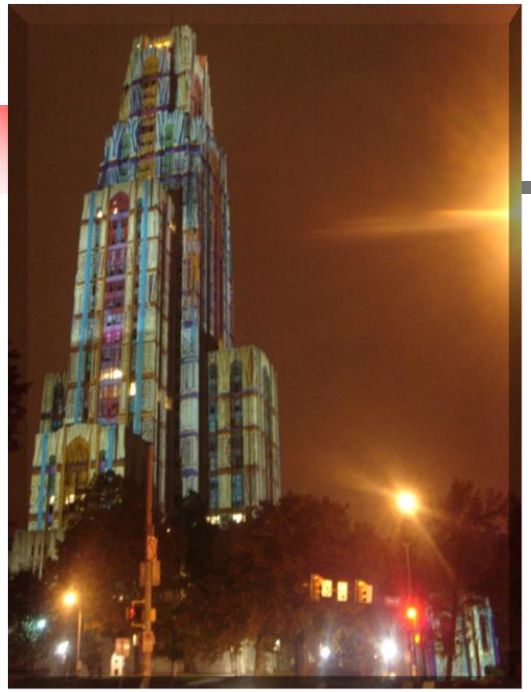
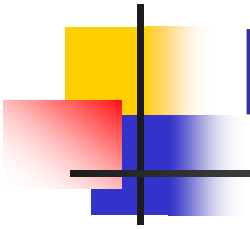
IS 2150 / TEL 2810
Introduction to Security



James Joshi
Associate Professor, SIS

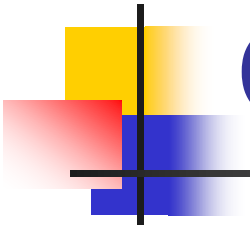
Lecture 10
Dec 9, 2015

Legal/Ethical Issues
Physical Security



Laws and Security

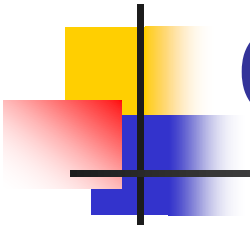
- Federal and state laws affect privacy and secrecy
  - Rights of individuals to keep information private
- Laws regulate the use, development and ownership of data and programs
  - Patent laws, trade secrets
- Laws affect actions that can be taken to protect secrecy, integrity and availability



Copyrights

- Designed to protect *expression* of ideas
- Gives an author exclusive rights to make copies of the *expression* and sell them to public

- Intellectual property (copyright law of 1978)
  - Copyright must apply to an original work
  - It must be done in a tangible medium of expression
- Originality of work
  - Ideas may be public domain
- Copyrighted object is subjected to fair use

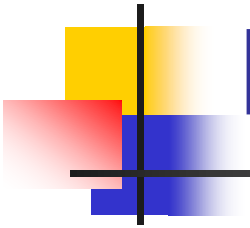


Copyright infringement

- Involves copying
- Not independent work
  - Two people can have copyright for identically the same thing
- Copyrights for computer programs
  - Copyright law was amended in 1980 to include explicit definition of software
  - Program code is protected not the algorithm
  - Controls rights to copy and distribute

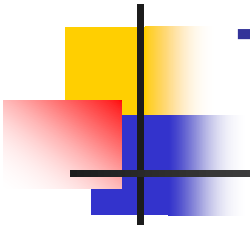
Patent

- Protects innovations
  - Applies to results of science, technology and engineering
  - Protects new innovations
    - Device or process to carry out an idea, not idea itself
  - Excludes newly discovered laws of nature
    - 2+2 = 4



Patent

- Requirements of novelty
  - If two build the same innovations, patent is granted to the first inventor, regardless of who filed first
  - Invention should be truly novel and unique
  - Object patented must be non-obvious
- Patent Office registers patents
  - Even if someone independently invents the same thing, without knowledge of the existing patent
- Patent on computer objects
  - PO has not encouraged patents for software – as they are seen as representation of an algorithm



Trade Secret

- Information must be kept secret
  - If someone discovers the secret independently, then there is no infringement – trade secret rights are gone
  - Reverse-engineering can be used to attack trade secrets
- Computer trade secret
  - Design idea kept secret
  - Executable distributed but program design remain hidden

Comparison

	Copyright	Patent	Trade secret
Protects	Expression of idea	Invention	Secret information
Object made public	Yes: intention is to promote	Design filed at patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years of company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue if secret improperly obtained
Examples	Object code, documentation	Hardware	Source code

Computer crime

- Hard to predict for the following reason
  - Low computer literacy among lawyers, police agents, jurors, etc.
  - Tangible evidence like fingerprints and physical clues may not exist
  - Forms of asset different
    - Is computer time an asset?
  - Juveniles
    - Many involve juveniles

Computer Crime related laws

- Freedom of information act
  - Provides public access to information collected by the executive branch of the federal government
- Privacy act of 1974
  - Personal data collected by government is protected
- Fair credit reporting act
  - Applies to private industries – e.g., credit bureaus
- Cryptography and law
  - France: no encryption allowed (to control terrorism)
  - US, UK, Canada, Germany:
    - Control on export of cryptography; but they are published!

Ethics

- An objectively defined standard of right and wrong
- Often idealistic principles
- In a given situation several ethical issues may be present
- Different from law

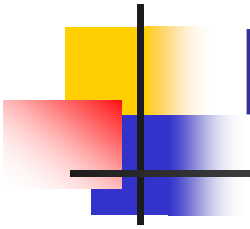
Law vs Ethics

Law

- Described by formal written documents
- Interpreted by courts
- Established by legislatures representing all people
- Applicable to everyone
- Priority determined by laws if two laws conflict
- Court is final arbiter for right
- Enforceable by police and courts

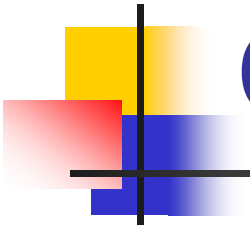
Ethics

- Described by unwritten principles
- Interpreted by each individual
- Presented by philosophers, religions, professional groups
- Personal choice
- Priority determined by an individual if two principles conflict
- No external arbiter
- Limited enforcement



Ethics Example

- Privacy of electronic data
  - "gentlemen do not read others' mail" - but not everyone is a gentleman!
  - Ethical question: when is it justifiable to access data not belonging to you
    - One approach: Protection is user's responsibility
    - Another: supervisors have access to those supervised
    - Another: justifiably compelling situation



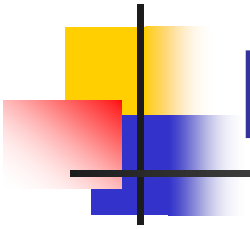
Codes of ethics

- IEEE professional codes of ethic
  - To avoid real or perceived conflict of interest whenever possible, and to disclose them to affected parties when they do exist
  - To be honest and realistic in stating claims or estimates based on available data
- ACM professional codes of ethics
  - Be honest and trustworthy
  - Give proper credit for intellectual property

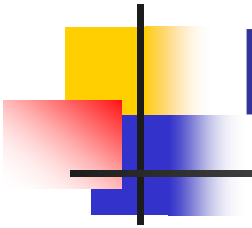
Physical Security

- Often ignored or considered as of little or no concern
  - If someone working late steals a laptop – the fancy firewall defenses won't help!
- A NY investment bank spent tens of thousands of dollars on comsec to prevent break-in during the day, only to find that its cleaning staff opened the doors at night!
- A company in SFO had more than $100,000 worth of computers stolen over a holiday; an employee had used his electronic key card to unlock the building and disarm the alarm system

Physical security in security plan

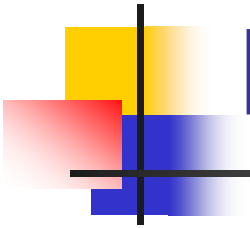


- Organizational security plan should include
  - Description of physical assets to be protected
  - Description of physical areas where the assets are located
  - Description of security perimeter
  - Threats (attacks, accidents, natural disasters)
  - Physical security defense and cost-analysis against the value of information asset being protected



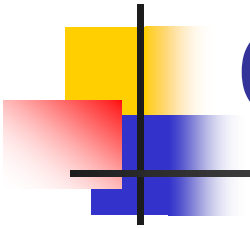
Disaster Recovery

- Natural disasters
  - Flood/Falling water
  - Fire
  - Earthquake
  - Other environmental conditions
    - Dust, explosion (terrorist act), heat/humidity, electrical noise, lighting
- Power loss
  - Uninterruptible power supply
  - Surge protectors
- Accidents: food & drink



Physical security plan

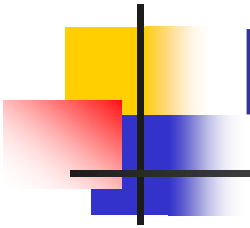
- Should answer (at least) the following
  - Can anybody other than designated personnel physically access the computer resources?
  - What if someone has an outburst and wants to smash the system resources?
  - What if an employee from your competitor were to come to the building unnoticed?
  - What are the consequences in case of fire?
  - How to react in case of some disaster?



Contingency planning

"key to successful recovery is adequate planning"

- Backup/off-site backup
- Cold-site/hot-site
  - Cold site: facility with power/cooling where computing system can be installed to begin immediate operation
  - Hot-site: facility with installed and ready to use computing system.
- Theft prevention
  - Prevent access: guards; locks; cards
  - prevent portability: locks, lockable cabinets
  - detect exit: like in library

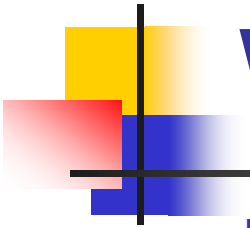


Disposal of Sensitive Media

- Shredders
  - Mainly for paper; also used for diskettes, paper ribbons and some tapes
- Sanitizing media before disposal
  - Completely erase data
  - ERASE and DELETE may not be enough
  - Overwrite data several times
- Degaussers
  - Destroys magnetic fields
  - Fast way to neutralize a disk or tape

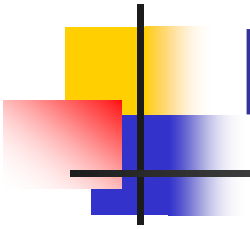
TEMPEST: Emanations protections

- Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
  - All electronic and electromechanical info. processing equipment can produce unintentional data-related or intelligence-bearing emanations which, if intercepted and analyzed, disclose the info. transmitted, received, handled or otherwise processed (NSTISSAM 1-00)
  - program certifies an equipment as not emitting detectable signals
- Enclosure
  - Completely cover a tempest device
    - Shielded cable
    - Copper shielding a computer?
- Emanation modification
  - Similar to generating noise



What is Formal Evaluation?

- Method to achieve *Trust*
  - Not a guarantee of security
- Evaluation methodology includes:
  - Security requirements
  - Assurance requirements showing how to establish security requirements met
  - Procedures to demonstrate system meets requirements
  - Metrics for results (level of trust)
- Examples: TCSEC (Orange Book), ITSEC, CC



Formal Evaluation: Why?

- Organizations require assurance
  - Defense
  - Telephone / Utilities
  - "Mission Critical" systems
- Formal verification of entire systems not feasible
- Instead, organizations develop formal evaluation methodologies
  - Products passing evaluation are trusted
  - Required to do business with the organization

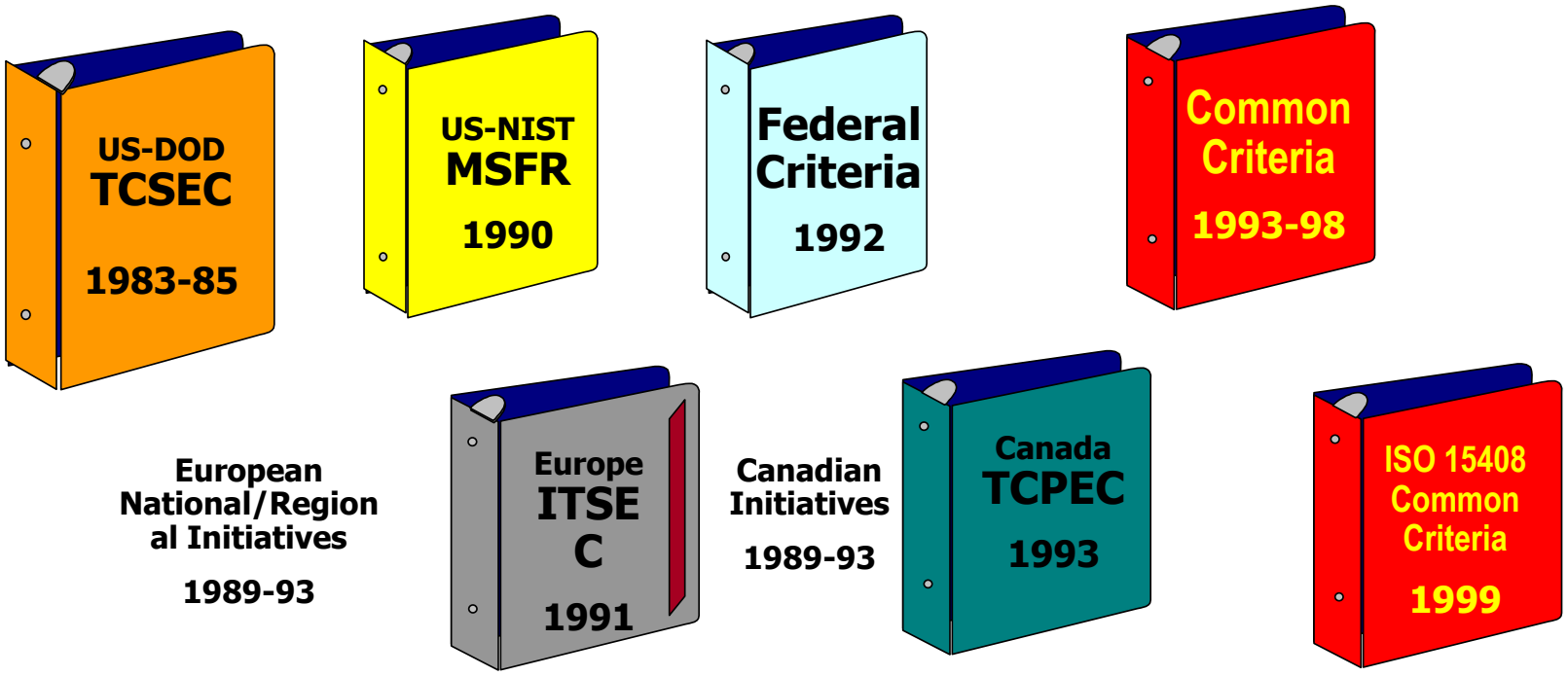
Mutual Recognition Arrangement

National Information Assurance partnership (NIAP), in conjunction with the U.S. State Department, negotiated a Recognition Arrangement that:

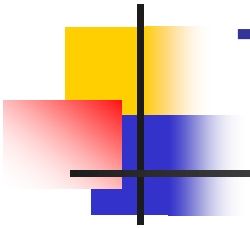
- Provides recognition of Common Criteria certificates by 24 nations (was 19 in 2005)
- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

An Evolutionary Process

Two decades of research and development…

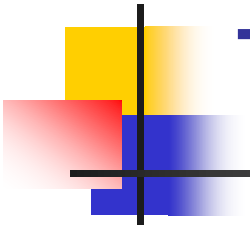


Common Criteria: Origin



TCSEC

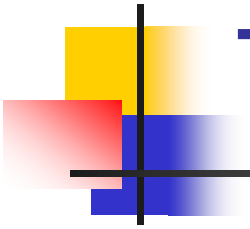
- Known as Orange Book, DoD 5200.28-STD
- Four trust rating divisions (classes)
  - D: Minimal protection
  - C (C1,C2): Discretionary protection
  - B (B1, B2, B3): Mandatory protection
  - A (A1): Highly-secure



TCSEC: The Original

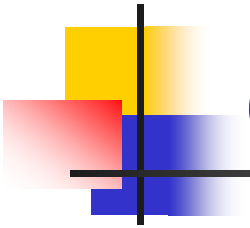
- Trusted Computer System Evaluation Criteria
  - U.S. Government security evaluation criteria
  - Used for evaluating commercial products
- Policy model based on Bell-LaPadula
- Enforcement: Reference Validation Mechanism
  - Every reference checked by compact, analyzable body of code
- Emphasis on Confidentiality
- Metric: Seven trust levels:
  - D, C1, C2, B1, B2, B3, A1
  - D is “tried but failed”

TCSEC Class Assurances



- C1: Discretionary Protection
  - Identification
  - Authentication
  - Discretionary access control
- C2: Controlled Access Protection
  - Object reuse and auditing
- B1: Labeled security protection
  - Mandatory access control on limited set of objects
  - Informal model of the security policy

TCSEC Class Assurances *(continued)*

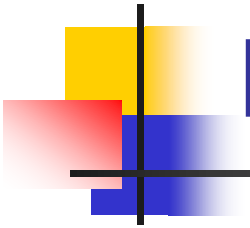


- B2: Structured Protections
  - Trusted path for login
  - Principle of Least Privilege
  - Formal model of Security Policy
  - Covert channel analysis
  - Configuration management
- B3: Security Domains
  - Full reference validation mechanism
  - Constraints on code development process
  - Documentation, testing requirements
- A1: Verified Protection
  - Formal methods for analysis, verification
  - Trusted distribution

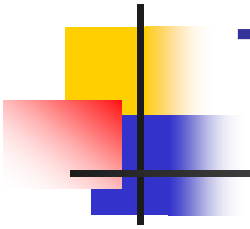
How is Evaluation Done?

- Government-sponsored independent evaluators
  - Application: Determine if government cares
  - Preliminary Technical Review
    - Discussion of process, schedules
    - Development Process
    - Technical Content, Requirements
  - Evaluation Phase

TCSEC: Evaluation Phase



- Three phases
  - Design analysis
    - Review of design based on documentation
  - Test analysis
  - Final Review
- Trained independent evaluation
  - Results presented to Technical Review Board
  - Must approve before next phase starts
- Ratings Maintenance Program
  - Determines when updates trigger new evaluation

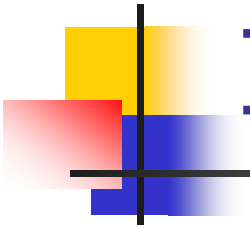


TCSEC: Problems

- Based heavily on confidentiality
  - Did not address integrity, availability
- Tied security and functionality
- Base TCSEC geared to operating systems
  - TNI: Trusted Network Interpretation
  - TDI: Trusted Database management System Interpretation

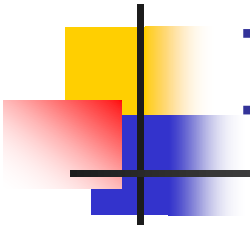
Later Standards

- CTCPEC – Canadian Trusted Computer Product Evaluation Criteria
- ITSEC – European Standard (Info Tech SEC)
  - Did not define criteria
  - Levels correspond to strength of evaluation
  - Includes code evaluation, development methodology requirements
  - Known vulnerability analysis
- CISR: Commercial outgrowth of TCSEC (Commercial International Security Requirements)
- FC: Modernization of TCSEC
- FIPS 140: Cryptographic module validation
- Common Criteria: International Standard
- SSE-CMM: Evaluates developer, not product



ITSEC: Levels

- E1: Security target defined, tested
  - Must have informal architecture description
- E2: Informal description of design
  - Configuration control, distribution control
- E3: Correspondence between code and security target
- E4: Formal model of security policy
  - Structured approach to design
  - Design level vulnerability analysis
- E5: Correspondence between design and code
  - Source code vulnerability analysis
- E6: Formal methods for architecture
  - Formal mapping of design to security policy
  - Mapping of executable to source code



ITSEC Problems:

- No validation that security requirements made sense
  - Product meets goals
  - But does this meet user expectations?
- Inconsistency in evaluations
  - Not as formally defined as TCSEC

- Replaced TCSEC, ITSEC
- 7 Evaluation Levels (functionally tested to formally designed and tested)
- Functional requirements, assurance requirements and evaluation methodology
- Functional and assurance requirements are organized hierarchically into: *class*, *family*, *component*, and, *element*. The components may have *dependencies*.

IT Security Requirements

CC defines two types of IT security requirements--

Functional Requirements

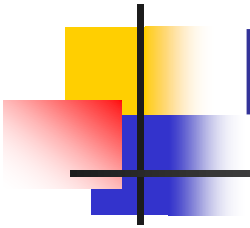
- for defining security behavor of the IT product or system:
- implemented requirements become security functions

Examples:
- *Identification & Authentication*
- *Audit*
- *User Data Protection*
- *Cryptographic Support*

Assurance Requirements

- for establishing confidence in security functions:
- correctness of implementation
- effectiveness in satisfying security objectives

Examples:
- *Development*
- *Configuration Management*
- *Life Cycle Support*
- *Testing*
- *Vulnerability Analysis*

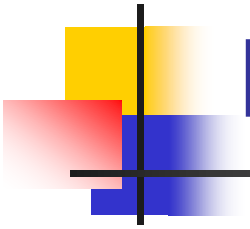


Documentation

- Part 1: Introduction and General Model
- Part 2: Security Functional Requirements
- Part 3: Security Assurance Requirements
- CEM

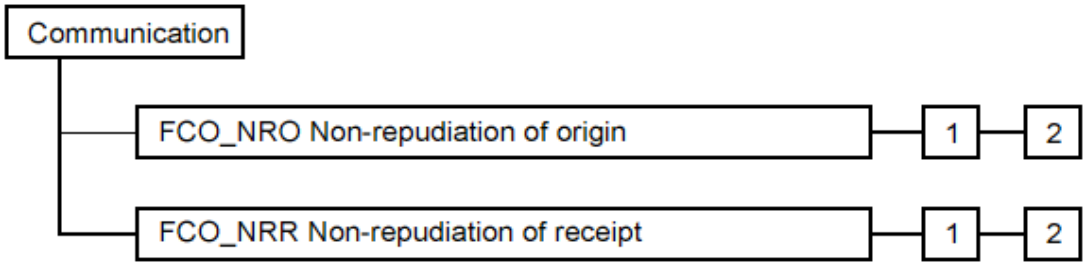
- Latest version: 3.1 (variations exist)
- http://www.commoncriteriaportal.org/public/expert/index.php?menu=2

Common Criteria: Functional Requirements



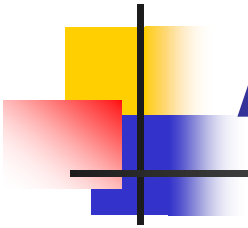
- 314 page document
- 11 Classes
  - Security Audit, Communication, Cryptography, User data protection, ID/authentication, Security Management, Privacy, Protection of Security Functions, Resource Utilization, Access, Trusted paths
- Several families per class
- Lattice of components in a family

Class Example: Communication



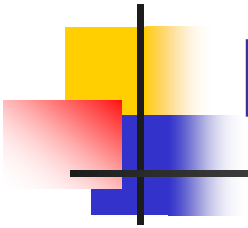
- Non-repudiation of origin
  1. Selective Proof. Capability to request verification of origin
  2. Enforced Proof. All communication includes verifiable origin

Common Criteria: Assurance Requirements



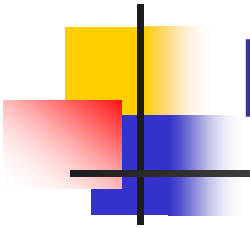
- 231 page document
- 10 Classes
  - Protection Profile Evaluation, Security Target Evaluation, Configuration management, Delivery and operation, Development, Guidance, Life cycle, Tests, Vulnerability assessment, Maintenance
- Several families per class
- Lattice of components in family

Common Criteria: Evaluation Assurance Levels



1. Functionally tested
2. Structurally tested
3. Methodically tested and checked
4. Methodically designed, tested, and reviewed
5. Semi-formally designed and tested
6. Semi-formally verified design and tested
7. Formally verified design and tested

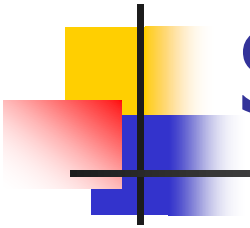
Common Criteria: Evaluation Process



- National Authority authorizes evaluators
  - U.S.: NIST accredits commercial organizations
  - Fee charged for evaluation
- Team of four to six evaluators
  - Develop work plan and clear with NIST
  - Evaluate Protection Profile first
  - If successful, can evaluate Security Target

Common Criteria: Status

- About 80 registered products (2005)
  - Only one at level 5 (Java Smart Card)
  - Several OS at 4
  - Likely many more not registered
- 223 Validated products (Oct, 2007)
  - Tenix Interactive Link Data Diode Device Version 2.1 at EAL 7+



Summary

- Legal/Ethical Issues
- Physical Security
  - TEMPEST
  - Contingency planning
- Security evaluations