HCD iTC Network SG Minutes * 8 September 2020

Attendees

- Tom Benkart (Acumen Security)
- Gerardo Colunga (HP Inc)
- Anantha Kandiah (Teron Labs)
- Kwangwoo Lee (HP Inc, HCD iTC Chair)
- Ira McDonald (High North, HCD iTC Network SG Leader, IEEE-ISTO PWG)
- Anders Staaf (Combitech AB)
- William Wagner (TIC, IEEE-ISTO PWG)

Preface

This meeting was announced and chaired by Ira McDonald.

These minutes were prepared by Ira McDonald with help from the participants.

Minutes

- (0) Revised Agenda

```
(1) Administrivia
(2) HCD iTC Alignment Sources
(3) Experts for Secure Channel Protocols
(4) IPsec
(5) SSH
(6) TLS
(7) Consensus on Alignment Sources
(8) IPP
(9) HCD cPP Schedule for Network SG
(10) Next Meetings
```

- (1) Administrivia

```
- Roll call

- Agenda discussion
```

- (2) HCD iTC Alignment Sources

```
- ND cPP

- CCUF Crypto WG

- FDE cPP

- others?
```

- (3) Experts for Secure Channel Protocols

```
- Volunteers
  - HTTPS - Ira McDonald

  - IPsec - Gerardo Colunga
```

- SSH - Anantha Kandiah

- TLS - Anantha Kandiah

- (4) IPsec

  - While there is an Initiator and Responder, there is not a fixed Client of Server (Tom Benkart)

  - So no HCD separation of Client and Server SFRs for IPsec

- (5) SSH

  - ND cPPv2.2e does separate Client and Server SFRs for SSH

  - So HCD separation of Client and Server SFRs for SSH

  - CCUF Crypto WG has done work on SSH requirements
    - contacts are Ashit Vora, Michael Vogel, Terry Diaz

  ACTION: 09/08/20 - Kwangwoo Lee to contact CCUF Crypto WG about SSH requirements - OPEN

- (6) TLS

  - TLS/1.3 should be added to both Client and Server SFRs for HCD (Ira McDonald)
    - Not necessary to change selection, because currently permitted (Tom Benkart)

  - TLS/1.3 is being requested by many large enterprise clients of HCDs (Ira McDonald)
    - Agree we need TLS/1.3 in selection in HCD cPP (Gerardo Colonga, Kwangwoo Lee)

  - IETF TLS/1.3 deprecated SHA-1 hash, symmetric encryption modes (e.g., AES_CBC), and TLS versions (e.g., TLS/1.0 and TLS/1.3) should not be allowed in HCD cPP (Ira McDonald)
    - Choice should be up to customer and not PP (Tom Benkart)

    - HCD cPP is a security profile and should be authoritative (Ira McDonald)

  - IETF TLS/1.3 spec takes precedence over any Common Criteria Protection Profile text for protocol conformance (Ira McDonald)
    - [Rough consensus agreement with this stance]

  - HCD cPP should not invent new TLS SARs (Tom Benkart), but instead should defer to the experts in the Network Device TLS WG
    - [Rough consensus agreement with this stance]

  - Suggest adding informative notes to PP / SD for IETF TLS Best Practices (Ira McDonald)
    - Exact Compliance means evaluation labs *cannot* vary from stated SARs (Tom Benkart)

    - Agree we should add informational references to IETF TLS Best Practices (Kwangwoo Lee)

  - Network Device cPPv2.2e primary source of HCD cPP TLS requirements? (Ira McDonald)
    - [Rough consensus agreement with this stance]

    - Network Device TLS WG is addressing TLS/1.3 (Anantha Kandiah)

    - Network Device TLS WG is also addressing DTLS/1.3 (Anantha Kandiah)

- (7) Consensus on Alignment Sources

  - HCD cPP IPsec/SSH/TLS requirements should come (mainly) from ND cPPv2.2e (Ira McDonald)
    - [Rough consensus agreement with this stance]

- (8) IPP

```
- Should HCD cPPv1.0 address requirements for IPP? (Ira McDonald)
  - IPP goes to parking lot for a later version of HCD cPP (Kwangwoo Lee)
```

- (9) HCD cPP Schedule for Network SG

```
- Timeline for requirements from Network SG? (Kwangwoo Lee)
  - text sometime in November 2020 for Public Draft

  - exact deadline in November is TBD
```

ACTION: 09/08/20 - Kwangwoo Lee and Ira McDonald to determine exact timeline for secure channel requirements from Network SG
- OPEN

- (10) Next Meetings (All)

```
- Keep current bi-weekly timeslot for Network SG

- Network SG - Tuesday 22 September 2020 9-10am US Eastern
  - IPsec SFRs/SARs overview (Jerry Colunga)
  - TLS SFRs/SARs overview (Anantha Kandiah)
  - IPsec or TLS further discussion?

- Network SG - Tuesday 6 October 2020 9-10am US Eastern
  - SSH SFRs/SARs overview (Anantha Kandiah)
  - HTTPS SFRs/SARs overview (Ira McDonald)
  - IPsec or TLS further discussion?
```