Enabling Secure Mobile Operations with Commercial Products

Grant Wagner
Technical Director
Trusted Systems Research
National Security Agency

October 16, 2014
Overview

• Moving to Commercial Products
• Mobile Client Considerations and Solutions
• Infrastructure Considerations and Solutions
• Operations Considerations and Solutions
Commercial Solutions for Classified

CSfC
Commercial Solutions for Classified

• NSA’s “Commercial Solutions for Classified” (CSfC) program specifies a method to use commercial and Open Source products to secure a classified network

• The method uses multiple different layers of commercial encryption on top of each other
  – Reduction of a single flaw exposing classified data

• The method specifies a “Defense in Depth” including monitoring to detect issues before they become critical
Defense in Depth

- Monitoring the system detects potential issues
  - Network traffic can be profiled and verified IE:
    - All traffic must be encrypted
    - All traffic must be from approved devices
- Monitoring can trigger shutdowns before large compromises
- Inner encrypted traffic is extremely well defined
  - Allows easy detection of odd traffic
  - Provides confidence of data correctness
Wireless

• WiFi (802.11abgn) does provide encryption (WPA2), however, it is not Suite-B compliant
  – WPA2-enterprise uses AES-128 with RSA certs

• While WPA2 security may not be sufficient as an encryption tunnel, it does make sense to use it
  – WPA2 is “free” on most WiFi cards
  – It does provide additional security
  – It does protect infrastructure information
  – It does provide a legal boundary for monitoring clients
Client Encryption Tunnel Requirements

• Client device is a single laptop
  – No external encryption hardware desired

• Must provide proper isolation and separation of encryption tunnels
  – Cannot install multiple tunnels on the same OS instance (Windows, Linux)

• With proper hardware and hypervisor support, virtual machines can provide the necessary protections
  – VT-x and VT-d (Intel) or AMD’s AMD-V and AMD-Vi CPU extension required
  – Proper Hypervisor (Xen, XenClient XT, KVM, etc) provides underlying isolation support
Laptop Virtualization (Standard)

- Basic Laptop with virtualized guest
  - Guest has virtual network card that can hook to real network card driver in hypervisor
  - Network card is exposed to hypervisor
    - The network card driver in the hypervisor provides a single point of failure to compromise the entire system
    - Breakout can occur and affect entire system, hypervisors and VM’s

```
Guest OS:
• Windows, Linux, etc.

Virtual Net Driver

Hypervisor:

Network Card Driver

Laptop Hardware

Network Card Hardware
```
Laptop Virtualization (Network Protection)

- Laptop with Network card protection
  - Network card is “passed through” to VM
  - Outside attack can compromise Network Driver VM (NDVM), but not the entire system with a single point of failure
- The guest and NDVM communicate through dedicated “private” network channel
- All guest traffic must cross through the Network protection VM
  - Allows the NDVM to add firewalls, monitoring, etc. without changing the guest.

Guest OS:
- Windows, Linux, etc.

Network Protection:
- Linux w/ SELinux
  - Virtual Net Backend
  - Network Card Driver

Hypervisor:

Laptop Hardware

Network Card Hardware
Laptop Virtualization Adding Encryption

- Laptop now has a layer of encryption
  - All guest traffic is encrypted before getting to the network
  - The guest doesn’t know about the encryption layer. All programs operate normally
  - The encryption vm is isolated from both the guest and NDVM
- Additional monitoring and protection can be added to the Encryption VM
- Firewalls are added to the Encryption VM to prevent non-encryption traffic from leaving

**Diagram:**

- **Guest OS:** Windows, Linux, etc.
- **Encryption:** Linux w/ SELinux
- **Network Protection:** Linux w/ SELinux
- **Hypervisor:**
- **Laptop Hardware:**
  - Laptop Virtualization
  - Adding Encryption
  - Virtualization
  - Adding
  - Encryption
  - Laptop
  - Now
  - has
  - a
  - layer
  - of
  - encryption
  - All
guest
  - traffic
  - is
  - encrypted
  - before
  - getting
to
  - the
  - network
  - The
guest
  - doesn’t
  - know
  - about
  - the
  - encryption
  - layer. All programs operate normally
  - The encryption vm is isolated from both the guest and NDVM
- **Additional monitoring and protection can be added to the Encryption VM**
- **Firewalls are added to the Encryption VM to prevent non-encryption traffic from leaving**
Laptop Virtualization Adding Layered Encryption

- Laptop now has two layers of encryption
  - Guest still is not aware of encryption, all programs operate normally
- All traffic is transparently encrypted twice before leaving the client

<table>
<thead>
<tr>
<th>Guest OS: Windows, Linux, etc.</th>
<th>Encryption: Linux w/ SELinux</th>
<th>Encryption: Linux w/ SELinux</th>
<th>Network Protection: Linux w/ SELinux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Net Driver</td>
<td>Virtual Net Backend</td>
<td>Virtual Net Backend</td>
<td>Network Card Driver</td>
</tr>
</tbody>
</table>

Hypervisor: 

Laptop Hardware

Network Card Hardware
Encryption VM’s

- IPSec Tunnels provide:
  - Full Suite-B encryption
  - Client validation using ECDSA certificates

- Firewalls:
  - Allows authorized traffic to/from only known infrastructure devices
  - Protects both sides of connection, upstream and down

- SELinux:
  - Prevents unauthorized programs from running
  - Prevents unauthorized file accesses

- Monitoring:
  - Verifies system operation

- VM is read-only
  - Prevents modification

Diagram:

- Encryption VM’s: Linux w/ SELinux
- IPSec Encryption Tunnel
- Firewall
- Monitoring
- Virtual Net Backend
- Firewall
- Encrypted
- Virtual Net Driver
- Raw Data
Network Driver VM

• **WPA2 encryption**
  – Provides protection from casual eves-droppers
  – Makes the network look like a “normal” wireless network
  – Uses `wpa_supplicant` to control the network
  – Uses RSA certificates to validate clients and servers

• **Firewalls:**
  – Allows authorized traffic to/from only known infrastructure devices
  – Protects both sides of connection, upstream and down

• **SELinux:**
  – Prevents unauthorized programs from running
  – Prevents unauthorized file accesses

• **Monitoring:**
  – Verifies system operation

• **VM is read-only**
  – Prevents modification

![Diagram of network components](diagram.png)
Infrastructure Architecture
Infrastructure Requirements

• Must support enterprise number of clients
  – Uses 10GBs interconnects
  – Requires beefy machines
  – Should support failover and load-balancing
    • Not required for initial development
• Modularly designed
  – Black box
  – Can add boxes as needed
• Clearly defined communication paths
• Clearly defined security boundaries
• Mirrors client buildup
Infrastructure “Tier”

- Each “Tier” represents a single “Black Box” of encryption and protection
  - Includes IPSec encryption components
  - Includes firewalls
  - Includes necessary monitoring
  - Includes necessary reporting paths
- Lines up similarly to the client boxes
  - Not an exact match
    - Clients include firewalls at VM boundaries
    - Infrastructure uses dedicated hardware VPN endpoints
    - Infrastructure includes management components
Wireless Tier Components

- The WLC validates each client
  - Uses WPA2 and RSA certificates and a radius (AAA) server
  - Used DHCP to give client IP addresses (Non-fixed IP addresses)
- Accounting
  - AAA Accounting for clients
  - Syslog for all network devices
- Monitoring
- Management
Core Tier Components

- Each Tier has a VPN endpoint and a firewall
  - Mirrors the Client VM’s
- Each Tier is responsible for a single encryption tunnel
- Firewall controls all traffic flow between components
- Each Tier feeds to the next Tier above it
Support Tier Components

- The VPN endpoints must validate clients
  - Uses Suite-B certificates and a radius (AAA) server
  - Provides fixed IP addresses for each client
- Accounting
  - AAA Accounting for clients
  - Syslog for all network devices
- Monitoring
- Management
All Tiers Combined

• Each Tier has its own infrastructure, support, and monitoring components
  – No inter-tier communication paths other than the narrowly defined VPN endpoints and monitoring reports
• Tier 1 includes the WLC (shared by T3 and RD), the Access Points (APs), and Distributed Antenna System (DAS)
  – Tier 1 does not do Suite-B encryption and is not counted as one of the CSfC tunnels
  – Tier 1 does do WPA2 encryption, RSA cert based identity tracking, and Client verification
• Tier 2 is a pure outer encryption tunnel
• Tier 3 terminates the inner encryption tunnel, and feed classified data to the infrastructure
  – The system is designed to have the client guest appear to be directly connected to the infrastructure
Distributed Antenna Systems
Wireless Monitoring
Wireless DAS

- DAS (Distributed Antenna System) is a method to separate the Access Point from the Antenna itself using RF-over-Fiber optics
  - Allows the antenna to be located a large distance from the AP
  - The AP can be locked in a room with limited access controls
    - This reduces insider threats from accessing the infrastructure from direct access to the AP
  - The DAS antenna is wide-band, and allows sharing the antenna across a large number of systems, including WiFi, RFID, Cellular, EMS, etc
- The DAS system allows multiple sensors to be connected to each antenna, allowing a much closer look at the RF environment.
  - This RF sensor network provides a great first-line defense on protecting the wireless network
DAS

- Separation of DAS antenna from the protected infrastructure in the Comms Center
- Fiber Optics carry “RF-Over-Fiber”
  – No digital signals

Floors 1-5 Office Space

<table>
<thead>
<tr>
<th>TX</th>
<th>RX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coax</td>
<td>Amplifier &amp; Transceiver</td>
</tr>
</tbody>
</table>

Comms Center

<table>
<thead>
<tr>
<th>AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
</tr>
<tr>
<td>AP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor 1</td>
</tr>
<tr>
<td>Sensor 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor 2</td>
</tr>
<tr>
<td>Sensor 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor 2</td>
</tr>
<tr>
<td>Sensor 2</td>
</tr>
</tbody>
</table>
Provisioning and Updates
Provisioning

• Provisioning used to build a new client
• Scripted set of setup steps
  – Boot the installer
  – Format the hard drive
  – Install all the necessary VM’s (including Guests)
  – Configure system
  – Install RSA and ECDSA certificates
• Several steps have admin interaction to avoid unauthorized machine creation
  – Certs must be authorized by an admin
Provisioning System

- Each provisioning system operates the same (High/Low)
- Each provisioning system has two physical machines
  - Fileserver contains VM’s disk images, configuration files, and other large file
  - VM Server contains the PXE/Cobbler boot VM and all the CA’s
- Admin logs into the VM server and accesses the various VM’s to provision a laptop
- Provisioning uses physical Ethernet cable to talk with laptop
  - No wireless provisioning
- Once provisioned, the laptop communicates wirelessly to join the Windows 7 guest to the domain
Synchronizer System

• Synchronizer allows a method to perform Over-The-Air (OTA) updates of the laptop clients
  – Provides a way of downloading an installer and new support VM’s to the laptops
  – Installer saves configurations and guest VM images and updates the rest of the laptop

• Laptops can be individually selected for different OTA loads
  – Different groups can have different builds
  – Allows testing of advanced features without affecting all laptops
Questions/Answers Discussion