

STATE OF ALABAMA

Information Technology Standard

STANDARD 643S1-00: WIRELESS NETWORKS

State policy prohibits access to State networks via unsecured wireless communication mechanisms. Only wireless systems that meet State standards, or have been granted an exclusive waiver by the State CIO, are approved for connectivity to State networks. This standard describes how wireless networks are to be planned, implemented, and maintained by State of Alabama entities.

OBJECTIVE:

Ensure all organizations deploy, manage, and/or utilize wireless technologies with an acceptable level of security.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-48: Wireless Network Security, and NIST Special Publication 800-97: Guide To IEEE 802.11i: Establishing Robust Security Networks, State of Alabama organizations that deploy, manage, or utilize wireless networks shall comply with the following requirements:

INITIATION

Undertake wireless network deployment for operations only after conducting a thorough risk assessment to understand WLAN threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.

The authentication server (AS) should be among the most secure servers in the enterprise because a breach of an AS could allow an adversary to access the network without a physical connection, perhaps even beyond the organization's physical perimeter, therefore, AS operating system and application security configuration shall meet or exceed State standards for server security.

Administration and network management of WLAN infrastructure equipment requires strong authentication and encryption of all communication. If an organization uses Simple Network Management Protocol (SNMP) to manage its equipment, it shall use SNMPv3. Use SSL/TLS or an equivalent protection (e.g., IPsec VPN) for Web-based administration.

Promote awareness of the technical and security implications of wireless technology.

PLANNING AND DESIGN

Conduct a site survey to determine the proper location of access points (APs), given a desired coverage area. The site survey shall result in a report that proposes the location for each AP, graphically notes its usable coverage area, and assigns it an IEEE 802.11 radio channel. The estimated usable range of each AP should not extend beyond the physical boundaries of the facility unless required. Place APs in secured areas to prevent unauthorized physical access and user manipulation. Position APs away from exterior walls and windows; use interior walls or position near

the center of the room if possible. After deployment, empirically test AP range boundaries to determine the precise extent of wireless coverage. Include survey results in site security plans.

Create a dedicated Virtual LAN (VLAN) to support AP connections to the distribution system (e.g., enterprise wired network).

Ensure that network management information between APs/ASs and network management servers or console is transmitted over a dedicated management VLAN. Out of band channels are particularly useful during denial of service attacks, when severe congestion on data channels may prevent administrators from implementing corrective security measures if those data channels are the only ones available to them.

Both APs and ASs shall send event data to a secure audit server in real time so that the integrity of previously captured audit data is protected even when the AP or AS is compromised. Events to be captured shall include, at a minimum, both successful and unsuccessful authentication and association attempts. Store audit records in accordance with applicable State standards.

Utilize the Protected Extensible Authentication Protocol (PEAP) method for WLAN authentication.

Document the fallback procedure for when WLAN authentication fails. This may involve:

- Calling the help desk to reset a password.
- Verifying user identification and authorization.
- Installing client certificate if necessary.

Deploy wireless intrusion detection systems to detect suspicious or unauthorized activity. The radio coverage of wireless intrusion detection devices should be at least as great as that of the WLAN they are intended to protect.

PROCUREMENT

The Wi-Fi Alliance industry group certifies WLAN products as meeting specific standards. When a WLAN product is marked as Wi-Fi compliant, the product was evaluated by the Wi-Fi Alliance laboratory and meets the requirements found in the IEEE 802.11a, b, or g standards. Products certified as Wi-Fi WPA2 implement the requirements of the IEEE 802.11i specification.

Procure only WPA2-Enterprise certified devices and AP products. Only WPA2-Enterprise certified products are capable of fully implementing the IEEE 802.11i RSN protections.

Procure products that use FIPS-validated cryptographic modules.

Procure devices and APs that support NIST AES key wrap with 128-bit HMAC-SHA-1 to protect transient keys during the 4-Way and Group Key Handshakes.

Procure ASs and APs that communicate in a secure manner.

Procure products that support PEAP. Test interoperability between devices and ASs before final procurement.

Procure APs and ASs that terminate associations after a configurable time period.

Procure APs that log security relevant events and forward them to a remote audit server in real time. The AP shall support the functional audit requirements in applicable State standards.

Procure APs that can support an independent management interface to the distribution system (e.g., wired network). An independent management interface enables maintainers to utilize an out of band channel for key transfer and other administrative functions.

Procure APs that support SNMPv3 if the organization plans SNMP-based AP management.

Procure APs that support authentication and data encryption for administrative sessions (e.g., SSL/TLS support for Web-based administration and secure shell (SSH) for command-line administration).

Procure client devices whose software can be configured to specify valid ASs by name.

Procure APs and ASs that can support IPsec or alternative security methods to establish a mutually authenticated secure communications channel between AP and AS.

Procure APs and ASs that support Network Time Protocol (NTP). The nonce in the 4-Way Handshake shall be based on NTP time whenever possible. NTP allows distributed devices to synchronize timestamps, which is critical to effective log analysis.

Procure products that can be upgraded easily in software or firmware so that they can take advantage of wireless security patches and enhancements released after original delivery.

Organizations planning to deploy a product not meeting the above standards must submit a security plan to the State IT Security Council for analysis and approval.

IMPLEMENTATION

Disable all insecure and unused management protocols (e.g., SNMPv1 and SNMPv2) on the APs, and configure remaining management protocols for least privilege (i.e., read only) unless write access is required (e.g., to change configuration settings as part of an automated incident response procedure). Disable SNMP if it is not used.

Ensure that all APs have strong, unique administrative passwords.

Disable WEP and all other unused protocols in the configuration of each AP.

Activate logging, direct log entries to a remote audit server, and review logs in accordance with State log management standards.

OPERATIONS AND MAINTENANCE

Enforce user authentication at the wireless access point before granting access to State network resources. All implementations must support and employ strong user authentication which checks against an external database such as RADIUS or Kerberos.

Implement two-factor authentication whenever practical, particularly for administrative connections to the WLAN infrastructure.

Proactively search reports on newly discovered wireless threats and vulnerabilities. Newly discovered security vulnerabilities of vendor products shall be handled in accordance with State of Alabama vulnerability management programs.

Ensure passwords are being changed in accordance with State standards.

Maintain a complete inventory of all WLAN components, especially APs. A complete inventory of an organization's authorized APs is the basis for identifying rogue APs during security audits.

Perform comprehensive WLAN security assessments semi-annually. WLAN security assessments shall include verification of device, AP and AS configuration settings, review of audit logs, and radio detection of rogue APs (scan monthly for rogue APs).

User authentication mechanisms shall be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.

Ensure that management traffic destined for APs is on a dedicated wired subnet or VLAN.

When practical, use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.

Authorized personnel shall restore an AP to its proper security configuration following a reset (security settings typically are returned to factory defaults after a reset event).

DISPOSITION

When disposing of a WLAN component, remove all sensitive data and configuration information.

- Use degauss devices when feasible,
- Disk wiping utilities can be used for devices that have hard disks, or
- Clear configuration settings manually using the management interface.

When disposing of a WLAN component, ensure that its audit records are retained as needed to meet legal or other requirements. Collecting audit records in a centralized hardened system (as required by State IT Standard 677S1) and performing regular backups of that system shall facilitate the retention of records.

PRODUCT REGISTRATION

All wireless APs connected to the State network that are not managed by ISD shall be registered with ISD. Non-registered APs are not authorized and shall be removed from service.

APs are subject to periodic vulnerability scanning in accordance with State of Alabama Risk Management Policy and applicable State standards.

ADDITIONAL INFORMATION:

Information Technology Policy 643: Wireless Security

http://cybersecurity.alabama.gov/documents/Policy_643_Wireless_Security.pdf

Information Technology Standard 643S2: Wireless Clients

http://cybersecurity.alabama.gov/documents/Standard_643S2_Wireless_Clients.pdf

Information Technology Standard 643S3: Bluetooth Security

http://cybersecurity.alabama.gov/documents/Standard_643S3_Bluetooth_Security.pdf

Information Technology Dictionary

http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
643S1-00	09/01/2011	Replaces Standard 640-03S1 (format and number change only)