CISSP: Certified Information Systems Security Professional Examnotes

Abstract

- This study guide will expose you to the CISSP exam, how you can obtain certification, and where to acquire more information about it. This is not a definitive guide to the exam it is merely a source for you to learn more about the CISSP. CISSP candidates generally have more than 6-10 years security experience and are in High-level security positions. The exam is in written format and taken when given quite a few times a year.

Exam Info

- CISSP Certification was designed to recognize mastery of an international standard for information security and understanding of a Common Body of Knowledge (CBK)

CISSP Exam Structure

- The CISSP Certification examination consists of 250 multiple-choice questions (English Language)
- Candidates have up to 6 hours to complete the examination
- Ten CISSP information systems security test domains are covered in the examination pertaining to the Common Body of Knowledge:
    - Access Control Systems & Methodology
    - Applications & Systems Development
    - Business Continuity & Disaster Recovery Planning
    - Cryptography

- Law, Investigation & Ethics
- Operations Security (Computer)
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications & Network Security (I & II)

Exam Information Specifics from FAQ's

- All test questions are multiple choices with four possible answers. They are designed to test a candidate's knowledge of information security facts and concepts and their application.
- The examination tests the expected knowledge a 3-5 year practitioner should have. It is designed to test for the minimum level of competency acceptable for someone to be certified as an information systems security professional. A knowledgeable candidate should not find the examination difficult.
- The CISSP examination is not vendor or commercial product specific. There are questions on the security models and methodologies used by these systems but only security products that are commonly used and freely available (i.e., SATAN) are acceptable for examination questions
- There is no fixed passing score for the examination. The cut score for each examination is calculated by equating the scoring values associated with each question. Passing rates estimated to be in the 70% to 80% range. Less than 8% of those tested achieve scores higher than 85%.
- In order to sit for the examination, applicants must subscribe to the (ISC)2 Code of Ethics and have at least three years of direct work experience in one or more of the ten test domains of the information systems security Common Body of Knowledge
- No affiliation with any organization is required for taking the test. For additional information, please call ISC2 at 727-738-9657 or 888-333-4458 " North America Only"

Study Tips

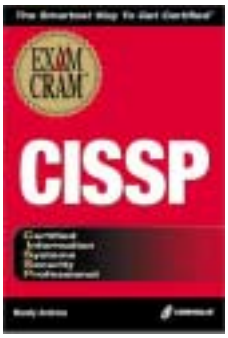
- It is recommended that you be in the security field with many years experience with security before sitting this exam. It is long and really tests your security knowledge. Seminars are recommended, as they are one of the only ways to even take the exam.
- Make sure you prepare for the exam with as many sources as possible. Up to now, there weren't any study guides out there, now you have quite a few to choose from including an Exam Cram (listed below).

Links and Publications

These Links below should be all you need to get your start on this certification:

- (ISC)2 Home Page
- CISSP Home Page
- Exam Scheduling
- CISSP Site

This is one of the best Prep guides available, as it is short and to the point. There are other guides available, but of course go more into detail. For a truly condensed guide, this is it.



CISSP NOTES

These Notes are for a “last read” before sitting the exam:

Common Body of Knowledge 1

Operational Security

Preventive:

Designed to lower amount and impact of unintentional errors entering the system and to prevent unauthorized intruders from internally or externally accessing the system

Data validation, pre-numbered forms, and review for duplications

Detective

Track unauthorized transactions and lessen errors by detecting quickly

Corrective

Data recovery

Recovery

Help rebuild system, application, or network after security incident

Orange Book

Trusted Computer Security Evaluation Criteria

Assurance:

Operational Assurance

Basic features and architecture of system

System integrity, covert channel analysis (storage and timing), trusted recovery

Trusted facility management

Assignment of specific individual to administer security of system

Separation of duties, don't have system administrator and security administrator as same person

In highly secure systems have three administrative roles: system administrator, security administrator, and enhanced operator function

Two-man control means each reviews and approves the work of the other

Dual control requires both operators to complete a task. Rotation of duties

Mandatory taking of vacations

Trusted recovery:

Ensures security is not breached when system crashes or has other failures

Required only for B3 and A1 levels in Orange Book

Problem management goals:

Reduce failures to a manageable level

Prevent occurrence or re-occurrence of a problem

Mitigate negative impact of problems

Initial Program Load vulnerabilities

Common Body of Knowledge 2

Security Architecture and Models

OS components:

Process management

I/O

Memory management

System file management

IT Architecture:

Logical (functional) components

Technical (physical) components

Closed security environment:

Application developers have sufficient clearances and authorizations to provide acceptable presumption that they will not introduce malicious logic

Configuration control provides protection from introduction of malicious logic prior to and during the operation of systems. Open security environment does not have the foregoing protections

Types of I/O:

Block devices (write blocks of data; hard disk)

Character devices (not addressable; keyboard and printer)

CPU operating states:

Ready state

Problem state

Supervisory state

Wait state

Programming languages (Three types):

Machine (1GL)

Assembly (2GL)

High-level (3-5GL)

Assembler

Translates from assembly language to machine language

Disassembler

Translates machine language to assembly

Compiler

Translates high-level language to machine code

Decompiler

Translates machine language into high level language

Interpreter

Translates high level language one command at time to machine code

Staffing:

Define position, determine sensitivity of position, filling position, training hired person.

Delphi Technique

Group does not meet as a whole. Individual members submit anonymous comments.

Total Quality Management (TQM):

Pursuit of complete customer satisfaction

Continuously improve products and services, through the full and active involvement of the entire workforce

Quality Assurance typically focuses on the quality of the end-product. Under TQM, QA focuses on assuring quality throughout production and service process

Quality Circles are team of voluntary employees that get together to discuss quality issues

Quality Council is management

ISO 9000:

Addresses quality of system processes not product performance to specifications

Provides baseline for TQM

Benchmarking:

Internal

Competitive

Industry

Best-in-Class

RAM Type

Dynamic RAM (DRAM; multi-phase clock signals)

SRAM (single-phase clock)

Memory

Real or Primary (RAM)

Secondary (hard disk)

Sequential Memory

Information must be obtained sequentially searching from the beginning (tape)

Instruction Cycles:

Two phases

Fetch and execute

Run or operating state

Application or problem state

Pipelining

Overlaps steps of instructions

Scalar processor

Executes one instruction at a time

Security Modes of Operation:

Dedicated Security Mode:

Each subject must have clearance for all information on system and valid need to know for all information

System high Security Mode:

Each subject must have clearance for all information on system and valid need to know some of the information

Not all users may have needed to know

Compartmented Security Mode:

Each subject must have clearance for most restricted information on system and valid need to know that information.

Multilevel Mode:

Some subjects do not have clearance for all information

Each subject has needed to know all information to which they will have access

Common Body of Knowledge 3

Business Continuity Planning and Disaster Recovery Planning

Business Continuity Planning (BCP)

Plans and framework to ensure business can continue in an emergency

Minimize cost associated with disruptive event and mitigate risk

Foreign Corrupt Practices Act of 1977 imposes civil and criminal penalties if publicly held companies fail to maintain adequate controls over their info systems

Business Impact Assessment (BIA)

Identify what impact a disruptive event would have on the business

Impact may be financial (quantitative) or operational (qualitative)

Includes execution of vulnerability assessment

BIA has three goals:

Criticality prioritization

Downtime estimation

Resource requirements

Must identify which business units are critical to continuing acceptable level of operations

Disaster Recovery Planning (DRP)

Quickly recovering from an emergency with minimum of impact on business

Plan of action for before, during, and after a disruptive event

Primary objective:

Capability to move critical processes to an alternate site and return to the primary site and normal processing within a time frame that minimizing loss to the organization

Number one priority is people and Plan from top down

Subscription services:

Hot site

Warm site

Cold site

Database Shadowing

Uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers

Contingency Planning

Provides alternatives for those chance events that could impact normal operations

Two essentials for contingency planning:

Information backup

Management commitment

Includes three parts:

Emergency response

Recovery

Resumption

Hierarchical Storage Management (HSM)

Software that dynamically manages storage and retrieval of electronic information from storage media that varies in speed and cost

Six resource categories that support critical business functions:

Human resources

Processing capability

Computer-based services

Automated applications and data

Physical infrastructure

Documents

Common Body of Knowledge 4

Security Management Practices

AAA

Authentication: testing or reconciliation of evidence of user's identity

Accountability:

System ability to determine actions of user within the system and to identify the user

Audit trails (must be protected) and log files

Authorization: rights and permissions granted to a user or process

Privacy

Level of confidentiality and privacy protection of a user

Audit trails:

User accountability; reconstruction of events, intrusion detection, and problem analysis

Audit records:

Keystroke monitoring/logging and event-oriented logs

Protect integrity by requiring digital signatures to access, set up as write once

Use software for rapid analysis

Risk Management (RM):

Prime objective of security controls is to reduce effects of threats and vulnerabilities to a level that is tolerable (i.e., mitigate risk). Risk Analysis (RA). A "risk" is a potential harm or loss to a system; the probability that a threat will materialize

Lattice model:

Every resource and user is associated with one of an ordered set of classes. Resources of a particular class may only be accessed by those whose associated class is as high or higher than that of the resource.

Bell-LaPadula Model (Orange Book):

Most common model

Defines relationships between objects and subjects

Relationships are described in terms of subject's assigned level of access or privilege (security clearance) and the object's level of sensitivity (security classification). Enforces lattice principle, which specifies that subjects are allowed write access to objects at the same or higher level as the subject, read access to objects at the same or lower level, and read/write access to only those objects at the same level as the subject

Common Body of Knowledge 5

Access Control Systems

ACL:

Register of (1) users who have been given permission to use an object and (2) the types of access they have been permitted.

Controls:

Can be used to mitigate risks

Controls can relate to subjects (entities or individuals; active entity) or objects (files, systems, or other resources; passive entities). Controls can be preventive, detective, or corrective. These can be implemented by:

Administrative controls:

Policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation.

Logical or technical controls:

Restrict access to systems and the protection of information. Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols (Kerberos, IPSec).

Physical controls:

Guards and building security, biometric access restrictions, protection of cables, file backups.

Three types of access rules:

Mandatory access control (MAC):

Authorization of subject's access to an object depends on labels (sensitivity levels), which indicate subject's clearance, and the classification or sensitivity of the object

Every Object is assigned a sensitivity level/label and only users authorized up to that particular level can access the object

Access depends on rules and not by the identity of the subjects or objects alone

Only administrator (not owners) may change category of a resource

Orange book B-level

Output is labeled as to sensitivity level

Unlike permission bits or ACLs, labels cannot ordinarily be changed

Can't copy a labeled file into another file with a different label

Discretionary Access Control (DAC):

Subject has authority, within certain limits, to specify what objects can be accessible (e.g., use of ACL)

User-directed means a user has discretion

Identity-based means discretionary access control is based on the subjects identity

Very common in commercial context because of flexibility, Orange book C level

Relies on object owner to control access

Intrusion Detection Systems (IDS):

Monitors network traffic or to monitor host audit logs to detect violations of security policy. Detects attacks by two major mechanisms: signature –based ID (knowledge-based) or a statistical anomaly-based ID (Behavior-based)

Two general types:

Network-Based IDS:

Doesn’t consume network or host resources

Reviews packets and headers

Monitors network traffic in real time.

Won’t detect attacks against a host by a user logged in at the host’s terminal (only the network is monitored)

Host-Based IDS:

Reviews system and event logs to detect attack on host

Efficacy is limited by lack of completeness of most host audit log capabilities

Resident on centralized hosts

Common Body of Knowledge 6

Telecommunications and Network Security

LAN Transmission Methods:

Unicast

Multicast

Broadcast

LAN Topologies:

Bus

Ring

Star

Tree

Mesh

Ethernet:

10BaseT, UTP, 100 Meters

10Base2, Thin Coax (Thinnet), 185 meters

10Base5, Thick Coax (Thicknet), 500 meters

10BaseFL, Fiber, 2000 meters

Network topologies:

Ethernet

Token Ring

Fiber Distributed Data Interface (FDDI) token ring passing media with dual rings

Open Systems Interconnect (OSI) Model from International Standards Organization (ISO):

Layer 7	Application Layer Confidentiality Authentication Data integrity Non-repudiation Gateways Protocols: FTP, SNMP, SMTP, DNS, TFTP, NFS, S-HTTP
Layer 6	Presentation Layer Confidentiality Authentication Encryption Gateways EBCIDC and ASCII
Layer 5	Session Layer NO SECURITY Gateways Protocols: RPC and SQL
Layer 4	Transport Layer Confidentiality Authentication Integrity Gateways Protocols: TCP and UDP or SSL and SSH-2
Layer 3	Network Layer Confidentiality, authentication, data integrity, virtual circuits, routers. IP and IPSec. ARP, RARP, ICMP
Layer 2	Data Link Layer

	Confidentiality Bridges Switch Protocols: HDLC, PPTP, L2F, L2TP, Token ring and Ethernet, PPP and SLIP
Layer 1	Physical Layer Confidentiality ISDN Repeaters and hubs Sends and receives bits

DOD or TCP/IP Model

Process and Application Layer

Host-to-Host

Internet

Network Access (Link)

TCP:

Acknowledged

Sequenced

Connection-oriented

Reliable

High overhead

UDP:

Unacknowledged

Subsequence

Connectionless

Unreliable

Low overhead (faster)

Backup Concepts (must physically secure):

Full

All data, usually done weekly

Incremental

Only copies files that have been added or changed that day

Differential

Only files that have been changed since last backup

Common Body of Knowledge 7

Cryptography

Cryptology is cryptography and cryptanalysis

Cryptography: science of codes

Cryptanalysis: science of breaking codes

Cryptography

This is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

Confidentiality (the information cannot be understood by anyone for whom it was unintended)

Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

Authentication (the sender and receiver can confirm each others identity and the origin/destination of the information)

Cryptanalysis

Cryptanalysis refers to the study of ciphers, ciphertext, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, ciphertext, or cryptosystem.

Breaking is sometimes used interchangeably with weakening. This refers to finding a property (fault) in the design or implementation of the cipher that reduces the number of keys required in a brute force attack

Man-in-the-middle attack:

This differs from the above in that it involves tricking individuals into surrendering their keys. The cryptanalyst/attacker places him or herself in the communication channel between two parties who wish to exchange their keys for secure communication (via asymmetric or public key infrastructure cryptography). The cryptanalyst/attacker then performs a key exchange with each party, with the original parties believing they are exchanging keys with each other. The two parties then end up using keys that are known to the cryptanalyst/attacker. This type of attack can be defeated by the use of a hash function.

PKI

A PKI (public key infrastructure) enables users of an unsecure public network such as the Internet to securely and privately exchange data and money with a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on

The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

A public key infrastructure consists of:

A certificate authority (CA) that issues and verifies digital certificate

A certificate includes the public key or information about the public key

A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor

One or more directories where the certificates (with their public keys) are held

A certificate management system

Common Body of Knowledge 8

Applications and Systems Development

Configuration Management:

British Standards Institute 7799:

Tracking and issue of new versions

A configuration item is a component whose state is to be recorded and against which changes are to be progressed

Configuration control controls changes to the configuration items and issues versions of the items from the software library

Object Oriented Systems:

A revolutionary concept that changed the rules in computer program development, object-oriented programming (OOP) is organized around "objects" rather than "actions," data rather than logic. Historically, a program has been viewed as a logical procedure that takes input data, processes it, and produces output data. The programming challenge was seen as how to write the logic, not how to define the data. Object-oriented programming takes the view that what we really care about are the objects we want to manipulate rather than the logic required to manipulate them. Examples of objects range from human beings (described by name, address, and so forth) to buildings and floors (whose properties can be described and managed) down to the little widgets on your computer desktop (such as buttons and scroll bars).

The first step in OOP is to identify all the objects you want to manipulate and how they relate to each other, an exercise often known as data modeling. Once you've identified an object, you generalize it as a class of objects (think of Plato's concept of the "ideal" chair that stands for all chairs) and define the kind of data it contains and any logic sequences that can manipulate it. Each distinct logic sequence is known as a method. A real instance of a class is called (no surprise here) an "object" or, in some environments, an "instance of a class." The object or class instance is what you run in the computer. Its methods provide computer instructions and the class object characteristics provide relevant data. You communicate with objects - and they communicate with each other - with well-defined interfaces called messages

Database security threats:

Aggregation

Inference

Database security issues

Granularity of the access to objects in DB refers to fineness with which access can be controlled or limited. Aggregation is act of obtaining info of a higher sensitivity and combining it with lower levels of sensitivity. Inference is ability of users to infer or deduce info about data at sensitivity levels for which they do not have access. A link that enables an inference to occur is called an inference channel.

Data Warehouse and mining:

A data warehouse is a central repository for all or significant parts of the data that an enterprise's various business systems collect. The term was coined by W. H. Inmon. IBM sometimes uses the term "information warehouse." Typically, a data warehouse is housed on an enterprise mainframe server. Data from various online transaction processing (OLTP) applications and other sources is selectively extracted and organized on the data warehouse database for use by analytical applications and user queries. Data warehousing emphasizes the capture of data from diverse sources for useful analysis and access, but does not generally start from the point-of-view of the end user or knowledge worker who may need access to specialized, sometimes local databases. The latter idea is known as the data mart.

Data mining and a decision support system (DSS) are two of the kinds of applications that can make use of a data warehouse

Data mining is the analysis of data for relationships that have not previously been discovered

Data mining results include:

Associations, or when one event can be correlated to another event

Sequences or one event leading to another later event

Classification or the recognition of patterns and a resulting new organization of data

Clustering, or finding and visualizing groups of facts not previously known

Forecasting or simply discovering patterns in the data that can lead to predictions about the future

Common Body of Knowledge 9

Physical Security

Five threats:

Interruptions in computing services

Physical damage

Unauthorized disclosure of information

Loss of control of system integrity

Physical theft

Environmental controls:

Electrical Power:

Noise (EMI, RFI), use power line conditioning, proper grounding, and cable shielding, limiting exposure to magnets, electric motors, and heaters

Humidity range should be 40-60% (ESD)

ESD – Electrostatic Discharge

Use Hygrometer to measure humidity

Static electricity controls: anti-static sprays, antistatic flooring, proper grounding, anti-static table or floor mats, HVAC to control humidity

EPO: Emergency Power Off

Air conditioning should have separate EPO

Three methods to protect power: UPS, power line conditioning, backup power sources

Fire detection and suppression:

Three elements – oxygen, heat, and fuel

Water suppresses temperature

Soda acid reduces fuel

CO2 (lethal if removes all O2) reduces oxygen

Fire Detectors: Heat sensing, flame sensing, flame actuated, smoke actuated, automatic dial-up

Fire extinguishing systems: Wet pipe (water all the time), dry pipe (water only when activated), Deluge, Preaction (dry until heat, then loads water; most recommended for computers)

Gas discharge systems employ pressurized inert gas usually from under raised floor

CO2 and Halon

Halon now listed as danger to environment and is being phased out

Halon not safe above 10% concentration

Use in >900 degrees creates toxic gas

Halon 1211 (portable extinguishers) and Halon 1301 (flooding systems)

FM-200 is good replacement

Fire contaminants: smoke, heat, water, suppression medium contamination (CO2 or Halon)

Common Body of Knowledge 10

Law, Investigation, and Ethics

Two types of evidence:

Audit evidence

Physical examination

Computer Incident Response Team (CIRT)

Federal Computer Security Act of 1987: first to require government agencies to do security training and adopt security plans

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy with a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets.

IPSec:

IP security. Two main protocols are Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides integrity, authentication, and non-repudiation. ESP provides encryption.

LDAP, DNS and x.500:

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version it did not include security features

In a network, a directory tells you where in the network something is located. On TCP/IP networks (including the Internet), the domain name system (DNS) is the directory system used to relate the domain name to a specific network address (a unique location on the network). However, you may not know the domain name. LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).

Pretty Good Privacy:

A technique for encrypting messages developed by Philip Zimmerman

PGP is one of the most common ways to protect messages on the Internet because it is effective, easy to use, and free. PGP is based on the public-key method, which uses two keys, one is a public key that you disseminate to anyone from whom you want to receive a message. The other is a private key that you use to decrypt messages that you receive. To encrypt a message using PGP, you need the PGP encryption package, which is available free from a number of sources. The official repository is at the Massachusetts Institute of Technology. PGP is such an effective encryption tool that the U.S. government actually brought a lawsuit against Zimmerman for putting it in the public domain and hence making it available to enemies of the U.S. After a public outcry, the U.S. lawsuit was dropped, but it is still illegal to use PGP in many other countries

S/MIME:

Secure Multipurpose Internet Mail Extensions

Symmetric key encrypted with public key cryptography. Uses X.509

SSL:

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library, which can be downloaded for noncommercial use or licensed for commercial use. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

TLS:

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. The TLS protocol is based on Netscape's SSL 3.0 protocol; however, TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0. The most recent browser versions support TLS. The TLS Working Group, established in 1996, continues to work on the TLS protocol and related applications. SSL and TLS use X.509.

Wireless Application Protocol (WAP):

WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). While Internet access has been possible in the past, different manufacturers have used different technologies. In the future, devices and service systems that use WAP will be able to interoperate

The WAP layers are:

Wireless Application Environment (WAE)

Wireless Session Layer (WSL)

Wireless Transport Layer Security (WTLS)

Wireless Transport Layer (WTP)

The Wireless Markup Language (WML) is used to create pages that can be delivered using WAP

Data must be unencrypted at gateway between wireless and wired network to be re-encrypted using SSL

Good Luck on the Exam!

Study Guide By: Examnotes.net