Network Security Subcommittee - Summary

F2F 52 - March 2021

Summary of Subcommittee Discussion

- Near Term Objectives Published
- Cloud Services Team Output Discussed
- Ballot Report and Upcoming Ballots
- Illustrative Design Document Proposal Discussed

Near Term Objectives Discussed

- Tighten up existing language in NCSSRs
  - Try to close off loopholes like whether OS system files are “part of configuration”
- Tighten up OS Patching rules
  - There’s a continuum between “Critical Vulnerability” and “Everything Else”

Cloud Services Team

- Exploring risks and opportunities for CAs to operate **safely** within cloud service infrastructures
  - Goal is to use the operational principles of cloud providers to enhance security, not diminish
- Unlikely to include all CA services
  - Component analysis categorizes by risk and “coreness” to a CA
- Will produce a parallel standards document to NCSSRs
  - Focussed entirely on deployment and usage of Cloud Services
  - Initial outlines/drafts expected Q2 2021
  - Will be floated to wider working group for comments (on the understanding that these are early drafts!)
  - Inputs start from existing standards (NIST Framework, FEDRAMP etc.)
  - Adding in CA/B specific requirements (NCSSRs, analysis of incident reports)
  - Eventually producing a companion document for NCSSRs.
- CAs might need to make technological changes to be able to extend services to the cloud

Ballot Status

- Past
  - SC38 - abandoned owing to creeping complexity
  - SC39 - passed
- Current
  - SC40 - still tightening up wording to avoid exploitable ambiguity
- Future Proposals
  - Removal of “suspicious bit” database from BR 4.1.1
  - Requirement to store compromised key information in perpetuity
  - Reorganize BR 5.4 and 5.5 on audit/archive log with regard to what gets stored and for how long

Illustrative Design Document Proposal

- Trial Balloon floated for a companion to NCSSRs - illustrative design
  - Description of a design which embodies intent of NCSSRS
  - NOT normative - other designs are possible which are still totally compliant
  - Document would attempt to show what the NCSSRs are intended to mean
    - As a way of avoiding all possible interpretations of NCSSR ballot texts
- Probably owned by Document Structuring Group

Thanks!

Mailing lists:

Main:
netsec@cabforum.org

Non-archived:
netsec-management@cabforum.org