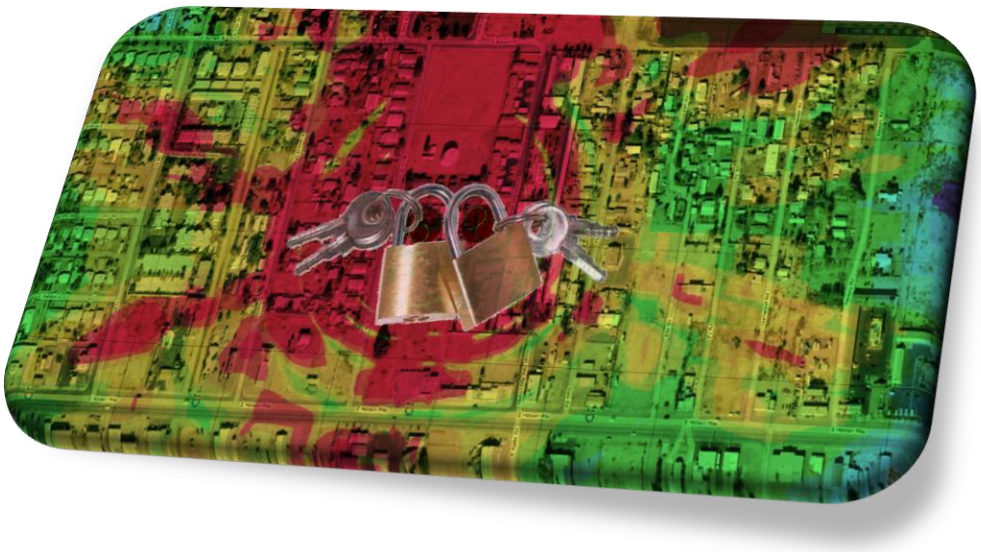
A CDM Wireless White Paper

239 Wiggins Rd.
Louisburg, NC 27549
1+ (919) 556-7480
www.cdmwireless.com



Wireless Encryption for CDM Devices

Casey Annis, Wireless Engineer

Published, January 16th, 2012, Updated 3/17/16

Contents

Introduction

CDM Wireless, a provider of innovative wireless solutions continues to educate and keep our customers abreast of our technologies and latest industry trends by distributing a new series of white papers focusing on the basics of Wireless and Wi-Fi systems.

There are several aspects and strategies for securing a wireless network and Viper radios have many features that all work together for protecting the network according to end user requirements.

This white paper will cover a major one of the security features – wireless encryption, to provide our distribution, integration and end user partners with some insight into the wireless security features, modes and encryption options of their Viper equipment.

Problem Statement

With the widespread use of wireless data networks there has been a correlated rise in network intrusion attempts via the very same architecture. Since the early 2000's, Wi-Fi security algorithms (WPA and WPA2) have been used on most wireless devices.

The IEEE and the Wi-Fi consortium have worked and continue to work on developing newer and more secure wireless encryption algorithms and key exchange routines to constantly stay ahead of those "would be" network intruders.

Previous Options

In previous versions of the Wi-Fi standards the only option for encrypting your wireless network was the Wireless Equivalency Protocol (WEP), which was fully abandoned by 2003 and considered highly ineffective and practically useless.

Although the IEEE had improved methods for using revolving key pairs and stronger encryption bit rates, new exploits were found that would allow anyone with a prebuilt software package to compromise a WEP secured network in under a minute.

In 2004 WEP was replaced with a new and more secure technology that is today's standard for securing wireless networks. That technology is called Wireless Protected Access. WPA has undergone several changes to keep the protocol secure and is currently deployed as WPA2.

Industry Standard

Today, the highest standard for securing enterprise wireless networks is WPA2 AES-256. AES is the encryption of choice for the US Federal government and NASA.

CDM Solutions

CDM Viper radios offer several wireless encryption and security strategies to ensure the highest protection and stability of the entire network.

Viper radios are factory programmed for WPA2 with AES key strength up to 256 bits. With the additional inclusion of technologies such as EAP and RADIUS key exchange authorization, Viper radios can be customized for highly stringent security needs.

Our equipment has been utilized in some of the most security conscience and critical protection installations around the world, including professional sports arenas, medical facilities, banks, U.S. Federal facilities and military bases.

WPA2 Provides Multiple Security Stances

WPA2 utilizes a variable bit encryption scheme that allows the end user to decide the level of encryption utilized. The encryption bit size is determined by the length of the provided security key. The numbers of characters in the security key are multiplied by a factor of eight (8) to arrive at the final encryption key. Example, if you use an eight-digit key, then you will have a 64-bit encryption profile. By default, Viper radios are assigned a 16 digit key which produces an AES-128 profile. To fully benefit from the protection of WPA2, a random key of 32 characters long should be utilized in order to generate a 256-bit encryption profile.

CDM will, at the request of the customer, generate Encryption keys for each system so that a unique key is distributed with every sale. Without such a request CDM generates a 128-bit key that is common to all systems and must be finalized by the end customer.

EAP

CDM Viper radios can also be configured to use Extensible Authentication Protocol to further enhance the protection of your wireless network.

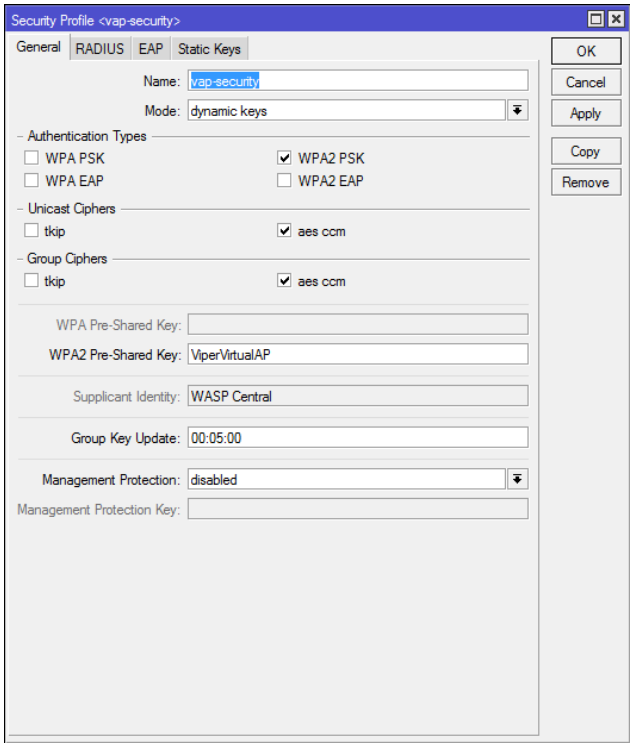
TLS Certificates:

The system can be configured to use TLS Certificates to authorize and encrypt wireless traffic in a way that is very similar to the way secure https connections are made.

The access point can check the validity and issuer of a wireless client's TLS certificate to verify the devices authenticity A client can also be configured to check the validity of an access point's certificate to ensure a complete two-way authentication system.

RADIUS:

When used in combination with the wireless access list and wireless security profiles, a RADIUS server can provide an even stronger security stature than any one standalone process. An authentication server can verify the mac-address of a client and its security key via a remote process. This method allows you to store and protect your encryption keys at a centralized location. In the event your access point is compromised, your network access keys are not compromised as well.



Implementation

CDM Wireless distributes all of our Viper radios with a pre-installed 128-bit key that can be customized by the end user or a request can be made for a stronger key that will be kept confidential and in reserve for the customer and any future orders can be configured the same. Since it is CDM's default practice to assist all of our customers with the design, configuration and implementation of their entire wireless infrastructure, our customers may contact us at any time to discuss strategies to secure their installations.

Summary

By utilizing a Viper wireless solution and relying on our experience and expertise in the wireless industry, CDM Wireless can provide our end users with a unique and scalable wireless security profile.