Information Security

Dr./ Ahmed Mohamed Rabie

طريقة الدخول للمقرر الدراسي عبر صفحة الانترنت


كليات الجامعة
كلية التربية
كلية العلوم
كلية التجارة
كلية الآداب
كلية الزراعة
كلية التربية النوعية
كلية التربية الرياضية
كلية الفنون التطبيقية
كلية الهندسة
كلية الحقوق
كلية الآثار
كلية التمريض
كلية الحاسبات والمعلومات

7		د / أحمد محمد ربيع سيد	تكنولوجيا المعلومات	مدرس

أحمد محمد ربيع سيد
كلية الحاسبات والمعلومات

البيانات الشخصية

الوظيفة : مدرس
القسم : تكنولوجيا المعلومات
التخصص :
هاتف العمل :
البريد الإلكتروني : amrabie@du.edu.eg

المقررات الدراسية

الأبحاث العلمية علي موقع الجامعه

There is no research

السيرة الذاتية

الموقع الشخصي


تمهيدي ماجستير فنون تطبيق
Wireless and Mobile Netwo
Communication Terchnology
Inbternet Applications
Information Security

Course Description

المرفقات:

1 - تحميل الملف

26-02-2022 06:27

0

اقرأ المزيد

Lecture 1

26-02-2022 06:28

0

اقرأ المزيد

عدد الصفحات (1):

1

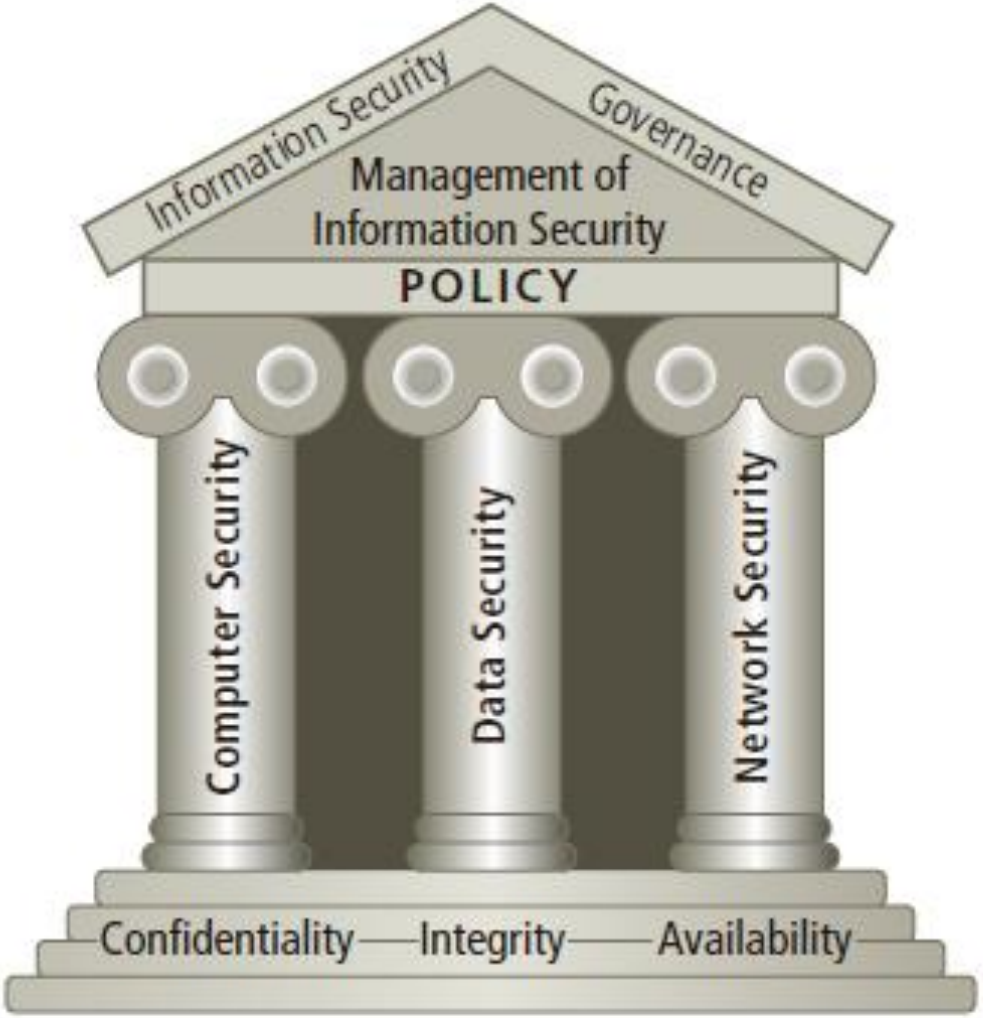
رابط الموقع الشخصي

http://staff.du.edu.eg/1058

Chapter 1

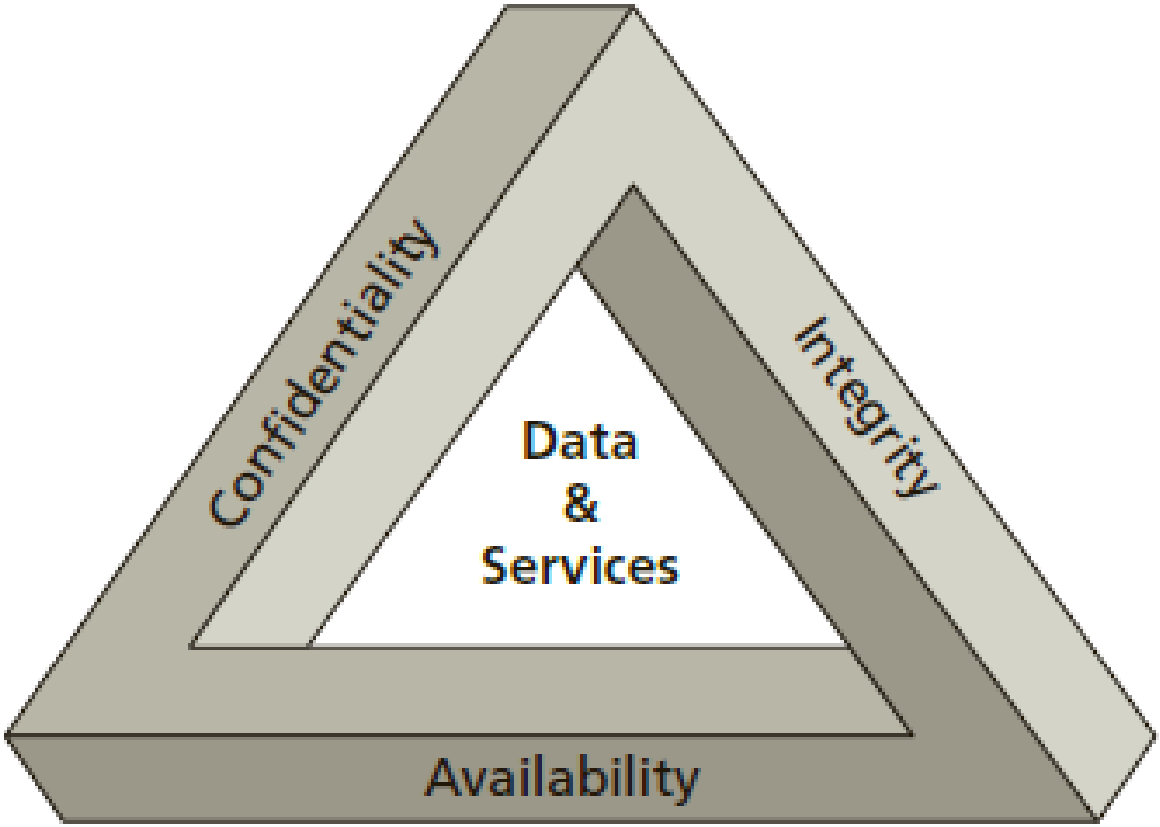
Introduction to Information Security

The Committee on National Security Systems (CNSS) defines **information security** as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information. Information security includes the broad areas of information security management, data security, and network security.



Components of information security

The C.I.A. triad has been the standard for computer security in both industry and government since the development of the mainframe. This standard is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics is as important today as it has always been, but the C.I.A. triad model is generally viewed as no longer adequate in addressing the constantly changing environment.



The C.I.A. triad

Confidentiality To ensure confidentiality, you must prevent the disclosure of data or information to unauthorized entities.

Integrity: The second part of the CIA triad, ensures that data is protected from unauthorized modification or data corruption.

Availability means ensuring that data is accessible when and where it is needed.

Protection Mechanisms

Protection mechanisms are common characteristics of security controls. Not all security controls must have them, but many controls offer their protection for confidentiality, integrity, and availability through the use of these mechanisms. These mechanisms include using multiple layers or levels of access, employing abstraction, hiding data, and using encryption.

1- Layering: Layering, also known as defense in depth, is simply the use of multiple controls in a series. No one control can protect against all possible threats. Using a multilayered solution allows for numerous, different controls to guard against whatever threats come to pass. When security solutions are designed in layers, most threats are eliminated, mitigated, or thwarted.

Layering also includes the concept that networks comprise numerous separate entities, each with its own unique security controls and vulnerabilities. In an effective security solution, there is a synergy between all networked systems that creates a single security front. Using separate security systems creates a layered security solution.

2- Abstraction is used for efficiency. Similar elements are put into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective. Thus, the concept of abstraction is used when classifying objects or assigning roles to subjects. The concept of abstraction also includes the definition of object and subject types or of objects themselves (that is, a data structure used to define a template for a class of entities).

Abstraction is used to define what types of data an object can contain, what types of functions can be performed on or by that object, and what capabilities that object has. Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function.

3- Data hiding is exactly what it sounds like: preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject. Forms of data hiding include keeping a database from being accessed by unauthorized visitors and restricting a subject at a lower classification level from accessing data at a higher classification level.

Preventing an application from accessing hardware directly is also a form of data hiding. Data hiding is often a key element in security controls as well as in programming.

4- Encryption is the art and science of hiding the meaning or intent of a communication from unintended recipients. Encryption can take many forms and be applied to every type of electronic communication, including text, audio, and video files as well as applications themselves.

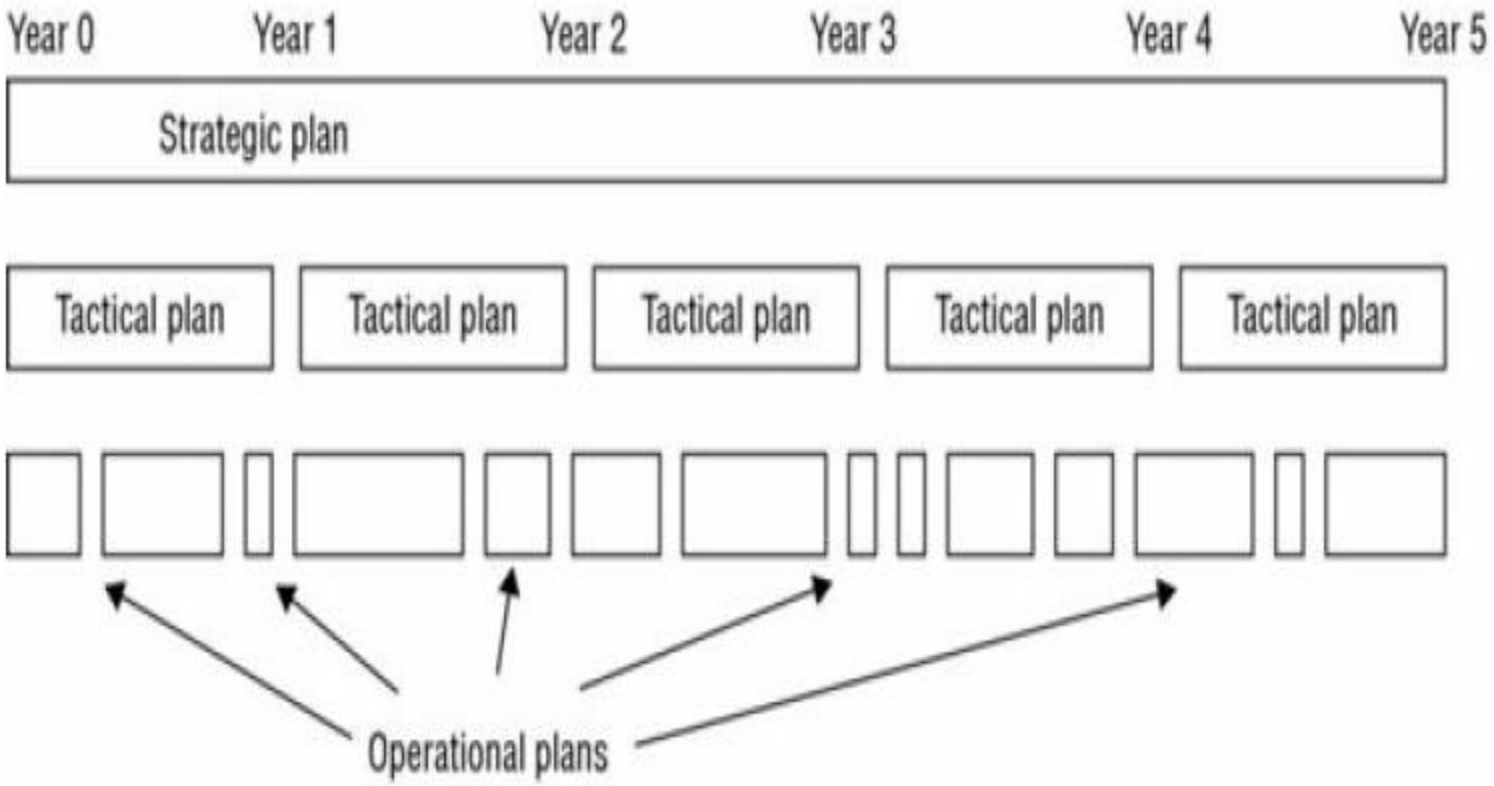
Encryption is an important element in security controls, especially in regard to the transmission of data between systems. There are various strengths of encryption, each of which is designed and/or appropriate for a specific use or purpose.

The information security (InfoSec) team should be led by a designated chief security officer (CSO) who must report directly to senior management. Placing the autonomy of the CSO and the CSO's team outside the typical hierarchical structure in an organization can improve security management across the entire organization. It also helps to avoid cross-department and internal political issues.

Security Management Planning

Security management planning team should develop three types of plans.

1- Strategic Plan: A strategic plan is a long-term plan that is fairly stable. It defines the organization's security purpose. It also helps to understand security function and align it to goals, mission, and objectives of the organization. It's useful for about five years if it is maintained and updated annually.



Strategic, tactical, and operational plan timeline comparison

2- Tactical plan: The tactical plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan or can be crafted ad-hoc based upon unpredicted events. A tactical plan is typically useful for about a year and often prescribes and schedules the tasks necessary to accomplish organizational goals. Some examples of tactical plans are project plans, acquisition plans, hiring plans, budget plans, maintenance plans, support plans, and system development plans.

3- Operational Plan An operational plan is a short-term, highly detailed plan based on the strategic and tactical plans. It is valid or useful only for a short time. Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans spell out how to accomplish the various goals of the organization. They include resource allotments, budgetary requirements, staffing assignments, scheduling, and step-by-step or implementation procedures.

Operational plans include details on how the implementation processes are in compliance with the organization's security policy. Examples of operational plans are training plans, system deployment plans, and product design plans.

Security is a continuous process. Thus, the activity of **security management planning** may have a definitive initiation point, but its tasks and work are never fully accomplished or complete. Effective security plans focus attention on specific and achievable objectives, anticipate change and potential problems, and serve as a basis for decision making for the entire organization. Security documentation should be concrete, well defined, and clearly stated. For a security plan to be effective, it must be developed, maintained, and actually used.

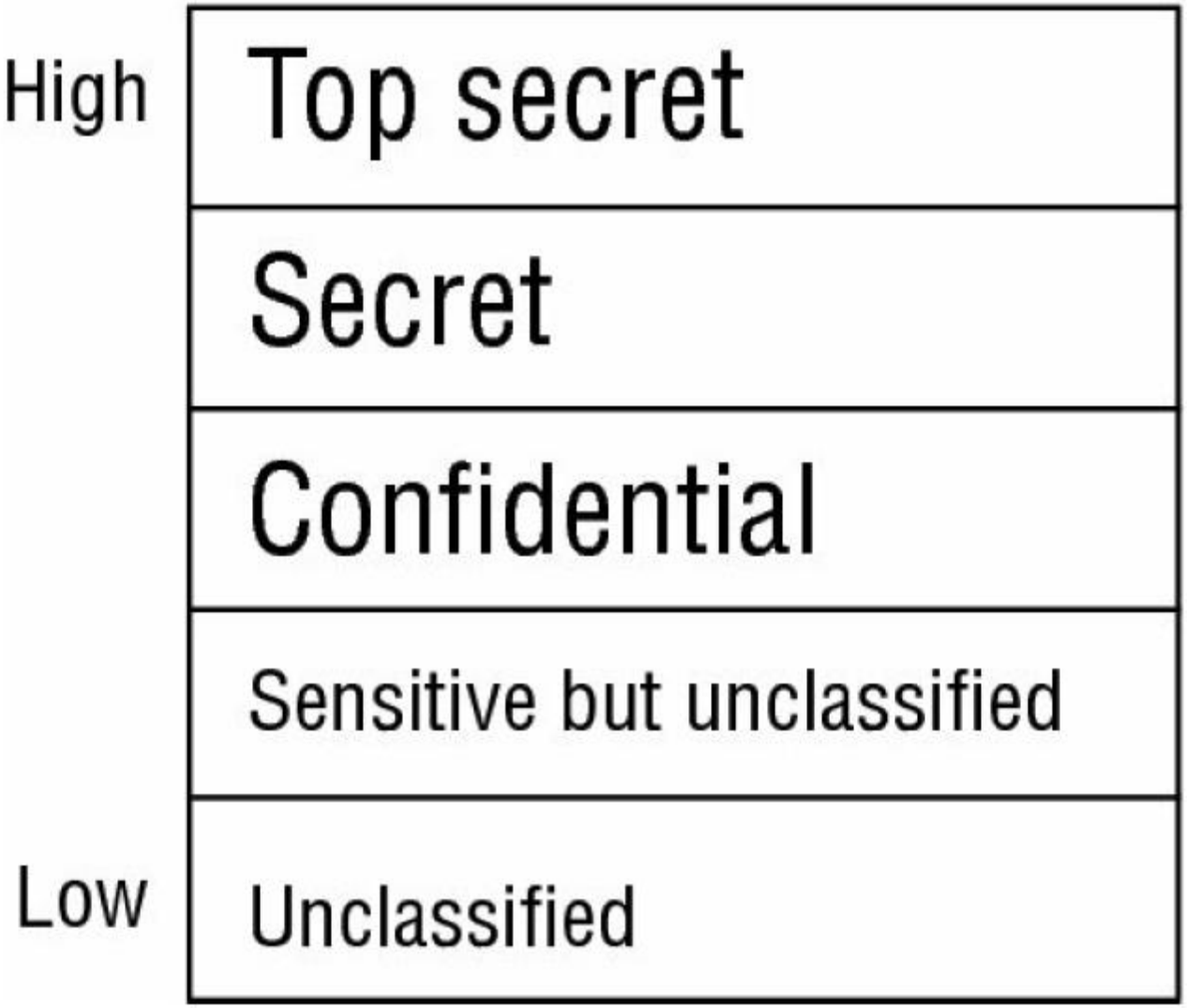
Data Classification

Data classification, or categorization, is the primary means by which data is protected based on its need for secrecy, sensitivity, or confidentiality. It is inefficient to treat all data the same way when designing and implementing a security system because some data items need more security than others. Securing everything at a low security level means sensitive data is easily accessible. Securing everything at a high security level is too expensive and restricts access to unclassified, noncritical data.

Data classification, or categorization, is the process of organizing items, objects, subjects, and so on into groups, categories, or collections with similarities. These similarities could include value, cost, sensitivity, risk, vulnerability, power, privilege, possible levels of loss or damage, or need to know. The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity. Data classification is used to provide security mechanisms for storing, processing, and transferring data.

The two common classification schemes are government/military classification and commercial business/private sector classification. There are five levels of government/military classification (listed here from highest to lowest):

Top Secret The highest level of classification. The unauthorized disclosure of top-secret data will have drastic effects and cause grave damage to national security.



- Levels of government/military classification

Secret Used for data of a restricted nature. The unauthorized disclosure of data classified as secret will have significant effects and cause critical damage to national security.

Confidential Used for data of a private, sensitive, proprietary, or highly valuable nature. The unauthorized disclosure of data classified as confidential will have noticeable effects and cause serious damage to national security. This classification is used for all data between secret and sensitive but unclassified classifications.

Unclassified The lowest level of classification. This is used for data that is neither sensitive nor classified. The disclosure of unclassified data does not compromise confidentiality or cause any noticeable damage.