WHITE PAPER

Date: September 15, 2015
Subject: **White Paper: DVR System Security Approach**
Issued By: Image Vault, LLC – A Member of the FireKing Security Group
Issued To: To all Image Vault Dealers, Distributors and End-Users
Document #:

Overview

The operating system (OS) implementation utilized on Image DVRs has been hardened to be more secure and resilient to malicious attacks.

Security Strategy

The underlying strategy employed with the DVR is that of prevention. This is made possible by providing minimal access by the removal of all unnecessary system services, applications and components. The DVR is a dedicated-purpose Network Appliance device that is specifically made to address security considerations with the device itself and the networks in which it will be used.

System Overview

The system was designed using Microsoft Windows Embedded Standard 2009/ 7[i] for both security and reliability:

- **Fewer components** – The OS configuration is composed of approximately 4-5% of the possible components available (applications, drivers, etc.). The reduced complexity of the OS greatly increases security and reliability.
- **Access point control** – The system controls points of access by restricting hardware interaction to approved units (such as mass storage devices).
- **Reduced network visibility –** By utilizing good security practices, as well as removing unnecessary system services, the network visibility of the unit is reduced to eliminate any possible vulnerability.
- **Data Execution Prevention (DEP) –** The system utilizes hardware-enforced no-execute (NX) technology to prevent the execution of memory in essential Windows programs and services. This helps prevent a common attack that involves overrunning data buffers with code and then executing the code.
- **Privilege control** – System users are restricted from normal "PC" operations. Users do not have the ability to use the system for web browsing, e-mail, etc.

System Updates

Updates required for the DVR, or the underlying Operating System, will be provided by Image Vault on the Software Resources website or announced via Service Bulletin[ii]. Many updates from Microsoft will not apply to the DVR OS due to the system's components being excluded from the configuration; and therefore no associated Image Vault updates will be released.

Operating System Updates & Lifecycle

Microsoft Updates required for the underlying Operating System are assessed for viability monthly as distributed by Microsoft. These updates are packaged and provided by Image Vault on the Software Resources website or announced via Service Bulletin. Many updates from Microsoft will not apply to the DVR OS, due to the system's components being excluded from the configuration; and therefore no associated Image Vault updates will be released.

Unlike the desktop products, Microsoft provides an extended lifecycle for embedded products. Windows Embedded Standard 2009 will receive security updates (extended support) into January 2019[iii]. The current edition of Windows Embedded Standard 7 will receive security updates into October 2020[iv] (adjusted as Service Packs are released). After these expiration times are reached, additional support options are possible through Microsoft.

Network Access

A large number of viruses and worms that have affected Windows Embedded systems, in recent times, have come through DCOM, RPC and MSMQ services. The DVR design starts by never including unnecessary services, never running unnecessary services, and never exposing services to the network without need.

By default, the only TCP port accessible is that of the Image Vault remote connection. Additional network ports may only be opened for network POS connections.

In addition to limited open network ports, the system implements the Windows Firewall on the network connections as a reserve measure, as well as to add greater control over the interface.
ICMP echo requests are allowed to reach the system. Many other packet types are not allowed in order to prevent several common routing attacks.

On a fully booted system, the main Recorder process is the only one allowed external access (see Table 1).

Protocol	***Port(s)/Type***	***Usage***
TCP	32001	Recorder Client Connection (Playback, EVA Collector)
TCP	*user-defined*	Network POS listening ports, as configured by user
ICMP	*Echo Request*	Used to ping the system on the network

Table 1 – Allowed incoming network access after startup

The DVR uses the configured hostname (in Recorder Setup) as the NetBIOS computer name.
NetBIOS is configured to operate as a Hybrid Node[v] (H-Node), but with all incoming NetBIOS ports blocked by the Firewall service, as per above.

Other initiated network connections originate on the DVR system and are client operations.
Examples of this include attaching an IP camera or configuring automatic time synchronization.

Local Operating System Access

Local operating system access is rarely, if ever required. Local OS access is strictly controlled, and is possible only through the recorder application and with override keys generated by Image Vault.

Security Testing

In order to ensure the system's continuous security, Image Vault utilizes Nessus Vulnerability and Compliance Scanning Technology to perform product security testing on a quarterly basis.

Payment and Cardholder Information Concerns

The Image Vault DVR is a non-payment product. The DVR allows integration with POS devices; however, it does not directly store or process sensitive cardholder information[vi]. POS data is acquired via serial port or TCP/IP connection through PCI compliant network. POS data is not "fetched" by the DVR; rather it is "pushed" by the POS device to the DVR.

In order to ensure proper Network Security, it is recommended a properly configured Managed Switch is used to secure traffic between the DVR and POS System.

Multiple NIC's are available on the DVR to maintain physical segregation between outside traffic and POS system traffic.

The hardening of OS and removal of unnecessary system services achieves a high degree of isolation of the DVR from the network.

[i] https://msdn.microsoft.com/en-US/library/hh505866%28v=winembedded.60%29.aspx
[ii] http://www.fireking.com/video-security/service
[iii] http://www.microsoft.com/windowsembedded/en-us/product-lifecycles.aspx
[iv] http://www.microsoft.com/windowsembedded/en-us/product-lifecycles.aspx
[v] http://support.microsoft.com/kb/119493(NetBIOS over TCP/IP Name Resolution and WINS)
[vi] Connection to a PCI Compliant POS device implies that POS data being transmitted to the DVR has been truncated of all sensitive cardholder data.