The Printer Working Group

PWG August 2020 Face-to-Face
IDS Session – HCD Security Guidelines

Alan Sukert, IDS Chair
Ira McDonald, IDS Editor

19 August 2020

HCD Security Guidelines Agenda

- HCDSEC Current Status
- HCDSEC Development Plan
- HCDSEC Network Security Approach
- HCDSEC Network Security Examples
- Questions/Comments?

HCDSEC Current Status

- IDS Charter updated for HCDSEC project August 2019
- HCDSEC review at PWG February 2020 F2F
  - https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120.docx
- HCDSEC status at PWG May 2020 F2F
  - Development plan and priorities
- HCDSEC status update at PWG August 2020 F2F
  - Development plan and priorities
  - Network Security examples

HCDSEC Development Plan

- HCDSEC Interim draft in January 2020
  - https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120.docx
- HCDSEC Interim draft in Q3 2020
  - Section 4 Network Security (minimum requirements)
- HCDSEC Interim draft in Q4 2020
  - Section 5 Local Security
  - Section 6 System Architecture
- HCDSEC Prototype draft in Q1/Q2 2021
  - Section 7 Conformance
  - Section 8 Internationalization Considerations
  - Section 9 Security Considerations
  - Section 10 References

HCDSEC Network Security Approach

- Define functional groups of protocol requirements (e.g., End-to-End Security for TLS, SSH, etc.)
- Define multiple scalable HCD requirements (i.e., essential security versus value-add security)
- Emphasize “secure by default” configuration (e.g., admin password setup and firewall default blocking)
- Firewall Types
  - Static (heuristic, w/out signatures or updates) – inspects and validates packet header addresses, ports, options
  - Dynamic (rule-based, w/ signatures and updates) – inspects and validates packet contents (session thru application layer)
- Antivirus and IDS Scanner Types
  - Static (heuristic, w/out signatures or updates)
  - Dynamic (rule-based, w/ signatures and updates)

HCDSEC Network Security Examples

- 4.1 Firewalls and Scanners
  - Conforming HCDs MUST implement and enable at least a Static Firewall on open network interfaces.
  - Conforming HCDs SHOULD implement and enable a Dynamic Firewall on open network interfaces.
  - Conforming HCDs MUST implement and enable at least a Static Antivirus Scanner on open network interfaces.
  - Conforming HCDs SHOULD implement and enable a Dynamic Antivirus Scanner on open network interfaces.
  - Conforming HCDs SHOULD implement and enable at least a Static Intrusion Detection Scanner on open network interfaces.

HCDSEC Network Security Examples

- 4.2 Datalink Security
  - Conforming HCDs SHOULD support MACsec for datalink encryption and integrity.
  - Conforming HCDs SHOULD support IEEE 802.1AR for datalink authentication.
- 4.3 End-to-End Security
  - Conforming HCDs MUST support TLS/1.2 for end-to-end transport security.
  - Conforming HCDs SHOULD support TLS/1.3 for end-to-end transport security.
  - Conforming HCDs SHOULD support SSH for end-to-end transport security.

HCDSEC Network Security Examples

- 4.4 Job Security
  - Conforming HCDs MUST implement and enable at least IPP Everywhere/1.1 on open network interfaces.
  - Conforming HCDs SHOULD implement and enable PWG Job Logging (Syslog over TLS) on open network interfaces.
- 4.5 Configuration Security
  - Conforming HCDs SHOULD support SNMPv3 over TLS in an isolated process for necessary remote HCD configuration.
  - Conforming HCDs SHOULD support Secure Shell (SSH) in an isolated process for necessary remote HCD configuration.
  - Conforming HCDs MAY support NetConf in an isolated process for necessary remote HCD configuration.

IDS: HCDSEC Questions / Comments

?