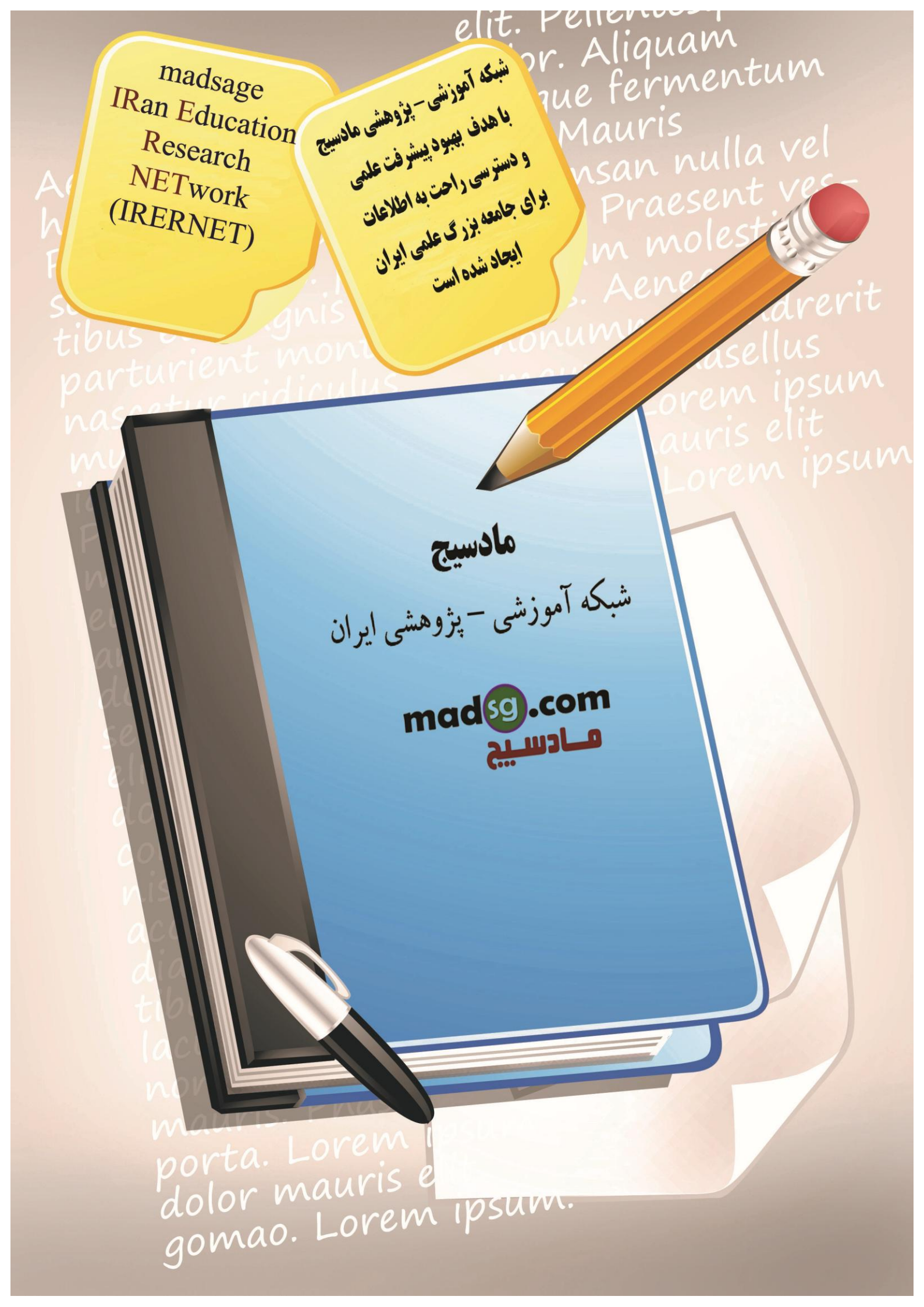
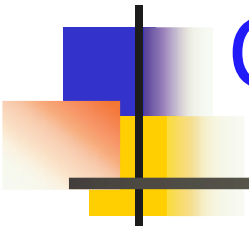

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

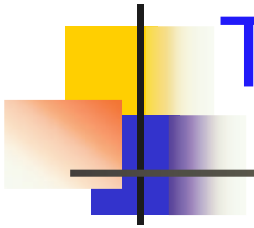


CIS 739 - Computer Security

Lecture 9 – Evaluating Systems

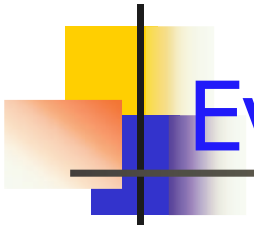
Mehdi Kharrazi

*Slides Adopted from Previous Lecture by Nasir Memon @ Polytechnic UNIVERSITY



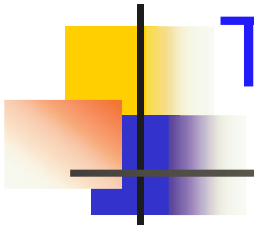
Trusted Systems

- Perfect security is an ultimate but unachievable goal.
- A trusted system is one that has been shown to meet specific security requirements under specific conditions.
- Formal security evaluation techniques facilitate the development of trusted systems.
- Different evaluation techniques and methodologies.



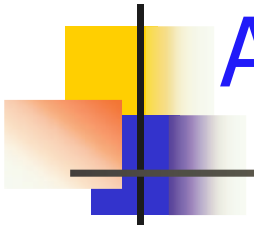
Evaluation methodologies

- Consist of:
  - Requirements defining security functionality of system.
  - Assurance requirements that delineate the steps for establishing system meets its functional requirements.
  - Methodology for determining product meets functional requirements based on analysis of assurance evidence
  - A measure of evaluation of the result (levels of trust)
- A formal evaluation methodology is a technique used to provide measurements of trust based on specific requirements and evidence of assurance.



Trusted System Design Elements

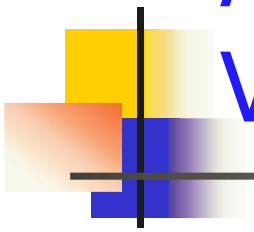
- Principles of the design of secure protection systems
  - Least privilege.
  - Economy of mechanism.
  - Open design.
  - Complete mediation.
  - Permission-based.
  - Separation of privilege.
  - Least common mechanism.
  - Easy to use.



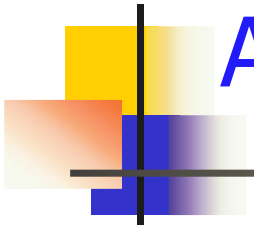
Assurance Methods - Testing

- Testing – Functional, Unit, Integration, System etc.
  - Can demonstrate existence but not absence
  - Hard to get adequate test coverage
  - Black box testing does not observe internal effects
  - White box testing needs code modification!
- Testing – Tiger team
  - Failure to penetrate does not mean there are no holes.

Assurance Methods - Formal Verification

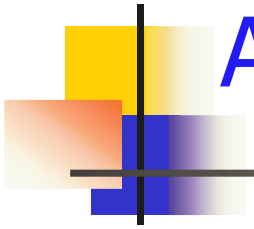


- The OS is reduced to a theorem which is then proven.
- Not very practical in large systems as it needs
  - Time
  - Complexity
- Theorem provers can assist but still too much human activity needed.
- Not used much



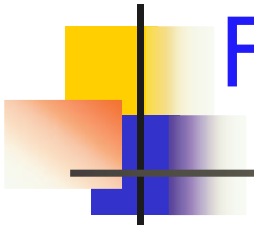
Assurance Methods - Validation

- Validation – Includes verification by one or more of the following
  - Requirement checking
  - Design and code reviews
  - Module and system testing



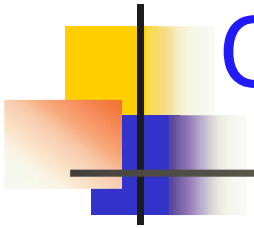
Assurance Methods - Evaluation

- For non-experts, evaluation by independent experts is best.
  - US Orange book evaluation
  - European ITSEC evaluation
  - German Green Book
  - British Criteria
  - ITSEC criteria
  - US Combined Federal Criteria
  - Common Criteria



Formal Evaluation: Why?

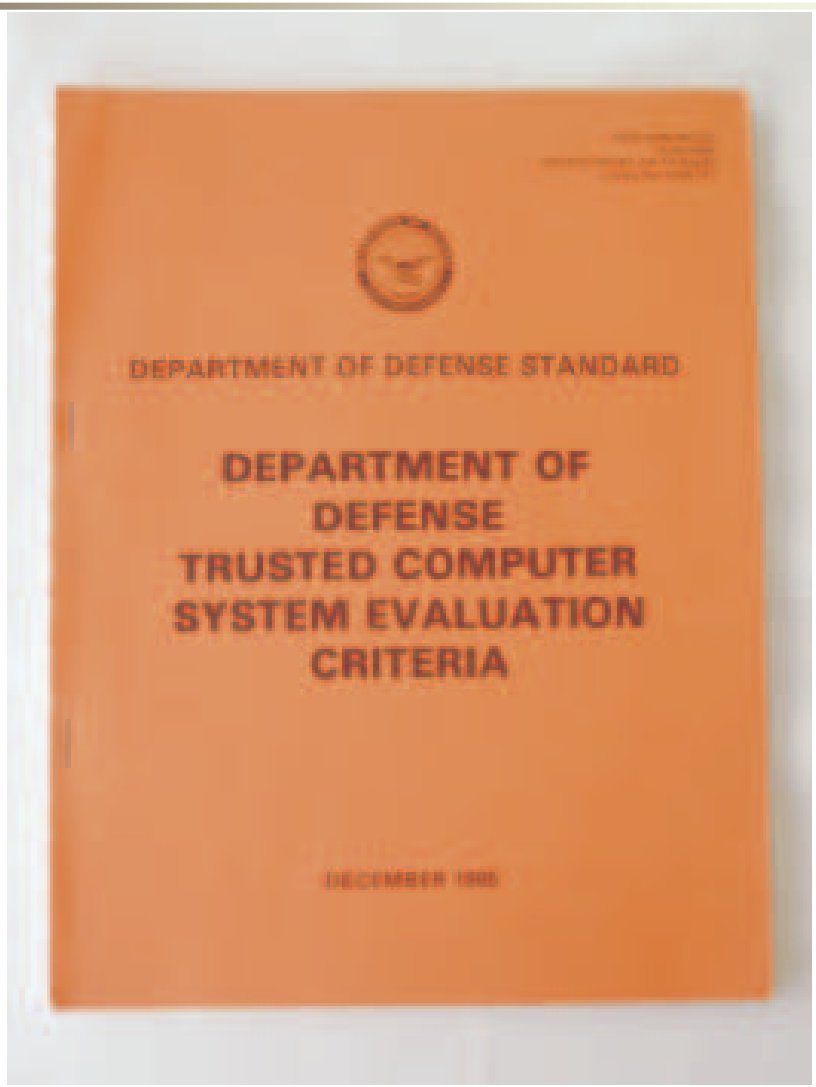
- Organizations require assurance
  - Defense
  - Telephone / Utilities
  - "Mission Critical" systems
- Formal verification of entire systems not feasible
- Instead, organizations develop formal evaluation methodologies
  - Products passing evaluation are trusted
  - Required to do business with the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

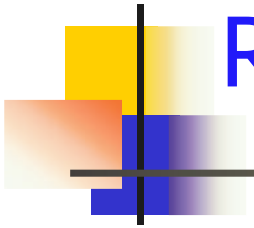


Orange Book

- Trusted Computer Security Evaluation Criteria (TCSEC).
- DoD. Late 70's.
- Four basic divisions A, B, C and D. With A highest degree of security and D lowest (did not meet all requirements!).
- Complete set of ratings
  - D, C1, C2, B1, B2, B3 and A1
- See text for detailed description for each level.

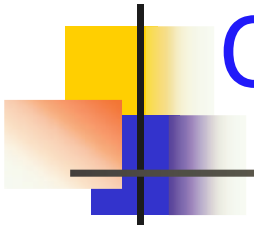
Why is it called the Orange Book?





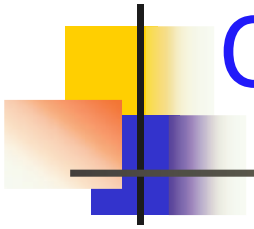
Rainbow Series

- Orange Book: DoD Trusted Computer System Evaluation Criteria, 1983
- Green Book: DoD Password Management Guideline, 1985
- Yellow Book: Guidance for applying TCSEC in Specific Environments, 1985
- Tan Book: A Guide to Understanding Audit in Trusted Systems, 1988
- Bright Blue: Trusted Product Security Evaluation Program, 1990
- Neon Orange Book: Discretionary Access Control in Trusted Systems, 1987
- Aqua Book: Glossary of Computer Security Terms, 1988
- Red Book: Trusted Network Interpretation, 1987
- Amber Book: Configuration Management in Trusted Systems, 1988



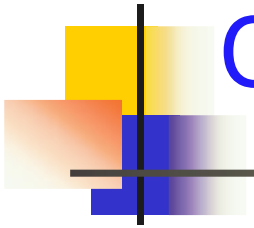
Orange Book

- TCSEC Functional Requirements
  - Discretionary access control requirements
  - Object reuse requirements
  - Mandatory access control requirements
  - Label requirements (enables enforcement of MAC)
  - Identification and authentication requirements
  - Trusted path requirements
  - Audit requirements
  - System architecture requirements – tamperproof, process isolation, principle of least privilege, well defined user interface etc.



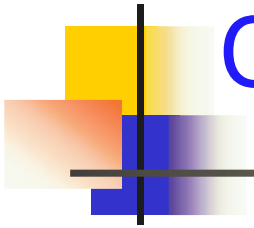
Orange Book

- Assurance Requirements
  - Configuration management requirements
  - Trusted distribution requirement
  - Design specification and verification requirements
  - Testing requirements
  - Product documentation requirements



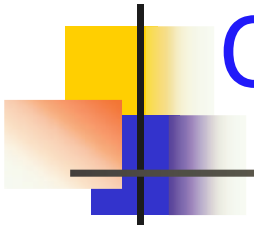
Orange Book

- C1 – Discretionary security protection.
  - Co-operating users processing data at same level of integrity.
  - DAC provides access control.
  - TCB has to have its own execution domain
- C2 – Controlled access protection
  - discretionary control with fine granularity.
  - Audit logs.
  - Objects accessed by TCB should not be accessible to subjects.
  - No object reuse
  - Many commercial systems



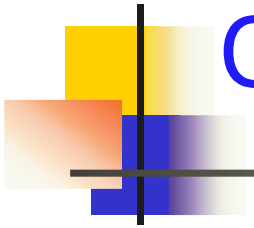
Orange Book

- B1 – Labeled Security Protection
  - Intended for products that handle classified data and enforce mandatory BLP policies.
  - Labels for subjects and objects.
  - Formal or informal model for security policy required.
- B2 – Structured Protection
  - Adds requirements to design of system
  - MAC governs control to physical devices
  - Trusted path for login and authentication
  - A formal model for security policy and Descriptive Top Level Specification (DTLS) required.
  - Covert channel analysis
  - TCB and hardware provide separation mechanisms
  - Security testing



Orange Book

- B3 – Security Domains
  - Highly resistant to penetration
  - Tight security management policies and procedures
  - Intrusion detection
  - Trusted recovery
  - Convincing argument needed for consistency between formal model and informal DTLS.

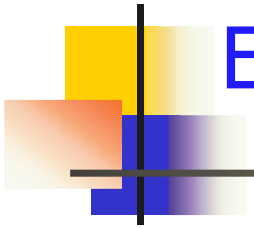


Orange Book

- A1 – Verified Design
  - A formal model for security policy
  - A formal top level specification (FTLS)
  - Consistency proofs between model and FTLS
  - TCB informally shown to be consistent with FTLS
  - A formal analysis of covert channels
  - Stringent configuration management and distribution control

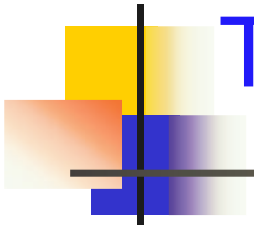
How is Evaluation Done?

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



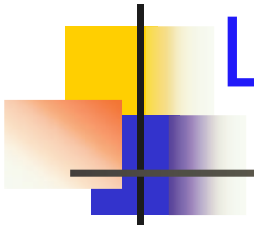
TCSEC: Evaluation Phase

- 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



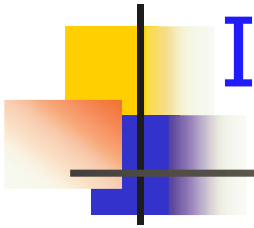
TCSEC: Problems

- Based heavily on confidentiality
- Tied security and functionality
- Base TCSEC geared to operating systems
  - TNI: Trusted Network Interpretation
  - TDI: Trusted Database management System Interpretation



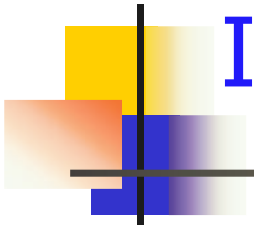
Later Standards

- CTCPEC – Canada
- ITSEC – European Standard
  - Did not define criteria
  - Levels correspond to strength of evaluation
  - Includes code evaluation, development methodology requirements
  - Known vulnerability analysis
- CISR: Commercial outgrowth of TCSEC
- 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

FIPS 140

- For evaluating cryptographic modules:
  - cryptographic algorithms,
  - specification, ports and interfaces,
  - roles, services and authentication,
  - finite state model,
  - physical security,
  - operational environment,
  - key management,
  - electromagnetic interference,
  - self testing, design assurance, etc.

- Replaced TCSEC, ITSEC
- CC Documents
  - Functional requirements
  - Assurance requirements
  - Evaluation Assurance Levels
- CC Evaluation Methodology
  - Detailed process model for each level
- National Scheme

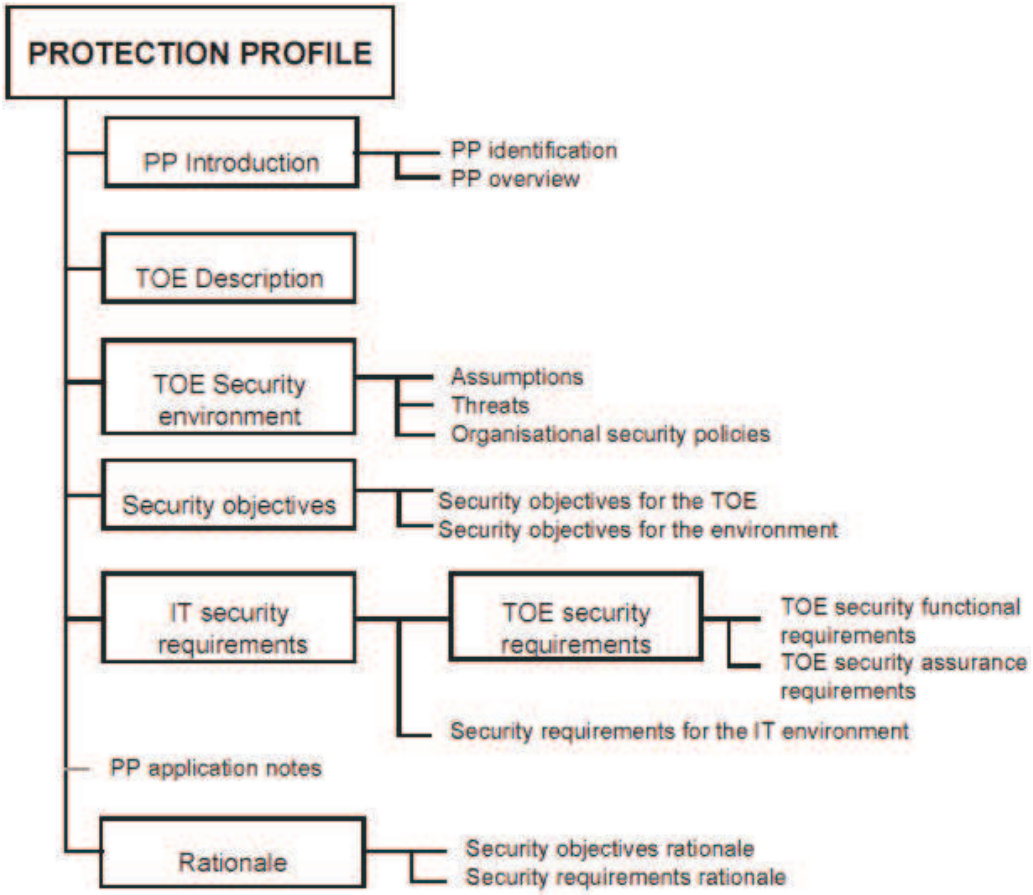
Common Criteria: Origin

Common Criteria: Protection Profile

Domain-specific set of security requirements

- Narrative Overview
- Domain description
- Security Environment (threats, overall policies)
- Security Objectives: System, Environment
- IT Security Requirements
  - Functional drawn from CC set
  - Assurance level
- Rationale for objectives and requirements

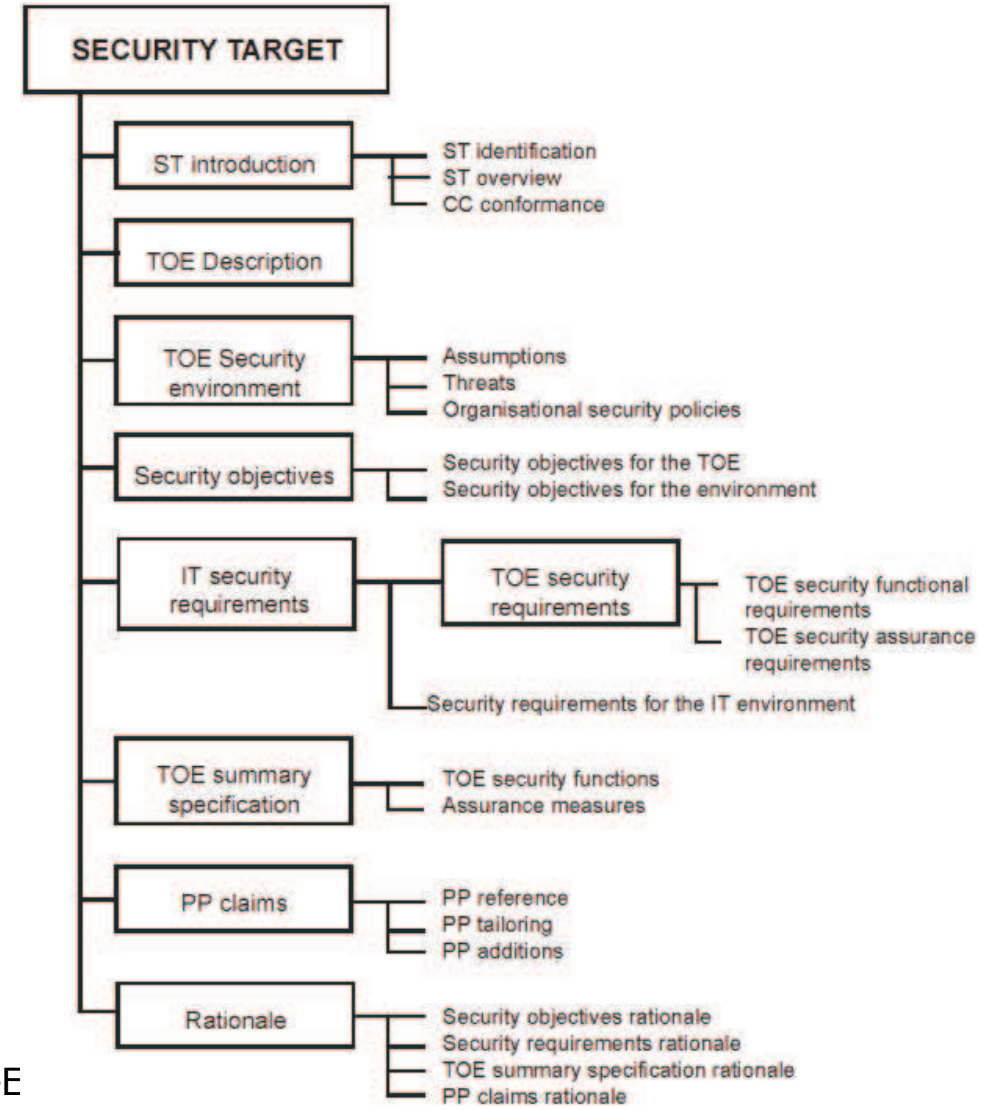
TOE: Target of Evaluation



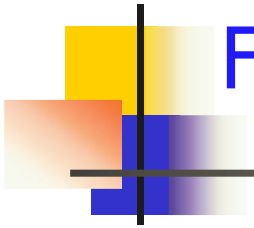
Common Criteria: Security Target

Specific requirements used to evaluate system

- Narrative introduction
- Environment
- Security Objectives
  - How met
- Security Requirements
  - Environment and system
  - Drawn from CC set
- Mapping of Function to Requirements
- Claims of Conformance to Protection Profile

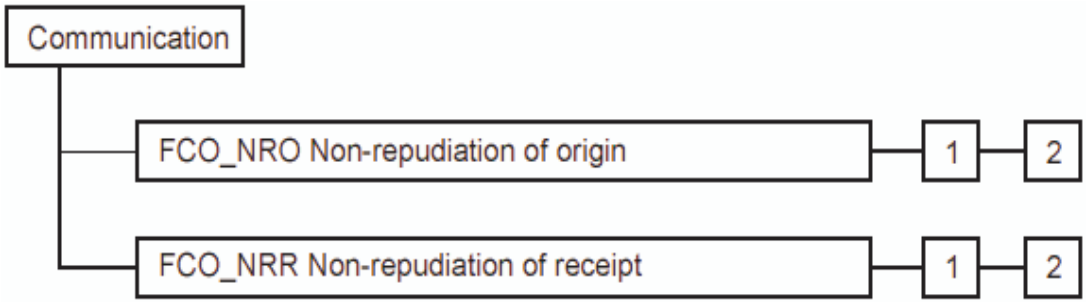


Common Criteria: Functional Requirements



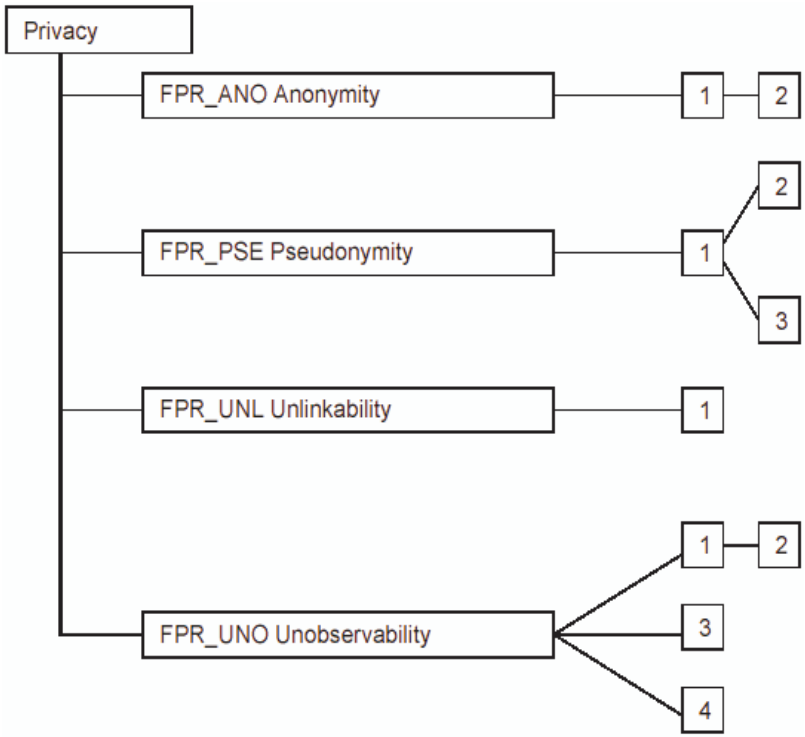
- 362 page document
- 17 Classes
  - Audit, Communication, Cryptography, User data protection, ID/authentication, Management, Privacy, Protection of Security Functions, Resource Utilization, Access, Trusted paths
- Several families per class

Class Example: Communication



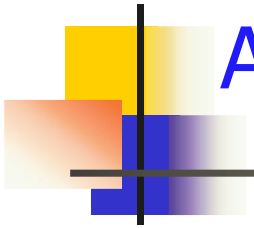
- Non-repudiation of origin
  1. Selective Proof. Capability to request verification of origin
  2. Enforced Proof. All communication includes verifiable origin

Class Example: Privacy



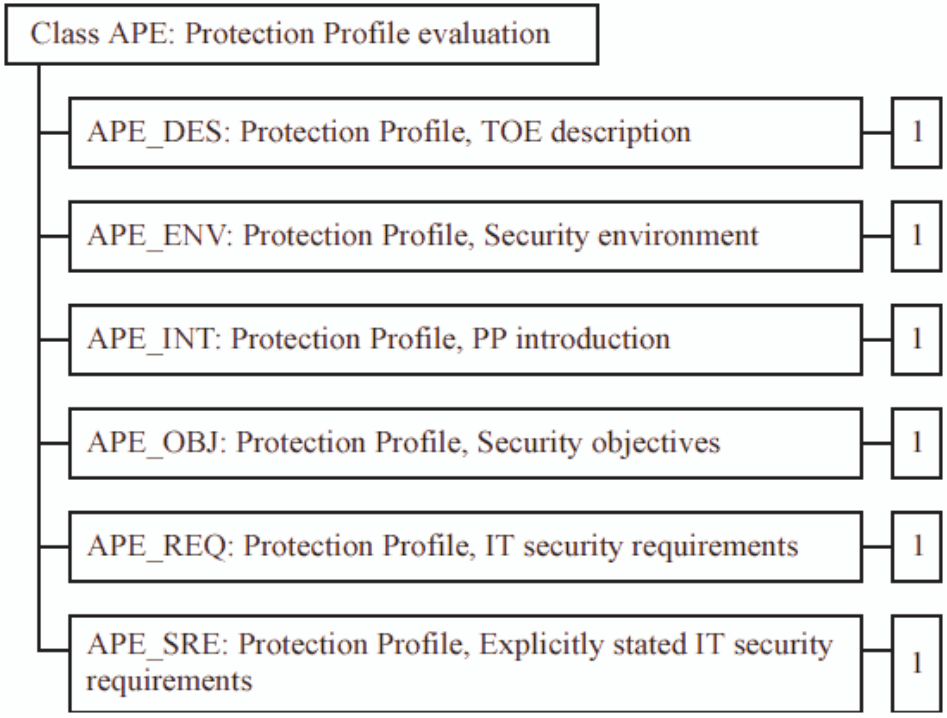
1. Pseudonymity
   1. TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*]
   2. TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*]
   3. The TSF shall [selection: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*]
2. Reversible Pseudonimity
   1. ...
3. Alias Pseudonimity
   1. ...

Common Criteria: Assurance Requirements



- 216 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

Example: Protection Profile Evaluation

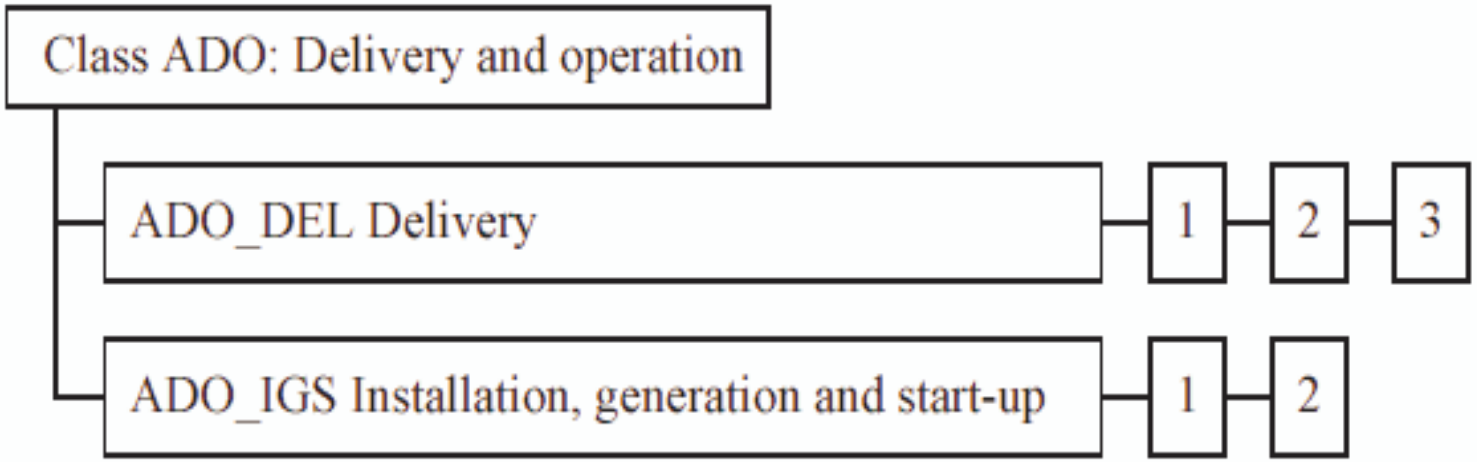


Security environment

- In order to determine whether the IT security requirements in the PP are sufficient, it is important that the security problem to be solved is clearly understood by all parties to the evaluation.

1. Protection Profile, Security environment, Evaluation requirements
   - Dependencies: No dependencies.
   - Developer action elements:
- The PP developer shall provide a statement of TOE security environment as part of the PP.
   - Content and presentation of evidence elements:
- The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.
- The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.
- The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.
   - Evaluator action elements:
- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- The evaluator shall confirm that the statement of TOE security environment is coherent and internally consistent.

Example: Delivery and Operation



1- Installation, generation and start-up

A. Installation, generation, and start-up procedures
   - Dependencies: AGD_ADM.1 Administrator guidance

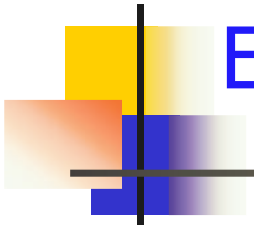
B. Developer action elements:
   - The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

C. Content and presentation of evidence elements:
   - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

D. Evaluator action elements:
   - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
   - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

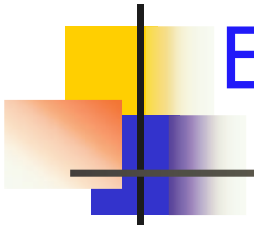
2- Generation Log

Common Criteria: Evaluation Assurance Levels



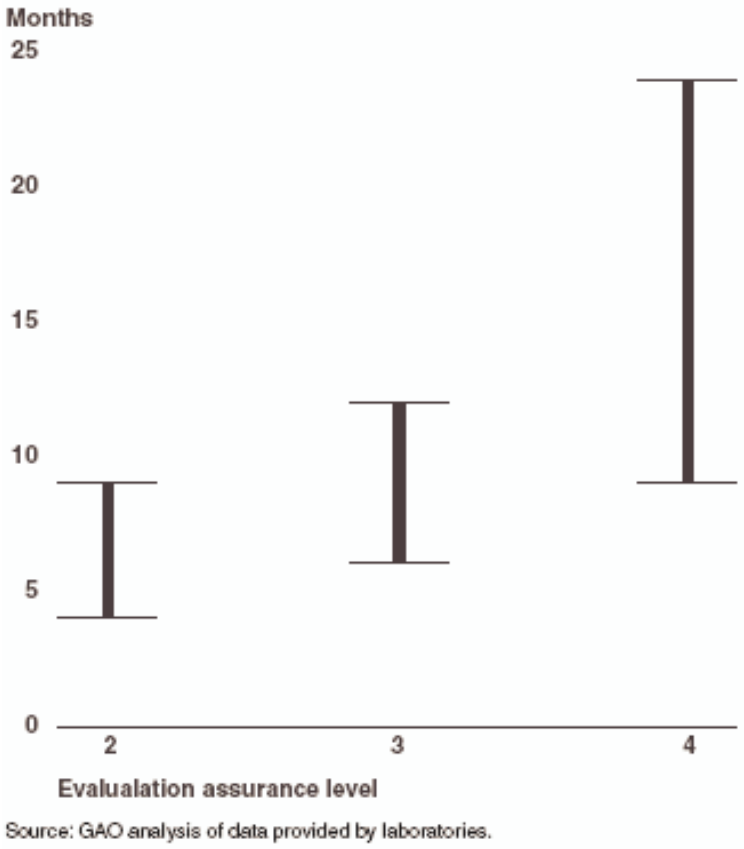
1. Functionally tested
2. Structurally tested
3. Methodically tested and checked
4. Methodically designed, tested, and reviewed
5. Semiformally designed and tested
6. Semiformally verified design and tested
7. Formally verified design and tested

Common Criteria: Evaluation Process

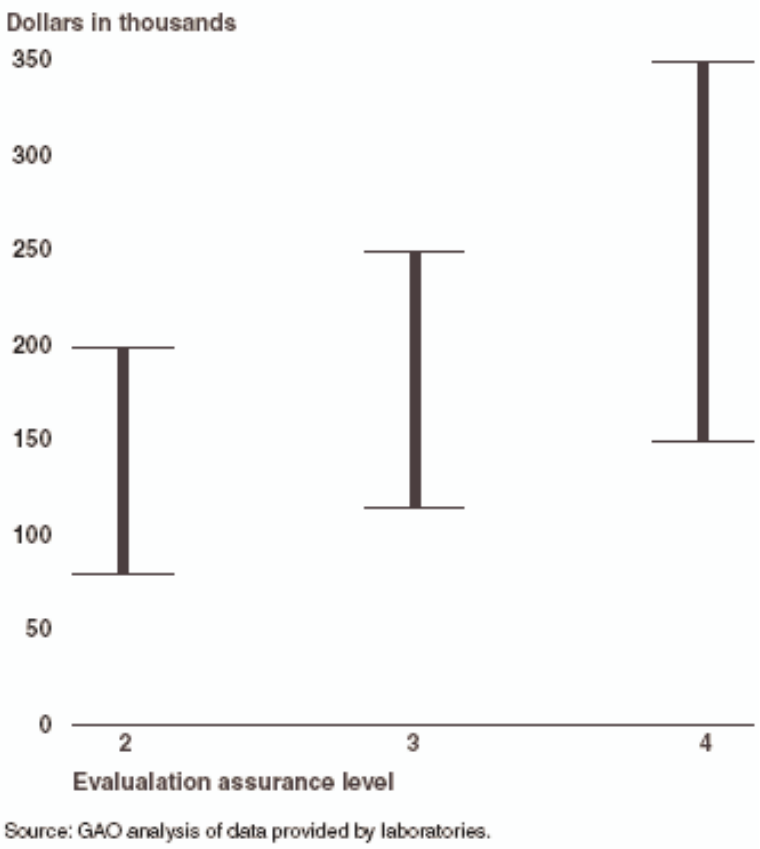


- National Authority authorizes evaluators
  - U.S.: NIST accredits commercial organizations
  - Fee charged for evaluation
- Team of four to six evaluators
  - Develop work plan and clear with NIST
  - Evaluate Protection Profile first
  - If successful, can evaluate Security Target

Cost and Schedule (2006)



Source: GAO analysis of data provided by laboratories.



Source: GAO analysis of data provided by laboratories.

Common Criteria: Status

- Many registered products
  - Only one (actually 2) at EAL7
    - Tenix Interactive Link Data Diode Device
  - Several OS at 4 (XP, 2003)
  - Likely many more not registered
- New versions appearing on regular basis

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)