C13a. Cryptographic Transition Planning

Panel Discussion

Abstract

Representatives from industry standards bodies, certification labs, and implementers discuss how organizations can best prepare for inevitable transitions to new cryptographic algorithms in preparation for technological changes (e.g. quantum computing) or in response to catastrophic failure of an algorithm or protocol.

Participants

- Moderator
  - Ralph Spencer Poore, PCIP, CISSP, CISA, CFE, CHS-III, ISSA Distinguished Fellow
    - Director, Emerging Standards, PCI Security Standards Council
- Panelists
  - Dawn Adams, Cryptographic and Security Testing (CST) and Payment Assurance (PA) Lab Manager, EWA-Canada
  - Todd Arnold, Senior Technical Staff Member (STSM), IBM Master Inventor, IBM Cryptographic Coprocessor Development
  - Terence Spies, Chief Technologist, HP Security Voltage, Hewlett-Packard Enterprise
    - Subcommittee Chair, ANSI X9F1

Concepts

- Cryptography has long history of algorithms and implementations that have outlived their useful lives.
- The need for a change may result from computational improvements, cryptanalytic breakthroughs, discovered exploitable flaws, loss of vendor support, change in threat/risk profiles, or new mandates.
- In the Financial Services sector, for example, transition time has exceeded a decade beyond the end of life dates.
- Transitions are inevitable; planning is essential