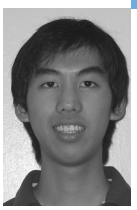
CALVIN ARDI AND DANIEL CHEN

Architecture and Threat Analysis of a Campus Wireless Network



Calvin Ardi is an undergraduate at the University of California at Berkeley, graduating in May 2009 with a BS in Electrical Engineering and Computer Sciences. His interests include learning about communication and social networks, and teaching an introductory course on UNIX system administration.

calvin@rescomp.berkeley.edu

Daniel Chen is currently an undergraduate at the University of California at Berkeley and works for the campus as a system administrator for the Residential Student Services Program. He has interned in the past for Mozilla Corporation, doing work on infrastructure security, and plans to graduate in December of 2008 with a BS in Electrical Engineering and Computer Sciences.

dchen@rescomp.berkeley.edu

AS OF FALL 2007, THERE WERE 34,953 enrolled undergraduate and graduate students [18] and over 20,000 employed faculty and staff [10] at the University of California, Berkeley. How do we design a wireless network that can support convenient access and operate efficiently across a multitude of different devices on a shared medium spanning miles in area and, in an adversarial context, ensure that unauthorized use or abuse of the network does not occur? We examine the AirBears wireless network at the University of California, Berkeley, to gain insight into how such a system can be engineered and deployed.

These days, wide-area deployed wireless networks are available at company workplaces and universities for general use (though not necessarily for the public). However, there do not seem to be very many studies or formal evaluations on the engineering and deployment of such large-scale wireless networks. Lathrop and Welch [8] present a white paper in which they conduct a study of the wireless local area network (WLAN) located at the United States Military Academy. They detail many possible attacks that can be used on their 802.11a WLAN and present recommendations on how to secure authentication to and communication on the network. Our study focuses on the architecture of a large-scale 802.11b/g WLAN, and we present possible scenarios in which a malicious user could launch attacks.

Other studies [17,11,15] focus primarily on usage analysis of WLANs. Schwab and Bunt [15] present the results and usage analysis of a traffic trace on their then newly deployed campuswide wireless network at the University of Saskatchewan in Canada. Through their analysis, they were able to gather information about wireless network use and possibly use it in their design of expanded access throughout campus. Whereas they focus on traffic analysis and usage patterns to influence wireless network design choices, our study attempts to find some of the shortcomings and possible attack scenarios that are inherent within the wireless technology used and the network architecture on AirBears. The discovery and analysis of these shortcomings could possibly be used in design choices when evaluating or engineering a large-scale wireless network.

Site-Specific Policy Concerns

As AirBears primarily serves an academic community, several interesting site-specific policy decisions have arisen. The AirBears team, for example, makes an attempt to upgrade access modules or other network elements whenever possible, but it refrains from doing so at the beginning and end of academic semesters, when students and campus groups would expect and require the proper functioning of the network (for class registration and final exams, respectively).

The network must also be constructed in a manner that allows a wide range of devices to connect, so long as the networked device adheres to a set of security standards [21]. Users may be accessing the network from wireless network-enabled phones, PDAs, or laptop computers with various wireless network adapters. It should not be expected of the users that they purchase specialized hardware or software (aside from the network adapter) to access the network. This contrasts with a corporate environment, in which the allowable devices that can connect to the network and software used can be strictly regulated and uniform throughout (i.e., every employee receives the same laptop computer with more or less the same set of software).

DESIRED SYSTEM PROPERTIES

Keeping the general mission in mind, we would like to construct a system that has the following properties:

- Access Control: Network access ought to be open to all legitimate and authorized users, yet control be fine-grained enough to block or revoke access from specific users, if necessary.
- Confidentiality: Wireless communication physically transpires over a shared medium. We would like to ensure that the network protects access to information at higher levels, so that end users may assume that unauthorized access to their information will not occur.
- Integrity: As with any network, we would like to ensure that data is internally consistent and complete; however, in a security context, we want to prevent an attacker from having the capability of modifying data and presenting it as unmodified.
- Availability: Legitimate users of a wireless network ought to have timely service and access to the network when authorized. Thus, we would like to keep illegitimate users from preventing legitimate usage.
- Scalability: We would like to have a network that can expand with minimal to no architecture change to serve both a larger population and a larger physical area with this property.

System Overview

The AirBears network is deployed widely over campus [5] to reach as many users as possible. There are roughly five networking elements used to implement the AirBears network (Figure 1, next page):

- Access Managers: Access managers enforce layer three access control. Each access manager serves captive portal pages to obtain user authentication information.
- Control Servers: Control Servers house user authentication and authorization data. They interface with the directory servers to verify user identity.
- Access Points: 802.11b/g access points provide link-layer connectivity from users to access managers.
- Routers: Routers serve their typical function in a network: allowing information to be passed through the network beyond topologically local elements.
- Distribution Switches: A distribution switch provides typical link-layer connectivity in an efficient manner. Additionally, distribution switches can perform packet classification at port, user, and application levels.

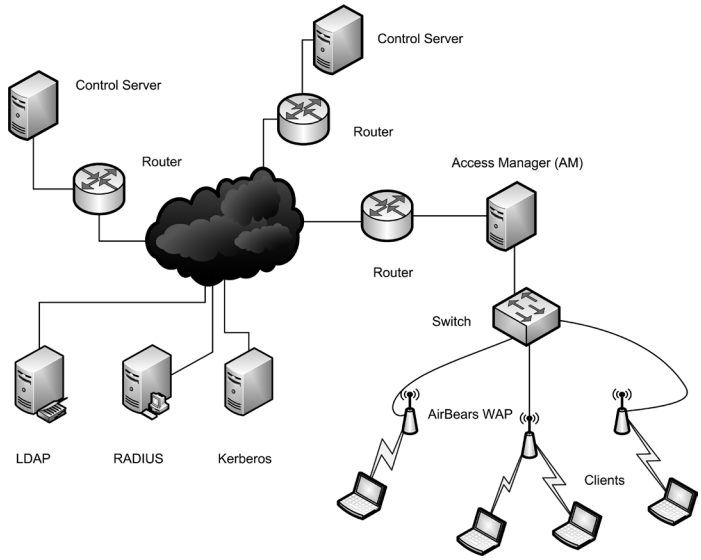


FIGURE 1: NETWORK TOPOLOGY OF THE AIRBEARS WIRELESS NETWORK

Authentication

AUTHENTICATION ELEMENTS

Authentication is realized through interaction among an access manager, a control server, and a user directory, as well as a relatively unintelligent access point that provides layer-two access from users to access managers. Access managers enforce layer-three access control by MAC address; unauthenticated users are required to make a captive portal request to gain access to the network. Load-balanced and mirrored control servers interact with user directories to validate user credentials. Finally, user directories store the credentials of users and handle efficient retrieval of such information.

CREDENTIALS

Each user has an identifier, referred to as a CalNet ID [16]. This electronic identity, based on Kerberos technology, allows users to access UC Berkeley online services. A CalNet ID is a unique nine-digit number and is automatically assigned to registered students, faculty, and staff members. Affiliates and other users may be granted an identifier, along with access to certain applications, by a CalNet Deputy, someone who is authorized and trusted to activate CalNet IDs or reset passphrases.

Passphrases have complexity requirements of nine or more characters, selected from three or more character classes: lowercase or uppercase letters, digits, or nonalphanumeric characters. This information is stored in a centralized Kerberos directory.

In general, users with a valid CalNet ID have access to the AirBears wireless network, among other services that are CalNet-enabled. Additionally, short-term guest accounts specifically for access to the AirBears wireless network can be granted by faculty and staff in certain locations. Guest accounts are given randomly generated identifiers and passwords and are enabled for up to a week. Because such guest information tends to be more mercurial and requires less permanent storage, guest information is stored in an LDAP directory access tree.

Session Overview

A user begins by opening a Web browser and attempting to make an HTTP request. This request is intercepted by the access manager via captive portal, and the user is redirected to an authenti-

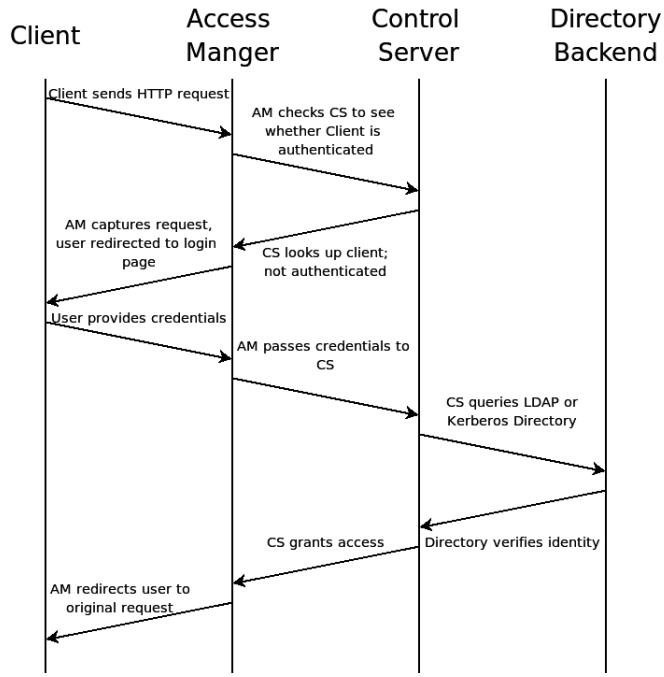


FIGURE 2: A TYPICAL AUTHENTICATION SESSION

cation page. SSL protects user communication with the access manager and allows the user to verify the identity of an access manager.

To proceed with authentication, a user enters credentials into the Web page. The access manager passes these credentials through to the control server, which makes decisions about how to authenticate the user using the RADIUS protocol. Guest accounts are attached to the LDAP profile of a user; the control server will make an SSL-enabled LDAP query against the campus LDAP directory to authenticate a guest. To authenticate a normal user, the control server accesses an active directory using Kerberos.

Once the identity of the user has been validated, the control server will grant a RADIUS access-allowed token to the user, which allows the user to access the network. Only the user's MAC address is associated with the connection and traffic, with a separate log, contained and written to elsewhere, associating the MAC address with the user's identification number. From that point onward, the access manager will be able to determine that a user is authenticated by querying the control server. A user remains authenticated until a session has a 15-minute idle timeout.

Threats

Our attack taxonomy, adapted from Lathrop and Welch [8], characterizes attacks as detailed in the following sections.

UNAUTHORIZED ACCESS

Before an attacker can carry out any attacks at all, he or she must have link access to the network. "Unauthorized access attacks" refers to situations where an attacker circumvents or bypasses authentication or authorization mechanisms designed to prevent unauthorized usage. To some extent, wired networks can rely on physical security to prevent unauthorized network access; short of walking into a building and plugging a computer into an Ethernet jack, an attacker is incapable of accessing the same layer-two segment as a legitimate user. As shown in Lathrop and Welch [8], an attacker can make a simple yagi antenna out of a Pringles can, a steel rod, and some washers, doubling the range at which a wireless network can be accessed. Clearly, in the wireless case, we cannot depend on physical security; any host that can

associate with an access point is potentially part of the same network as a legitimate user and can carry out attacks.

Cryptography and some sort of authorization protocol are typically employed to prevent unauthorized users from associating with an access point; however, as is shown later, particular forms of cryptography have implementation flaws that make them weak. AirBears does not employ encryption, nor does it have any layer-two access control mechanisms, so users associated with the same access point are vulnerable to layer-two ARP attacks, even if the system does not allow an attacker to authenticate.

Additionally, a client associating with the AirBears network is automatically assigned a routable IP address, despite not having authenticated with the access manager. After association, a user will generally attempt to visit a Web site, triggering a DNS lookup. Other types of access (aside from HTTP and DNS queries) are blocked or dropped in some fashion. The campus DNS servers respond with the appropriate answer records, but authentication through the captive portal must be successful before network access is completely enabled. The problem lies within the DNS query access. Whereas other captive portal systems affect DNS by returning the IP of the machine to authenticate with (typically an RFC1918 address with a low TTL), querying the campus DNS nameservers returns the correct answer records. This in itself is not inherently exploitable, but we have verified that DNS traffic to any DNS nameserver is allowed. A simple check can be done by using a multi-platform utility called nslookup and specifying a DNS server to query other than the default ones given through DHCP.

This sets the stage for IP over DNS; by setting up a custom nameserver on a machine the user owns along with specialized software on the client machine, the user effectively has access to the Internet by tunneling all traffic over DNS queries and answers (by appending packets and traffic into certain records). Although this requires a more technically knowledgeable user, there are several Web sites [19,12,7,13] that offer tutorials and the software needed to set up such a tunnel.

SESSION PIGGYBACKING

Even if an attacker cannot bypass authentication mechanisms to gain access to a network, the legitimate session of a user may be piggybacked upon to provide such access. Although the attack presented here is site-specific, lessons can be learned about session piggybacking in general.

By default, AirBears keeps a user authenticated for 15 minutes, even after the user disconnects. Another feature of the network is that the associated state of a client is stored on a central control server; thus, a legitimate user can associate with different access points and remain connected to the network. Unfortunately, the only information used to authenticate a client is its MAC address, so an attacker can passively snoop traffic to determine the MAC address of a legitimate user, then quickly spoof the MAC address of that user's wireless card to gain access to the network after the user disconnects but before that user's session times out.

MAN IN THE MIDDLE

Given the network identifier (SSID), the average user knows the fundamentals of how to connect to the campus wireless network by simply connecting to the network as named. Several man-in-the-middle attacks, combined with some social engineering, can lead to a threat of security as well as individual privacy.

In general, the user does not necessarily know the details of Secure Sockets Layer (SSL) certificates, specifically the importance of a fingerprint. It is assumed, however, that the user does understand whether a Web site being visited is secure or not, given the key indicators of the Web browser being used. For example, Mozilla Firefox 2 highlights the URL of the address and displays a locked padlock in the address bar and on the bottom righthand corner of the application window to signify that communication between the user and the Web site is encrypted. Other browsers present similar indications. These key indicators, however, may not be enough if users are not educated to look for them. Schechter et al. [14] conducted a study measuring the efficacy of security indicators and found that users would enter their passwords even after HTTPS

indicators were removed, a strong sign that a fraudulent login site can be used to harvest credentials.

Consider the scenario in which a rogue access point (AP or ad hoc) is also named "AirBears," a secure Web site emulating the captive portal that the legitimate AirBears network employs, but with an untrusted SSL certificate. Casual users are most likely to click through the warning and continue to enter their credentials, at which point the attacker gains CalNet credentials and any other sniffed information, while still proxying traffic to the Internet.

An alternative situation could be a slight modification to the captive portal Web page. Users are notified that an SSL certificate error should be *expected* and should accept the "temporary" self-signed certificate (or, even worse, install a root certificate). In an attempt to show some sort of validity, a key fingerprint is provided, in addition to the official-looking site.

In order to verify that such an error is to be expected, one would most likely try to find this information from official sources. We are presented with a catch-22: To verify this information from the Web page, we need to connect to the Internet in some fashion. At the same time, to connect to the Internet we need to present our credentials through what could possibly be a malicious rogue access point.

In a conversation with an AirBears administrator, we learned that there was a period of time in which a client connecting to the AirBears network was presented with a SSL certificate mismatch error, owing to some issues with the certificate expiry date. Out of the average of 1500–2000 users connecting to AirBears on a daily basis, only a small percentage refused to log on, with a smaller subset actually reporting the problem by phone or email.

SNIFFING AND EAVESDROPPING

In this threat, an attacker can determine the contents of packets by passively listening to packet transmissions, threatening the confidentiality of the data stream. Cryptography enables a network to protect packet transmissions; however, wireless cryptography protocols have been riddled with flaws in the past.

For instance, Wired Equivalent Privacy (WEP) encryption has been criticized for security flaws in both the design and implementation of the protocol. WEP uses an RC4 stream cipher for encryption. Because the number of IV sequences that can be generated is finite, keystream reuse occurs, which allows a number of techniques, such as frequency analysis and dragging cribs [8], to decode the keystream. Moreover, because the WEP protocol uses a weak message authentication code, messages can be modified, injected, and spoofed, which means that an attacker can insert messages into a communication stream to more easily break the encryption scheme [4]. Even without these flaws, WEP uses a single static shared key to encrypt communications; keeping such a key secret in a system of thousands of users is clearly impractical.

AirBears does not implement any form of encryption currently; if a user wishes to have secure communications, he or she must rely on end-to-end encryption at the application layer.

DENIAL OF SERVICE

Denial of service occurs when an attacker carries out attacks that do not compromise legitimate user data but either abuse legitimate network mechanisms or overutilize network resources in a manner that results in degraded performance for a legitimate user. Note that many classes of attacks that apply to wired networks can apply equally to wireless networks; however, these shall not be discussed, as they are covered elsewhere in the literature.

A number of features in IEEE 802.11 standards introduce denial-of-service vulnerabilities because a lack of authentication exists in management frames. As explored by Bellardo and Savage [3], deauthentication, disassociation, and power-saving messages can cause denial of service. Deauthentication and disassociation attacks are relatively straightforward; an attacker will simply masquerade as a wireless access point and send deauthentication or disassociation messages to a client. This causes the client to end its session with the access point.

Greenstein *et al.* [6] note that 802.11 clients actively scan for networks to which they have been connected in the past. In particular, Windows XP looks for these networks by sending probe request frames, each containing the SSID of the preferred networks. The determined attacker can make note of this and set up a fake AP with the same SSIDs that were sniffed. After a disassociate attack is launched on the victim, the victim then proceeds to connect to the next available preferred wireless network or the fake AP. The user might notice the slight disruption in network connectivity, but so long as the user is able to make use of the network and Internet, he or she is none the wiser. The attacker then proceeds to capture all traffic, perhaps even launching injection attacks to steal authentication information or presenting a fake captive portal authentication page.

A power-saving attack is a little less straightforward. Wireless clients are allowed to enter a sleep state and poll an access point for buffered information periodically; when a client is asleep, an attacker can forge the polling message, which is unauthenticated, resulting in the access point discarding buffered data. In the same vein, power conservation features require synchronized clocks; an attacker can fake time synchronization messages to cause a wireless client and an access point to fall out of sync.

Additionally, there are several publicly accessible resources through the AirBears network that can be overutilized by an attacker to perform a denial-of-service attack. First, the airwaves themselves are in contention; by ignoring MAC-level protocols and broadcasting over a channel with a high-powered transmitter, an attacker can effectively jam the wireless communication medium, preventing legitimate users from communicating with one another.

A more subtle resource attack lies in the nature of the network layer authentication mechanism presented in our framework. Because AirBears provides network access control only at the network layer, an attacker can simply associate with an access point and obtain a public IP. In fact, a large majority of clients connected to the AirBears AP have not authenticated themselves through the captive portal, owing to the default behavior of automatically associating with an available preferred network. If an attacker were to fake 802.11 association frames simulating a large number of users, the IP pool of the AirBears network could quickly be exhausted, preventing legitimate users from using the network.

Countermeasures

EDUCATION

Currently, there is no formal system in place to educate users (students, staff, and faculty alike) about the importance of the CalNet ID, good practices, and general information about AirBears. There exists an online FAQ [20], where it is mentioned that communication across the network is not encrypted, but it does not go into more detail about the authentication process and how to validate the captive portal page. The Web site has been infrequently maintained and not updated to reflect the current technology. Additionally, a bit of work and digging through various Web pages is needed to arrive at the FAQ.

Residential Computing at UC Berkeley [2], a department dedicated to technical and network support for the residence halls on campus, requires that each student living in the dorms attend an information session outlining policies and good security and privacy practices before the student is allowed to connect to the residential wired and wireless networks. This program could be expanded throughout the Berkeley campus; users who wish to gain access to the wireless network would need to attend an information session. Concepts such as unencrypted communication and ways to safeguard privacy and personal information can be taught and discussed, empowering the users to look out for and resist social engineering methods.

END-TO-END AND OTHER ENCRYPTION

Because the medium is unencrypted, users should have the option of encryption through the use of a Virtual Private Network (VPN). Although technically savvy users have the option of tunnel-

ing traffic over Secure Shell (SSH), in most cases the average user does not have SSH access to a machine or knowledge of tunneling over SSH to provide the necessary encryption of transmitting data over a wireless network.

This does not solve all problems; any traffic that takes place after reaching the computer being tunneled to (VPN or otherwise) is unencrypted if end-to-end encryption isn't available or used. Many sites, for example, will authenticate users through HTTPS, but then switch over to HTTP for regular use. To protect privacy and security, users should be informed of and make extensive use of connecting to sites in a secure manner.

As mentioned earlier, WEP has been proven multiple times to be insecure and deprecated for use in securing wireless networks. Its successors, Wi-Fi Protected Access (WPA) and WPA2 provide confidentiality by implementing some and all, respectively, of the IEEE 802.11i standard (now incorporated into the IEEE 802.11-2007 standard) [1]. Combined with 802.1X's support for authentication and RADIUS servers for key exchange, implementation of the 802.11i architecture would handle client authentication and encrypted communication between the client and AP.

Although WPA/WPA2 is an effective means of providing confidentiality, it may never be fully implemented or required on the AirBears network. In a conversation with the AirBears administrators, it was noted that there are still a significant number of wireless devices in use that do not support WPA. Until the legacy hardware is no longer used, only a hybrid (and perhaps overly complicated) implementation of WPA and no encryption on separate networks can be done, at best.

LINK-LAYER ACCESS CONTROL

Proper link-layer access control mechanisms can prevent attackers from gaining access to a network, which makes it impossible for them to carry out attacks. Related work done by Mishra and Arbaugh [9] indicates that the IEEE 802.1x standard can be made secure given proper message authentication for management frames and symmetric authentication; such a framework would both prevent denial-of-service attacks from occurring owing to authenticated management frames and also provide a secure mechanism for access control.

A link-layer scheme to prevent public IPs from being overutilized by an attacker could prevent denial of service by IP hogging. Using virtual LANS (VLANs) to emulate separate physical broadcast domains allows separation of authenticated users from unauthenticated users. In the context of the AirBears architecture, a user should initially be placed into an unauthenticated VLAN and given a private RFC1918-compliant address via NAT. Upon authentication, a user can be transferred to an authenticated VLAN and given a public IP address. This defeats the IP hogging denial-of-service threat described earlier. Additionally, restricting DNS queries and lookups to campus nameservers prevents the piggybacking of unauthorized network traffic over DNS query and answer records.

POLICY

Difficult technical problems such as defeating wireless denial-of-service attacks that jam access points can be handled and prefaced with written policy and acceptable use agreements. An incomplete solution proposed by Xu et al. [22] stems from the observation that such jamming is easy to detect. The countermeasure of enabling access points to automatically switch channels upon detecting an attack assumes that an attacker only has the capability of jamming a single channel. A stronger countermeasure is easier, given policy: If such jammers are easy to detect, they can be easily located and disabled. Anecdotal evidence from campus network operators indicates that such attacks occur infrequently and are dealt with through campus policy. In particular, AirBears operators claim eminent domain over the airspace of the campus, and they are legally entitled to disable and physically remove such jamming devices.

Conclusions

Deploying a large-scale wireless network across a campus spanning miles in area poses interesting design questions. We provide an insight into the architecture of AirBears, a wireless network accessible by a large number of students, faculty, and staff. In particular, we look at how to provide convenient network access while maintaining a degree of fine-grained access control, availability, and ability to scale by deploying more access points and servers without requiring major modifications to the overall architecture. Additionally, we analyze AirBears from an adversarial standpoint, sketching out several attacks and explaining why they are potentially threatening to the system and users alike. Furthermore, we make various proposals that could be implemented to increase user privacy, knowledge, and security while decreasing potential unauthorized use and abuse of the network and its resources.

We can derive several lessons from observing a large-scale wireless deployment, including a need for lower level access control; clearly, network-layer access mechanisms are insufficient to protect users of a network from many forms of attack. We need to use encryption to protect access to a wireless network and to protect communications within the wireless network. We observe that several problems which are very difficult to solve technically can be ameliorated somewhat with policy. We also learn the value of user education and usable interfaces; although man-in-the-middle problems are theoretically solved, a typical user is more likely to ignore a certificate error and be susceptible to such an attack than to heed the warning.

Future directions of study may focus on the still unsolved problems of denial of service by jamming, usable interfaces for security verification, and improved specifications for wireless network access control.

ACKNOWLEDGMENTS

We thank Professor Vern Paxson for his help and suggestions. Thanks are also owed to Fred Archibald and Christopher Chin for their helpful discussions and insight.

REFERENCES

[1] IEEE Standard 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[2] Residential Computing at UC Berkeley: http://www.rescomp.berkeley.edu/helpdesk/register/.

[3] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *12th USENIX Security Symposium* (2003).

[4] Nikita Borisov, Ian Goldberg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *7th Annual International Conference on Mobile Computing and Networking* (2001).

[5] UC Berkeley AirBears wireless coverage: http://airbears.berkeley.edu/map.

[6] Ben Greenstein, Ramakrishna Gummadi, Jeffrey Pang, Mike Y. Chen, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall, "Can Ferris Bueller Still Have His Day Off? Protecting Privacy in the Wireless Era," Technical Report, Intel Research Seattle, University of Southern California, University of Washington, Carnegie Mellon University.

[7] Iodine IPv4 over DNS tunnel: http://code.kryo.se/iodine/.

[8] Scott Lathrop and Donald Welch, "A Survey of 802.11a Wireless Security Threats and Security Mechanisms," Technical Report ITOC-TR-2003-101, EECS Dept., U.S. Military Academy, New York, 2003.

[9] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the 802.1x Standard," Technical Report CS-TR-4328, CS Dept., University of Maryland, College Park, Maryland, 2002.

[10] University of California, statistical summary of students and staff: http://ucop.edu/ucophome/uwnews/stat.

[11] T. Ojala, T. Hakanen, T. Makinen, and V. Rivinoja, "Usage Analysis of a Large Public Wireless LAN," *2005 International Conference on Wireless Networks, Communications and Mobile Computing,* 13–16 June 2005, 1:661–667.

[12] NSTX (IP over DNS) HOWTO: http://thomer.com/howtos/nstx.html.

[13] OzyManDNS: http://www.doxpara.com.

[14] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer, "The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies," *IEEE Symposium on Security and Privacy*, 2007.

[15] David Schwab and Rick Bunt, "Characterizing the Use of a Campus Wireless Network," *INFOCOM*, 2004.

[16] CalNet Identity Management Services: http://calnet.berkeley.edu.

[17] Diane Tang and Mary Baker, "Analysis of a Local-Area Wireless Network," in *MobiCom '00: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (New York: ACM, 2000), pp. 1–10.

[18] Division of Student Affairs, University of California, Berkeley, Office of Student Research: https://osr2.berkeley.edu.

[19] NSTX tunneling network packets over DNS: http://savannah.nongnu.org/projects/nstx.

[20] University of California, Berkeley, CNS, Frequently Asked Questions about AirBears: http://airbears.berkeley.edu/faq.shtml.

[21] University of California, Berkeley, minimum security standards for networked devices: https://security.berkeley.edu/MinStds.

[22] Wenyuan Xu, Timothy Wood, Wade Trappe, and Yanyong Zhang, "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service," Technical Report, Wireless Information Network Laboratory, Rutgers, 2004.