((ISC)2 Press) (Kindle Locations 1989-2002). Auerbach Publications. Kindle Edition.

QUESTION 202
What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?

A. Micrometrics
B. Macrometrics
C. Biometrics
D. MicroBiometrics

Correct Answer: C
Explanation:
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 203
RADIUS incorporates which of the following services?

A. Authentication server and PIN codes.
B. Authentication of clients and static passwords generation.
C. Authentication of clients and dynamic passwords generation.
D. Authentication server as well as support for Static and Dynamic passwords.

Correct Answer: D
Explanation:
A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to
designated RADIUS servers, and then acting on the response which is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all
configuration information necessary for the client to deliver service to the user.

RADIUS authentication is based on provisions of simple username/password credentials. These credentials are encrypted
by the client using a shared secret between the client and the RADIUS server. OIG 2007, Page 513

RADIUS incorporates an authentication server and can make uses of both dynamic and static passwords.

Since it uses the PAP and CHAP protocols, it also incluses static passwords.

RADIUS is an Internet protocol. RADIUS carries authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server. RADIUS features and functions are described primarily in the IETF (International Engineering Task Force) document RFC2138.

The term " RADIUS" is an acronym which stands for Remote Authentication Dial In User Service.

The main advantage to using a RADIUS approach to authentication is that it can provide a stronger form of authentication. RADIUS is capable of using a strong, two-factor form of authentication, in which users need to possess both a user ID and a hardware or software token to gain access.

Token-based schemes use dynamic passwords. Every minute or so, the token generates a unique 4-, 6- or 8-digit access number that is synchronized with the security server. To gain entry into the system, the user must generate both this one-time number and provide his or her user ID and password.

Although protocols such as RADIUS cannot protect against theft of an authenticated session via some realtime attacks, such as wiretapping, using unique, unpredictable authentication requests can protect against a wide range of active attacks.
RADIUS: Key Features and Benefits
Features Benefits

RADIUS supports dynamic passwords and challenge/response passwords.

Improved system security due to the fact that passwords are not static.

It is much more difficult for a bogus host to spoof users into giving up their passwords or password-generation algorithms.

RADIUS allows the user to have a single user ID and password for all computers in a network.

Improved usability due to the fact that the user has to remember only one login combination.

RADIUS is able to:

Prevent RADIUS users from logging in via login (or ftp).
Require them to log in via login (or ftp)
Require them to login to a specific network access server (NAS);
Control access by time of day.

Provides very granular control over the types of logins allowed, on a per-user basis.

The time-out interval for failing over from an unresponsive primary RADIUS server to a backup RADIUS server is site-configurable.

RADIUS gives System Administrator more flexibility in managing which users can login from which hosts or devices.

Stratus Technology Product Brief
http://www.stratus.com/products/vos/openvos/radius.htm

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 43, 44.

Also check: MILLER, Lawrence & GREGORY, Peter, CISSP for Dummies, 2002, Wiley Publishing, Inc., pages 45-46.

QUESTION 204
Which of the following is not a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources

D. Automated login for remote users

Correct Answer: D
Explanation:
An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.
Source: TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).

QUESTION 205
What does the simple security (ss) property mean in the Bell-LaPadula model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: A
Explanation:
The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

QUESTION 206
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.

Correct Answer: D
Explanation:
Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris.

A camera like device records the patterns of the iris creating what is known as Iriscode. It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.

Reference(s) used for this question:
AIO, 3rd edition, Access Control, p 134.
AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition

The following answers are incorrect:

concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue. the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http://www.nature.com/news/ageing- eyes-hinder-biometric-scans-1.10722

there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

QUESTION 207
Which of the following is the WEAKEST authentication mechanism?

A. Passphrases
B. Passwords
C. One-time passwords
D. Token devices

Correct Answer: B
Explanation:
Most of the time users usually choose passwords which can be guessed , hence passwords is the BEST answer out of the choices listed above.

The following answers are incorrect because:

Passphrases is incorrect as it is more secure than a password because it is longer.
One-time passwords is incorrect as the name states , it is good for only once and cannot be reused.
Token devices is incorrect as this is also a password generator and is an one time password mechanism.

Reference:
Shon Harris AIO v3 , Chapter-4: Access Control , Page: 139 , 142.

QUESTION 208
Which of the following are not Remote Access concerns?

A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges
D. Access badges

Correct Answer: D
Explanation:
Access badges are more relevant to physical security rather than remote access.

"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.

"Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring.

"Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.

References:
AIO3, pp. 547 - 548

QUESTION 209
Which of the following does not apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Explanation:
Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password- generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

QUESTION 210
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.

Correct Answer: D
Explanation:
Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.

The following answers are incorrect: