

**16th Annual  
Computer Security Applications Conference  
December 11-15, 2000  
New Orleans, LA**

# **Developing Protection Profiles Getting Started**

**Douglas E. McGovern, Ph.D.**  
Ray-McGovern Technical Consultants, Inc.  
22304 East 67th Street, Broken Arrow, OK 74014  
918/355-3522 918/355-1026 (fax)  
demcgovern@aol.com



# Common Criteria

- **New Language - translation problems possible**
- **New Concepts -**
  - **Assumptions, Threats, Policies**
  - **SFRs, SARs, EALs**
  - **Not always what they seem at first glance**

# Basic Principle

- **What are the Security Issues you're trying to address?**
  - state them in your own terms & own jargon
- **Get very clear on what you're confused about**

# Then Learn CC Jargon

- **Assumption**
- **Threat**
- **Security Policy**
- **SFRs, SARs**
- **Evaluation Assurance Levels**

# Issue #1 - Security

- **Each Credit/Debit card must be unique**
- **Account number is added in final stages of production**
- **Cards can be stolen earlier**
- **Therefore: put unique serial number in chip at earliest possible point (which is when it's made)**

# Rationale

- **Do it early on**
- **Use your own natural language - “Each Credit/Debit card must be unique to prevent criminals from making copies of legitimate cards that could be used off-line, bypassing on-line checks.”**
- **Then translate to CC jargon**

# Translate

- **Unique serial number per chip could be in:**
  - **ACM\_CAP.4.1C - “The reference for the TOE shall be unique to each version of the TOE.”**
- **Does that clearly translate?**
- **If the “TOE” is a smart card and each “version” is a new card, maybe OK**

# Back Translate

- **After you translate from your words to CC:**
  - does the CC statement translate back to your words?
- **If not:**
  - refine
  - iterate
  - write application notes
  - create new SFRs or SARs

## Issue # 2 - Stress

- **Initial requirement is that the IC resist attempts to compromise it by subjecting it to environmental stress**

# Stress - Common Criteria

- **CC provides:**
  - **FPT\_PHP.3 “The TSF shall resist [assignment: physical tampering scenarios] to the [assignment: list of TSF devices/ elements] by responding automatically such that the TSP is not violated.”**
- **Sufficient?**

# Stress - Assignment

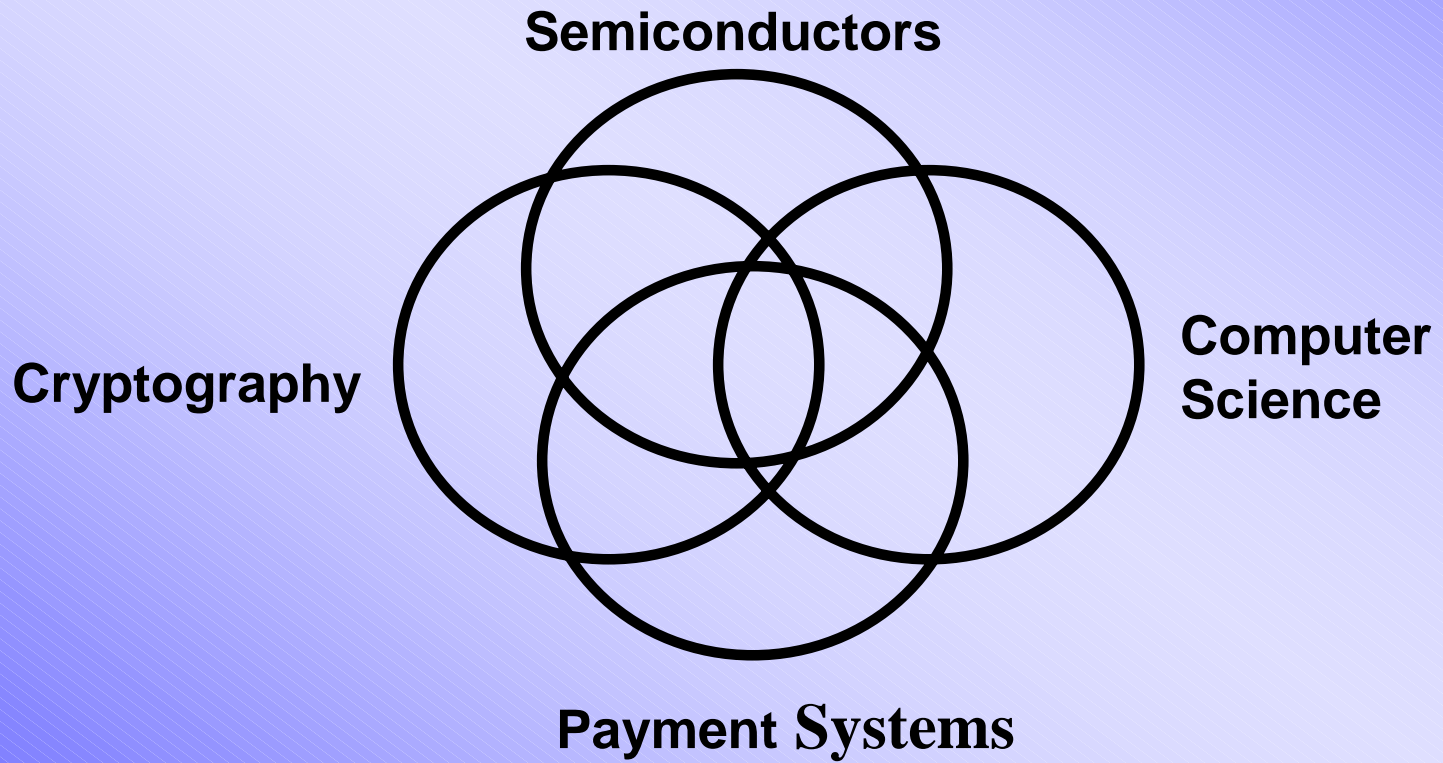
- **Assign:**
  - “The TSF shall resist [environmental stress] to the [IC] by responding automatically such that the TSP is not violated.”
- **Makes it clear enough**
  - IF the lab knows the technology
  - may need to specify further with testing methodology

## Issue #3 - Understandability

- **Get very clear on what other people are confused about**
- **Intersection of disciplines leads to misunderstandings**
- **Intersection of understandings leads to different interpretations**

# Smart cards

- different industries - different jargon



# Jargon Trap - “Module”

- In semiconductors, refers to a functional part of an integrated circuit
- In smart cards, refers to the chip package
- In Common Criteria, Modularity (ADV\_INT) is an SAR dealing with complexity of the TSF; module is a chunk of code

# Jargon Trap - “User”

- **Person, program, or gadget?**
- **Person:**
  - professional or not?
  - everyday or infrequent User?
  - bank, store clerk, consumer, or ??
- **Program: “external IT entity”**
- **Gadget: telephones, terminals, PCs, or ??**

# Jargon Trap - “Load”

- **Computers**
  - (v) to insert data or to install a program
- **Cryptography**
  - (v) insert a code
- **Semiconductors**
  - (v) install a module in a card
- **Financial smart cards**
  - (n) the \$ on a payment card

# Misunderstandings

- **Smart card folk may not understand Common Criteria**
  - “what’s a TOE?”
- **Common Criteria folk may not understand smart cards**
  - “what’s a photomask?”
- **Some things nobody understands**
  - “is differential power analysis a covert channel?”

# Differing Interpretations

- **“is this a threat or an attack?”**
- **“this needs to be changed:”**
  - **“include instructions on evaluation in PP”**
  - **“remove this information to a separate document for additional review and consideration”**

# Getting Started - Summary

- If you don't first know what you want, and why you want it, you'll never get it
- Get very clear on what you're confused about
- Translate, check, and back translate. Be creative if necessary, but be very clear
- Other people need to understand it, too

# Questions?