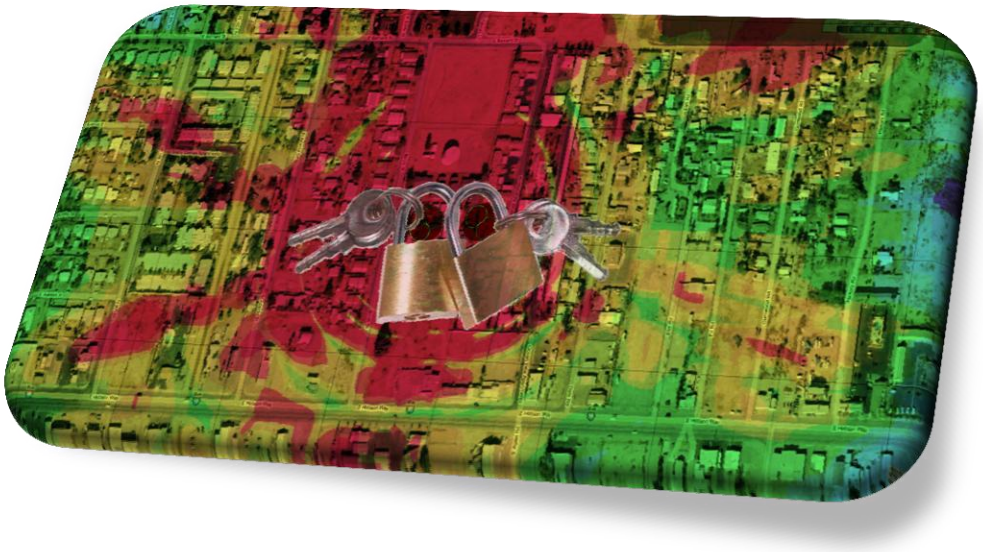
A CDM Wireless White Paper

810 Building C
Youngsville, NC 27596
1+ (919) 556-7480
http://www.cdmwireless.com



Wireless Encryption for CDM Devices

Casey Annis, Wireless Engineer

Published: Monday, January 16th, 2012

Contents

Introduction

CDM Wireless, a provider of innovative wireless solutions, in our desire to educate and keep our customers abreast of our progress is distributing a new series of white papers focusing on the basics of Wireless and Wi-Fi systems.

This particular issue will provide our distribution, integration and end user partners with some insight into the wireless security feature set of their Viper and Raptor 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. This can be a cause of concern for anyone considering the deployment of a wireless infrastructure regardless of scale, infrastructure or vendor. 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 incarnations of the Wi-Fi standards the only option for encrypting your wireless network was the Wireless Equivalency Protocol, or WEP, and it has gained notoriety in recent years as being highly ineffective and practically useless.

In later installments, methods for using revolving key pairs and stronger encryption bit rates were included. Yet it was only a matter of months before new exploits were found that would allow anyone with a prebuilt software package to compromise a WEP secured network in under a minute.

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

CDM Solutions

The latest industry standards for wireless security are implemented in all of our CDM Wireless product lines and our commitment to the design and implementation of your secure wireless network is without peer in this industry. CDM employs several wireless encryption strategies to ensure the stability and security of our customer's concerns of proprietary and sensitive data transport.

The Viper and Raptor equipment incorporates a wireless security technology called WPA2 with a key strength of up to 256 bits, which is in excess of the standard requirements the U.S. Government has for its data transfer protocols. With the additional inclusion of technologies such as EAP and RADIUS key exchange authorization; CDM can build a customized wireless security to fit your most stringent 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, military bases and active combat theatres.

WPA2 Provides Multiple Security Stances

WPA2 utilizes a variable bit encryptions scheme that allows the end user to decide just how much encryption to utilize. The encryption bit size depends upon 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. If you use only an eight digit key then you will have a 64-bit encryption profile. To fully benefit from the protection of a WPA2 encryption profile a random key of 63 characters long should be utilized in order to generate a 256-bit 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 Wireless equipment lines can be configured to use Extensible Authentication Protocol to further enhance the protection of your wireless network.

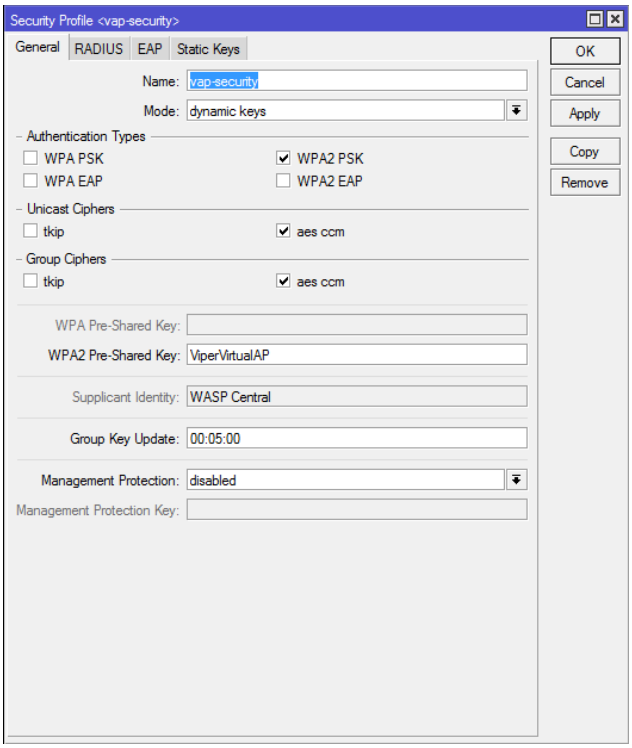
TLS Certificates:

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 http 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 allows you to store your encryption keys on a remote and centralize location so that if your access point is compromised in any way your network access keys are not compromised as well.



Implementation

As mentioned earlier CDM Wireless distributes all of our systems 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 CDM Wireless infrastructure, our customers can contact us at any time to discuss strategies to secure their installations and expect our assistance in deploying that strategy in a timely manner.

Summary

By utilizing a CDM 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.