CS 526 Homework 6 Solutions

Q1) Common Criteria (3 points)

Identify specific requirements in the Common Criteria that are relevant to the *Principle of Fail-Safe Defaults*.

The principle of fail-safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object.

The CC (common criterion) defines a set of constructs which classify security requirements into related sets called components. The CC functional requirements (CC part 2) define desired security behaviors. Assurance requirements (CC part 3) are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

For every class in CC functional requirement, we discuss the relevance of principle of fail-safe defaults as follows:

Audit (FAU)
Security auditing involves recognizing, recording, storing and analyzing information related to security activities. Audit records are produced by these activities, and can be examined to determine their security relevance. The class is made up of families, which define, amongst other things, requirements for the selection of auditable events, the analysis of audit records, their protection and their storage. *FAU is not very related to principle of fail-safe defaults* since it just log the security activities, but not grant or deny access to that object.

Communications (FCO)
The communications class provides two families concerned with assuring the identity of a party participating in data exchange. The families are concerned with non-repudiation by the originator and by the recipient of data. *FCO, including non-repudiation of origin FCO_NRO and non-repudiation of receipt (FCO_NRR), is related to principle of failsafe defaults* since it is necessary to assure the identity of a party participating in data exchange before applying the principle of fail-safe defaults.

Cryptographic Support (FCS)
This class is used when the TOE (Target of evaluation) implements cryptographic functions. These may be used, for example, to support communications, identification and authentication, or data separation. The two families cover the operational use and management of cryptographic keys. *FCS is not very related to principle of fail-safe defaults* since it just provide cryptographic support, which is necessary for securely granting or denying access, but not the operations as granting and denying itself..

User Data Protection (FDP)

This class contains families specifying requirements relating to the protection of user data. These families address user data within the TOE during import, export and storage, in addition to security attributes related to user data. *Some families in this class are related to principle of fail-safe defaults. User data protection security function policies, including FDP_ACC and FDP_IFC, and forms of user data protection, including FDP_ACF, FDP_IFF, FDP_ITT, FDP_RIP, FDP_ROL, FDP_SDI, are related since it involves the access control policy and functions. But off-line storage, import and export (FDP_DAU, FDP_ETC, FDP_ITC), and Inter-TSF communications including data confidentiality and integrity are not related for not involving identity assurance and granting and denying mechanisms.*

Identification and Authentication (FIA)

The requirements for identification and authentication ensure the unambiguous identification of authorized users and the correct association of security attributes with users and subjects. Families in this class deal with determining and verifying user identity, determining their authority to interact with the TOE, and with the correct association of security attributes with the authorized user. *FIA is related to principle of fail-safe defaults* since it is necessary to assure the identity of a party participating in data exchange before applying the principle of fail-safe defaults.

Security Management (FMT)

This class is used to specify the management of TSF security attributes data and functions. Different management roles and their interaction, such as separation of capability, can be defined. The class is used to cover the management aspects of other functional classes.

FMT is related to principle of fail-safe defaults since management of security attribute is able to affect access control matrix.

Privacy (FPR)

Privacy requirements provide a user with protection against discovery and misuse of this identity by other users. The families in this class are concerned with anonymity, pseudonymity, unlinkability and unobservability. *FPR is not very related to principle of fail-safe defaults* since FPR_ANO ensures that a user may use a resource or service without disclosing the user's identity. FPR_PSE ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use. FPR_UNL a user may make multiple uses of resources or services without others being able to link these uses together. FPR_UNO ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Protection of the TOE Security Functions (FPT)

This class is focused on protection of TSF (TOE security functions) data, rather than of user data. The class relates to the integrity and management of the TSF mechanisms and data. *FPT is not very related to principle of fail-safe defaults* since it focuses on the integrity and management of TSF mechanisms but not on the identity of a party participating in data exchange and granting or denying access to objects.

Resource Utilization (FRU)

Resource utilization provides three families which support the availability of required resources, such as processing capability and storage capacity. The families detail requirements for fault tolerance, priority of service and resource allocation. *FRU is not very related to principle of fail-safe defaults* since it focuses on the resource utilization but not on the identity of a party participating in data exchange and granting or denying access to objects.

TOE Access (FTA)

This class specifies functional requirements, in addition to those specified for identification and authentication, for controlling the establishment of a user's session. The requirements for TOE access govern such things as limiting the number and scope of user sessions, displaying the access history and the modification of access parameters**.** *FTA is related to principle of fail-safe defaults* since it is able to control TOE access.

Trusted Path/Channels (FTP)

This class is concerned with trusted communications paths between the users and the TSF, and between TSFs. Trusted paths are constructed from trusted channels, which exist for inter-TSF communications; this provides a means for users to perform functions through a direct interaction with the TSF. The user or TSF can initiate the exchange, which is guaranteed to be protected from modification by un-trusted applications. *FTP is related to principle of fail-safe defaults* since it is able to control interaction between user and TSF.

For every assurance class in CC assurance requirement, we discuss the relevance of principle of fail-safe defaults as follows:

Configuration Management (ACM)

Configuration management requires that the integrity of the TOE is adequately preserved. Specifically, configuration management provides confidence that the TOE and documentation used for evaluation are the ones prepared for distribution. The families in this class are concerned with the capabilities of the CM, its scope and automation. *ACM is related to principle of fail-safe defaults* since it ensures that all change is authorized.

Delivery and Operation (ADO)

This class provides families concerned with the measures, procedures and standards for securing delivery, installation and operational use of the TOE, to ensure that the security protection offered by the TOE is not compromised during these events. *ADO is not related to principle of fail-safe defaults* since it concerns the correct delivery, installation, generation, and start-up of the TOE.

Assurance Maintenance

Class Maintenance of Assurance (AMA)

This class provides requirements that are intended to be applied after a TOE has been certified against the CC. These requirements are aimed at assuring that the TOE will continue to meet its security target as changes are made to the TOE or its environment. The class contains four families. The first covers the content of the assurance maintenance plan, which covers the nature of proposed changes and the controls which govern them. *This is not related to principle of fail-safe defaults*. The second family covers the security categorization of TOE components. *This is not related to principle of fail-safe defaults*. The third and fourth cover the analysis of changes for security impact, and the provision of evidence that procedures are being followed. *These are not related to principle of fail-safe defaults.* This class provides building blocks for the establishment of assurance maintenance schemes.

Protection Profile Evaluation (APE)

The goal here is to demonstrate that the PP is complete, consistent and technically sound. Further, the PP needs to be a statement of the requirements for an evalutable TOE. The families in this class are concerned with the TOE Description, the Security Environment, the Security Objectives and the TOE Security Requirements. *This is not related to principle of fail-safe defaults.*

Development (ADV)

The families of this class are concerned with the refinement of the TSF from the specification defined in the ST to the implementation, and a mapping from the security requirements to the lowest level representation. *This is slightly related to principle of failsafe defaults as it concerns the underlying implementation mechanisms for correctly enforcing principle of fail-safe defaults.*

Guidance Documents (AGD)

Guidance documents are concerned with the secure operational use of the TOE, by the users and administrators. *This is slightly related to principle of fail-safe defaults since it may affect the operational documents.*

Life Cycle Support (ALC)

The requirements of the families concerned with the life-cycle of the TOE include lifecycle definition, tools and techniques, security of the development environment and the remediation of flaws found by TOE consumers. *This is related to principle of fail-safe defaults since during life cycle support; some flaws in underlying implementation related to fail-safe defaults might be identified and fixed.*

Security Target Evaluation (ASE)

The goal here is to demonstrate that the ST is complete, consistent and technically sound, and is a suitable basis for the TOE evaluation. The requirements for the families of this class are concerned with the TOE Description, the Security Environment, the Security

Objectives, any PP Claims, the TOE Security Requirements and the TOE Summary Specification. *This is not related to principle of fail-safe defaults.*

Tests (ATE)
This class is concerned with demonstrating that the TOE meets its functional requirements. The families address coverage and depth of developer testing, and requirements for independent testing. *This is slightly related to principle of fail-safe defaults. The "slightly" means the tests may expose some flaws on the underlying implementation mechanisms for fail-safe defaults.*

Vulnerability Assessment (AVA)
This class defines requirements directed at the identification of exploitable vulnerabilities, which could be introduced by construction, operation, misuse or incorrect configuration of the TOE. The families identified here are concerned with identifying vulnerabilities through covert channel analysis, analysis of the configuration of the TOE, examining the strength of mechanisms of the security functions, and identifying flaws introduced during development of the TOE. *This is related to principle of fail-safe defaults. Vulnerability assessment may expose some flaws on the underlying implementation mechanisms for fail-safe defaults.*

TA's note: It was enough to point to the classes and make a short explanation of the relevance to get full credit. Points have been cut off from those answers that either lack substantial coverage of relevant classes or lack of explanation.

Extra points have been given for very detailed coverage of relevant classes.

Q2) 26.9.3 (a) (2 points)

Consider the scheme used to allow customers to submit their credit card and order information. Section 26.3.3.2 states that the enciphered version of the data is stored in a spooling area that the Web server cannot access. Why is the file kept inaccessible to the Web server?

The web server does not need to know about the enciphered files once they are made so hence it should have no access to them. This demonstrates the principle of least privilege.

Also since the files are made by the web server but are then stored in the spooling area, it takes more than one subject to handle the order information. This goes along with principle of separation of privilege. So if the web server were to be hacked, the order files that contain the order information are still out of reach.

The files are encrypted, so that even when they are compromised, the customer information cannot be obtained. This follows the “principle of fail-safe defaults”.

TA’s note: To obtain full credit it is necessary to cite the “principle of least privilege” or explain why the web-server does not need to know the credit card and order information. Also, “separation of privilege” and “principle of fail-safe defaults” were keywords that would fit in the answer.

Q3) 26.9.5 (3 points)

(Courtesy of Steve Mellema)

A security analyst wishes to deploy intrusion detection monitors to determine if any attackers penetrate the Drib's network.

a) Where should the intrusion detection monitors be placed in the network's topology and why?

The monitors should be placed at the inner and outer firewalls. All traffic to and from the outside world has to be filtered through the firewalls, so a monitor has the ability to see all of the data transfer if it resides at these locations. Any attempts to penetrate the Drib network will be recorded by the monitors for evaluation.

b) If the analyst wished to monitor insider attacks (that is, attacks by people with access to Drib's internal network), how would your answer to part (a) change (it at all)? Justify your changes (or lacks of changes).

There would be a change in the configuration. The monitors would not only be placed on the inner and outer firewalls, but also on each of the customer data, corporate data, and development subnet firewalls. No data can pass through the internal network without being viewed by these firewalls, so they should be monitored to look for insider attacks. We keep the monitors on the inner and outer firewalls because a record of the traffic from an alleged attacker to the DMZ and Internet is helpful in determining whether or not allegations are true.

TA's note: For part a, the DMZ side of the outer firewall was enough to get full credit. For part b, each subnet must have an IDS to monitor insider attacks.