





Chapter 3 - Key Topics





 Description	 Element	 Page	 Summary
<u>Differences & definitions of subject, object, & access controls</u>	List	106	A subject makes a request to access an object, access controls regulate the subject/object interaction.
<u>The key concepts in the identification process</u>	List	108	Secure identities should be <i>securely issued</i> , be <i>unique</i> , and <i>non-descriptive</i> .
<u>Authentication Methods</u>	Table 3-2	109	Authentication by knowledge is something the user knows such as a password or pin. Authentication by ownership is something the user owns such as a smart card, token, or badge. Authentication by characteristic is something the user is or does such as fingerprints, hand geometry, or keystroke dynamics.
<u>Defining multifactor authentication</u>	Paragraph	109	Multifactor authentication is using more than one authentication method such as a password & a badge.
<u>Access Control Phases</u>	Table 3-3	111	Identification , the process of providing identity. Authentication , the process of proving the identity. Authorization , the process of providing access to a resource with specific access rights. Accounting , the process of auditing & monitoring user operations on a resource.

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Access control process key concepts</u>	List	111	<p>Asset/Data Classification, process of classifying data based on the risk for the organization using on CIA. Asset Marking, marking, & labeling assets. Access policy definition, the process of defining policies that govern access to an asset. Data Disposal, the process of disposing or eliminating an asset or data.</p>
<u>Security Roles & Responsibilities</u>	List	115	<p>Executives & Senior Management, the ultimate responsibility of data/assets. Data Owner, responsible for a specific piece or subset of data. Data Custodian, responsible for day-to-day tasks on behalf of the data owner. Ensures availability and security policies are followed. System Owner, responsible for the security of systems that handle data owned by various owners. Security Administrator, responsible for the process of granting rights and maintaining records of access. End-User, responsible for adhering to security policies. Security Officer, in charge of design, implementation, management, & review of security policies. Information System Security Professional, responsible for drafting InfoSec policy standards, guidelines, guidance on threats. Auditor, responsible for determining compliance to policy.</p>

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Access control types based on purpose</u>	List	117	<p>Administrative Controls - policies, procedures around definitions of access controls, definitions of information classifications, roles, responsibilities, and anything needed to manage access control from the administrative perspective. Subtypes include <i>Operational, security policies & procedures, Operational, security policies & procedures, Security education & training, Auditing & monitoring policies</i>.</p> <p>Physical Controls, aimed at protecting physical boundaries and employee safety.</p> <p>Technical Controls or <i>logical controls</i> are technological controls such as firewalls, IPSs, IAM systems, encryption.</p>

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Access control types based preventative, detective, corrective, deterrent, recovery, compensating capacities</u>	List	118	<p>Preventative Controls - enforce security policy and should prevent incidents from happening. Examples, ACLs, passwords, & fences. Deterrent Controls - discourages attackers from proceeding. For example, a system banner warning of unauthorized access. Detective Controls - aim at monitoring & detecting any unauthorized behavior or hazard. Useful while an attack is taking place & in post-mortem analysis.</p> <p>Detective Controls - aim at monitoring & detecting any unauthorized behavior or hazard. Useful while an attack is taking place & in post-mortem analysis.</p> <p>Recovery Controls - used after an environment or system has been modified because of unauthorized access, restores initial behavior. Examples, back, redundancy, disaster recovery plan.</p> <p>Compensating Controls - Offer an alternative to primary control, usually as a temp solution. For example, a security guard checking a badge because a card reader is temporarily out-of-order.</p>

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Overview of Access Control Models</u>	Table 3-5	120	<p>Discretionary Access Control (DAC) - Access decisions & permissions are decided by the object owner (DoD - Trusted Computer System Evaluation Criteria). Mandatory Access Control (MAC) - Access decisions are enforced by the access policy enforcer (example, the OS), use security labels (DoD - Trusted Computer System Evaluation Criteria). Role-based Access Control (RBAC) - Access decisions are based on the role or function of the subject (INCITS 359-2004). Attribute-based Access Control (ABAC) - Access decisions are based on the attributes or characteristics of the subject, object, & environment (NIST SP 800-162).</p>
<u>Pros & Cons of Access Control Models</u>	Table 3-6	120	<p>Discretionary access control (DAC) is simpler than other models, but security policy may be bypassed, and this model is not centralized. Mandatory Access Control (MAC) offers strict control over information at the cost of complex administration. Role-based Access Control (RBAC) is scalable and easy to manage; however, it increases role definitions. Attribute-based Access Control (ABAC) is flexible, more complex than DAC or MAC.</p>
<u>The main characteristics of DAC</u>	List	121	<p>In the DAC model authorization is decided by the object owner, access permissions are associated with the object, and access control is enforced by access control lists.</p>

 Description	 Element	 Page	 Summary
<u>The main characteristics of MAC</u>	List	123	In the MAC model the OS or policy enforcer decides on whether to grant access, not the owner, this policy is enforced by security labels.
<u>The main characteristics of RBAC</u>	List	124	In the RBAC model decisions are based on the role of the subject which an organization assigns based on policy, permissions are tied to roles, not users.
<u>The main characteristics of ABAC</u>	List	126	In the ABAC model decisions are made based on the attributes associated with subjects, objects, or the environment. These attributes are characteristics of subject, object, or environment. User role, identity, security classification can all be considered attributes.
<u>RADIUS vs. TACACS+ Comparison</u>	3-7	133	RADIUS - UDP based, encrypts user password in ACCESS-REQUEST, authentication & authorization in same exchange, accounting in another. No command authorization, strong accounting, RFC 2865 (authentication and authorization) and RFC 2866 (accounting). TACACS+ - TCP based, can encrypt full payload, AAA all performed in own exchange, allows command authorization, basic accounting, Cisco proprietary.
<u>The main characteristics of IPS/IDS</u>	List	145	IDS - works with a packet copy (promiscuous mode). No traffic delay, cannot stop traffic but can work with other security devices to block traffic, some malicious traffic may pass even if flagged. IPS - Intercepts traffic (inline mode), adds latency due to packet processing, can stop malicious traffic, drops malicious packets.

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>The advantages and disadvantages of IPS & IDS</u>	Table 3-8	146	IDS - promiscuous mode. No traffic delay, cannot stop traffic but can work with other security devices to block traffic, some malicious traffic may pass even if flagged. IPS - inline mode, adds latency due to packet processing, can stop malicious traffic, drops malicious packets.
<u>Categories of IPS/IDS events</u>	List	146	False Positive - System raises an event on legitimate traffic that is not malicious. False Negative - Failure to recognize a malicious event. True Positive - Correct behavior when threat is detected. True Negative - Correct behavior when no event is triggered on non-malicious traffic.
<u>The main characteristics of network IDS/IPS</u>	List	147	Network detection methodologies: <i>pattern matching, stateful pattern-matching recognition, protocol analysis, heuristic-based analysis, anomaly-based analysis, global threat correlation</i>
<u>The main characteristics of host-based IDS/IPS</u>	Paragraph	147	Used on the host endpoint and interacts with the host OS but may also provide protection on the host NIC. Used for end-host security policy enforcement and or compliance/audit control.
<u>Network-Based vs. Host-Based Detection/Prevention Systems</u>	Table 3-9	147	NIDS/NIPS - software deployed on a dedicated machine, easy to update. HIDS/HIPS - Software installed on-top of host OS, may require multi-OS support. May require an update of several endpoints

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Network-Based vs. Host-Based Antivirus/Antimalware Systems</u>	3-10	149	<p>Network-based Antivirus/Antimalware - Dedicated machine, easy to maintain/update, visibility into all network traffic, delay due to packet processing, no visibility into whether an attack was successful or not, no visibility into encrypted traffic, can block at entry point.</p> <p>Host-based Antivirus/Antimalware - Software installed on-top of OS, may require support for multiple OS's, updating multiple endpoints, only host visibility, can slow OS, can verify the success of the attack, visibility after encryption, block encrypted packets, an attacker able to reach host before block.</p>
<u>Untitled</u>			