CWSP Guide to Wireless Security

Wireless Security Policy

Objectives

- Define security policy
- List the elements of the security policy cycle
- Describe several types of wireless security policies

What is a Security Policy?

- One of the most important assets any organization possesses is its data
- Security policy is a very important component of information security
- Security policy
  - Series of documents that clearly defines the defense mechanisms an organization will employ
    - To keep information secure
  - Outlines how the organization will respond to attacks
    - Duties and responsibilities of its employees

What is a Security Policy? (continued)

- Proper development of a security policy
  - Accomplished through the security policy cycle
    - Never-ending process of identifying what needs to be protected, determining how to protect it, and evaluating the adequacy of the protection

What is a Security Policy? (continued)



Figure 11-1 Security policy cycle

Risk Identification

- Seeks to determine the risks that an organization faces against its information assets
  - Information then becomes the basis of developing the security policy itself
- Steps
  - Asset identification
  - Threat identification
  - Vulnerability appraisal
  - Risk assessment

Risk Identification (continued)



Figure 11-2 Risk identification elements

Risk Identification (continued)

- Asset Identification
  - Asset is any item that has a positive economic value
  - Asset management: process of tracking the assets
  - Types of assets
    - Data
    - Hardware
    - Personnel
    - Physical assets
    - Software
  - Identifying assets is one of the most critical steps in risk identification

Risk Identification (continued)

Table 11-1 Hardware and software attributes

Attribute Name	Description
Equipment name	The name of the device commonly used, such as ACCESS POINT HALLWAY G228
Equipment type	Type of equipment, such as access point or wireless intrusion detection device
Manufacturer	The name of the manufacturer
Model and part number	The identification numbers used by the manufacturer
Manufacturer serial number	The unique serial number assigned by the manufacturer
Inventory tag number	The number assigned by the organization to the item; this is useful as a cross-reference to the order inventory, which contains additional information such as the date purchased, the vendor's name, and the cost
Software or firmware version	The version of the software or firmware, including all updates and service packs installed
Location	The building and room number where the equipment is installed
Addresses	The Media Access Control (MAC) and the IP address of the hardware or the hardware on which the software resides
Unit	The name of the organizational unit responsible for the asset
Function	A description of what the equipment does

Risk Identification (continued)

- Asset Identification (continued)
  - Factors to determine an asset's relative value
    - How critical is this asset to the goals of the organization?
    - How difficult would it be to replace it?
    - How much does it cost to protect it?
    - How much revenue does it generate?
    - How quickly can it be replaced?
    - What is the cost to replace it?
    - What is the impact to the organization if this asset is unavailable?
    - What is the security implication if this asset is unavailable?

Risk Identification (continued)

- Threat Identification
  - Threat agent
    - Any threat that exists against an asset
    - Not limited to those from attackers, but also includes natural disasters
  - Threat modeling
    - Constructs scenarios of the types of threats that assets can face
      - To better understand who the attackers are, why they attack, and what types of attacks may occur

Risk Identification (continued)

Table 11-2 Common threat agents

Category of threat	Example
Acts of God	Fire, flood, earthquake
Compromise of intellectual property	Software piracy or copyright infringement
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Hardware failure or errors	WIPS blocks all traffic
Human error	Employee drops wireless network interface adapter into lake
Sabotage or vandalism	Attacker implants worm that erases files
Software attacks	Virus, worm, denial of service
Software failure or errors	Bug prevents program from properly loading
Technical obsolescence	Program does not function under new version of operating system
Theft	Access point is stolen from hallway
Utility interruption	Electrical power is cut off

Risk Identification (continued)

- Threat Identification (continued)
  - Attack tree
    - Visual image of attacks that may occur against an asset
    - Shows the goal of the attack, the types of attacks that may occur, and the techniques used in the attacks
- Vulnerability appraisal
  - Takes a current snapshot of the security of the organization as it now stands
  - Every asset must be viewed in light of each threat
  - Depends on background/experience of the assessor

Risk Identification (continued)

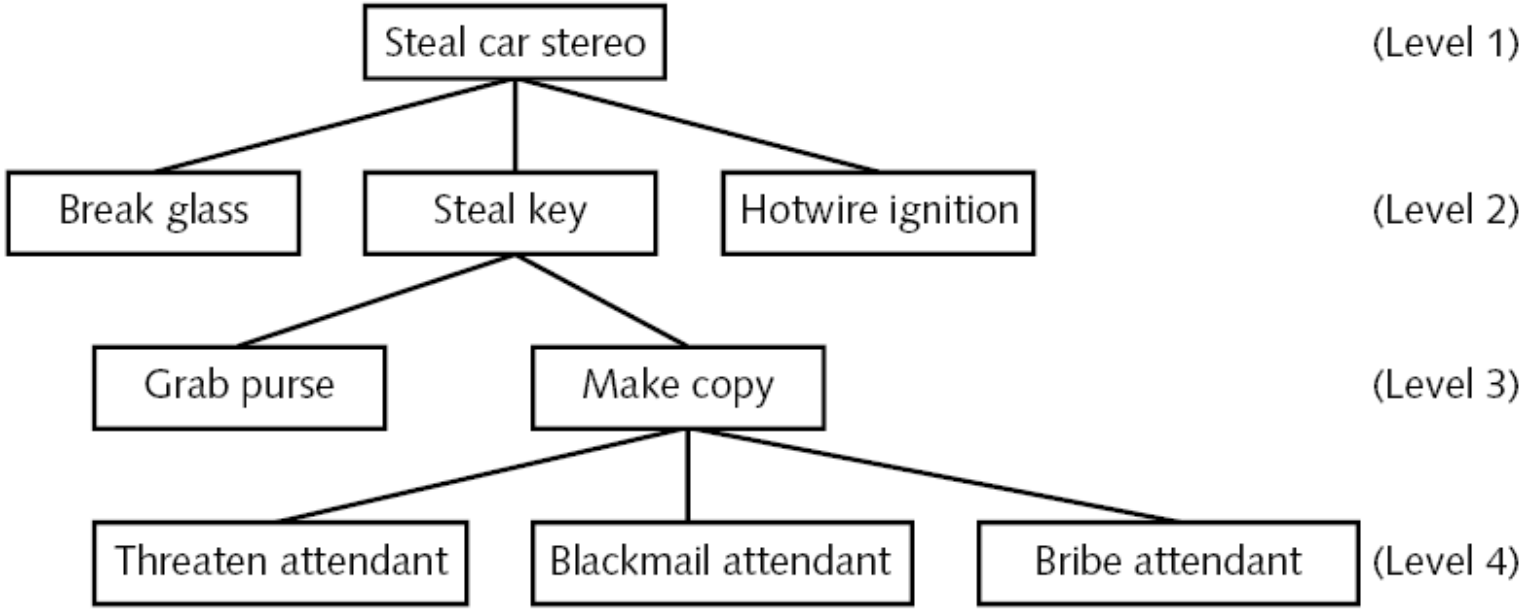

Figure 11-3 Attack tree for stealing car stereo

Risk Identification (continued)

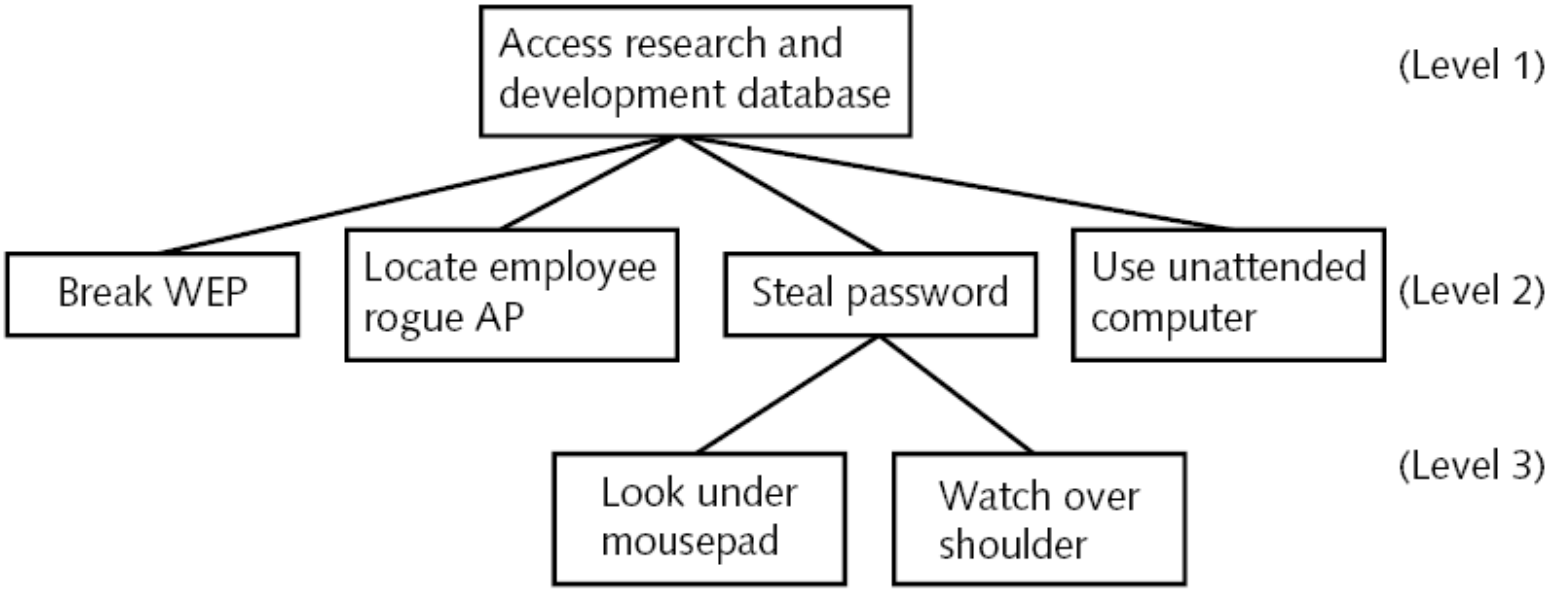

Figure 11-4 Attack tree for accessing a research and development database

Risk Identification (continued)

- Risk assessment
  - Determine damage that would result from an attack
    - And likelihood that a vulnerability is a risk
  - Requires a realistic look at several types of attacks
    - Then, an analysis of the impact can be determined
  - Calculating the anticipated losses can be helpful in determining the impact of a vulnerability

Risk Identification (continued)

Table 11-3 Vulnerability impact scale

Impact	Description
No impact	This vulnerability would not affect the organization. For example, the theft of a mouse attached to a wireless laptop computer would not affect the operations of the organization.
Small impact	Small impact vulnerabilities would produce limited periods of inconvenience and may result in changes to a procedure. A wireless network interface adapter card that fails may require that a spare card be made available and that all cards are periodically tested.
Significant	A vulnerability that results in a loss of employee productivity because of downtime or causes a capital outlay to alleviate it may be considered significant. Malware that is injected into the network through an unprotected access point could be classified as a significant vulnerability.
Major	Major vulnerabilities are those that have a significant negative impact on revenue. The theft of the latest product research and development data through a rogue access point could be considered major.
Catastrophic	Vulnerabilities that are ranked as catastrophic are events that would cause the organization to cease functioning or be seriously crippled in its capacity to perform. A tornado that destroys the office building could be a catastrophic vulnerability.

Risk Identification (continued)

- Risk assessment (continued)
  - Formulas for calculating the anticipated losses
    - Single Loss Expentacy (SLE)
      - Expected monetary loss every time a risk occurs
    - Annualized Loss Expentacy (ALE)
      - Expected monetary loss that can be expected for an asset because of a risk over a one-year period
  - Next step is to estimate the probability that the vulnerability will actually occur

Risk Identification (continued)

- Risk assessment (continued)
  - Risks for the most important assets should be reduced first

Risk Identification (continued)

Table 11-4 Risk identification steps

Risk Identification Action	Steps
A. Asset identification	1. Inventory the assets 2. Record asset attributes 3. Determine the asset's relative value
B. Threat identification	1. Classify threats by category 2. Design attack tree
C. Vulnerability appraisal	1. Determine current weaknesses in assets 2. Use vulnerability scanners on hardware and software
D. Risk assessment	1. Estimate impact of vulnerability on organization 2. Calculate loss expectancy 3. Estimate probability the vulnerability will occur 4. Decide what to do with the risk

Designing the Security Policy

- Definition of a policy
  - Policy is a document that outlines specific requirements or rules that must be met
  - Characteristics
    - Policies define what appropriate behavior for users is
    - Policies identify what tools and procedures are needed
    - Policies provide a foundation for action in response to inappropriate behavior
    - Policies may be helpful in the event that it is necessary to prosecute violators
    - Policies communicate a consensus of judgment

Designing the Security Policy (continued)

- Definition of a policy (continued)
  - Policy is the correct means by which an organization can establish standards for wireless security
  - Standard is a collection of requirements specific to the system or procedure that must be met by everyone
  - Guideline is a collection of suggestions that should be implemented
- Attitudes toward a security policy
  - Must have users “buy in” to policy and willingly follow it
  - Not all users have positive attitudes about security policies

Designing the Security Policy (continued)

Table 11-5 Attitudes towards security

User Group	Attitude toward security
Users	Want to be able to get their work done without restrictive security controls.
System support personnel	Concerned about the ease of managing systems under tight security controls.
Management	Concerned about cost of security protection for attacks that may not materialize.

Designing the Security Policy (continued)

- Balancing control and trust
  - Creates effective security policies
  - Models of trust
    - Trust everyone all of the time
    - Trust some people some of the time
    - Trust no one at any time
  - Control
    - One of the major goals of a wireless security policy
    - Security needs and the culture of the organization will play a major role in deciding the level of control

Designing the Security Policy (continued)

- Elements of a security policy
  - Due care
  - Separation of duties
  - Need to know
  - Due care
    - Obligations imposed on owners and operators of assets
      - To exercise reasonable care of the assets and take necessary precautions to protect them
    - Care that a reasonable person would exercise under the circumstances

Designing the Security Policy (continued)

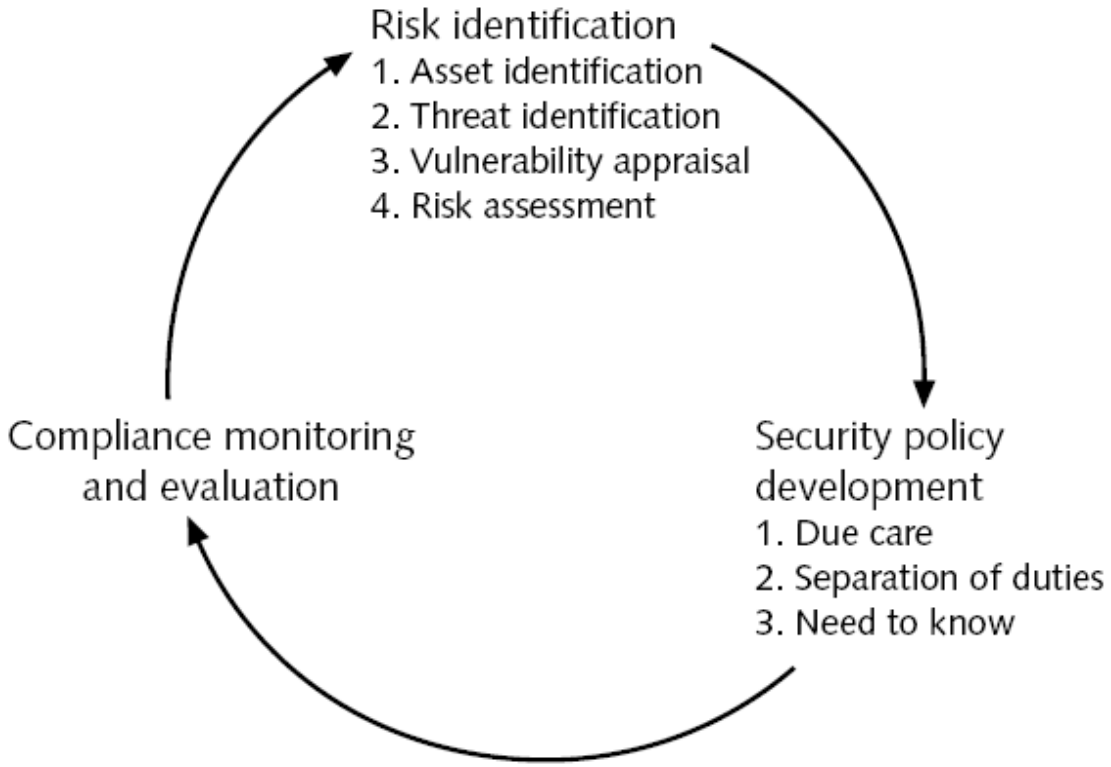

Figure 11-5 Security policy elements

Designing the Security Policy (continued)

- Elements of a security policy (continued)
  - Separation of duties
    - One person's work serves as a complementary check on another person's actions
    - No single person should have total control from initialization to completion
    - Requires the segregation of administrative, development, security, and user functions
      - To provide security checks and balances
  - Need to know
    - Restrict who has access to the information

Designing the Security Policy (continued)

- Elements of a security policy (continued)
  - Need to know (continued)
    - Only that employee whose job function depends on knowing the information is provided access
    - Access to data should always be on a need-to-know basis
    - Need-to-know decisions should be conducted at the management level of the organization
      - And not by individual users
- Policy creation
  - Consider a standard set of principles

Designing the Security Policy (continued)

Table 11-6 Policy *must* and *should* statements

Security Policy Must	Security Policy Should
Be implementable and enforceable	State reasons why the policy is necessary
Be concise and easy to understand	Describe what is covered by the policy
Balance protection with productivity	Outline how violations will be handled

Designing the Security Policy (continued)

- Policy creation (continued)
  - Should be the work of a team and not one or two technicians
  - Types of representatives
    - Senior-level administrator
    - Member of management who can enforce the policy
    - Member of the legal staff
    - Representative from the user community
  - Team should first decide on the scope and goals of the policy
    - Scope states who is covered by the policy

Designing the Security Policy (continued)

- Policy creation (continued)
  - Team should first decide on the scope and goals of the policy (continued)
    - Goals outline what the policy attempts to achieve
  - Team must decide how specific to make the policy
  - Points to consider when creating a security policy
    - Communication is essential
    - Provide a sample of people affected by the policy with an opportunity to review and comment

Designing the Security Policy (continued)

- Policy creation (continued)
  - Points to consider when creating a security policy (continued)
    - Prior to deployment, give all users at least two weeks to review and comment
    - The team should clearly define and document all procedures
    - Allow users given responsibility in a policy the authority to carry out their responsibilities

Compliance Monitoring and Evaluation

- Necessary to ensure that polices are consistently implemented and followed properly
- Involves the proactive validation that internal controls are in place and functioning as expected
- Principles
  - Clear definition of the controls
  - Continual oversight
  - Validation by an external unit
  - Use of scanning tools
- Fine-tune the policies because of changes in the organization or the emergence of new threats

Compliance Monitoring and Evaluation (continued)

- Change management
  - Manages the process of implementing changes
- Some of the most valuable analysis occurs when an attack penetrates the security defenses
- Incident response
  - Outlines the actions to be performed when a security breach occurs
  - Most incident responses include the composition of an incident response team (IRT)

Compliance Monitoring and Evaluation (continued)



Figure 11-6 Compliance monitoring and evaluation

Compliance Monitoring and Evaluation (continued)

- Incident response
  - Incident response team (IRT) members
    - Senior management
    - IT personnel
    - Corporate counsel
    - Human resources
    - Public relations
  - IRT must convene and assess the situation
    - Quickly decide how to contain the incident
    - Determine the cause of the attack, assess its damage, and implement recovery procedures

Compliance Monitoring and Evaluation (continued)

- Code of ethics
  - Encourages members of professional groups to adhere to strict ethical behavior within their profession
  - Codes of ethics for IT professionals
    - Institute of Electrical and Electronics Engineers (IEEE)
    - Association for Computing Machinery (ACM)
  - States the values, principles, and ideals that each member of an organization must agree to
  - Intended to uphold and advance the honor, dignity, and effectiveness of the organization
  - Helps clarify ethical obligations and responsibilities

Types of Wireless Security Policies

- Most organizations choose to break security policy down into subpolicies
  - That can be more easily referred to

Types of Wireless Security Policies (continued)

Table 11-7 Examples of security policies

Name of security policy	Description
Acceptable encryption policy	Defines requirements for using cryptography in wireless transmissions
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and wired as well as wireless computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments, investigate incidents, to ensure conformance to security policies, or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel
Demilitarized zone security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail

Types of Wireless Security Policies (continued)

Table 11-7 Examples of security policies (continued)

Name of security policy	Description
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
VPN security policy	Establishes requirements for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the organization's network through a wireless connection
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Acceptable Use Policy (AUP)

- Defines what actions the users of a system may perform while using the wireless network
- Typically covers all computer use, including wireless, Internet, e-mail, Web, and password security
- Should have an overview regarding what is covered by this policy
- Should provide explicit prohibitions regarding security and proprietary information
- Policy for unacceptable use should also be outlined

Password Management Policy

- Should clearly address how passwords are managed
- Users should be reminded of how to select and use passwords
- Should specify what makes up a strong password
- Public access WLAN use policy
  - Addresses accessing public hotspots

Password Management Policy (continued)

- Public access WLAN use policy (continued)
  - Provisions
    - Do not use a public access wireless network without first determining its level of security
    - All wireless devices must be configured for security
    - All wireless network interface card adapters must be configured for security
    - Only access secure Web sites that are protected by Secure Sockets Layer (SSL)
    - All documents transferred over a public access WLAN must be encrypted
    - Do not use instant messaging

Password Management Policy (continued)

- Public access WLAN use policy (continued)
  - Provisions (continued)
    - Do not connect to the organization's network without using the virtual private network (VPN)
- Virtual Private Network (VPN) policy
  - Regulates the use of an organization VPN

Summary

- Security policy
  - Document that outlines the protections that should be enacted to ensure that the assets face minimal risks
- Four steps in risk identification
  - Inventory the assets and their attributes
  - Determine what threats exist against the assets
  - Determine whether vulnerabilities exist
  - Make decisions regarding what to do about the risks
- A security policy development team should be formed to create the security policy

Summary (continued)

- Compliance monitoring is the validation that the controls are in place and functioning properly
- Because a security policy is comprehensive and detailed, most organizations break it into subpolicies