UCSB Office of Information Technology
Campus Network Programmers
Network Policy Document
Wireless Data Networking Circular
DRAFT 4/28/2003 8:06 AM

Wireless data networking products based upon Institute of Electrical and Electronics Engineers (IEEE) 802.11[1] technologies are commonly available and very inexpensive. They are also quite popular, in large part due to the "out of the box" experience of immediate, easy network access. Typical wireless products include "access points", which connect between wired and wireless networks, and network cards, typically used by "mobile users" with laptop computers or personal digital assistants (PDAs).

While these products may be configured for use in a home environment, institutional deployments require additional considerations. These issues include deployment conflicts, roaming support, access control, accountability, user privacy, Wired Equivalent Privacy (WEP) deficiencies, and technology evolution. Examining these considerations highlights deficiencies inherent to standard wireless products currently available in the market.

Deployment conflicts occur when wireless technologies interfere with each other or other institutional research or services. Deployment conflicts may occur as individual access points are installed in relatively close proximity. 802.11b wireless supports eleven channels, which are radio frequency ranges used for wireless communications. These channels overlap, resulting in only three non-overlapping channels[2]. Without coordination, overlaps are likely to occur and will reduce network performance. Within the campus environment, it is possible for deployment of wireless networking to impact research projects that are sensitive to radio frequencies. Also, the institution has an interest in prioritizing deployments such that a campus-wide deployment of wireless networking would generally have priority over individual deployments. Other deployment conflicts may arise when adjacent access points provide conflicting or insufficiently distinguishable information to mobile users.

Roaming support refers to network architectures that permit a mobile user to switch between access points without experiencing a significant disruption in their network connection. This is similar to cellular telephone systems. Individual access point deployments may not support roaming, but in a larger infrastructure it is generally desirable to support a consistent access model with roaming support.

---

[1] Frequently referred to as "WiFi", and based upon 802.11b, 802.11a, or 802.11g standards.

[2] See http://www.extremetech.com/article2/0,3973,709233,00.asp for more information and a case supporting the use of four channels.

Access control refers to the ability to limit network access to known parties. Unrestricted wireless access to the campus data network creates an environment where activities in violation of policy or law, or detrimental to operation of the network, may occur without effective institutional recourse. As wireless networking grows in popularity, the existence of "open" or unrestricted access points creates an unmanaged environment with the potential for significant institutional liability. Most access points are completely open by default, and many lack the ability to provide granular access control.

Accountability is related to access control, in the sense there is an institutional need to reliably identify the individual computer systems from which unusual or clearly improper activity originates. Access points commonly support Network Address Translation (NAT), which modifies traffic passing through such that the source computer may not be readily distinguished from others using the access point. It is possible to have a deployment that provides access control, but lacks adequate information to permit accountability, particularly when problems are discovered "after the fact."

User privacy is a concern in any shared network, where online activities and personal data may be exposed to a third party. Such exposure may include web browsing habits, credit card information, user names and passwords, or private email viewed during a wireless network session. Default wireless installations typically provide no protection against data being intercepted by a third party as it is transmitted. The use of WEP can reduce the exposure, although the value is limited. Current wireless technology standards do not provide reliable user privacy. Mandatory use of VPN (virtual private network) clients can provide strong encryption and user privacy, but this approach requires significant effort to design, deploy, and maintain, and rarely supports a wide range of client platforms.

WEP is an encryption technique intended for use between mobile users and access points. It is a system based upon a single shared key, meaning data is encrypted and decrypted using the same secret key. All users of a particular access point must know the WEP key, and thus they can all read each other's wireless data. In a home environment, a shared WEP key is only known by a very few trusted parties, but widely distributing a shared key in an institutional setting eliminates much of its value. The implementation of WEP encryption has also proven to be flawed[3], so untrusted parties may intercept encrypted traffic and ultimately discover the shared key. A WEP key may be discovered within a day using readily available tools.

Wireless networking products have been available for several years, yet manufacturers and vendors have been slow to address the deficiencies described above. This may be due to initial marketing plans, which appear to target end-users rather than enterprise information technology departments. The primary 802.11 industry trade association, The Wi-Fi Alliance[4], has recently adopted some interim technology drafts (known

---

[3] See http://www.cs.rice.edu/~astubble/wep/wep_attack.html regarding passive WEP key cracking.

[4] http://www.wi-fi.org

collectively as WPA, or Wi-Fi Protected Access) in an attempt to address concerns that have resulted in deferred or limited wireless installations in enterprise markets. Similarly, the IEEE has been working on additional standards designed to correct deficiencies in authorization, accounting, and privacy inherent to most current products. Certain vendors have implemented proprietary or draft standards-based technologies[5], although interoperability and backwards compatibility may not be possible with these implementations. Due to the deficiencies described above, there is no guarantee that present-day investments in wireless data networking will continue to be allowed to operate at UCSB; therefore, they should be considered disposable in the near term.

To summarize, most current standard wireless network devices do not inherently provide effective user privacy, access control, accountability, or conflict management. Additional information regarding the above deficiencies is available from numerous online sources[6]. OIT will track the evolution of wireless technologies and issue updated network attachment requirements as necessary.

---

[5] For example, the Symbol AP 4131 has a pre-standard implementation of TKIP, which provides wireless data privacy through rapid, automatic key rotation.

[6] See *"Wireless Network Security: 802.11, Bluetooth, and Handheld Devices"* at http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf and *"Your 802.11 Wireless Network has No Clothes"* at http://www.cs.umd.edu/~waa/wireless.pdf for additional overview of common wireless security issues.