It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:

physical attack of various forms (microprobing, drills, files, solvents, etc.)

freezing the device

applying out-of-spec voltages or power surges

applying unusual clock signals

inducing software errors using radiation

measuring the precise time and power requirements of certain operations (see power analysis)

Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of- specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.

Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos).

Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 72
What security model implies a central authority that define rules and sometimes global rules, dictating what subjects can have access to what objects?

A. Flow Model
B. Discretionary access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: D
Explanation:
As a security administrator you might configure user profiles so that users cannot change the system's time, alter system configuration files, access a command prompt, or install unapproved applications. This type of access control is referred to as nondiscretionary, meaning that access decisions are not made at the discretion of the user. Nondiscretionary access controls are put into place by an authoritative entity (usually a security administrator) with the goal of protecting the organization's most critical assets.

Non-discretionary access control is when a central authority determines what subjects can have access to what objects based on the organizational security policy. Centralized access control is not an existing security model.

Both, Rule Based Access Control (RuBAC or RBAC) and Role Based Access Controls (RBAC) falls into this category.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 221). McGraw- Hill. Kindle Edition.
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 73
Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

A. Division D
B. Division C
C. Division B
D. Division A

Correct Answer: A
Explanation:
The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security.

Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information.

Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess.

Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security- relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB).

Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process.

TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:

Division D - minimal security
Division C - discretionary protection
Division B - mandatory protection
Division A - verified protection

Reference:
page 358 AIO V.5 Shon Harris
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 197.

Also:

THE source for all TCSEC "level" questions:
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

QUESTION 74
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:

A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative

Correct Answer: B
Explanation:
The detective/technical control measures are intended to reveal the violations of security policy using technical means.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 75
Which TCSEC level is labeled Controlled Access Protection?

A. C1
B. C2
C. C3
D. B1

Correct Answer: B
Explanation:
C2 is labeled Controlled Access Protection.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security.

Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.
D -- Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C -- Discretionary protection

C1 -- Discretionary Security Protection
Identification and authentication
Separation of users and data
Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
Required System Documentation and user manuals
C2 -- Controlled Access Protection
More finely grained DAC

Individual accountability through login procedures
Audit trails
Object reuse
Resource isolation

B -- Mandatory protection

B1 -- Labeled Security Protection
Informal statement of the security policy model
Data sensitivity labels
Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities
All discovered flaws must be removed or otherwise mitigated Design specifications and verification
B2 -- Structured Protection
Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened
Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed B3 -- Security Domains
Satisfies reference monitor requirements
Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined
Audit security-relevant events
Automated imminent intrusion detection, notification, and response Trusted system recovery procedures
Covert timing channels are analyzed for occurrence and bandwidth An example of such a system is the XTS-300, a precursor to the XTS-400

A -- Verified protection

A1 -- Verified Design
Functionally identical to B3
Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures
An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400
Beyond A1
System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).
Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.
Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.

Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

The following are incorrect answers:

C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.

Reference(s) used for this question:

HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

And AIOv4 Security Architecture and Design (pages 357 - 361) AIOv5 Security Architecture and Design (pages 358 - 362)

QUESTION 76
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:

A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.

Correct Answer: C
Explanation:
Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

QUESTION 77
The Orange Book is founded upon which security policy model?

A. The Biba Model
B. The Bell LaPadula Model
C. Clark-Wilson Model
D. TEMPEST

Correct Answer: B
Explanation:
From the glossary of Computer Security Basics:
The Bell-LaPadula model is the security policy model on which the Orange Book requirements are based. From the Orange Book definition, "A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving the system is secure. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode." The Biba Model is an integrity model of computer security policy that describes a set of rules. In this model, a subject may not depend on any object or other subject that is less trusted than itself.
The Clark Wilson Model is an integrity model for computer security policy designed for a commercial environment. It addresses such concepts as nondiscretionary access control, privilege separation, and least privilege. TEMPEST is a government program that prevents the