Open and free IEEE 802.1X / WPA / WPA2 / IEEE 802.11i

Preface

This document will give a short status report on free, open source components in the IEEE 802.1X authentication chain, consisting of supplicant (client), authenticator (edge network device) and the authentication server. Products are available to cover all components in the chain, but not all are equally suitable for production use. This document will also provide reasons for choosing open source alternatives where possible.

Why open source?

There are several reasons for using open source solutions. Open source components tend to be much more flexible than "off-the-shelf" ones. The initial cost and TCO tend to be lower, and you usually do not need to worry about end-of-life issues for the products. The open source community tends to wait for standards to emerge rather than implementing drafts; therefore, while it may take some months for bleeding-edge protocols to sieve through. When they do, the implementation of them is often more stable. Because the code is open, you can rest assured that your engineers or the Internet security community will weed out security risks quickly and effectively.

Professional support for open source products is provided by numerous consulting businesses around the globe. In addition, the communities around each component maintain mailing lists for developers and end users.

The supplicants:

There are two free, open source supplicants, wpa_supplicant[3] from the HostAP project and xsupplicant[4] from the Open1x project[4]. wpa_supplicant and Xsupplicant are licensed under BSD and GNU General Public License(GPL) and support most 802.1X/EAP authentication methods.

The wpa_supplicant and Xsupplicant projects are mainly focusing on the unix like operating systems. wpa_supplicant is also available for Windows and there is a code fork of Xsupplicant, named Wire1x[5], supporting major Windows operating systems.

Windows EAP plug-ins:

A SourceForge[7] project called wEAP[6] has also been initiated to write open source plug-ins for Windows. It is hoped that the wEAP project will bring more authentication flexibility to the native Microsoft supplicant. In the last year, the SecureW2[9] EAP-TTLS plug-in for Windows has gone open source.

The authenticator:

HostAP[2] is an open source initiative designed to make a wireless AP from a Linux box. It supports 802.1X/EAP authentication, WPA and WPA2 key exchange and RADIUS authentication and accounting.

An example would be to build an access point with a wired 802.1X supplicant and a VPN client authenticating to a remote RADIUS server behind the corporate firewall. For normal use, these systems would be both more expensive and more bulky than off-the-shelf appliances.

The authentication server (RADIUS server):

There are a number of free open source RADIUS servers. However only some support EAP authentication. For example, FreeRADIUS is a high-performance and highly configurable RADIUS server that supports EAP. HostAPd also has an integrated EAP authenticator.

FreeRADIUS[1] runs on most POSIX systems. It supports all common inner and outer authentication mechanisms. The server has no graphical user interface or GUI to administer it, but it does come with a PHP and web-based GUI tool for administering users in SQL or LDAP databases. The configuration files are stored in plain-text, which makes it easy to use for the administrator who has complex needs which may not be supportable in a GUI. Its debugging features are outstanding and easy to understand.

"Free but not open" or "open but not free"

There are also other products which either are commercialized open source, or are free but pre-compiled (closed). Among those is the Radiator RADIUS server. It is priced and supported as a general commercial product, but the license allows access to the source code, enabling the customer to add changes. Microsoft Windows XP/2000 and Mac OS X have built-in supplicants. Although these are supplied with the operating system at no extra cost, they are pre-compiled into the OS.

Useful links:

[1] FreeRADIUS site: http://www.freeradius.org/

[2] Host AP : http://hostap.epitest.fi/

[3] wpa_supplicant: http://hostap.epitest.fi/wpa_supplicant/

[4] Open1x : http://www.open1x.org/

[5] Wire1x: http://wire.cs.nthu.edu.tw/wire1x/

[6] wEAP: http://weap.sf.net/

[7] SourceForge: http://sourceforge.net/

[8] GPL: http://www.gnu.org/copyleft/gpl.html/

[9] SecureW2: http://www.securew2.com/