care?

Problems

Attacking the Problems

Conclusion

Topics



Introduction ➔
Why Do We
Care?
Problems
Attacking the
Problems
Conclusion

- Why Do We Care?
- Problems
- Attacking the Problems
- Conclusion

Why Do We Care?

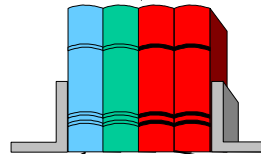
DoD Information Assurance Policy



Department of Defense
DIRECTIVE 8500

Supersedes:
DoD Directive 5200.28
DoD Manual 5200.28-M
DoD CIO Memorandum 6-8510

Mandates



DoD Information Technology
Security Certification and
Accreditation Process
(DITSCAP)
(C&A Process)

National Security
Telecommunications and
Information Systems Security
Policy (NSTISSP) No. 11
(Mandates Evaluated Products)

Other Standards and
Processes



Introduction

Why Do We
Care? ➔

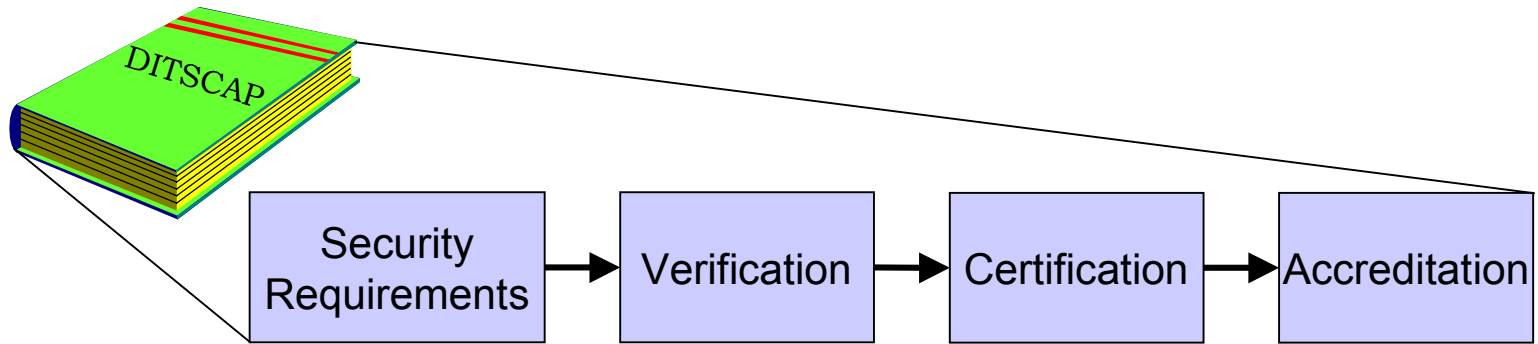
Problems

Attacking the
Problems

Conclusion



DITSCAP C&A Process



Certification :

Given security policies and specifications for a particular operating environment, determine the extent to which the system meets the security policy objectives for use in that environment.



Accreditation:

Authorization to operate a system under a set of specified conditions.

Introduction

Why Do We Care? ➔

Problems

Attacking the Problems

Conclusion

Security Evaluation Standards



- An international standard (ISO 15408) that provides:
 - Catalog of Security Functional and Assurance Requirements
- The US national Scheme provides:
 - Common Evaluation Methodology (CEM), for evaluating how well design and behavior of a product meet its security requirements
 - Scheme is jointly run by NIST and NSA
 - Other nations have their own schemes



Introduction

Why Do We Care? ➔

Problems

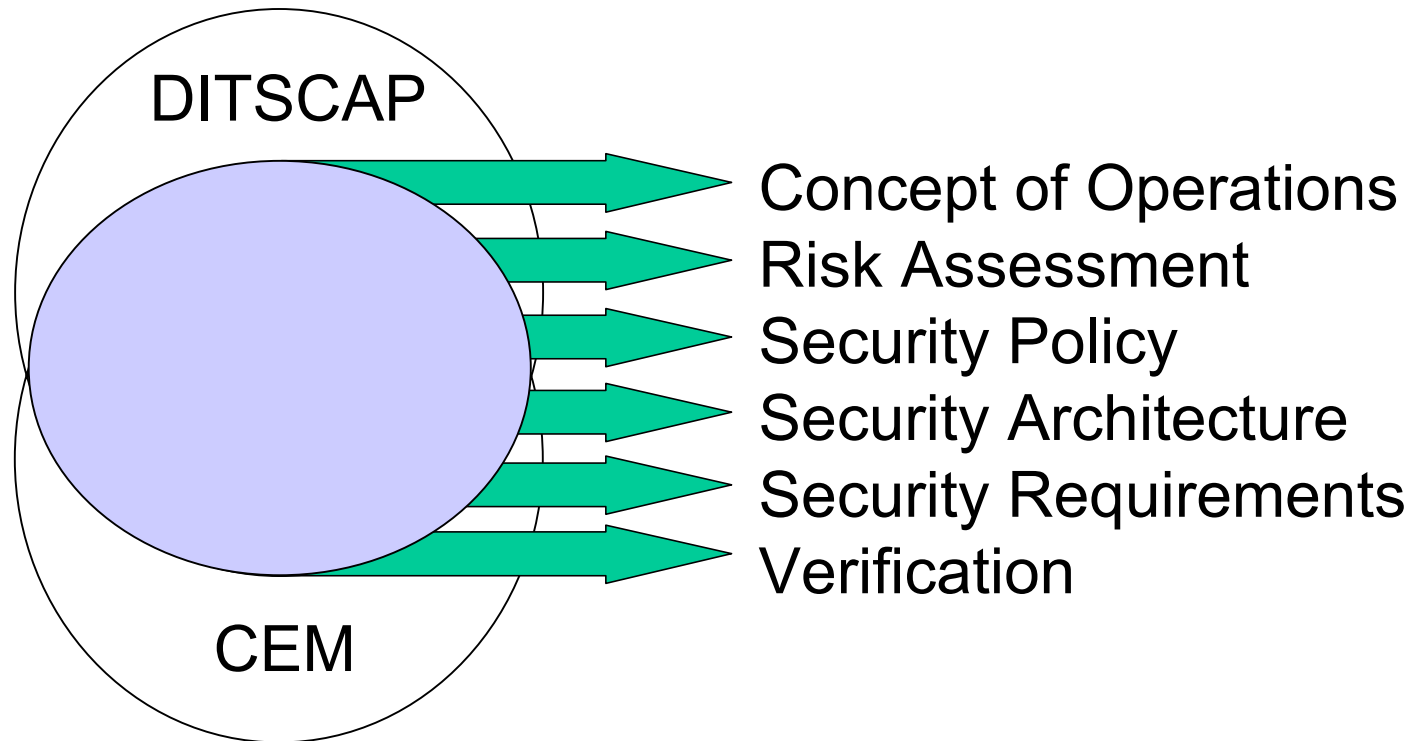
Attacking the Problems

Conclusion



Developing Assurance

Minimize Duplication, Leverage Formal Evaluation



Introduction

Why Do We Care? ➔

Problems

Attacking the Problems

Conclusion



But Real Life Intrudes

- Programs perform C&A idiosyncratically
- Most programs are insufficiently informed about CC
 - Do not take advantage of evaluated products, CC methodology
- Results:
 - Lack of uniformity, confusion between programs
 - Lower security assurance
 - Higher than necessary costs





COSTS



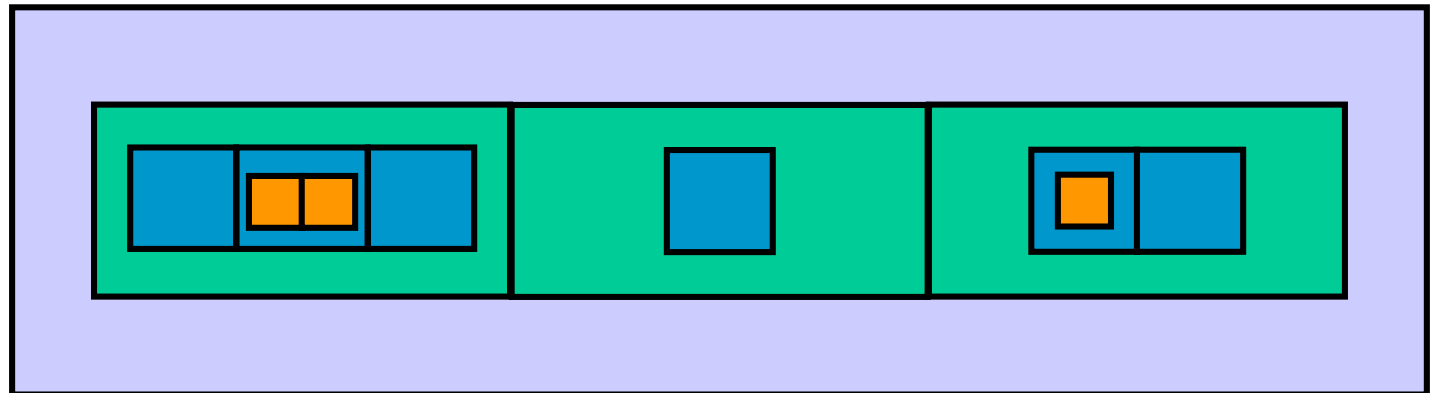
- Requiring CC evaluated products is intended to lower Government costs
 - Vendors pay for evaluations
 - Government gets security assurance
- Programs not requiring evaluated products defeat the purpose
 - Government pays for ad hoc analysis and testing
 - Less rigor than CC evaluation, less assurance





CEM Not Suited For Systems

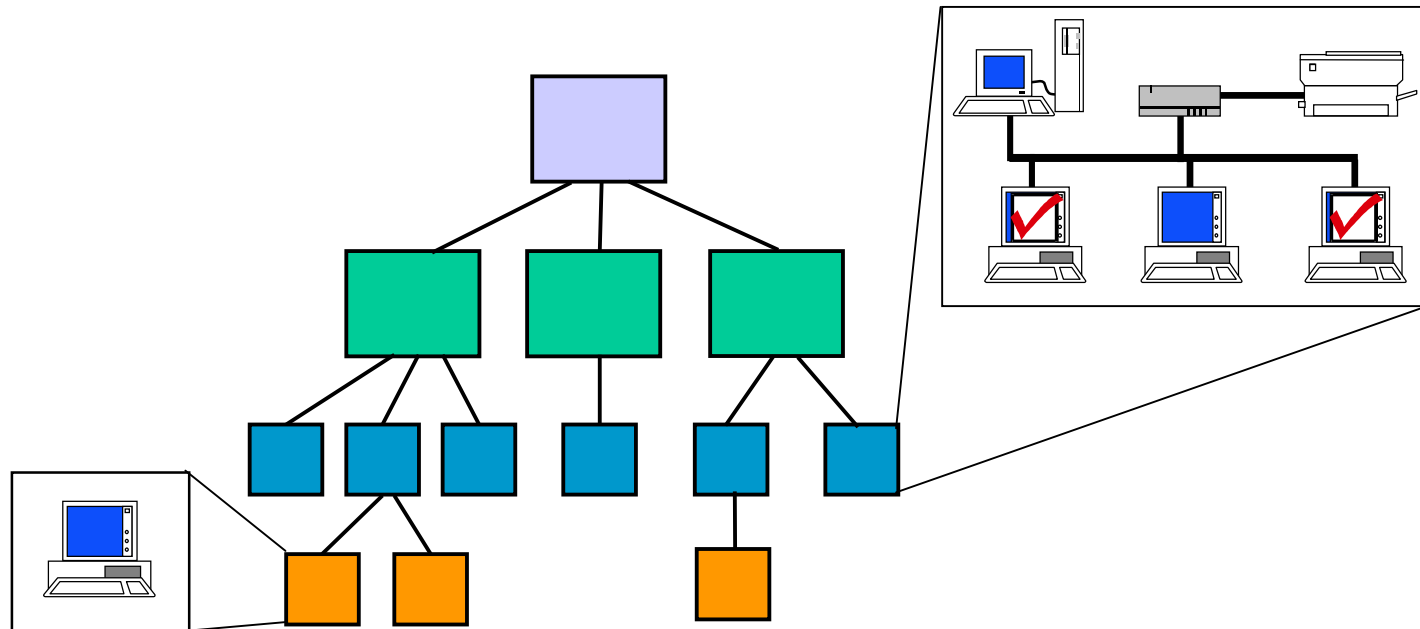
- Complexity & Size
- Security requirements spread among component products
- Need to show that combining products maintains security





Proposed Methodology

- Decompose System Requirements into Subsystem Requirements Recursively to Product Level
 - Provides path for recomposition of system from component products





Issues

- Educating the Programs
 - Mistaken perception of increased cost
 - Contractor acceptance of “new” way to do C&A
- Codifying the methodology
 - Working Group (Aerospace, Mitre, SPAWAR)
 - Aerospace working with NSA
- Balancing between CCTL evaluation and traditional DITSCAP analysis
 - CCTL more rigorous, more costly
- DAA awareness/enforcement

Introduction

Why Do We Care?

Problems

Attacking the Problems →

Conclusion



Conclusion

- C&A would benefit from adoption of modern security evaluation methods (e.g., the CC & the CEM)
 - Higher security assurance
 - Lower costs over time
- Methodology is being developed
- Need an effective program to educate the C&A community

Introduction

Why Do We Care?

Problems

Attacking the Problems

Conclusion ➔



References

- DoD CIO Guidance and Policy Memorandum 6-8510
 - <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>
- DITSCAP
 - <http://iase.disa.mil/ditscap/ditsdoc.html>
- Common Criteria & Common Evaluation Methodology
 - <http://www.commoncriteria.org/cc/cc.html>
 - <http://www.commoncriteria.org/cem/cem.html>
- NSTISSP 11
 - http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf