Leveraging DTECH Products in a Campus WLAN CSfC Solution

Abstract

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off - the- Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators. (https://www.nsa.gov/ia/programs/csfc_program/)

This paper provides an example of DTECH's commercial off the shelf (COTS) products being utilized to implement a CSfC Campus Wireless Local Area Network (WLAN) Capability Package. The CSfC WLAN Capability Package describes a CSfC system that meets the demand for using commercial End User Devices (e.g. tablet and laptop computers) to access secure enterprise services over a campus wireless network. The Campus WLAN Capability Package Version 1.1 enables customers to implement layered encryption using commercial products between a Red Network infrastructure and End User Devices (EUDs).

References:

- https://www.nsa.gov/ia/_files/Campus_WLAN.pdf
- www.dtechlabs.com

1 Introduction

The M3C4G Product Family consists of modular common back plane components that share a power supply/UPS, gigabit Ethernet network, and chassis.

The NSA CSfC Campus WLAN Capability Package v1.1 defines the architecture and requirements necessary to field a WLAN CSfC Solution. CSfC Solutions must use certain products from the NSA's CSfC Components list. Even though DTECH's M3C4G products don't appear directly on the CSfC Components list, DTECH products embed CSfC components or can be used to host software that is a CSfC Approved Component.

2 Campus WLAN Architecture and Components

2.1 Campus WLAN Capability Package Overview

The following Architecture diagram is sourced from the Campus WLAN Capability Package document.

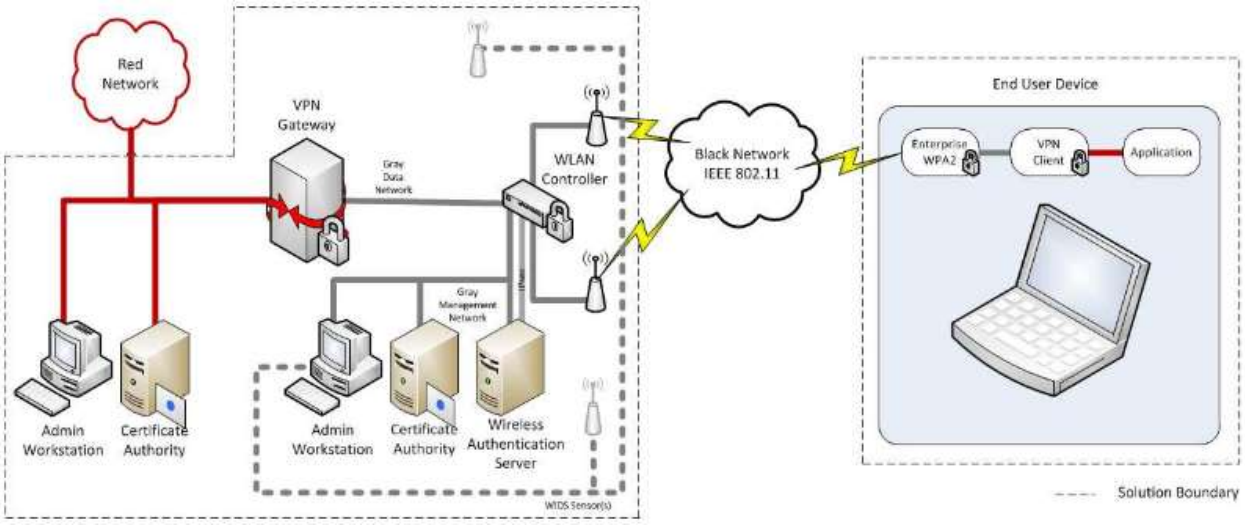

Figure 1: Two Layers of Encryption Protected Data across an Untrusted Network

In the Campus WLAN architecture, see Figure 1. The 2 layers of cryptographic services are provided using IPsec as the inner layer of cryptographic services and WPA2 Enterprise on the 802.11 air interface as the second or outer layer of cryptographic services.

In Figure 1 each component shown is prescribed to fulfil an important role. The WLAN Controller and attached WLAN Access Points make up what is referred to in the Capability Package as the Wireless Access System. The Wireless Authentication Server is used by the Wireless Access System to validate wireless client authentication requests. Notice that the traffic between the Wireless Authentication Server and the Wireless Access System is IPSec protected. The Certificate Authorities are the servers that create, revoke and otherwise maintain the list of certificates used within the solution. The Admin Workstations are computers that are used exclusively for managing the CA, VPN Gateway, WIDS, and any other solution infrastructure asset. Wireless Intrusion Detection Sensors are used to recognize wireless based system attacks. Other optional network assets not shown in Figure 1 include Network-based Intrusion Detection System/Intrusion Prevention System (IDS/IPS). Finally, the End User Devices are envisioned to be mobile devices such as laptops and tablets implementing WPA2 Enterprise cryptography and an IPSec VPN client.

2.2 The DTECH M3C4G Products as Campus WLAN Solutions

The DTECH M3C4G product line provides a compelling set of features. In particular, the M3C4G's size, UPS, and compact packaging would allow for the creation of a rapidly deployable Campus WLAN infrastructure. An M3C4G Campus WLAN system would be ideal in rapid response environments where

classified communications are required but wired distribution mechanisms are too cumbersome or consuming to provide.

The individual capabilities and components prescribed within the Campus WLAN Capability Package can map across many different DTECH product combinations. The following section provides just one example of what a M3C4G Campus WLAN solution might look like. For a complete picture of CSfC component interoperability please refer to the DTECH CSfC Compliance Matrix.

2.3 M3C4G Products as a Campus WLAN Infrastructure Solution

An example Campus WLAN solution built from DTECH M3C4G components is shown below in Table 1. This solution includes the solution's optional component: the Network-based Intrusion Detection System.

Table 1: DTECH M3C4G CSfC Campus WLAN Capability Functional to Physical Mapping

Function	M3C4G Model	CSfC Component
WLAN Controller, WLAN Aps, and WIDS	N/A	These components would be provided by non-DTECH products
Gray CA, Wireless Authentication Server, Gray Admin Workstation	M3-PM-SVR3	Windows Server 2012 R2 VM (with IDS/IPS software, CA software, and as a workstation) Aruba Clearpass Policy Manager VM (Authentication Server)
VPN Gateway	M3-PM-RTR3C	Cisco ESR 5915
Red CA, Red SIEM, Red IPS/IDS, Red Admin Workstation, Red content server/services	M3-PM-SVR3Q	Windows Server 2012 R2 VM (with IDS/IPS software, CA software, and as a workstation), Windows Server 2012 R2 VM (as content server)

The resulting system would look like what is depicted below in Figure 2.

Figure 2: DTECH Example M3C4G Campus WLAN Infrastructure

This example stack up is easily modified to add more compute power for applications or mission specific interfaces. The inclusion of additional M3C4G modules can provide E&M ports for LMR integration, telephony ports, MANET radio, switches, and/or more computers/servers.

3 Conclusion

The CSfC Campus WLAN Capability Package provides government users with a set of instructions and guidance on how to go about properly using commercial products to field classified services. The DTECH M3C4G product line provide an industry leading combination of small size and rugged design that meets the requirements of government users in even the most challenging of conditions. When composing CSfC solutions to meet the NSA published CSfC Capabilities Packages DTECH products can be effectively used either directly or as host platforms across the entire spectrum of CSfC components. In those cases where DTECH equipment is already fielded or in use, modifying those systems to provide a CSfC solution would require only minimal modification or reconfiguration.

4 Points of Contact:

Nick Podolak
Senior Principal Software Engineer
CUBIC | DTECH LABS
nicholas.podolak@dtechlabs.com
http://www.dtechlabs.com/

Or contact an account manager at sales@dtechlabs.com . They may assist in getting any questions answered or support needed regarding DTECH products used for CSfC or any other requirements you may have.