Information Security CENG418

week-7

- Basic Concepts and Definitions for Information Security

Glossary

- **Access:** The ability to make use of information stored in a computer system.
- **Access control list:** A list of principals that are authorized to have access to some object.
- **Authenticate:** To verify the identity of a person (or other agent external to the protection system) making a request.
- **Authorize:** To grant a principal access to certain information.
- **Certify:** To check the accuracy, correctness, and completeness of a security or protection mechanism.
- **Complete isolation:** A protection system that separates principals into compartments between which no flow of information or control is possible.

Glossary

- **Discretionary:** Controls on access to an object that may be changed by the creator of the object.
- **Domain:** The set of objects that currently may be directly accessed by a principal.
- **Encipherment:** The (usually) reversible scrambling of data according to a secret transformation key, so as to make it safe for transmission or storage in a physically unprotected environment.
- **Grant:** To authorize (*q. v.*).
- **Hierarchical control:** Referring to ability to change authorization, a scheme in which the record of each authorization is controlled by another authorization, resulting in a hierarchical tree of authorizations.
- **Permission:** A particular form of allowed access, e.g., permission to READ as contrasted with permission to WRITE.

Glossary

- **Prescript:** A rule that must be followed before access to an object is permitted, thereby introducing an opportunity for human judgment about the need for access, so that abuse of the access is discouraged.
- **Principal:** The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system.
- **Privacy:** The ability of an individual (or organization) to decide whether, when, and to whom personal (or organizational) information is released.
- **Propagation:** When a principal, having been authorized access to some object, in turn authorizes access to another principal.
- **User:** Used imprecisely to refer to the individual who is accountable for some identifiable set of activities in a computer system.

Security definition

- The NIST Computer Security Handbook defines *computer security* as:
  - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources

Computer Security Triad

- Three key objectives are at the heart of computer security
  - Confidentiality; Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - Integrity; Assures that information and programs are changed only in a specified and authorized manner
  - Availability; Assures that systems work promptly and service is not denied to authorized users.

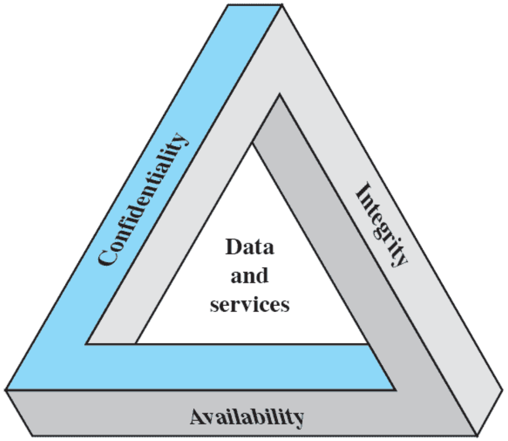


Figure 14.1 The Security Requirements Triad

Additional Concepts

- Two further concepts are often added to the core of computer security
  - Authenticity; verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
  - Accountability; supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

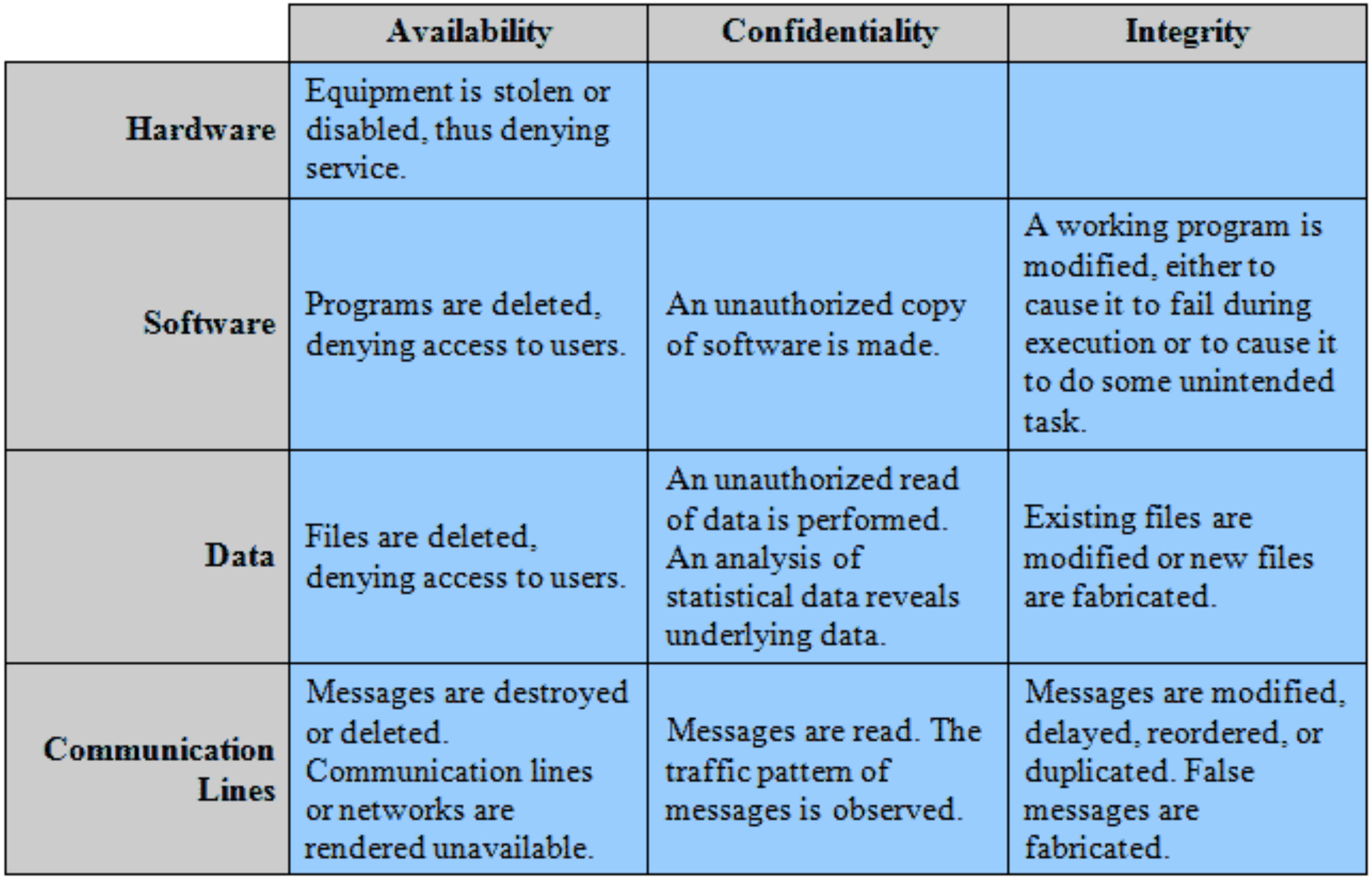
Threats

- RFC 2828, describes four kinds of threat consequences
  - Unauthorised Disclosure; an unauthorized entity gains access to data.
  - Deception; receiving false data from unauthorized entity and beleiving it to be true.
  - Disruption; interrupts or prevents the correct operation of system services and functions.
  - Usurpation; results in control of system services or functions by an unauthorized entity.

Assets

- The assets of a computer system can be categorized as
  - hardware,
  - software,
  - data,
  - communication lines and networks.

Assets in Relation to the CIA Triad



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Basic Principles of Information Protection

General Observations:

- Every day new applications are developed and these involve both storing information and simultaneous use by several individuals.
- The key concern is multiple use requirement of these applications.
- All users should not have identical authority, some scheme is needed to ensure that the computer system implements the desired authority structure.

For example: *credit bureau data banks; law enforcement information systems; time-sharing service bureaus; on-line medical information systems; and government social service data processing systems.*

These examples span a wide range of needs for organizational and personal privacy.

All have in common controlled sharing of information among multiple users.

Basic Principles of Information Protection

1) General Observations:

The potential security violations in three categories.

1) **Unauthorized information release:** an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to "*traffic analysis*," in which the intruder observes only the *patterns of information use and from those patterns can infer some information content.* It also includes unauthorized use of a proprietary program.

2) **Unauthorized information modification:** an unauthorized person is able to *make changes in stored information*--a form of sabotage.

3) **Unauthorized denial of use:** *an intruder can prevent an authorized user from referring to or modifying information*, even though the intruder may not be able to refer to or modify the information. Causing a system "crash". This is another form of sabotage.

The term "**unauthorized**" in the three categories listed above means that release, modification, or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system.

Basic Principles of Information Protection

- The term ***protection*** to be just *security techniques that control the access of executing programs to stored information*.
  - An example of a protection technique is labeling of computer-stored files with lists of authorized users.
- Similarly, the term ***authentication*** is used for those security techniques that *verify the identity of a person* (or other external agent) making a request of a computer system.
- The **objective** of a ***secure system*** is to *prevent all unauthorized use of information, a negative kind of requirement*.

Basic Principles of Information Protection

2) Functional Levels of Information Protection:

It is convenient to divide protection schemes according to their functional properties.

- **All-or-nothing systems**: These are systems that *provide isolation of users*, sometimes moderated by total sharing of some pieces of information. More commonly, *such systems also have public libraries to which every user may have access*.

- **Controlled sharing:** Significantly more complex machinery is required to control explicitly *who may access each data item stored in the system*.
  - For example, such a system might provide each file with a list of authorized users and allow an owner to distinguish several common patterns of use, such as reading, writing, or executing the contents of the file as a program.

Basic Principles of Information Protection

2) Functional Levels of Information Protection:

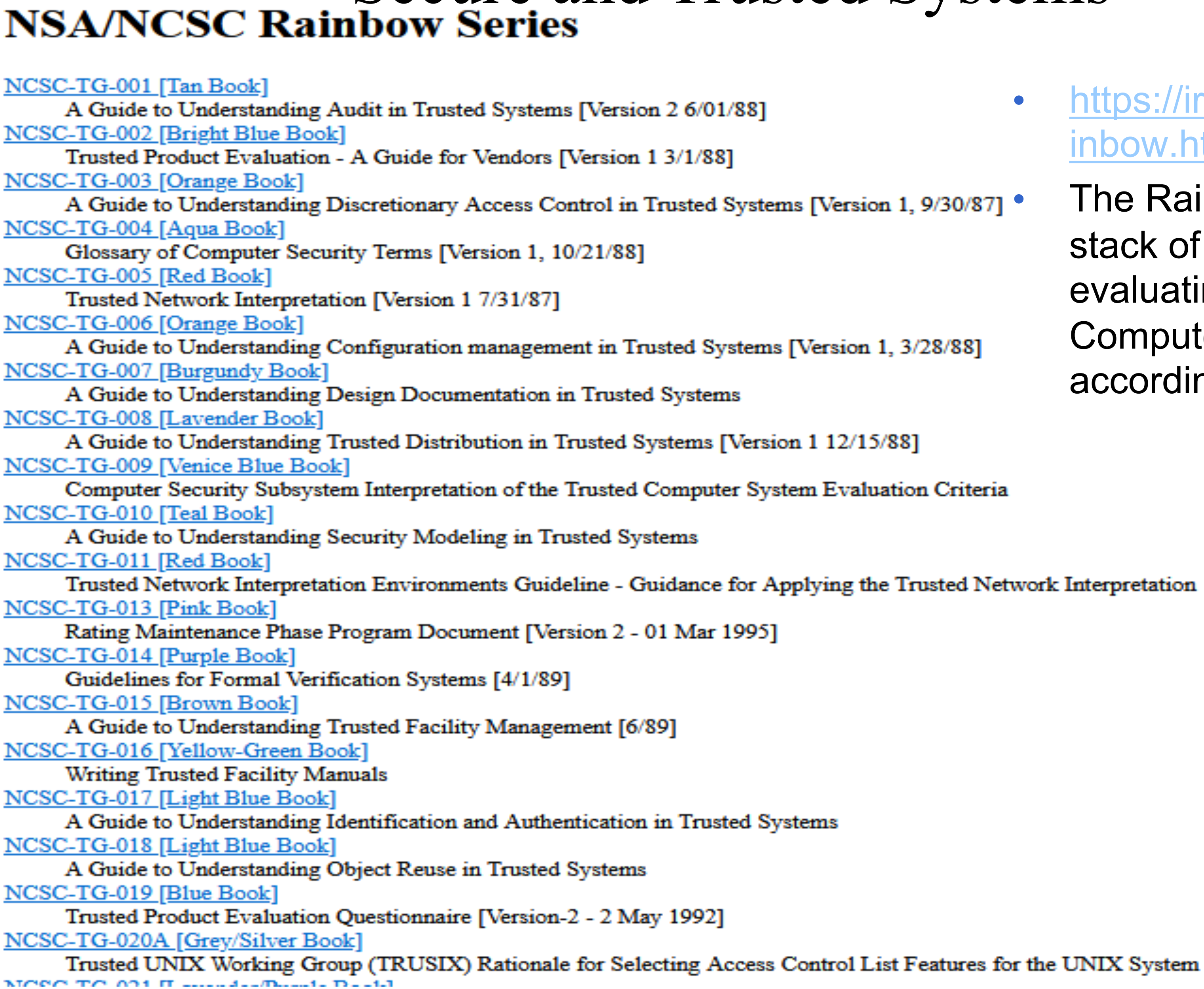
- **User-programmed sharing controls:** *A user may want to restrict access to a file in a way not provided in the standard facilities for controlling sharing*. A protected subsystem is a collection of programs and data with the property that only the programs of the subsystem have direct access to the data (that is, the protected objects).
  - For example, he may wish to permit access only on weekdays between 9:00 A.M. and 4:00 P.M. Possibly, he may wish to permit access to only the average value of the data in a file. Maybe he wishes to require that a file be modified only if two users agree. For such cases, and a myriad of others, a general escape is to provide for user-defined protected objects and subsystems.
- A specialized use of *protected subsystems* is the implementation of protection controls based on data content.
  - For example, in a file of salaries, one may wish to permit access to all salaries under $15 000. Another example is permitting access to certain statistical aggregations of data but not to any individual data item.

Basic Principles of Information Protection

2) Functional Levels of Information Protection:

- **Putting strings on information:** The previous three levels have been concerned with establishing conditions for the release of information to an executing program. This fourth level of capability is to maintain some control over the user of the information even after it has been released.
  - For example; The printed labels on classified military information declaring a document to be "Top Secret" are example of a constraint on information after its release to a person authorized to receive it.

Reference Sites for Secure and Trusted Systems



NSA/NCSC Rainbow Series

NCSC-TG-001 [Tan Book]
A Guide to Understanding Audit in Trusted Systems [Version 2 6/01/88]
NCSC-TG-002 [Bright Blue Book]
Trusted Product Evaluation - A Guide for Vendors [Version 1 3/1/88]
NCSC-TG-003 [Orange Book]
A Guide to Understanding Discretionary Access Control in Trusted Systems [Version 1, 9/30/87]
NCSC-TG-004 [Aqua Book]
Glossary of Computer Security Terms [Version 1, 10/21/88]
NCSC-TG-005 [Red Book]
Trusted Network Interpretation [Version 1 7/31/87]
NCSC-TG-006 [Orange Book]
A Guide to Understanding Configuration management in Trusted Systems [Version 1, 3/28/88]
NCSC-TG-007 [Burgundy Book]
A Guide to Understanding Design Documentation in Trusted Systems
NCSC-TG-008 [Lavender Book]
A Guide to Understanding Trusted Distribution in Trusted Systems [Version 1 12/15/88]
NCSC-TG-009 [Venice Blue Book]
Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria
NCSC-TG-010 [Teal Book]
A Guide to Understanding Security Modeling in Trusted Systems
NCSC-TG-011 [Red Book]
Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation
NCSC-TG-013 [Pink Book]
Rating Maintenance Phase Program Document [Version 2 - 01 Mar 1995]
NCSC-TG-014 [Purple Book]
Guidelines for Formal Verification Systems [4/1/89]
NCSC-TG-015 [Brown Book]
A Guide to Understanding Trusted Facility Management [6/89]
NCSC-TG-016 [Yellow-Green Book]
Writing Trusted Facility Manuals
NCSC-TG-017 [Light Blue Book]
A Guide to Understanding Identification and Authentication in Trusted Systems
NCSC-TG-018 [Light Blue Book]
A Guide to Understanding Object Reuse in Trusted Systems
NCSC-TG-019 [Blue Book]
Trusted Product Evaluation Questionnaire [Version-2 - 2 May 1992]
NCSC-TG-020A [Grey/Silver Book]
Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System
NCSC-TG-021 [Lavender/Purple Book]

- https://irp.fas.org/nsa/rainbow.htm
- The Rainbow Series is stack of books on evaluating "Trusted Computer Systems" according to the NSA.

Reference Sites for Secure and Trusted Systems

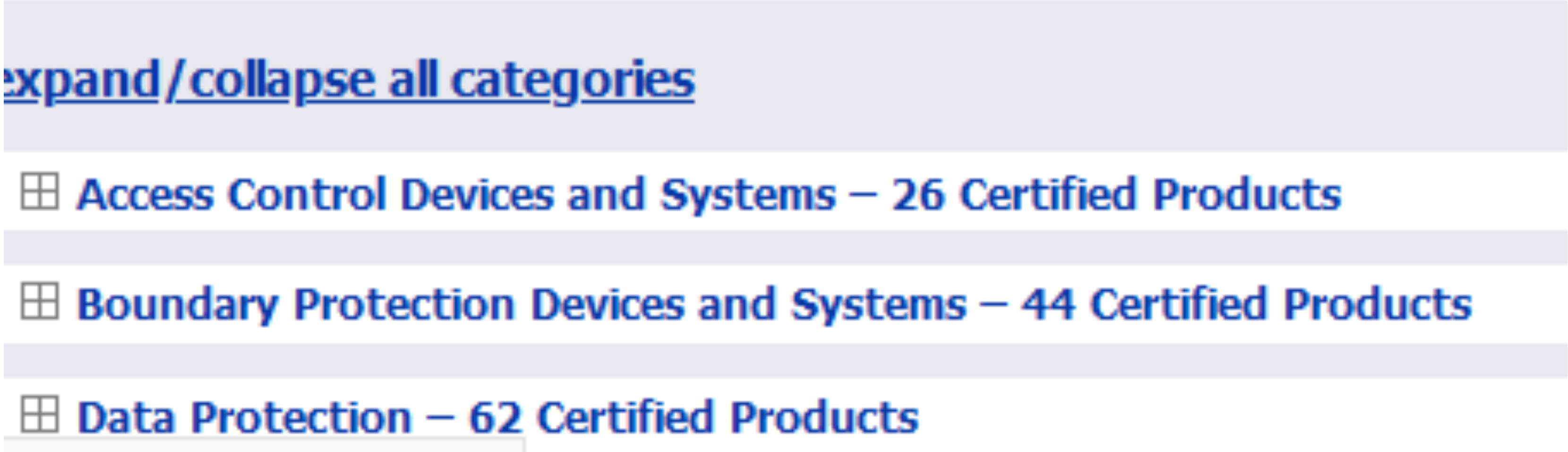
- The common criteria
  - Lists all evaluated protection profiles and products
  - https://www.commoncriteriaportal.org/index.cfm?
- The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA).

Reference Sites for Secure and Trusted Systems

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- These certificates are recognized by all the signatories of the CCRA.

Reference Sites for Secure and Trusted Systems

- https://www.commoncriteriaportal.org/products/#AC
- Certificates will remain on the CPL for five years



xpand/collapse all categories

⊞ Access Control Devices and Systems – 26 Certified Products

⊞ Boundary Protection Devices and Systems – 44 Certified Products

⊞ Data Protection – 62 Certified Products