Wireless Networking and Security Standards

Esther Silver on January 28, 2020

Policy Type

Standard

Summary

These standards address the need for an organized approach in deploying wireless technologies on the UCSF enterprise network. Adherence to these standards will allow UCSF schools, departments and individuals (including students in residence halls connected to the UCSF network) to deploy wireless networks without compromising the integrity of the campus network. These standards also encourage choices that will result in optimal compatibility between campus wireless local area network (WLAN) installations and will facilitate compatibility with the Medical Center's WLAN. Compatibility will result in better user experiences and lower support requirements.

Definition of Terms

Access point: The term access point includes special-purpose hardware as well as general-purpose computers that are configured to act as base stations or transceivers for wireless LANs. For pure peer-to-peer applications (where it may not be clear which system is the base station), one unit should be registered, so that the channel, SSID, and other information are in the database.

IEEE Institute of Electrical and Electronics Engineers or IEEE, the organization responsibility for setting industry-wide data communications standards including wireless LAN standards.

Radio Frequency (RF) Site Survey: A procedure that identifies the optimal locations for access points in order to maximize coverage and minimize interference. Typically this is done

with specialized equipment operated by trained personnel.

Secure Mounting: Mounting access points in a physically secure manner introduces physical security in addition to network security. Access points are far less likely to be stolen or removed without authorization. In addition, unauthorized configuration changes to the access points are less likely to occur. Secure mounting is easy to implement, and provides a baseline of security and interoperability.

SSID: The SSID (Service Set Identifier) is a token in wireless data communication packets that identifies an 802.11 (wireless) network. It identifies the name of a wireless network. All of the wireless devices on a WLAN must employ the same SSID in order to communicate with each other. Wireless access points can be configured to broadcast their SSID or not to broadcast their SSID.

VPN: An approach to providing authentication and secure data communications. VPN (Virtual Private Network) technology creates an encrypted layer of networking on top of another network, including a wireless network. VPN technology provides an effective and secure means of accessing computers on the UCSF network. A user's computer must run VPN client software in order to use VPN technology. VPN client software is available for nearly all computers and operating systems, including laptops.

WAP: Wireless access point. Also sometimes referred to as the wireless base station.

WEP: Wireless encryption protocol. WEP is an approved standard for encrypting data in a wireless network and is intended to protect privacy. An encryption key or password must be specified by the user, and the same key must be used by all parties wishing to communicate. WEP keys can be either 40-bits or 128-bits in length; 128-bit keys provide stronger encryption. WEP does not provide an authentication mechanism; that is, it does not control who can use your network. (The same can be said of any end-to-end encryption protocol, since anyone who knows the encryption key can decrypt encrypted data.)

WPA: The Wi-Fi Protected Access (WPA and WPA2) protocol implements the majority of the IEEE 802.11i [1] standard, specifying security mechanisms for wireless networks [2]. It replaced the short *Authentication and privacy* clause of the original standard with a detailed *Security* clause, in the process deprecating the broken WEP [3]. Further, the Temporal Key Integrity Protocol [4] (TKIP) for stronger encryption key protection was brought into WPA.

802.1x: 802.1X is an IEEE standard for providing authentication, controlling user traffic, and dynamically varying encryption keys for both wired and wireless Ethernet networks. 802.1X is particularly well suited for wireless LAN applications because it requires very little processing power on the part of the Authenticator. In wireless LAN applications, the Authenticator is the wireless access point.

802.11i: 802.11i is an amendment to IEEE 802.11 which replaces insecure components and updates standards to match newer technology.

Standard Practice

This section summarizes a model that is appropriate for wireless networks and wireless access points connecting to the UCSF enterprise network. Additional capabilities can be added by users and by Information Technology Services (ITS) as the central Authentication and Authorization system permits.

Access points that are configured to support the following standards are acceptable for use on the UCSF campus network following the posted procedure for notifying ITS of access point installation.

General:

1. Ownership
    1. Wireless LAN implementations are the responsibility of the units that control the space in which they operate unless an alternative responsible party is documented with ITS.
    2. Units are expected to know what is occurring in that space, and to take steps to make sure that all wireless implementations active in their space follow the standards defined here.
    3. Every wireless LAN installation within UCSF must be authorized by the leadership of the unit in which it is occurring. While they may choose to delegate details to technical staff, the department chair or other responsible person should know what activities are occurring and take responsibility for verifying that a security plan exists and that proper coordination is occurring with other units close enough that interference might occur.
2. Due diligence
    1. Anyone installing wireless LAN equipment is required to check the registration database prior to installation for conflicting station identifiers (SSID), and not to install any new equipment that might reasonably be expected to interfere with existing equipment without first discussing their plans with contacts for the existing equipment.
    2. Any installation over three (3) wireless access points by a department in proximity to each other must be accompanied by a Radio Frequency Site Survey.
    3. Service Set Identifiers (SSID) must be set so that they do not conflict with reserved UCSF names and so that they will not cause confusion with neighboring wireless networks.
3. All wireless access points must be securely mounted so that they are inaccessible to unauthorized personnel.
4. All wireless access points must be registered with ITS.

Interference Management:

1. Conflicting or overlapping set service identifiers (SSID) can cause confusion and could inadvertently allow data leakage. ITS and the Medical Center reserves the following SSID names for Campus wide initiatives:
    1. CommunityCenter
    2. UCSF
    3. UCSFMC-HotSpot
    4. UCSFguest
    5. UCSFnet
    6. UCSFvpn

7. UCSFwpa
2. Wireless access points utilize shared public radio spectrums and can interfere with the operation of communications and computational devices
    1. Wireless access point owners are responsible for ensuring non-interference with proper operation of the UCSF wired and wireless networks.
    2. Wireless communication networks must be consistent with Federal and State laws and regulations

Security and Information Protection:

1. Every wireless LAN implementation within UCSF must be done in accordance with a security plan. This plan must address at least the following issues:
    1. Restricting access to the network so that only authorized people can use it
    2. Preventing unauthorized users from being able to see confidential data appearing on the network, particularly UCSF passwords
2. The Security Incident Response program will include a wireless security response procedure in the event of unauthorized wireless access points are detected.
3. Vendor default settings such as encryption keys, SNMP passwords, preshared keys (PSK), and passphrases for wireless access points must be changed based on the UCSF Password Standard [5].
4. Wireless access point owners and managers are responsible for updating software, hardware and firmware of devices to ensure that vulnerabilities are addressed.
5. Wireless networks which provide access to the UCSF campus network must limit usage to authorized users with one of the following methods:
    1. *As of July 1st 2010 this option is mandatory for wireless networks comprised of three (3) or more access points.*
    2. *As of July 1st 2010 this option is restricted to wireless networks comprised of two (2) or less access points.*
    3. Legacy host based authorization systems utilizing the machine address code (MAC) may continue to be used until June 30th 2010. In the interim it is strongly recommended that the vpn@UCSF [6] system be used to protect the communications of the wireless network user.
6. Encryption and Data Protection:
    1. WPA2/AES-CCMP as defined by 802.11i is strongly recommended for departments that deal with highly sensitive information such as patient and HR/staff information. WPA2/AES-CCMP provides a higher degree of encryption protection for sensitive data being transmitted wirelessly.
    2. WPA and WPA2 (RSN) as defined by 802.11i are the standard protocols for UCSF wireless security.
    3. WEP on existing wireless access points must be updated to WPA or phased out by June 1, 2010. In the interim it is strongly recommended that the vpn@UCSF [6] system be used to protect the communications of the access point users.
7. Wireless networks which do not support encryption and authentication:
    1. Until June 30th 2010 it is strongly recommended that the vpn@UCSF [6] system be utilized to protect communications to provide both user authentication as well as data protection.
    2. Starting July 1st, 2010 unencrypted wireless networks must restrict user access to the following:
        1. Informational pages regarding network access, local service or customer support and helpdesk.

    2. Access to vpn@UCSF [6] or an ITS approved authentication portal
    3. Access to a specific system or service for which the wireless network has been created so long as that system or service contains no restricted or private data.
8. Wireless network security awareness should be part of the existing end user security education program.

Operational/Functional Impact

Wireless access points are radio transmitters and receivers. As such, they do not respect walls, building, or even campus boundaries. They can be subject to interference from other access points or interfere with other communications devices just as one radio station can cause interference to another. Therefore, the use of wireless LAN is by default a community matter. Users will have to work collaboratively with others to install wireless technology, and registration of access points to minimize interference and maximize security is essential.

Technical Impact

To support implementation of these guidelines, ITS will:

1. Provide a web based device registration system which will notify users if they are attempting to use a duplicate SSID
2. Create web-based configuration instructions for a limited preselected list of vendor access points.
3. Assist units with configuration of a limited preselected list of vendor access points.
4. Assist departments in developing wireless plans if desired.
5. Recommend consultancies and value added resellers to assist in RF Site Surveys or the design of a wireless network solution.

Considerations and Rationale

The goal of this document is to provide wireless LAN security using open standards. The practice of proper deployment of the security standards has become the focus on risk mitigation in the use of wireless networking. This document will be reviewed by the Network and Security Committees in 12-18 months to ensure that it reflects the current state of the art in wireless technologies.

Compliance Issues

Existing access points which are not currently or are unable to become compliant with these standards are to be reconfigured to allow access only to non UCSF enterprise networks (the Internet). VPN use for UCSF intranet access is permitted. For non-compliance to this standard with business reasons, please contact Security & Policy (S&P) for an exception request and handling. Non-compliant access points without authorized exceptions to this standard will be disconnected from the UCSF enterprise network. Access points causing impact to the UCSF campus wired or wireless networks may be removed if attempts to remediate are unsuccessful.

For those exceptional wireless connectivity arrangements, ITS Security & Policy can assist in the risk analysis, the configuration, and provide information for upgrading of switches and routers connecting to these wireless access points.

Security Issues

Implementation and enforcement of these wireless security standards will increase the overall security of campus networks and systems.

Suggested Products

ITS and Enterprise Network Services provide managed wireless services for departments utilizing the Aruba Wireless LAN products. Departments currently seeking or planning to seek ENS managed services should only review products from the Aruba line.

Departments internally responsible for the management of wireless access devices should review the specific needs of their environment. Enterprise class wireless access devices will meet the requirements set out in this document such as those provided by Aruba and Cisco.

Acknowledgments

These standards were developed through the efforts of Network and Security Committees members and their advisers.

Links
[1] https://en.wikipedia.org/wiki/IEEE_802.11i-2004
[2] https://en.wikipedia.org/wiki/Wireless_LAN
[3] https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
[4] https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
[5] https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0
[6] mailto:vpn@UCSF