GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Authentication and Authorization: The Big Picture with IEEE 802.1X

By A Arthur Fisher

December 21, 2001 - Assignment version 2.0

The Big Picture Challenge

Current authentication protocols (i.e. user login and password) successfully restrict access to properly configured workstations and servers. Traditionally, a user's privileges will allow (or deny) access to files or applications on the local machine or on other machines within its domain. Yet, authorized access to a particular machine (or domain) does not necessarily correlate with access to privileged network services. That is, a given computer is unable to grant differential network privileges (on a large scale) to different users. For example, a user and an administrator could independently login to the same workstation. The administrator may require enhanced network service access (such as outside FTP or access to a particular VLAN). Nevertheless, under traditional authentication protocols, neither the computer nor the network switch to which it is connected will be able to independently grant the administrator enhanced access to these network services.

Network services are typically restricted in a switch or router (layer 2 or 3 device) by the computer's hardware (MAC) or IP address. A manual entry in the device's ACL or VLAN list can allow or deny individual network services and access. However, a new protocol is necessary to automate this process and correlate it to the privileges to which a user is granted access when he logs onto a particular computer. For example, the sales manager of an organization should be able to logon to any of the company's workstations and be instantly connected to the sales VLAN.

A further deficit of existing authentication protocols is that they do not adequately accommodate roaming users such as those found in large corporate environments and on school campuses. Laptops can have multiple MAC addresses; consider a laptop with an 802.11a, 802.11b, Bluetooth and an Ethernet adapter. So, continuing with the example above, if the sales manager has a wireless card in his laptop, he should be able to securely connect to the sales VLAN from any corporate Access Point (AP). When he is seated in his office, he may connect through his Ethernet port, but he should still maintain the same access. Unfortunately, this is more information than a typical IT department can manage for an entire enterprise.

Next, consider the near future. Over the next few years there will be a transition from IPv4 to IPv6. This transition will allow for the billions of

© SANS Institute 2000 - 2005 Author retains full rights.

Internet-addressable devices expected to propagate into society. With broadband connections making their way into consumers' homes, there will be more connectivity generally, as well as a greater number of home networks. Customer Premises Equipment (CPEs, such as DSL routers, wireless APs and other consumer-targeted equipment) ought to enforce security policy. Everything from computers and servers to phones, PDAs, household appliances, cars, and clocks will require not only IP addresses, but also a security mechanism to properly maintain their desired functionality.

A great number of these new devices will be wireless. Consider large-scale deployment of Shared Use APs. This will pave the way for wireless computer roaming, just as a heavy population of Cellular Sites has enabled the usage of mobile phones. Issues such as consortia of wireless access providers all sharing access information will be focal. Both management and function of authentication and authorization will require performance on an Internet-sized scale.

A centralized database with a robust authentication and authorization framework must be developed to manage the entire process.

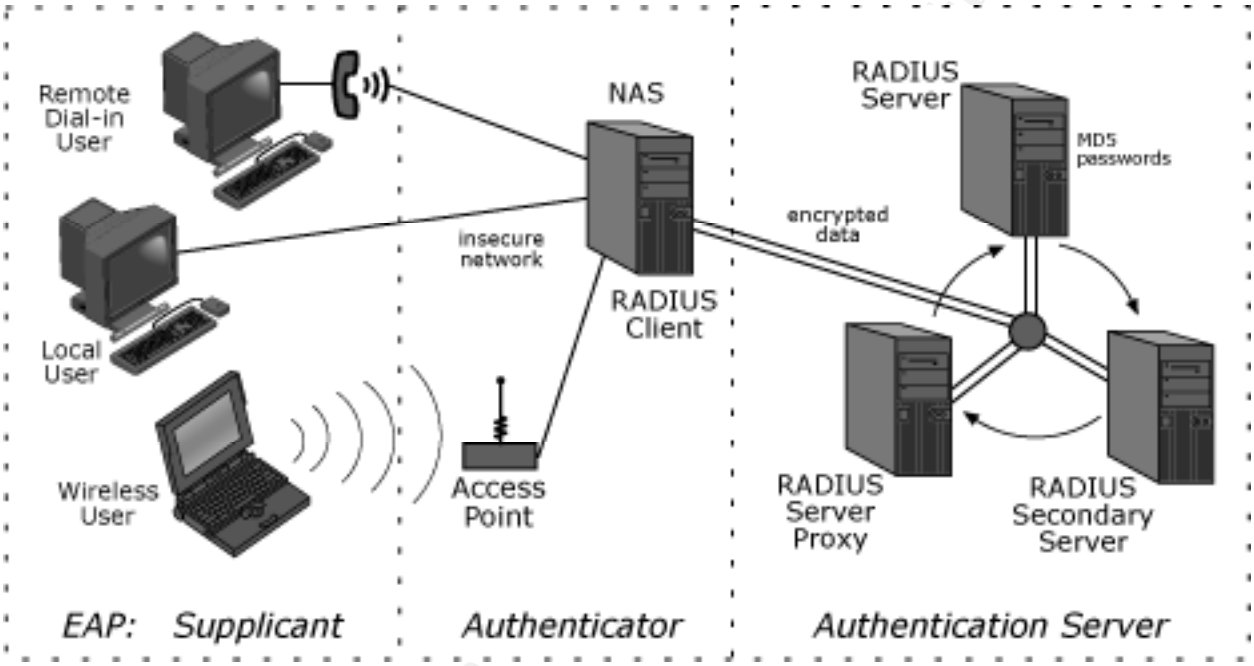
RADIUS Today

I begin by reviewing the authentication and authorization portion of the RADIUS (Remote Access Dial In User Service [RFC 2865]) process. (There are also nine other aspects to RADIUS, each with their own RFC.) A RADIUS database creates a great starting point for a complete authentication and authorization system because, in addition to such basic data as user-ID and password (information we usually expect to see), it can also contain more detailed information about a user's access privileges. Network-specific privileges, such as to which ports, services and VLANs the user is allowed access, can also be included. The type of information one can store in a RADIUS database is flexible. As we will see, a new standard called IEEE 802.1X can utilize a RADIUS, LDAP or other similar authentication method to take security to the next level.

A RADIUS-authenticated session incorporates the Network Access Server (NAS) to act as a client during the process of authenticating a user and subsequently allowing (or denying) him access to the network. The user may be locally connecting at the NAS (i.e. via a login prompt) or remotely connecting to the NAS via an AP (i.e. modem or 802.11 wireless connection). The user initiates an access request to the NAS, which acts as a gatekeeper. The NAS securely connects to a RADIUS server by using a shared secret key (symmetric encryption). In the event that a primary RADIUS server is down,

© SANS Institute 2000 - 2005, Author retains full rights.

a subsequent request can be routed to a secondary server. If the server cannot personally identify the user, it may act as a proxy for another RADIUS server with which it shares a secret key. A challenge and response process then takes place until authentication is satisfied. Next, the RADIUS server forwards access privileges to the NAS, which will accordingly allow or deny the user access to the network. Note that information stored on the RADIUS servers is encrypted for higher security measures.



The RADIUS method of authentication serves as a great foundation. It is very flexible and was built with "openness" in mind. Unfortunately, there is a weak link in this method; it lies in the communication between the NAS and the user's machine. This susceptibility is no more evident than in the Wired Equivalent Privacy (WEP) protocol, which is the highly vulnerable security aspect built into the IEEE 802.11 wireless standard. At this point, the RADIUS Authenticator relies on the AP or NAS (which is sometimes the Authenticator itself) to securely communicate with the user's device. Some implementations have attempted to solve this problem by using a VPN tunnel; however, a stolen machine will still have access to the services in question.

WEP's vulnerabilities stem from some of the following problems: Users are usually authenticated by the hardware's MAC address, which can be spoofed or stolen. Also, most implementations use global keys, which rarely change (if ever). These keys are easily cracked with tools such as AirSnort and WEPcrack. Note, however, that 802.1X products, such as MDC's

© SANS Institute 2000 - 2005 Author retains full rights.

SecureSupplicant, force the shared key to be regenerated for each authenticated session, thus alleviating this particular problem. WEP also uses a weak implementation of the RC4 algorithm as well as a short Initial Vector (IV) sequence space without replay protection. See Intercepting Mobile Communications: The Insecurity of 802.11 for more details.

As yet, WEP still requires improvements so as to correctly integrate securely with 802.1X, since the implementation of 802.1X alone will not solve the entire security problem with an 802.11 wireless client. The challenge in improving 802.11's security is in allowing backwards compatibility to the millions of wireless cards already installed. WEP should be augmented in a way that allows for a gradual deployment of upgraded software patches, first to the Access Points and then to the users. 802.1X adds important security aspects to non-wireless authentication as well, but because wireless networks tend to be among the weakest-security parts of a typical network, I use them to demonstrate 802.1X's strengths.

IEEE 802.1X Defined

IEEE 802.1x is a new, open-standards-based protocol for authenticating network clients (or ports) on a user-ID basis. This process is called "port-level authentication". It takes the RADIUS methodology and separates it into three distinct groups: the Supplicant, Authenticator, and Authentication Server (see figure above). IEEE 802.1X provides automated user identification, centralized authentication, key management, and provisioning of LAN connectivity. It even provides support for roaming access in public areas.

Hereafter referred to as "Auth-x", IEEE 801.X was ratified in June of 2001. Auth-x builds on an existing protocol called Extensible Authentication Protocol (EAP [RFC 2284]) by tying EAP into the bigger picture, so to speak. EAP conducts the authentication process. It ties Point-to-Point Protocol (PPP) to the physical layer, OSI Layer 1. EAP over LAN (EAPOL) is EAP encapsulated into 802 frames. This is how the Authenticator and Supplicant actually communicate during the authentication process. Furthermore, EAP is compatible with Ethernet, Token Ring, 802.11, and other popular network protocols. Additionally, EAP supports many authentication methods such as Kerberos, public key, one-time passwords, etc. Finally, it can utilize Transport Level Security (TLS) and Secure Remote Password (SRP).

Auth-x authentication provides privileges not only to computers and machines, but also to network services. Upon authorization, Auth-x capable switches and routers will modify access privileges according to the individual

© SANS Institute 2000 - 2005, Author retains full rights.

entitlement. Alone, a RADIUS-authenticated session can provide only a limited amount of service privileges. However, the Auth-x protocol provides a method for authentication in conjunction with a RADIUS (or similar) database, as well as providing subsequent token distribution to compliant network hardware and software, resulting in more robust privileged service descriptions.

Early adopters, such as 3Com, HP, Cisco, Microsoft and Enterasys, have already begun implementing Auth-x's much-anticipated features; support is built into Windows XP. Cisco also offers support for Windows 9X, NT4, 2000, Mac OS & Linux. MDC offers a free Supplicant for Linux. Also, Cisco and Entrasys are currently both shipping Auth-x enabled hardware, and patches and firmware upgrades are available from these and other vendors. Not surprisingly, the specification was partially drafted by many of the above-mentioned companies, who were responding to customer concerns. The goal was to create a flexible, link layer, security framework.

Auth-x was designed to be inexpensive to implement on existing network hardware, utilizing existing network-access infrastructure (RADIUS, LDAP, Active Directory, etc.). EAP-compatible RADIUS servers include, among others, Microsoft Windows 2000 Sever (IAS), Cisco ACS, Funk RADIUS and Interlink Networks RADIUS Server. Other vendors that support Auth-x are AirWave, Compaq, Dell, IBM, Intel, Symbol, Toshiba, Telison and Wayport.

Put simply, Auth-x provides a means of restricting network access to authorized users. Typically, the user ID is the identifying agent. The Auth-x protocol requires two distinct steps. First, the Supplicant is **authenticated**, and then it is **authorized** access privileges ("the A&A process"). Privileges are distributed in the form of tokens, which can be defined to include anything that may interest a security professional, such as VLAN IDs, rate limits, filters, tunnels, etc.

Notice that the protocol alone will not force each user who comes into contact with a machine to authenticate. As with other security policies, user participation is a must. Auth-x is performed for each session, and it is possible for a machine to change hands without the original user having initiated a logoff, thereby forcing the new user to initiate a new session. Additionally, Auth-x alone will not prevent session hijacking. Rather, complimentary technology and protocols, such as encryption, IPSec, and Diffie-Hellman key exchange, should also be employed. However, the specification leaves this latter complimentary implementation up to the individual vendor.

© SANS Institute 2000 - 2005 Author retains full rights.

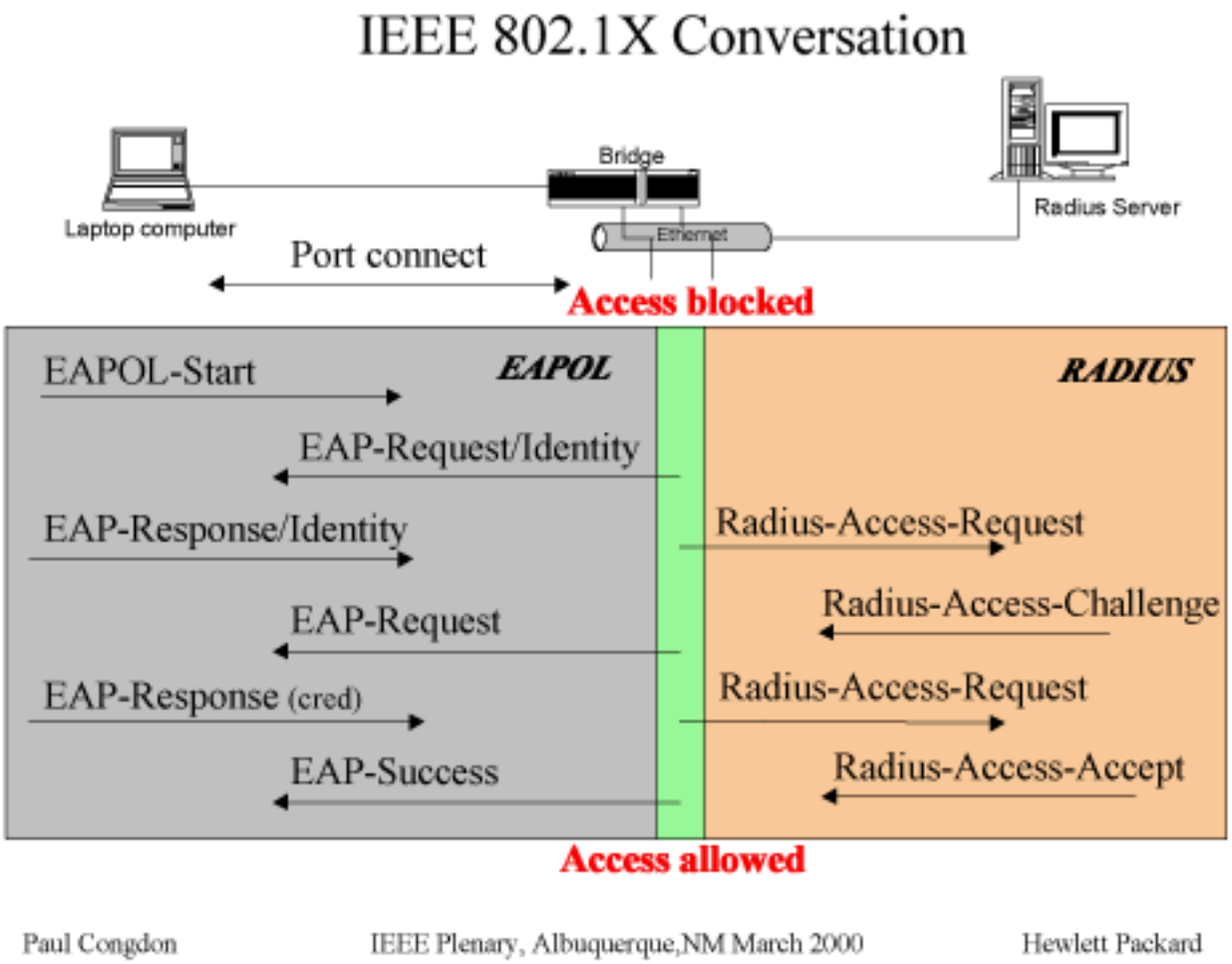
IEEE 802.1X Authentication

When the Supplicant initiates a request, it must first authenticate. The **authentication** process takes place by EAP at the link layer, which is necessary for security reasons. This layer provides just enough communication protocol to authenticate without allowing the Supplicant unauthorized access to the network. The authentication process can be accomplished independent of IP addresses and name resolution, which alleviates potential security holes and minimizes processing time. It is fast, simple, and inexpensive, and link layer authentication is already supported in PPP, IEEE 802 and most other popular applicable protocols. Avoiding the network layer means avoiding the complexities of secure communication across IPv4, IPv6, AppleTalk, IPX, SNA and NetBEUI and of requiring authorization between multiple layers.

The Supplicant communicates with the Authenticator using EAPOL. To begin authentication, Auth-x generates a unique per-station (user machine) session key. Once this has been completed, Auth-x will then specify an EAP-approved method that supports secure, dynamic, key derivation, such as Transport Layer Security (TLS [RFC 2716]). These keys should be changed frequently, and they should be mutually authenticated. The use of unique, secure, dynamic keys greatly improves security relative to that provided by WEP.

Within the scope of the entire A&A process, at this point the Supplicant is in an unauthorized state. It has only 802.1X network access, which does not include a valid IP address or a gateway address to which to forward packets. All non-Auth-x traffic (i.e. DHCP, SMTP, POP, HTTP) is denied. Should authorization fail, the Supplicant's link layer connection is dropped, and all access is denied without question.

© SANS Institute 2000 - 2005 Author retains full rights.



I now examine more closely the EAP process. A port begins in an unauthorized state, which allows EAP traffic only. Once the Authenticator has received a Supplicant's request to connect (an *EAPOL-Start*), the Authenticator replies with an *EAP Request Identity* message. The returning *Response Identity* message is delivered to the Authentication Server. According to Auth-x specification, the particular challenge and response algorithm used is flexible. A typical method is illustrated above (taken from Paul Congdon's *IEEE 802.1X Overview*). The result is an *Accept* or *Reject* packet to the Authenticator. Upon rejection, the Supplicant is dropped. Upon Acceptance, the Authenticator transitions the Supplicant's port into an authorized state, and then regular traffic begins. When the session has been completed, the Supplicant sends an *EAP-logoff* message, which forces the Authenticator to transition the port back into an unauthorized state. As mentioned above, the method for key exchange and key management is left to the vendor, but it should include a proven, secure method.

IEEE 802.1X Authorization

© SANS Institute 2000 - 2005 Author retains full rights.

After the Supplicant has successfully authenticated, the RADIUS server authorizes privileges through the distribution of tokens to participating devices and applications. Local computer and server privileges correlate with typical file and folder access privileges. Other authorization criteria can include access by group membership, rules by access type (i.e. dial-in, wireless, wired), and rules by time of day.

With Auth-x fully implemented, bandwidth and usage provisioning could be opted by the user much the same way one chooses his long distance or wireless phone usage plan. "Pay-per-packet" bandwidth could be authorized on demand, similar to the method currently being used for Pay-per-view. Through a web-based interface, the user could control the specifications of his usage (and thus, billing); he would also be able to make on-the-fly changes. Automated provisioning, filtering, and accounting would be controlled by RADIUS attributes in conjunction with 802.1X.

In the enterprise environment, better auditing capability of usage information will provide managers with the ability to optimize department performance. Usage reports will confer upon accounting management the ability to correctly bill and upon IT staff the ability to correctly allocate resources among departments. Automated assignment to a particular VLAN enhances security and will quickly become something we cannot live without.

Wrap-up

In the enterprise, Auth-x will provide IT staff and network managers with the ability to tighten security by enabling improved, automated implementation of their security policy. Auth-x brings authentication and authorization down to a port level, enabling true privilege-based management of network services. When deployed on a large scale, Auth-x becomes an important moderator for Internet traffic. In fact, in a few years, it will be hard to picture the Internet with out it. Auth-x puts security managers in control.

Bibliography

Roshan, Pejman. "802.1X Authenticates 802.11 Wireless." 9 Sept. 2001 URL:http://www.nwfusion.com/news/tech/2001/0924tech.html (12 Dec. 2001)

Aboba, Dr. Bernard. "Wireless LANs: The 802.1X Revolution." Dec. 2001 URL:http://www.drizzle.com/~aboba/IEEE/BAWUG.ppt (14 Dec. 2001)

© SANS Institute 2000 - 2005 Author retains full rights.

IEEE 802.1X Committee. "802.1x - Port Based Network Access Control." http://www.ieee802.org/1/pages/802.1x.html (12 Dec. 2001)

Miale, Drew. "Enterasys Networks Announces Support for the 802.1X Standard." 7 Mar. 2001 URL: http://www.enterasys.com/corporate/pr/releases/2001/mar/3-7a.html (11 Dec. 2001)

Meetinghouse Data Communications. "802.1X SecureSupplicant." URL:http://www.mtghouse.com/supplicant.html (11 Dec. 2001)

Congdon, Paul. "IEEE 802.1X Overview – Port Based Network Access Control." Mar. 2000 URL:http://www.google.com/search?q=cache:gTixIc9lApo:www.ieee802.org/1/mirror/8021/docs2000/P8021XOverview.PDF+eapol&hl=en (20 Dec. 2001)

Livingston, Rigney, Merit, Rubens, Simpson, Daydreamer, Willens, Livingston. April 1997. "Remote Authentication Dial In User Service (RADIUS) [RFC 2865]" April 1997 URL: http://www.ietf.org/rfc/rfc2865.txt?number=2865 (5 Dec. 2001)

Glossary

AAA – authentication, authorization, accounting
ACL - Access Control List – a list in a router or firewall to allow or deny specified traffic from a particular source to a particular destination
AP – Access Point – usually in the context of wireless access point: the point at which the wireless connection is bridged or routed to a wired connection.
CPE - customer premises equipment
EAP - Extensible Authentication Protocol – IETF RFC 2284
IPSec – IETF RFC 2401 - a layer 3 encryption method for providing secure tunnels.
NAS - Network Access Server
OSI – Open Systems Interconnect – a suite of network protocols.
PDA – Personal Digital Assistant (i.e. Palm, Handspring Visor, etc.)
RADIUS - Remote Authentication Dial In User Service – IETF RFCs 2865, 2618-2621, 2866-9 & 3162 – officially assigned port# 1812
STAs - stations
Supplicant: one who makes petition with earnestness and submission.
TLS - Transport Level Security
VLAN – Virtual LAN – the ability of a switch or switch group to designate a

© SANS Institute 2000 - 2005 Author retains full rights.

number of its ports to reside in their own virtual LAN
VPN – Virtual Private Network – a network connection through the Internet which utilizes cryptography to communicate securely
WEP - Wired Equivalent Privacy - part of the IEEE 802.11 specification

Questions

1.) Communication between which two parts of the RADIUS authentication process typically has the weakest security link?
a.) the Supplicant and the Authenticator
b.) the Authenticator and the Authentication Server
c.) the Authentication Server and Proxy Authentication Server
d.) the Authenticator and the secondary Authentication Sever

2.) With 802.1X installed, it is impossible for a user to gain access to the network without proper authorization.
a.) True
b.) False

3.) The IEEE 802.1X protocol specifies the use of Diffie-Hellman key exchange.
a.) True
b.) False

4.) The Challenge and Response method used in the Extensible Authentication Protocol (EAP) is:
a.) Diffie-Hellman
b.) Wired Equivalent Privacy (WEP)
c.) Transport Level Security (TLS)
d.) Left up to the vendor

5.) Which type of traffic is allowed at the link layer:
a.) POP
b.) EAP-logoff message
c.) DHCP
d.) FTP

6.) WEP requires that secure dynamic keys be generated for each session.
a.) True
b.) False

7.) A Supplicant gains network access by authenticating directly with the

© SANS Institute 2000 - 2005, Author retains full rights.

Authenticating Server
    a.) True
    b.) False

8.) The IEEE 802.1X protocol solves the security problems with WEP.
    a.) True
    b.) False

9.) EAPOL is used to communicate between:
    a.) the Supplicant and the Authenticator
    b.) the Authenticator and the Authentication Server
    c.) the Authentication Server and Proxy Server
    d.) the Authenticator and the secondary Authentication Server

10.) Which is a typical 802.1X authentication criterion?
    a.) MAC address
    b.) IP address
    c.) Switch Port number
    d.) User ID

© SANS Institute 2000 - 2005, Author retains full rights.