Network Security Subcommittee - Summary

F2F 51 - October 2020

NetSec Objectives

1. **Remove ambiguity from NCSSRs**
   CAs should not need to guess whether or not a technology deployment will meet requirements
2. **Ensure NCSSRs are technology neutral and enable newer deployment models.**
   However, new technologies have new dependencies and complexities - those need to be properly explored to ensure we do not lower the current security threshold.
3. **Try to encourage (eventually require) continuous automated monitoring and reporting**
   However, automation is no magic bullet - configurations must be checked (by humans) and in some cases, periodic human review of the monitored matter may still be required.

Considerations for the NetSec Team

- Ensure that the language of the NCSSRs pertains to System Architectures and Deployments
  - Not practice requirements for certificate issuance (belongs in the BRs)
- Clarify terms which “everybody knows what they mean” (when we don’t)
  - eg “System Accounts”
    - All accounts on a particular host (“system”) ?
    - Or those accounts which are for pseudo-users running services on the “system”?
- Get rid of avoidable loopholes
  - Minimize “system must do X, unless it can’t, in which case don’t bother” requirements

Practice Goals of the NetSec Team

- Reach out earlier
  - Where a ballot has got past primary drafting, reach out to the SCWG prior to a ballot being redlined and finalized, in order to solicit feedback and concerns
- Ensure that dependencies are explored in the discussion documents
  - Newer deployments should not weaken security properties that were in place
    - Unless those properties can be shown to be unnecessarily strict

Practice Goals of the NetSec Team (cont)

- Take a slightly more cynical view of the CA community
  - With each change, discuss
    - Does it open up any new behaviors that a bad actor might want to exploit?
    - Is it practical to close off such behaviors?
  - Recognize that utterly pathological misreadings of the BRs/NCSSRs cannot be prevented
    - Auditor role remains to determine whether a CA policy effects a substantive control or is syntactic adherence only
  - Acid test: Would DigiNotar have passed measurement against the new requirement?
    - If so, have we closed off as much bad behavior as we reasonably can?

Subgroups/Teams

Document Structuring Team

- **“Zones” Ballot** - rewriting with a goal of strengthening requirements for logical and physical security while preserving distinction for CA systems to be appropriately protected (if we’re removing the “zones” concept, something needs to replace it)
- **Offline CA Ballot** - we will soon start a broader public discussion of ballot’s objectives
- Improve BR section 5 (e.g. physical security, trusted roles, etc.)
- Continue efforts to improve NCSSR document structure

Threat Modelling Team

- Our current work mostly is focused on discussing risks
  - Shared accounts problem (they are sometimes necessary but should be prohibited)
  - Identified 6 main requirements for Zones
  - Discussed CA Equipment risks
- The newest idea is to preparing “risk analysis” section which could be included in Ballots
  - The main goal is to show each time which risks will be mitigated/avoided thanks to new proposals

Pain Points Team Update

Authentication control rules outdated. **(Ballot SC3-Passwords and Ballot SC3X-Account Lockout)**

Increased scalability and effectiveness of log integrity controls, and system configuration reviews by reducing reliance on human element.

Extension to System Account Management being discussed **(Ballot SC34)**

Reduced excessive log data retention requirements from 7 to 2 years **(Ballot SC 28)**

Clarified the applicability of various NCSSR provisions to offline equipment - **(Offline CAs Ballot)**

Timing requirements for remediation of critical vulnerabilities. → not addressed. Draft Ballot was not provided. Assumed to be obsolete.

Ballots were prepared for all pain points. They are addressed to the extent possible.
Pain point subgroup meetings will be put on hold to focus on other topics. It may be resumed when required.

New Subteam: Using Cloud Service Providers

We will be forming a new sub group to focus on the use of cloud service providers by certificates authorities. Questions we are examining:

- What do the BRs allow today?
- Are there services CAs operate that are improved by taking advantage of cloud service providers?
- Are there CA functions that are risky/riskier in a non-on-premise environment and options for mitigating the risky sufficiently?
- How do we divide responsibilities and ensure that the responsible party is meeting the necessary requirements?

It is well understood that this creates some audit challenges - the group will endeavor to explore them.

The team is eager for new participants who would like to contribute in discussing these issues.

Ballots

Ballot	Title	Status
SC28	Logging and Log Retention	Passed
SC32	Elimination of Zones	Abandoned - Redrafting
SCYY	Offline CA Provisions	Seeking broader discussion
SC34	Account Management	Redrafting

Thanks!

Mailing lists:

Main:
netsec@cabforum.org

Non-archived:
netsec-management@cabforum.org