

Staying Secure in an Insecure World: 802.1x Secure Wireless Computer Connectivity for Students, Faculty, and Staff to the Campus Network

Steven K. Brawn
Arizona State University West
4701 W. Thunderbird Road
Phoenix, AZ 85069
(602) 543-8295
sbrawn@asu.edu

R. Mark Koan
Arizona State University West
4701 W. Thunderbird Road
Phoenix, AZ 85069
(602) 543-8283
mkoan@asu.edu

Kelly Caye
Arizona State University West
4701 W. Thunderbird Road
Phoenix, AZ 85069
(602) 543-8297
Kelly.Caye@asu.edu

ABSTRACT

During this past year, the ASU West IT Department has successfully implemented network connectivity throughout the campus for users who desire to use their computers in places other than the usual designated office spaces and computer labs. Students and staff alike can now access their network file shares, check email, browse the web, and work on projects while sitting in the cafeteria, out on the grass, or under the shade of a tree.

With the constant threat of virus attacks, Trojans, hackers, etc., one of the highest priorities for this project was that of security. There are several ways to implement wireless connections, such as 802.11b, 802.11a, and 802.11g, but these solutions, by themselves did not prove secure enough for IT administration. For enhanced security, it was decided to implement the wireless connections on this campus with the addition of the new 802.1x protocol for secure authentication.

After extensive testing, wireless access points were established in popular public areas, in classrooms and office buildings, and were incorporated within new classrooms as well.

This paper will discuss the driving factors for this type of connectivity, why we chose to implement the 802.1x protocol for secure connectivity, and show the configurations necessary for wireless network connections.

Categories and Subject Descriptors

K.6.5, D.4.6 [Security and Protection]: Authentication, physical security, and unauthorized access.

General Terms: Security, design, verification.

Keywords: Authentication, wireless network, VPN, 802.1x, PEAP, Dynamic WEP.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10-13, Baltimore, Maryland, USA
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

1. INTRODUCTION

The Information Technology department at Arizona State University West, like most other universities, has an ever-increasing demand to accommodate students' needs to access the network from locations other than the classroom, office, or lab. With the advancement in network technology, more and more users are purchasing and using laptop computers and wireless network adapters. In order to meet the demands of students, faculty, and staff who desire to use these technologies, ASU West has developed an authentication process that works for both wired and wireless computers, and incorporates the security that is necessary for IT. This process uses the 802.1x security protocol, which includes features such as PEAP and WEP. How we came to the decision for this process over other, easier, processes, and how we implemented it will be discussed further.

This paper is not meant to be an expert "how-to" guide, nor will it answer all possible questions; however, it should enable the reader to have more information that can be used when thinking about implementing computer connectivity on other campuses.

1.1 Why use 802.1x?

The following issues were considered during the decision process to implement 802.1x at ASU West:

- Previous use of Microsoft PPTP VPN was slow and not scalable enough to meet future demand.
- 802.1x allows standard network access after authentication, instead of proxying the network traffic through a single appliance or server (e.g., as in a VPN). This alleviates network traffic bottlenecks.
- 802.1x allows for implementation via a variety of Extensible Authentication Protocols (Protected-EAP, LEAP, TTLS, TLS) and configurations.
- 802.1x forces the use of WEP (at a minimum) so wireless traffic always has at least minimal encryption.
- Clients (supplicants) for 802.1x are native in most current operating systems, and 3rd party clients can be purchased for older operating systems.
- Authentication process can be customized by user, computer, or groups of users/computers.
- Integrates with Windows Active Directory, LDAP, and several other directory services currently used at the university for authorization and authentication.

- Reporting capabilities for user attribution are available and extensible.

2. 802.1X IN 802.11 WIRELESS LANS

Increased use of laptop computers within the university and a demand for greater customer mobility has fuelled the need for our secure wireless network. The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling.

2.1 The 802.11 Protocol

Wireless networking hardware requires the use of basic technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking. Specifically, the 802.11b protocol was selected for use at ASU West because of its ubiquity and affordability.

2.2 PEAP

802.1X is a Microsoft and industry standard Extensible Authentication Protocol (EAP) based authentication protocol which provides network port authentication for 802.11 wireless LANS (WLAN's) [1]. 802.1x based security dramatically increases the security protection of the university's network.

IEEE 802.1x alone lacks the components that 802.11-based LANS need for user-based authentication. 802.1x is not the only authentication method; rather it utilizes Extensible Authentication Protocol (EAP) as its verification structure. *EAP provides a general framework for a broad assortment of authentication methods, including certificate-based authentication, TTLS, TLS, PEAP, token cards, and one-time passwords, etc.* Although EAP-TTLS and TLS are secure, the requirements for client certificates are too big of a hurdle for most institutions to deal with [2]. This is why ASU West currently uses the Microsoft industry standard of PEAP (Protected Extensible Authentication Protocol) for Windows. However, the 802.1x specification itself does not specify or mandate any authentication methods.

PEAP encrypts authentication data using a tunneling method. PEAP makes it possible for the wireless clients to authenticate to the RADIUS (Remote Authentication Dial In User Service) server without requiring them to provide certificates. It is only necessary for the server to provide a public key certificate.

PEAP provides the following services to the EAP methods it protects:

- Message authentication (imposters can't insert or falsify EAP messages)
- Message encryption
- Authentication of server to client (only the protected method needs to authenticate client to server)
- Key exchange (to establish dynamic WEP or TKIP keys)
- Fragmentation and reassembly (of very long EAP messages, if needed) [3]

3. HOW IT WORKS

ASU West uses Dynamic WEP (Wired Equivalent Privacy) and 802.1x based security. 802.1x authentication for wireless LANs has three main components: The supplicant (client); the authenticator (access point); and the authentication server (RADIUS server). *Note: Windows XP comes with supplicant software that is built in; users need to have a compatible network adapter.*

The supplicant never talks directly to the authentication server; instead, the access point serves as the medium through which the supplicant and RADIUS authentication server speak to each other. The authenticator enforces authentication before granting admission to services that are available. The authenticator is responsible for communication with the supplicant and for presenting the information received from the supplicant to the RADIUS authentication server. Authenticators or access points merely act as a "pass through" for EAP. One of the key points of 802.1x is that the authenticator can be very simple; all of the brains have to be in the supplicant and the authentication server [4]. This makes 802.1x ideal for wireless access points, which are typically small and have little memory and processing power.

3.1 The RADIUS Server

The RADIUS server is a widely deployed protocol for network authentication, authorization and accounting (AAA) access. RADIUS servers are simple, efficient and easy to implement -- making it possible for RADIUS to fit into the most inexpensive embedded devices. ASU West uses Cisco Access Control Server (ACS) RADIUS servers which integrate with Windows Active Directory.

The RADIUS server passes the user credentials to the ASU West Active Directory Forest via LDAP (Lightweight Directory Access Protocol) to obtain successful authentication before authorizing access to the network.

3.2 Access Points

In an 802.11 Wireless LAN environment a station must form an association with an access point in order to make use of the WLAN. The access point detects the client and enables the client's port as a "logical port". It forces the port into an unauthorized state, so only 802.1x traffic is forwarded. Traffic such as Dynamic Host Configuration Protocol, HTTP, FTP, and Simple Mail Transfer Protocol is blocked. Until the authentication is complete, only EAPOL frames are allowed to be exchanged; once the host authentication is successful, the port switches as a regular port [5].

This allows the supplicant to associate with the Access point before dynamically derived WEP keys are available. ASU West currently uses Dynamic WEP keys for encryption data algorithms between the client and the access point, which changes every 300 seconds. Once the association has been established, the client then sends a PEAP-start message.

The following diagram displays the dialogues between the different components:

window that appears, right-click *Wireless Network Connection* and select *Properties*.

- A. CHECK the box with the option to *Show Icon in notification area when connected*.
- B. Click the *Wireless Networks* tab, then click the *Add* button.
- C. In the *Wireless network properties* window, enter the value for the *Network Name (SSID)* as specified in step 2 above.
- D. Click the *Authentication tab*.
- E. UNcheck the option to *Authenticate as computer when computer information is available*.
- F. CHECK the box to *Enable IEEE 802.1x Authentication*.
- G. CHANGE the *EAP Type* to *Protected EAP (PEAP)*.
- H. Click the *Properties tab*. In the *PEAP Properties* window, MAKE SURE that the option to *Validate Server Certificate* is checked.
- I. In the *Select Authentication Method* box, select *Secured Password (EAP-MSCHAP v2)*. Click the *Configure* button next to the *Select Authentication Method* box.
- J. In the *EAP MSCHAPv2 Properties* box, UNCHECK the option to *Automatically use my Windows logon name and password*.
- K. Click *OK* three times to close the open windows. In the *Wireless Network Connection Properties* window, verify that the *Network name (SSID)* that you entered in the steps above appears as the preferred network.
- L. Click *OK* to close the *Wireless Network Connection Properties* window, and then close the *Network and Dial-up Connections* window.

Step 4. Connect to the network. This is now at the point to enter the user's login credentials. **NOTE:** Before completing this step, make sure the computer is located on the campus, in a wireless-supported location.

- A. Wait for the *Wireless Network Connection popup window* to appear in the lower right-hand corner of the desktop. **THIS MAY TAKE UP TO 1-2 MINUTES! BE PATIENT.** When it appears, click anywhere inside the yellow bubble, *except on the 'x' to close the window*.
- B. When the *Username/Password* window appears, enter the *campus ID and password, with the correct domain*.
- C. Wait for the *Validate Server Certificate* popup window to appear in the lower-right corner of the desktop. When it appears, click anywhere inside the yellow bubble, *except on the 'x' to close the window*.
- D. After a short delay while being authenticated, the computer should be able to have network access.

From this point forward, the user should not have to enter his or her login credentials again, as the computer will remember them. **NOTE:** *if the computer is connected to a different wireless network, it may need to have the network settings reconfigured.*

4.2 Windows 2000 Workstation

In order for 802.1x to work with Windows 2000, the workstation must have a minimum of Service Pack 4 installed. It also assumes that a compatible network card and drivers are properly installed.

Step 1. Start the Wireless Zero Configuration Service, and ensure that it is set to Automatic. This service is necessary whether or not a wired or wireless connection is used.

Step 2. Configure the wireless card. Installation and configuration will vary between different manufacturers, so be sure to refer to the specific instructions that come with the specific card. In general, you will need the following information to configure any wireless card:

SSID (or network name): see your network administrator

Network Type: Infrastructure, Base-Station, or Access Point

Network Security Type: PEAP or Host-Based PEAP

Dynamic WEP: ON

128bit WEP KEY: 11111111111111111111111111111111 (*a series of 26 1's. You will only need this number if your wireless card will not retrieve the WEP KEY automatically.*)

Step 3. Configure TCP/IP Properties. On the computer desktop, right-click *My Network Places* and select *Properties*. In the window that appears, right-click *Wireless Network Connection* and select *Properties*.

- CHECK the box with the option to *Show Icon in notification area when connected*.
- Click the *Authentication tab*.
- UNcheck the option to *Authenticate as computer when computer information is available*.
- CHECK the box to *Enable IEEE 802.1x Authentication*.
- CHANGE the *EAP Type* to *Protected EAP (PEAP)*.
- Click the *Properties button*. In the *PEAP Properties* window, MAKE SURE that the option to *Validate Server Certificate* is checked.
- In the *Select Authentication Method* box, select *Secured Password (EAP-MSCHAP v2)*. Click the *Configure* button next to the *Select Authentication Method* box.
- In the *EAP MSCHAPv2 Properties* box, UNCHECK the option to *Automatically use my Windows logon name and password*.
- Click *OK* three times to close the open windows. In the *Wireless Network Connection Properties* window, verify that the *Network name (SSID)* that you entered in the steps above appears as the preferred network.
- Click *OK* to close the *Wireless Network Connection Properties* window, and then close the *Network and Dial-up Connections* window.

Step 4. Connect to the network. This is now at the point to enter your login credentials. **NOTE:** Before completing this step, make sure the computer is located on the campus, in a wireless-supported location.

- When the *Username/Password* window appears, enter the *campus ID and password, with the correct domain*. **THIS MAY TAKE UP TO 1-2 MINUTES! BE PATIENT.**

- **Wait** for the *Validate Server Certificate* popup window to appear. When it appears, click **OK**.
- After a short delay while being authenticated, the computer should be able to have network access.

From this point forward, the user should not have to enter his or her login credentials again, as the computer will remember them. **NOTE:** *if the computer is connected to a different wireless network, it may need to have the network settings reconfigured.*

4.3 Windows ME Workstation

In order for the 802.1x security protocol to work on a Windows ME workstation, third-party software must be used. ASU West is currently using Funk Software's Odyssey Client for connectivity. It comes with a 30-day free trial period, after which the user must purchase the software, or it becomes disabled.

Please test other manufacturer's software products, and find the one that best suits your institutions needs, and follow their guidelines for installation and configuration.

Step 1. Configure the wireless card. Installation and configuration will vary between different manufacturers, so be sure to refer to the specific instructions that come with your specific card. In general, you will need the following information to configure any wireless card:

SSID (or network name): see your network administrator

Network Type: Infrastructure, Base-Station, or Access Point

Network Security Type: PEAP or Host-Based PEAP

Dynamic WEP: ON

128bit WEP KEY: 11111111111111111111111111111111 (*a series of 26 1's. You will only need this number if your wireless card will not retrieve the WEP KEY automatically.*)

Step 2. Install and configure the third-party client, per their instructions.

5. PROBLEMS ENCOUNTERED

It took a lot of time and effort to test each part of this process, from the Access Points, RADIUS Server, and different Operating Systems down to the different wireless cards. The majority of problems encountered during wireless configuration involve not paying attention to the option boxes that need to be either checked or unchecked, and they **DO** make a big difference! Another problem is that people tend to skip over the task of making sure the *Wireless Zero Network Service* is started, and set to *Automatic*.

Making sure the switches and routers are configured properly, or that they are compatible with this protocol is also essential.

6. CONCLUSION

Although it may seem more difficult and confusing to use the 802.1x security protocol, it makes a network much more secure by ensuring all users are authenticated before being granted network access, and encrypting the wireless transmissions during use. The initial setup takes time, and training is needed to help people configure their wireless computers, but in the end, it is well worth the time spent for the security that is set in place.

7. ACKNOWLEDGMENTS

Thanks to Joan Carter, Director of Network Services, ASU West, for invaluable information and support while writing this paper.

8. REFERENCES

<http://www.interlinknetworks.com/resource/wp5-1-1.htm>

[1] Introduction to 802.1X for Wireless Local Area Networks

[2] EAP Methods for Wirelss Authentication

[3] Wireless LAN Access Control and Authentication

<http://www.nwfusion.com/>

[4] What is 802.1X

[5] 802.1X authenticates 802.11 wireless