Global Information Assurance Certification Paper

Scott Baily
GSEC Version 1.3
April 7, 2002

Is IEEE 802.1X Ready for General Deployment?

Abstract: Wireless LANs have been recognized as insecure for some time, especially for their lack of data confidentiality and access control. This paper examines the suitability of deploying IEEE 802.1X as the principal authentication mechanism for Colorado State University's wireless network. After careful consideration of wireless security issues and how 802.1X addresses those issues, it was decided that CSU should not incorporate 802.1X into its wireless network at this time.

Introduction

Two significant challenges facing wireless local area network (WLAN) designers and administrators are maintaining privacy and preventing unauthorized access. Network security is often said to be a compromise between convenience and protection. That it is especially true for a wireless network, as the convenience provided to roaming wireless users is facilitated by broadcasting packets to anyone with compatible equipment within range of a transmitting device.

In July of 2001 the Institute of Electrical and Electronics Engineers, Inc. (IEEE) published standard 802.1X for Port-Based Network Access Control [1]. Though 802.1X was meant to provide an authentication and authorization framework suitable for any IEEE 802-based local area network with a point-to-point topology, it was especially intriguing to WLAN managers who were seeking a high quality, standards-based access control mechanism.

The paper examines the suitability of deploying 802.1X as the authentication and authorization mechanism for Colorado State University's (CSU) centrally supported wireless network. Other sites may have different objectives, evaluation criteria and existing equipment to consider when making a similar decision. The same technical issues apply and the evaluation process should be similar, however, for anyone evaluating IEEE 802.1X solutions for their wireless networks.

Background

CSU's centrally supported wireless network and its current authentication scheme have been described in detail by Redder [2] and is summarized below. Approximately 80 IEEE 802.11b [4] compliant Cisco Aironet 350 access points have been distributed in some 20 buildings across the square mile campus. The wireless network is on its own private VLAN which is trunked across the campus backbone network.

Once wireless stations associate with an access point, they have two means of leaving the private network to reach campus or Internet destinations. The recommended choice is to establish a Virtual Private Network (VPN) connection to a Cisco 3030 VPN concentrator which has interfaces on both the (private) wireless LAN and (public) campus network. User authentication is typically facilitated by a central Remote Authentication Dial In User Service (RADIUS, RFC 2865 [3]) server whose user database is populated with faculty, staff and student electronic identifiers (eIDs). Colleges and departments may optionally request the creation of special VPN groups with authentication performed on their own NT or radius servers. Either way, the VPN solution is encouraged as it provides data integrity and confidentiality otherwise not available on the wireless network.

Users operating devices for which VPN clients are not available, or those who choose not to use the VPN may instead authenticate via a Hyper Text Transfer Protocol Secure Socket Layer (HTTPS) connection to a Linux host which also runs an IP Tables firewall. The username and password supplied by the wireless user are validated against the same radius server as the primary VPN solution. Once successfully authenticated, a rule is added to the firewall configuration allowing that client's traffic to pass through.

Though both methods help to ensure the wireless network access is being restricted to University affiliates, the VPN path is clearly superior because it also offers data confidentiality and integrity.

Access Control Alternatives

The IEEE 802.11b standard [4] – also known as WiFi (short for wireless fidelity) – defines Direct Sequence Spread Spectrum (DSSS) radio transmissions in the 2.4 to 2.4538 GHz range supporting bandwidths up to 11 Mbps. The standard also defines two authentication mechanisms, shared key and open system. Shared key authentication is facilitated by WEP, described below. Open system authentication is more accurately considered "null" authentication since no formal authentication takes place. Nevertheless, most access points can be configured such that access is minimally restricted based upon:

- SSID – The Service Set Identifier, a 32-byte string also known as the network name. Unless the client is configured with the same SSID as the access point with which it is attempting to associate, the association will not take place. SSIDs are often broadcast by access points and are easily detected by sniffing wireless packets, so they cannot be regarded as reasonable security measures. Furthermore, supporting a large wireless user community requires documentation to be easily accessible. Widespread documentation makes the SSID known to valid users and potential intruders alike.

- MAC address – Most wireless access points offer the option of verifying client Media Access Control (MAC) addresses before allowing network access. One way to accomplish this is to define a list of approved MAC addresses on the

> access points. These lists may be created and maintained manually or through an automated registration process. MAC addresses are relatively easy to change, however, so an intruder need only sniff the wireless LAN long enough to obtain a list of valid addresses and assume the identity of an inactive client to gain network access..

Neither use of a valid SSID nor MAC address filtering offers robust access control, so CSU looked beyond the 802.11b standard for an authentication solution. As stated earlier, both the VPN and web-based logon solutions offer RADIUS authentication. The user database can be refreshed often, in this case hourly, to accurately reflect the current list of university affiliates and their user credentials.

The firewall implementation requires a fair amount of care and feeding, though, and standards-based authentication supported by all wireless clients and the access points would be a preferred solution.

What about WEP?

The IEEE 802.11 standard also provides privacy between stations through an encryption scheme referred to as Wired Equivalent Privacy (WEP). Either 40-bit or 128-bit encryption keys must be shared between access points and wireless clients. In a large university scenario, this presents the logistical challenge of distributing a shared encryption key to 20,000 users in such a way it may still be considered "secret". This alternative was quickly dismissed by the University as impractical for that reason.

Shared key authentication can be summarized as follows: The access point sends the station a text challenge. The station encrypts the challenge using the shared key and returns the encrypted string to the access point. If the access point decrypts the response and recovers the original challenge, the authentication succeeds and the station is granted access. This represents unidirectional authentication; the wireless client is authenticated to the access point but not vice-versa. Furthermore, note that it is the wireless device and not the user that is being authenticated.

WEP has been proven to be vulnerable to attack, as first documented by Shamir, Mantin and Fluhrer [5] in August, 2001. In that paper, the authors provide mathematical and theoretical justification to claims that the RC4 stream cipher used by WEP uses a weak key scheduling algorithm. Though concerns with RC4 were first documented years earlier, this paper broke new ground by detailing how these weaknesses could be exploited.

Soon after that paper was released news of Adam Stubblefield [6], a summer intern at AT&T, implementing the attack received wide media coverage. It was no surprise that publicly available implementations quickly followed, rendering WEP completely vulnerable.

AirSnort [14] and WepCrack [15] are the two best known public tools for disclosing WEP keys. Both require a platform running Linux and a wireless network interface card (NIC) which uses the Prism2 chipset (though AirSnort now has support for Orinoco cards). The Prism2 NICs are unique in that they allow drivers to set promiscuous mode operation, a prerequisite for these utilities. AirSnort must analyze an estimated 5-10 million captured packets, after which it can reveal the shared encryption key within seconds.

Wireless networking vendors' logical response by to WEP concerns was the development of proprietary solutions for dynamic key allocation. For example, each time a wireless client associates with an access point a unique session encryption key is used. This tactic effectively prevents tools such as WepCrack from gathering a sufficient number of packets for successful analysis.

Proprietary solutions generally dictate single-vendor implementations, e.g. the NIC, its drivers, and the access point must all from the same vendor. While a single-vendor deployment often simplifies system management, it also limits the ability to build systems by selecting "best of breed" components from multiple vendors. One of CSU's original goals was to avoid requiring our wireless users to purchase a specific 802.11b-compliant NIC. Users are free to choose from a list of NICs verified to work with the campus wireless network, and are likely to do fine with a NIC not on the list (though local support isn't guaranteed in that case).

Given the issues with WEP and the University's goal to offer a non-proprietary wireless solution, encouraging VPN use still seems to be a reasonable choice for providing authentication and confidentiality to campus wireless users.

Consideration of IEEE 802.1X Port Based Network Access Control

Now that 802.1X has had several months as an established standard, it seemed prudent to consider it as a replacement to the pre-standard, home-grown authentication alternative deployed at the University. This analysis involved understanding 802.1X by reading the defining IEEE document, conducting a literature review to understand how the industry is receiving the standard, and understanding issues pertaining to its deployment.

The operational fundamentals of 802.1X

Central to understanding the 802.1X specification are a few of its primary components:

Authenticator – In the general sense, this is a device such as an Ethernet switch to which another device seeking network access attaches via a point-to-point connection. In wireless LANs, the authenticator is an access point. Note that wireless LANs better represent shared media topologies than point-to-point configurations for which 802.1X was designed. The association established between a wireless client and an access point may be regarded by the system as a logical point-to-point link.

Authentication Server – As the name suggests, this is the actual source of authentication services provided to end points. This is one of the strengths of 802.1X, as it permits centralization of this service instead of requiring separate authentication services to run locally on each authenticator (although the standard does allow an entity to be both). Centralization simplifies the task of keeping the user credentials current and allows for server redundancy. Except in the smallest implementations, the authentication server would be expected to be a separate entity. When the authenticator and authentication server are separate, network connectivity between the two is assumed. In that case, the authenticator simply passes traffic between the supplicant (see definition below) and the authentication server.

Network Access Port – This is a device's point of attachment to the network. Since wireless clients do not have physical network connections, an association between a wireless client and an access point is considered a network access port.

Port Access Entity (PAE) – The PAE refers to the processes executing the authentication protocols and algorithms associated with a port. There are both Supplicant PAEs and Authenticator PAEs, each with their own respective roles in the authentication process. For example, the Supplicant PAE will respond to requests from the Authenticator PAE for information such as the user identifier.

Supplicant – The supplicant is the entity on the opposite end of the point-to-point link from the authenticator. A wireless client is an example of a supplicant. Documentation describing other authentication protocols (such as EAP) often uses the term "peer" instead of supplicant.

EAP – The Extensible Authentication Protocol (EAP, RFC 2284 [7]) was originally written as an optional authentication mechanism for the Point-to-Point Protocol (PPP, RFC 1661 [8]). After a link has been established between the authenticator and a peer, the authenticator sends authentication requests to the peer. Each request has a coded type field specifying the type of information being requested, and the peer must reply to each request using a matching type code..

EAP is "extensible" in the sense that any higher level authentication mechanism, such as one-time passwords, Kerberos, or some future technology may be used to validate the user's login credentials. The authenticator is not required to have knowledge of these authentication protocols, and can serve as a simple pass-through device between the peer and authentication server. Once a "success" or "failure" message is sent to the peer the authentication phase is complete.

EAPOL – EAP Over LAN (EAPOL) describes how EAP packets are to be encapsulated within Ethernet, Token Ring or FDDI frames. This provides a communications path between the Supplicant PAE and Authenticator PAE over which authentication can take

place. When EAP packets between the Authenticator and the Authentication Server go across the network, they are encapsulated within a secure protocol such as RADIUS. Figure 3 shows a typical exchange.

802.11X defines two logical ports of access between the supplicant and the authenticator; a controlled port and an uncontrolled port (see figure 1). Another way to think of this is the authenticator initially filters out all traffic from the supplicant except for that which is required for the authentication process to complete. The Authenticator PAE communicates with the Supplicant PAE via EAPOL protocol data units (PDUs) allowed to go through the uncontrolled port. Should the authentication process be successful, the controlled port is enabled and the supplicant is granted access.

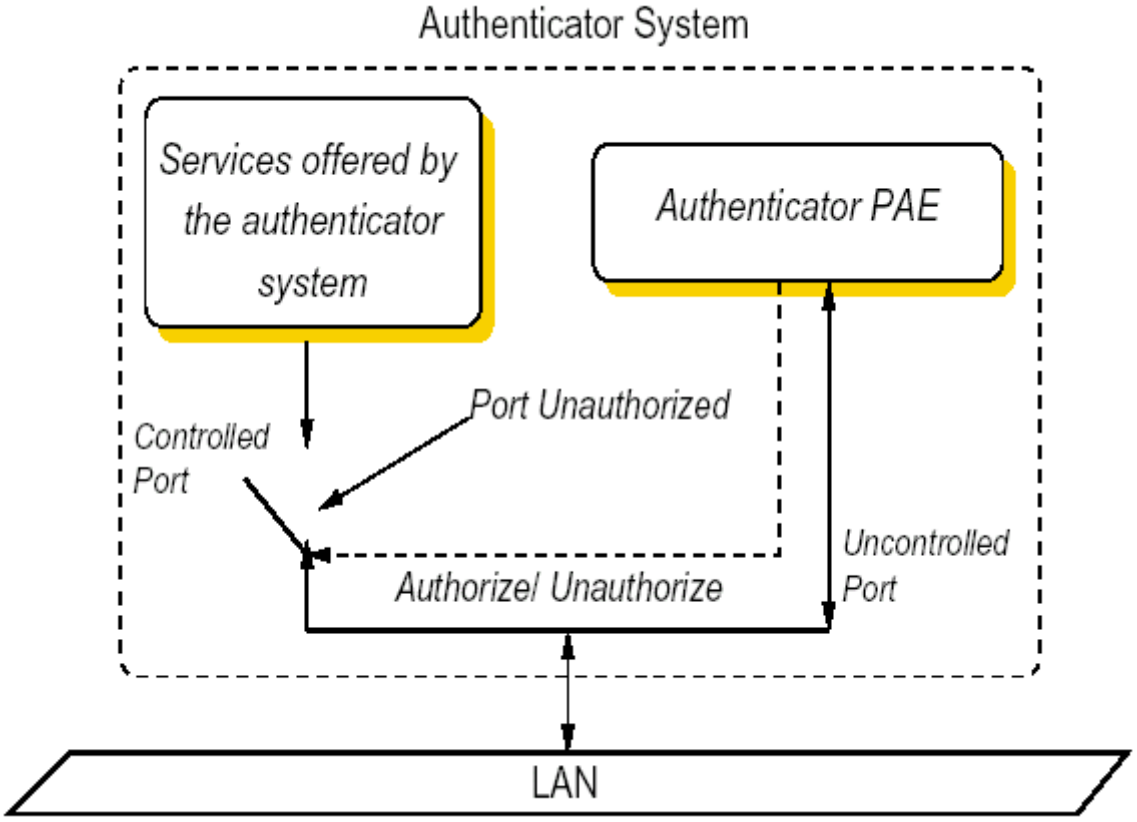

Figure 1. The Uncontrolled and Controlled ports in the Authenticator. Courtesy of Arbaugh [2]

Figure 2 shows the relationship between the Supplicant, Authenticator and Authentication Server entities. Note that the EAP messages between the Supplicant and the Authenticator are encapsulated within the native LAN (layer two) frames. Between the Authenticator and the Authentication Server, EAP is encapsulated within RADIUS packets. Radius requires a shared key between clients and server, implying authentication between those two entities.

How good is 802.1X?

Since the standard has had a chance to endure extensive testing and the scrutiny of industry analysts, it is worth investigating how well it has been received to date. So far, it seems to be generally regarded as less than an industrial strength authentication solution.

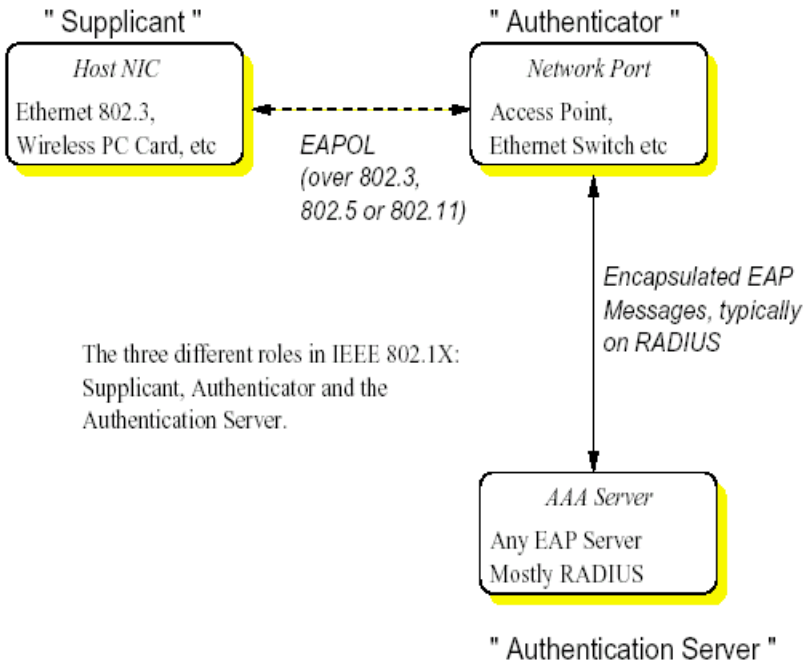

Figure 2. Elements of the 802.1X System. Courtesy of Arbaugh [9]

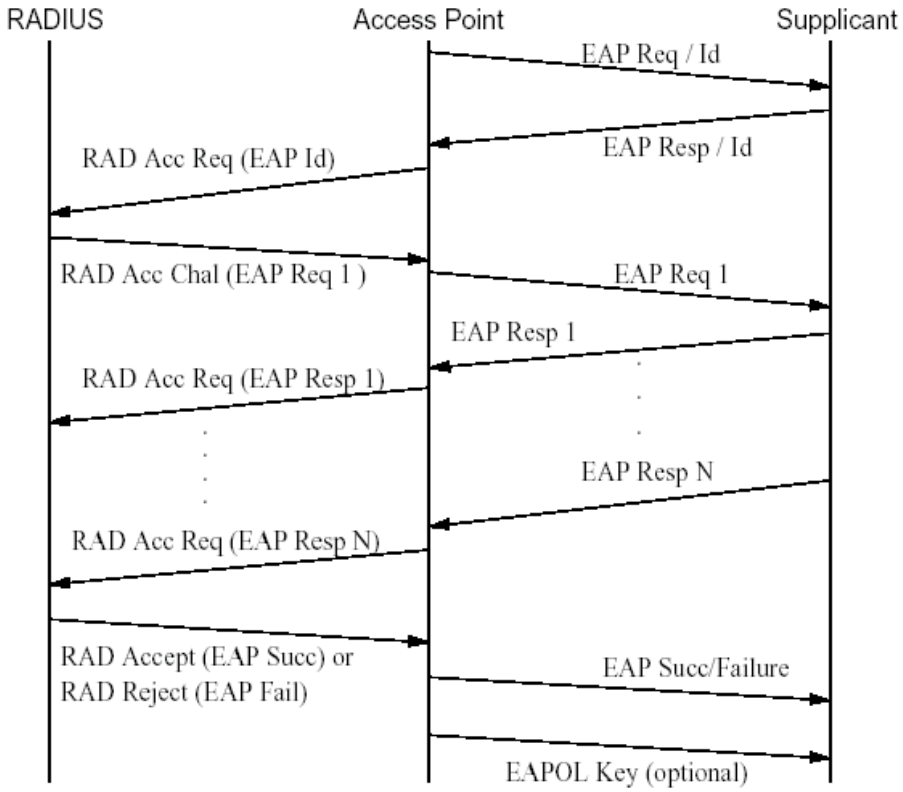

Figure 3. A typical EAP message exchange. Courtesy of Arbaugh [9]

Mishra and Aarbaugh [9] demonstrate that because mutual authentication between the wireless client and the access point is optional the system is vulnerable. The standard requires only one-way authentication, which takes place when the wireless client is authenticated. The authenticator is assumed to be trusted and legitimate, but given the relative ease with which access points may be inconspicuously added to a local area network this is a bad assumption. The lack of bi-directional authentication results in a man-in-the-middle attack vulnerability [9]. For example, an attacker can introduce a rogue access point into the system. This access point can associate with wireless clients as well as another, legitimate access point. The rogue AP can pass a wireless client's authentication traffic through to the authorized AP. Once the authorized access point detects an "EAP-Success" message, the association is complete and the logical port is enabled. After that, any additional wireless clients associated with the rogue AP may completely bypass the higher level authentication process.

Consider further Protected EAP (PEAP [10]), a work-in-progress proposed to the Internet Engineering Task Force (IETF) by Microsoft, Cisco, and RSA Security. These authors – representing corporations with major commitment to 802.1X – recognized the standard's shortcomings and proposed corrective measures just three months after IEEE released 802.1X.

One significant enhancement PEAP offers over EAP is the early negotiation of a Transport Layer Security (TLS RFC 2246) [11] channel. The main objective of TLS is to

provide data confidentiality and integrity to communicating entities. TLS does more than just protect the user identity, however. In addition to the trust relationship that already existed between the Authentication Server and the Authenticator, TLS also ensures that mutual authentication also takes place between the Supplicant and the Authentication Server.

Additional EAP deficiencies that are remedied by PEAP include fragmentation and reassembly support within the protocol, fast re-authentication for roaming devices via the TLS session resumption mechanism, and superior key management [10]. TLS can also provide the key hierarchy required to facilitate encryption key generation.

Implementation Issues

Microsoft Windows XP Professional comes with an 802.1X implementation supporting EAP-TLS. Windows 2000 is also supported with the addition of Service Pack 2 and a couple of additional patches described in [12].

The Microsoft implementation allows for separate authentication of users and their computers (wireless clients). Locally stored certificates are used during the authentication process. The stored user certificates are not available until after successful login to the computer.

In the Microsoft model, a Windows 2000 Internet Authentication Server (IAS) is used to provide the radius-based authentication. Since IAS servers need account information stored in Active Directory domains, Microsoft recommends installing and running IAS on Active Directory domain controllers. Microsoft documentation [12] suggests that any 802.1X-compliant access points should be compatible with their implementation.

Since Microsoft's EAP-TLS user and computer authentication make use of certificates, a certificate infrastructure is required. This entails installing, configuring and managing a Microsoft or a third party certificate authority (CA). EAP-TLS user authentication can be performed with either a smart card or a user certificate, while computer authentication requires the stored certificate.

Manufactures of wireless LAN equipment, such as Cisco Systems, have developed customized access point and client software to provide enhanced 802.1X support. The enhancements address privacy, mutual authentication, and other shortcomings of the standard discussed above. Cisco's implementation, called LEAP, can be configured to either use Microsoft's 802.1X support or to override it.

Third-party software is becoming available to support 802.1X on PDA devices and personal computers running pre-Windows 2000 operating systems. Implementation specifics should be closely examined to determine how the software compensates for 802.1X deficiencies, it at all. Proven compatibility with the 802.1X implementation in the existing wireless LAN is also important, and the effort to obtain and test an evaluation

copy would certainly be worthwhile.

Observations

The IEEE 802.1X committee took on a monumental task by attempting to define a port-based authentication solution equally suited for wired and wireless LAN topologies. Though the standard acknowledges the challenges associated with shared media LANs in general and wireless LANs specifically, its requirements fall short of the security wireless users and vendors require.

As a result of weaknesses in the standard, vendors are introducing "value-added" implementations which attempt to compensate for shortcomings in the 802.1X infrastructure. This is good in that the vendors have recognized the issues associated with minimum compliance implementations. The negative side effect is that these enhancements lose the interoperability typically associated with a standards-based product. IT organizations wishing to build networks and services compliant with industry standards will likely delay their implementation of 802.1X for that reason.

It is reasonable and expected that corporations such as Microsoft will first develop features like 802.1X support for their current platforms. The reality is that universities and other large customers must deal with a wide range of platforms and operating systems. If a site develops a policy to require 802.1X on its wireless LANs, then client support must be available for all locally supported wireless platforms. If security concerns about the minimally compliant implementations result in the decision to use a particular vendor's "enhanced" version, then care must be taken to ensure compatible client software is available for all platforms.

Even though Cisco Systems claims to have addressed the major deficiencies with EAP and 802.1X in LEAP, they recommend sites carefully consider their security requirements when designing wireless networks [13]. For those sites with the highest level of security concerns they recommend using Internet Protocol Security (IPSec), as available with most VPN solutions.

Being among first to implement a particular feature or standard isn't always the best position to find oneself. Those who have been in the networking business a while have noted that the earlier you get started implementing a particular technology, the longer it will take and the more it will cost. Deploying 802.1X may be another case in point.

Several sources were cited above as evidence supporting the claim that 802.1X, in its current form, is insufficient in several key areas. When researching the topic, no references were encountered which argued the contrary.

Conclusions

There is no question that the IEEE 802.11b standard itself lacks the privacy and access

control mechanisms necessary for WiFi networks to be considered secure. The much anticipated 802.1X standard attempted to address many concerns regarding wireless network security, but it failed to withstand the recent scrutiny of security analysts.

Though solutions exist which are based upon 802.1X and address the deficiencies described above, questions about interoperability remain unanswered. Some network managers may prefer single-vendor solutions because they are easier to implement and maintain. Others prefer the flexibility offered by standards-based implementation, as they can choose "best of breed" components when building systems.

Currently at Colorado State University, the preferred means of achieving privacy and authentication on wireless LANs is through a VPN. A Linux-based authentication and admission control mechanism was developed locally as an interim solution in lieu of an industry standard alternative. The University's preference is to deploy a standards-based wireless network, keeping the option open for a multi-vendor solution. Given that goal and the lack of a solid authentication standard, the University will hold its course and do nothing new at this time. We will wait for PEAP or some other set of recommendations the standards body will endorse as a viable solution to deficiencies in 802.1X.

Acknowledgements

I am grateful to Bill Aarbaugh for graciously allowing me to use figures from his analysis of the 802.1X standard [9] in this paper. Considerable credit also goes to Greg Redder, whose implementation of the University's interim authentication solution allows us to wait for an Authentication standard which better meets our needs and expectations.

References

[1] IEEE 802.1X Committee. "IEEE Std 802.1X, 2001 Edition, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control". July, 2001. URL: http://standards.ieee.org/reading/ieee/std/lanman/802.1X-2001.pdf

[2] Redder, Greg. "Implementation of a Secure Wireless Network on a University Campus" October 29, 2001. URL: http://rr.sans.org/wireless/wireless_univ.php

[3] Rigney, C. et. al. "Remote Authentication Dial In User Service (RADIUS)". IETF RFC 2865, June, 2000. URL: http://www.ietf.org/rfc/rfc2865.txt

[4] IEEE 802.11 committee, "IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications". 1999. URL: http://standards.ieee.org/getieee802/802.11.html

[5] Fluhrer, S., Martin, I., Shamir A. "Weaknesses in the Key Scheduling Algorithm of

RC4" from the Eighth Annual Workshop on Selected Areas in Cryptography. August, 2001. URL: http://www.crypto.com/papers/others/rc4_ksaproc.ps

[6] Stubblefield, A., Ioannidis, J., Rubin, A. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" URL: http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

[7] Blunk, L., Vollbrecht, J. "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284. January, 1998. URL: http://www.ietf.org/rfc/rfc2284.txt

[8] Simpson, W., Editor " The Point-to-Point Protocol", IETF RFC 1661, July, 1994. URL: http://www.ietf.org/rfc/rfc1661.txt

[9] Mishra, A., and Arbaugh, W. "An Initial Security Analysis of the IEEE 802.1X Standard", February, 2002. URL: http://www.cs.umd.edu/~waa/1x.pdf

[10] Andersson, H. et. al., "Protected EAP Protocol (PEAP)", IETF Internet Draft. 23 February, 2002. URL: http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-02.txt

[11] Dierks, T., and Allen, C. "The TLS Protocol", IETF RFC 2246, January 1999. URL: http://www.ietf.org/rfc/rfc2246.txt

[12] Davies, J. "Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000 Internet Authentication Service", October, 2001. URL: http://www.microsoft.com/WindowsXP/pro/techinfo/deployment/wireless/80211corp.doc

[13] Convery, S. and Miller, D. "SAFE: Wireless LAN Security in Depth" January, 2002. URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

[14] AirSnort URL: http://airsnort.shmoo.com/

[15] WepCrack URL: http://wepcrack.sourceforge.net/