Trusted Network Communications Architecture 2.0 Overview

20 July 2017
Why are we talking about this?

• The TCG’s Trusted Network Communications Workgroup is finalizing publication of the “Trusted Network Communications Architecture for Interoperability 2.0”
  • Should be published in a few weeks

• IETF’s Network Endpoint Assessment (NEA) is based on and compatible with Trusted Network Communications (TNC)

• NEA has been suggested as a core communications protocol for SACM, and SWIMA is an extension of NEA

• .::. Good to know how this related specification is evolving
Why was it revised?

• Goal of the revision is:
  • Bring TNC Architecture (first published in 2005; revised 2012) up to speed with current use
  • Clarify the role and utility of TNC for readers; make benefits clearer

• Hopefully this will help increase adoption of TNC (and, by extension, NEA)
What changed?

• Nothing normative!
  • The architecture is an informational document describing composition of the TNC technical specifications
  • All technical specifications continue to perform their current role and are unchanged

• Revised architecture changes how TNC is characterized
  • Reduce emphasis on “comply-to-connect” and emphasize ongoing measurement
  • Separate validation and enforcement roles
  • Add CMDB-related roles
  • Include more capability-based descriptions (rather than specification-based)
TNC Architecture 2.0 Diagram

http://www.trustedcomputinggroup.org/????????
TNC Architecture 2.0 Capability Diagram
Conclusion

• TNC Architecture 2.0 emphasizes the modular, composable nature of TNC
  • This aligns with the SACM requirements of Versatility (G-004), Architectural Flexibility (ARCH-002), and Topology Flexibility (ARCH-004)
  • These are qualities TNC has always had (in addition to fulfillment of other requirements), but now these qualities are explicitly identified

• In summary, there are no normative changes to TNC (and no interoperability impact to NEA), but hopefully the broad utility of TNC (and NEA) is better characterized in the new architecture specification