Proposed Outline for Phoenix Meeting Attribute Discussions

Begin at a high level to document how a multi-functional HCD differs from devices currently addressed at what exactly causes current MFDs to be quarantined on a network. For example most IA departments will start HCD testing with a port scan. Questions are then raised on the need to have the discovered ports active and on whether the vulnerabilities usually associated with those ports on a typical network workstation apply or if they are false positives for the particular device given its architecture and OS. Given the discovered port configuration and information on whether or not the HCD is using a potentially vulnerable OS that requires patching or remediation the IA staff generally develops an acceptable configuration for installation.

IT generally also generally confirms that the print drivers required for the HCD to operate are available and, if scanning is a target application that the device supports the required protocols and has the required ports enabled.

In order for required HCD network authentication to execute support for Kerberos, NTLM etc. may be required and might need to be confirmed.

A short list including items similar to the above should be created. To authenticate on the particular network the device may have to support the entry of computer like passwords or have other minimum capabilities for the target applications. Indentifying those applications up front may be used to determine whether additional assessments are required.

HCD Attributes

At this session it is suggested that the focus be on the Cisco Network Access Control Architecture to create an initial example. It is proposed that the existing packet structure be used and that the priority be on clarifying its flexibility to accommodate new items. It must also be clarified whether default responses are expected by the current architecture that would not apply to the HCD.

Discuss the existing attributesand credentials that might apply to an HCD that verify that the device is compliant in order to arrive at the decision that no network restrictions are warranted.

These must include device identity and an inventory of relevant configurations and software states. The list that applies to computers on a network may not generally apply to an HCD depending on its architecture. If the HCD is not based on a CPU running a soft public domain OS such as Windows or Linux its version state and patch state may not apply. Many items currently on the attribute list for computers then may be excluded once this is identified. Attributes defined for computers that address OS types, version numbers, service packs etc may not apply but the overall version number of the HCD may be an indicator of whether it has the acceptable or the certified firmware if not the acceptable OS configuration.

Discuss what unique attributes and posture credentials might need to be defined that are not addressed by the current NAC architecture. Security policies may require validation or certification for devices that process information. They may not apply to HCDs connected as simple output devices so identification of applications enabled may be required. An application attribute for an HCD may differ from that used for computers by addressing higher level applications.

The HCD may have to be authorized access mail servers, shared folders, the internet, etc. to address approved applications. The network should not block access to those connections or services if the HCD is not only to be connected but function as expected. An attribute clarifying required services to operate may be required.

Acceptable network defaults may have to be set and checked such as timeouts and number of acceptable retries.

Discuss whether auto remediation is an option for a HCD. Network downloads, for example, may not be supported.

Discuss the relevance and role from the standpoint of the HCD of each NAC component in the authorization process used to grant or deny access to the network.

Device Triggering Challenge

Network Access Devices

Access Control Servers

Policy Servers

At the Phoenix meeting I will present a list of proposed attributes addressing the above and options likely required to define acceptable, connectable HCDs.