|  |  |
| --- | --- |
| **TEXAS CTE LESSON PLAN**  [www.txcte.org](http://www.txcte.org) | |
| **Lesson Identification and TEKS Addressed** | |
| **Career Cluster** | Law, Public Safety, Corrections, and Security |
| **Course Name** | Court Systems and Practices |
| **Lesson/Unit Title** | Security Systems Analysis |
| **TEKS Student Expectations** | **130.341. (c)** **Knowledge and Skills**  (8) The student analyzes security systems and their role in an overall security strategy. The student is expected to  (A) summarize the purposes, types, and applications of physical and electronic access control systems, surveillance systems, and intrusion detection systems  (B) analyze how physical and electronic systems work together as an integrated system to support an overall protection strategy and  (C) analyze the roles of security surveys, inspections, and exercises to test existing protection measures. |
| **Basic Direct Teach Lesson**  (Includes Special Education Modifications/Accommodations and  one English Language Proficiency Standards (ELPS) Strategy) | |
| **Instructional Objectives** | The students will be able to:   1. Summarize the purposes, types, and applications of physical and electronic access control systems, surveillance systems, and intrusion detection systems. 2. Analyze how physical and electronic systems work together as an integrated system to support an overall protection strategy. 3. Analyze the roles of security surveys, inspections, and exercises to test existing protection measures. |
| **Rationale** | The duty of security services is to provide clients safety and protection. Services that are typically provided are guard and patrol services, such as bodyguard, guard dog, parking security, and security guard services. However, some security institutions may provide advanced special operations services if the client demands it. Examples of these services are the prevention of unauthorized activity or entry, traffic regulation, access control, and fire and theft prevention and detection. |
| **Duration of Lesson** | 6 to 7 Hours |
| **Word Wall/Key Vocabulary**  *(ELPS c1a,c,f; c2b; c3a,b,d; c4c; c5b) PDAS II(5)* | Refer Security Systems Analysis Key Terms |
| **Materials/Specialized Equipment Needed** | * Security Systems Analysis Key Terms * Computers with computer-based presentation software * White board/chalk board * Computer with Internet Access * Security Systems Analysis computer-based presentation * Security Systems Analysis Exam and Key * Discussion Rubric * Group Evaluation Rubric * Individual Work Rubric * Presentation Rubric * Research Rubric |
| **Anticipatory Set**  (May include pre-assessment for prior knowledge) | Have the class break into several small groups and discuss the questions below. Then discuss the questions as a class. Use the Discussion Rubric for assessment.   * What are the services that a security professional can provide? * What are the names of some people and/or companies (private and public) that need security services? * What are the physical threats that would require the use of security services? * What are the technological threats available that would require the use of security services? |
| **Direct Instruction \*** | 1. Security Awareness    1. Is an attitude held by security personnel and non-security client employees that places a high value on detecting, deterring, and reporting security exposures such as crime, safety hazards, fire hazards, theft, intrusions, and vandalism    2. Requires security personnel to protect the client’s employees, property, guests, and image, and assist the client’s personnel and visitors    3. Requires that non-security client employees are aware of the security program’s goals and methods and support the security program, abiding by its policies    4. Founded on the concept of preventative security    5. The three main security principles are       1. Availability       2. Integrity       3. Confidentiality   II. Physical Security   * 1. Two basic duties of performing physical security      1. Observe      2. Report   2. Three initial steps taken with a security threat      1. Identify it      2. Report it      3. Discuss and develop a solution that eliminates the problem   3. Cultivates security awareness among the clients and requires conscientious and highly visible security officers   4. A priority concern of top-level management of businesses, industries, and institutions   5. Has the ultimate goal of loss prevention which results in the maximum return on investments   6. Requires two basic investigative skills      1. Communication skills      2. Surveillance capabilities   7. Defines the primary hardware systems traditionally with      1. Locks      2. Security alarms      3. Access controls      4. Surveillance video  1. Electronic Access Control Systems    1. Security devices that allow the user and the system to communicate with each other; these include       1. Controller       2. Card reader       3. Door contacts       4. Control locking device    2. Not security alarm systems; the two systems do have a lot in common, but are usually implemented separately    3. Strategically positioned as a natural focal point for a security officer to initiate ownership of the physical security systems, systems that are traditionally supported by facilities personnel       1. The installation of an electronic access control system can be arranged the same way as a security alarm, with the access controllers positioned at a central location       2. Peripheral devices such as the door and the elevator controls, the credential readers, and the interfaces to other systems can connect to the access controllers by lengthy cabling       3. Example: a typical access control system has a controller, a credential reader, door position contacts, and a means of controlling the locking device or door operator   D. Require access credentials which are used in conjunction with access controls, typically in the form of access cards and card readers   * 1. The card data must be readable by the reader, and the reader data stream format must be supported by the controller   2. A controller is a chip, an expansion card, or a stand-alone device that interfaces with a peripheral device; this connection may be a link between two parts of a computer or a controller on an external device that manages the operation of that device      1. A contact chip – a small integrated circuit which must come in contact with a reader in order for the two to communicate with each other      2. A contactless chip – a small integrated circuit that functions through wireless technology (the circuit utilizes transceivers, antennas, and RFID)   3.Distinct functions of security and access control  a)Identification – the method used to verify a person’s identity  b)Authentication – identity confirmation  c)Authorization – access to a location and/or information that is granted to a proven individual  (1)Use of biometrics, passwords, passphrases, tokens, or other private information  (2)Biometrics – authorization and access that is based on an individual’s unique characteristics including handprints, fingerprints, or retinal scans  (3)Most common biometric systems  (a)Fingerprint  (bPalm Scan  (c)Hand Geometry  (d)Iris Scan  (e)Signature Dynamics  (f)Keyboard Dynamics  (g)Voice Print  (h)Facial Scan  (i)Hand Topography  E. Access control key points and mechanisms include   1. Passphrase – a statement, phrase or series of words that replaces a password and is used for access to a computer system 2. Passwords 3. Cryptographic keys – cryptographic operations in which a string of bits are used by a cryptographic algorithm to change a string of text into a cipher resulting in information that can only be read through private keys or digital signatures 4. Centralized Access Control Administration – access control that is administered and controlled at one location 5. Preventative administrative controls – includes policies, hiring practices, and security awareness 6. Preventative physical controls – includes badges, swipe cards, guards, and fences 7. Preventative technical controls – includes passwords, encryption, and antivirus software   IV. Surveillance Systems   * 1. Many people continue to rely on old-fashioned security methods such as door and window locks, but it is more practical to invest in surveillance cameras   2. Surveillance cameras      1. Currently among the most popular and in-demand security devices      2. Capable of obtaining 24-hour steady video      3. Found in various locations including         1. Public highways         2. Parks         3. Vehicles         4. Airplanes         5. Ships      4. Ideal for industrial and official establishments, and individual homes      5. Commonly used for standard property monitoring      6. Used indoors and outdoors      7. Used visibly and hidden      8. Serve a variety of purposes including employee theft and monitoring children (i.e. nanny cams)      9. Found in two categories         1. Hardwired            1. Effective but can easily accumulate wires         2. Wireless            1. Easier to setup, install, and place anywhere            2. Clutter-free and dependable (i.e. unaffected by accidental power shutdowns and/or interruptions)  1. Intrusion Detection System (IDS)    1. A program that monitors a system for malicious activity and in turn reports the activity    2. Designed to test/analyze network system traffic events against a given set of parameters and send out an alert or capture data when these thresholds are met    3. Uses collected information and a predefined knowledge-based systems to reason about the possibility of an intrusion    4. Detects attacks as soon as possible and takes the appropriate action, but does not usually take preventive measures when an attack is detected    5. Reactive rather than proactive    6. Configurable to run unattended for extended periods of time    7. Must recognize unusual activity and operate without unduly affecting the system’s activity    8. Consists of three components or modules    9. Event generator – a data source or sensor which is responsible for capturing and sending packets to the console    10. Analysis engine or console – responsible for analyzing the packets captured by the sensor and examining the data for the symptoms of attacks or other policy violations    11. Response manager – only acts when inaccuracies (possible intrusion attacks) are found in the system; acts by notifying someone or something in the form of a response   I. Types   1. Network IDS – a system that locates intrusions by investigating the network traffic and monitoring multiple hosts 2. Protocol-based IDS – a system or person that actively monitors and surveys the communication between a system and the server 3. Application Protocol-based IDS – a system or person that actively monitors and surveys the application-based communication between a system and a group of servers 4. Host-based IDS – a system on a host that detects intrusions by monitoring system calls, application logs, file-system modifications, and other host activities 5. Passive IDS – a system that alerts when unusual (suspicious or malicious) activity is detected and notifies the user when preventative action must be taken 6. Reactive IDS – a system that alerts when unusual activity (suspicious or malicious) is detected and takes action immediately by blocking the system threat   J. Detection approaches   * 1. Signature detection      1. Used to discriminate between anomalies or attack patterns (signatures) and known intrusion detection signatures      2. Often used in the IDS and many anti-malware systems such as anti-virus and anti-spyware, etc.      3. Scans the system against already known computer viruses, malware, or attacks      4. Alerts the user if an attachment is detected   2. Statistical anomaly detection   3. Monitors the normal activity of a system and then informs the user if unusual or anomalous activity is detected   4. Applies statistical tests to observed user behavior to determine with a high level of confidence whether or not the behavior is legitimate   5. Falls into two broad categories      1. Threshold detection – a program that records by counting the number of times that an incident occurs within a system      2. Profile-based anomaly detection – a program that monitors a system by analyzing previous system patterns and current system patterns that are highly deviated from an individual user’s activity   VI. Integrated Security Systems   1. Security services is one of the fastest growing areas of integrated building systems 2. Demand for security services has maintained steady growth since September 11, 2001 3. Security systems inherently require an integrated approach, except for local card entry locks 4. Physical access control is more than the use of a simple lock; instead the lock may be integrated with a biometrics ID system (i.e. the use of an ID card or personal identification number (PIN) in conjunction with a physical characteristic)    1. The biometric aspect of the process is to compare a stored biometric template to a real-time scan of an eye, a finger, or some other body part    2. The door lock must communicate with a server that has stored the template data in order for the biometric aspect to work 5. A high-resolution digital closed circuit television (CCTV) system permits easy access to stored images and the computer analysis of the images, which aids in decision-making (i.e. to focus on an individual/location or send a warning message/alarm) 6. Once data and control are connecting on a communication link, they can easily tie in with other systems, such as the fire alarm system, lighting control system, heating, ventilation and air conditioning (HVAC) system, and the computer access control system 7. The projected expansion of power over Ethernet (PoE)    1. A very important development in the integration of security with other building systems    2. Makes it possible to operate door locks and cameras with the same cable that ties them into the building’s local area network (LAN) 8. The installation of sophisticated access control systems in commercial buildings is a new trend toward systems convergence   1. After scanning the information, it takes a digital photo or captures the visitors signature  2. It then can contact the visitor’s host by phone, e-mail, or with a real-time network messaging  3. Example: scanning the photo ID, the business card or the passport ID of an arriving visitor, which instantaneously checks whether the visitor is expected or has been in the facility before, and makes sure that the visitor is not on a “watch list”   1. This surveillance system integrates all critical security functions, such as alarm, fire, and access systems, allowing the security staff to simultaneously monitor all systems from the centralized security command center    1. Also the capability to control all the lights throughout the entire building, as well as the HVAC system    2. Example: if an alarm is sounded, the signal automatically activates a camera located in the affected area, where the security personnel can instantly view the incident 2. Integrated security system design services include    1. Enterprise systems for local, regional, or global monitoring    2. Monitoring emergency operations center and fusion center design which manages and shares information between and across operations    3. Video surveillance systems    4. Access control systems    5. IDS    6. Physical security information management systems    7. Network design and bandwidth planning    8. Intercom systems and emergency communications    9. Door and window selection and hardware coordination    10. Conduit layouts with security power requirements    11. Lighting layouts with photometric detail    12. Design services for new construction and renovations/re-fits 3. Another aspect of the recent integrated security systems is the capability to use specific notification systems that can inform the building occupants of an event/crisis and inform them of the proper reaction   VII. Security Inspection   1. An important step toward preventing theft, burglary, and other crimes 2. Can indicate features which would make entry easy or difficult for a prospective offender when completed by trained security personnel 3. Shows how a location’s security can be improved 4. Requires observation of all entry points to determine what steps can reduce vulnerability 5. Begins at the front door and then includes the side and rear doors, windows, locks, lights, and landscaping 6. Are used by all professionals in the field of crime prevention, including both security services and law enforcement professionals   G. Requires the use of standard inspection forms/checklists that indicate security weaknesses and/or hazards that require attention including   * 1. Front entrance   2. Side or rear entrance   3. Entrances from the garage   4. Upper floor windows   5. Garage doors and windows   6. Basement doors and windows   7. Ground floor windows   8. Recommendations and comments   *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  NONE |
| **Guided Practice \*** | *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  NONE |
| **Independent Practice/Laboratory Experience/Differentiated Activities \*** | 1. Have the students act as if they are selling a form of security services (i.e. physical security, electronic security, cameras, etc). Have them create a sales pitch using computer-based presentation software (note: you may want to expand the role play and act as the CEO of a business with the students who are not presently acting as the board members; this activity can be completed either individually or in small work groups). Use the Presentation Rubric for assessment. 2. Have the students work in several small groups and create a security client (i.e. shopping center, celebrity, subdivision, etc.), including the client information and a floor plan and/or a sketch. After approximately 15 minutes have the groups exchange their client information. Then each group must develop a means to “attack” the client. After approximately 15 minutes, have the groups return the information about the client (who is under attack) to the original group. Next, the groups must create a strategy to protect their client. After approximately 20 minutes, students can present their plan to protect the client to the entire class. Use the Presentation Rubric and the Group Evaluation Rubric for assessment. 3. Have the students complete the security inspection form of an actual location (to find a sample form do an Internet search for the following: “security checklist David L. Berger Forensic Consultant”). Students can make a list and/or sketch of their ideas and present to the entire class how the location’s security can be strengthened. Use the Individual Work Rubric for assessment.   *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  NONE |
| **Lesson Closure** |  |
| **Summative/End of Lesson Assessment \*** | *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  For reinforcement, the students will research and explain the differences between surveillance systems and intrusion detection systems. Use the Individual Work Rubric for assessment. |
| **References/Resources/**  **Teacher Preparation** | 0205592406, *Introduction to Private Security: Theory Meets Practice,* Cliff Roberson and Michael L. Birzer, Prentice Hall, 2009  0750684321, *Introduction to Security,* Robert J. Fischer and Gion Green, Butterworth-Heinemann, 2008  Access Control Systems & Methodology, Jeff Smith, Purdue University Physical Access Control, Terry Martin & Alexandra Bakhto,  <http://www.giac.org/cissp-papers/282.pdf>  Do an Internet search of the following: security checklist David L. Berger Forensic Consultant  Investigator/Officer’s personal experience |
| **Additional Required Components** | |
| **English Language Proficiency Standards (ELPS) Strategies** |  |
| **College and Career Readiness Connection[[1]](#footnote-1)** | English/Language Arts Standards  III. Speaking  B. Develop effective speaking styles for both group and one-on-one situations.   * + 1. Participate actively and effectively in one-on-one oral communication situations.     2. Participate actively and effectively in group discussions.     3. Plan and deliver focused and coherent presentations that convey clear and distinct perspectives and demonstrate solid reasoning |
| **Recommended Strategies** | |
| **Reading Strategies** |  |
| **Quotes** |  |
| **Multimedia/Visual Strategy**  **Presentation Slides + One Additional Technology Connection** |  |
| **Graphic Organizers/Handout** |  |
| **Writing Strategies**  **Journal Entries + 1 Additional Writing Strategy** |  |
| **Communication**  **90 Second Speech Topics** |  |
| **Other Essential Lesson Components** | |
| **Enrichment Activity**  (e.g., homework assignment) | For enrichment, the students will write a research paper regarding their choice of electronic security system (surveillance cameras, motion detectors, etc). Use the Research Rubric for assessment. |
| **Family/Community Connection** |  |
| **CTSO connection(s)** | SkillsUSA |
| **Service Learning Projects** |  |
| **Lesson Notes** |  |

1. Visit the Texas College and Career Readiness Standards at <http://www.thecb.state.tx.us/collegereadiness/CRS.pdf>, Texas Higher Education Coordinating Board (THECB), 2009. [↑](#footnote-ref-1)