PWG -Imaging Device Security (IDS) Working Group

Irvine, CA - PWG F2F Meeting

February 18, 2009

Ron Nevo(Sharp), Dave Whitehead, (Lexmark)

PWG IP Policy

- Meeting conducted under rules of PWG IP Policy

Agenda

- Select Minute Taker- Lee?
- Morning session:
  - Approve Minutes from February 5 Conference Call
  - Review Action Items from February 5 Conference call
  - Review Secure time slides/proposal
  - Ciphersuite
  - Review Microsoft updates to their SOH document –How it will impact us?
- Afternoon session:
  - Review Attribute document – any comments?
  - Review NAP Binding Document with Brian Smithson updates
  - Decide how to present the bit-level contents of NAP packets?
  - Do we need IDS mapping document? NAP, NEA, TNC?
  - NEA Binding Document –start process- Who is the editor?
    - HCD-NEA Spec plans and schedule
  - New Action Items and Open Issues
  - Closing Summary

Action Items from February 5 Conference call

- Randy Turner will try to find other contacts that would be willing to work with the PWG to help deploy NEA health assessment. (Juniper, Symantec, Cisco are suggested candidates.) Is someone willing to sit down with the PWG and “have discussions”?

  Still needs to pursue this further. No new information to report.

- Randy Turner will post the Microsoft name(s) for the PWG to make contact with regard to logo requirements.

  Randy has requested a contact name, but no response yet.

- Joe Murdock will add NAP protocol information to document and update the conformance section.

- Joe Murdock will include sequence diagrams as illustrative examples for the NAP binding document.

- Dave Whitehead will coordinate with Randy Turner to generate a proposal to Microsoft on proceeding with obtaining NAP information on what they envision would be the content of a profile—including remediation. Need to identify the appropriate point of contact within Microsoft.

Action Items from February 5 Conference call

- *Randy said that Erhan Soyer-Osman has given him a name of someone (Chandra Nukala) that is willing to take architectural questions. However, it is important that we first do our homework on reading the available information on NAP and becoming familiar with it. We should avoid questions that have answers available in the current documentation. Randy will post links to relevant informative documents.*

- Everyone will review the latest Attributes document draft prior to the next teleconference, and prepare comments for discussion.

- Ron Nevo will examine which time protocols could be used for providing authenticated time (with high integrity), and make appropriate recommendations.

- Everyone will consider the Quarantine State attribute issue that Nancy Chen has raised and will provide recommendations for resolving.

- Brian will provide a proposed example illustrating the suggested format for review and acceptance.

- Issue- Which of the defined transport(s) are required to be supported in order to guarantee a device can attach to the network? MS defines DHCP, 802.1x, IPSec, and VPN and has extended each to add SOH information. So, in an environment where we are attaching wirelessly via 802.1x and receive our IP address from DHCP, what happens if we only support SOH over DHCP (or 802.1x)? Will we attach or fail?

Time Synchronization Discussions

Ron Nevo

Time –External/Internal source?

- MFP's on a network will either be able to access an external network time source or not. In most cases they may not be able to directly access an external source.
- Option 1 – MFP internal clock (on board clock) - no external synchronization
- Option 2 - External Network Source – such as NIST Time
- Option 3 –Internal Network Source
  - In this case the MFP must access a third party network appliance that provides the time for devices on the network and takes responsibility for Accessing the NIST time service or others.

Network Time Protocol (RFC-1305)

- The Network Time Protocol (NTP) is the most commonly used Internet time protocol, and the one that provides the best performance. Large computers and workstations often include NTP software with their operating systems. The client software runs continuously as a background task that periodically gets updates from one or more servers. The client software ignores responses from servers that appear to be sending the wrong time, and averages the results from those that appear to be correct.
- Many of the available NTP software clients for personal computers don't do any averaging at all. Instead, they make a single timing request to a signal server (just like a Daytime or Time client) and then use this information to set their computer's clock. The proper name for this type of client is SNTP (Simple Network Time Protocol).
- NTP uses Marzullo's algorithm, and includes support for features such as leap seconds. NTPv4 can usually maintain time to within 10 milliseconds (1/100 s) over the public Internet, and can achieve accuracies of 200 microseconds (1/5000 s) or better in local area networks under ideal conditions.
- In the Internet, NTP synchronizes computer system clocks to UTC; in isolated LANs, NTP is also commonly used to synchronize to UTC, but in principle it could be used to distribute a different time scale, for example local zone time.
- A less complex form of NTP that does not require storing information about previous communications is known as the **Simple Network Time Protocol** or **SNTP**. It is used in some embedded devices and in applications where high accuracy timing is not required. See RFC 1361, RFC 1769, RFC 2030, and RFC 4330.
- Note that NTP provides just the UTC time, and no information about time zones or daylight saving time. This information is outside its scope and must be obtained separately (most systems allow it to be set manually).

Network Time Protocol (NTP) time servers

- There are two levels, or tiers, of Network Time Protocol (NTP) time servers that are available on the Internet.

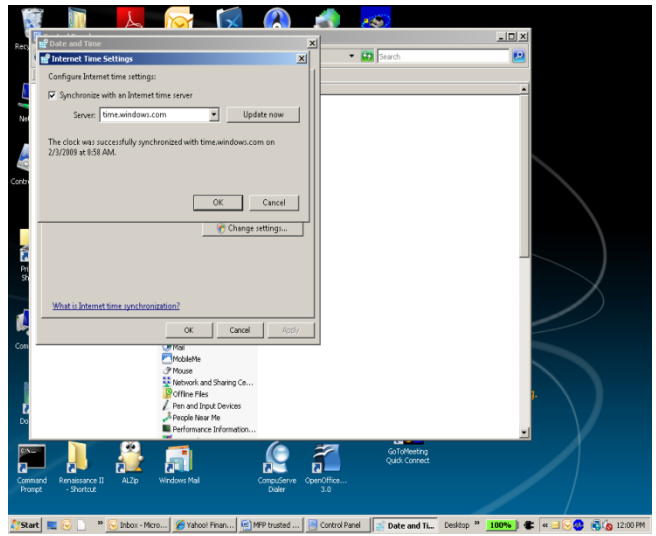
  The first-level time servers are primarily intended to act as source time servers for second-level time servers. The first-level time servers may also be capable of providing mission-critical time services. Some first-level time servers may have a restricted access policy.

  Second-level time servers are intended for general SNTP time service needs. Second-level time servers usually enable public access. It is recommended that you use second-level time servers for normal SNTP time server configuration because they are usually located on a closer network that can produce faster updates.

  The NTP uses port 123 so this port must be opened on a firewall or router to ensure proper communication with the NTP server.

How we synchronize the time in Windows?

- The most common use of this procedure is to synchronize the internal network's authoritative time source with a very precise external time source. However, you can run this procedure on any Windows XP-based computer.
- If the computer cannot reach the servers, the procedure does not succeed and an entry is written to the Event log.
- You can use computers on the Internet to provide accurate time information. For example, use the National Institute of Standards and Technology (NIST), which provides the NIST Network Time *service.*



NIST Time

- The National Institute of Standards and Technology (NIST) maintains a network of time servers that provide time and frequency services for the United States.
- The NIST Internet Time Service (ITS) allows users to synchronize computer clocks via the Internet. The time information provided by the service is directly traceable to UTC(NIST). The service responds to time requests from any Internet client in several formats including the DAYTIME, TIME, and NTP protocols.
- Requests in these formats generally do not support authentication, and no keys or passwords are needed to use these services.
- More information about the NIST may be found at the following Web sites:
- http://www.boulder.nist.gov/timefreq/service/its.htm (http://www.boulder.nist.gov/timefreq/service/its.htm)
- http://www.boulder.nist.gov/timefreq/ (http://www.boulder.nist.gov/timefreq/)
- The US Naval Observatory also maintains a network of time servers available for public access. To see a list of servers and their descriptions, visit the following US Naval Observatory Web site:
- http://tycho.usno.navy.mil/ntp.html (http://tycho.usno.navy.mil/ntp.html)

Definition in the IDS documentations

- **NAP-Binding document**
  - HCD secure time
  - HCD_Time_Source MUST be supported if the HCD implements any protocol or feature that requires an accurate time source.
  - **Secure Time Enabled:** When true, indicates the hard copy device is configured to acquire the current time from a known secure source in a secure manner.

- **IDS Attributes document**
  - HCD_Secure_Time_Enabled (Boolean)
  - The HCD_Secure_Time_Enabled attribute signifies that the time source used to set the device's clock(s) is considered, by the administrator(s), a trusted source. Note: An onboard clock source can be considered secure if its configuration is protected in some manner. (0 = not enabled)
  - Usage Considerations: Many security mechanisms rely on accurate time to enforce security. Examples include validity periods on X.509 certificates and Kerberos Tickets. As such, it is important to know that the device's internal clock(s) acquire time in a secure manner. If the time source is not secure, it could lead to denial of service (set time outside the validity period) and/or allow unauthorized access (set time to within validity period.) There are several ways to acquire the time including Network Time Protocol (NTP) and explicitly set by the user via some user interface. NTP has the ability to utilize encryption and integrity checks using pre-shared keys. The user interface to the clock can be protected using passwords. It is important to note that internal time of day clocks are often used in devices and may utilize a bus structure, such as I2C. In such cases, the bus used MUST NOT be accessible externally from the device.
  - HCD_Time_Source (UTF-8 string)
  - The HCD_Time_Source attribute is a variable length string that indicates where the device acquires its time setting. Examples of this attribute include: (“onboard” for a resident RTC or a URL for a known good (S)NTP server)

Recommendations

- The MFP sync does not require synchronization with high precision.
- Time accurate to the second rather than the millisecond or nanosecond is adequate and acceptable for accurate time stamped audit records.
- Synchronization at boot-up time and also at periodic intervals (e.g daily) should be adequate to minimize drift of an internal clock.
- The IDS group should recommend to synchronize the MFP with internal source. The accuracy of the internal source is the responsibility of the IT manager.
- It does not make sense that MFP will have a better time accuracy than the local server time !!!!
- In the attribute document we should have 2 options for clock: On board clock (Internal clock) or External Clock synchronization
- It is consider secure if the MFP has mechanism to protect the time settings