SC29 Ballot: System Configuration Management

Motivation & Background

Two sections of the current NSRs contain requirements for configuration management. Section 1(h) demands a weekly review and Section 3(a) a process to monitor, detect and report on security-related configuration changes.

The following questions were raised during our sub-committee meetings on this topic.

1. Do these sections describe requirements for change management controls or for ongoing configuration management? and
2. Would configuration management controls be more effective if CAs implemented solutions to continuously monitor configurations instead of reviewing them manually?

Considerations

Scope: Configuration Management and Change Management

Both Sections are concerned with ongoing configuration management. The control activity of Section 1(h) is triggered by the passing of time (“on a weekly basis”). That of Section 3(a) is performed continuously, independent of whether a change has been deployed.

Reviewing changes after their deployment can make sense e.g. as an implementation of the four-eyes principle or to confirm that they were deployed in accordance with the approved change description. However it would be unusual for s1(h) to require that a change is reviewed after it was deployed and not before.

The question has been raised as to whether this ballot should also cover OS patching, since that involves installing new packages on top of others. The view of the proposers is an unequivocal “yes” - patched packages from OS vendors should go through a CA run risk assessment.

---

1 “It’s not clear to me, for example, why reviewing the changes to the configurations is too complex. Are CAs regularly and routinely changing configuration so often that it’s untenable to review?”
process, and only those patches which are approved for installation should make their way to production systems.

Requirements for change management are missing from the current NSRs. It would be beneficial to define them but that is not the scope of this ballot.

Effectiveness: better scaling = broader scope

Undesired configuration changes are a significant source of security risk for CAs. Large CAs operate many systems that fall into the six categories mentioned in s1(h). Depending on the CA’s system architecture the number of such systems can easily reach > 100. The number of configurations to be reviewed depends on the CA’s security policies. However, the Subcommittee discussion has identified a list of 9 configurations that should always be included in configuration reviews. The list is not exhaustive. It is what the subgroup identified to be the minimum scope. Additional configurations have to be considered by CAs depending on their respective system architecture and risk profile.

- user access and authentication datastores
- mechanisms for administrative access (e.g. SSH, RDP)
- channels for configuration management (e.g. Puppet)
- network settings
- host-local firewall
- host-local IDP/IDS settings
- package repositories and other sources of system-level updates
- operating system logging service or its equivalent

CAs that perform configuration reviews at this level of detail would have to cover 900 configuration data points for 100 in-scope systems. We consider it unrealistic to perform a thorough review of so many data points without incurring a risk of overlooking something.

Similarly the WebTrust/PKI Assurance Task Force report which found and recommended that:

“Section 1h requires a weekly review of system configurations (...). In our experience this almost always includes a component of automated monitoring along with human review.

Systems are too complex to perform a meaningful human review of configuration changes. Software monitoring tools play a large part in achieving this requirement, but there is a required human element to inspect the monitoring software as well as consider changes in physical security. Consider better detailing the goals of this criterion.”

In contrast, continuous monitoring is an automated control that can cover a practically unlimited number of data points.
Effectiveness: Shorter Response Times

There was consensus in our discussions that unauthorized or unintentional configuration changes can introduce high security risks but the current wording allows CAs to comply with s1(h) without noticing such a change for several days. Whether the weekly human reviews have to be performed every 7 days or just once per week is a matter of interpretation but for the discussion of our proposal this is immaterial. The change we are proposing seeks to encourage CAs to rely on continuous monitoring rather than human reviews because alerts created by a continuous monitoring solution can notify a CA by orders of magnitude earlier than a human review i.e. within minutes not within days.

Practical Application

Continuous monitoring [i.e. the requirement/alternative put forth here] of configuration files can be most easily achieved by using Configuration Management systems, which allow for a maximally consistent and coordinated configuration of any system. The Information Systems Audit and Controls Association (ISACA) and Committee of Sponsoring Organizations (COSO) have been a champion for continuous monitoring/auditing of controls since the introduction of Sarbanes Oxley. In a 2015 ISACA Journal article titled A Practical Approach to Continuous Control Monitoring change management was identified as one of the optimal areas for continuous monitoring due to the risk of unauthorized changes, the frequency of potential changes, and the ability to design monitoring controls. The 2013 update to COSO includes 17 principles, separated based on five components. The fifth component is focused on monitoring and identifying deficiencies and responding to them timely.

For CAs to use Configuration Management seems to be desirable in principle over handcrafted configurations, and once such a system is in use there is little reason to review any changes or configuration (in so far as covered by the CM system) outside of the CM system. Being spared the human review should further incentivise CAs to implement such systems. However, if a CA based on whatever determination would consider CM to not be acceptable in their security architecture, they should still be allowed to only implement the continuous monitoring part in order to be spared manual human review in order to not tempt a CA to implement a CM system against their own best judgement just to evade manual human reviews.

Human review in any case, is like all things human, error prone, and not necessarily deterministic. Continuous monitoring should be able to be performed in a much more uniform and systematic manner and can achieve a level of granularity, detail and coverage that cannot be generally accepted from human reviewers.

Risk vs Benefit Considerations

The current wording of s1(h) does not provide any details about how the human reviews shall be performed or why they are better than continuous monitoring.
Human reviews can identify issues not covered by an automatic monitoring solution but they become meaningless if the amount of data to be reviewed exceeds the limit of what a reviewer can realistically evaluate.

Processes and tooling for collecting and analyzing configuration data can help mitigate this weakness but in its current wording s1(h) does not require this.

Given that continuous monitoring offers scaling and response time advantages we think it is not a good rule that CAs can only meet their obligations by performing human reviews.

**Ballot**

The following motion has been proposed by Neil Dunbar of TrustCor and endorsed by Tobias Josefowitz of OPERA and Dustin Hollenback of Microsoft.

--- MOTION BEGINS ---

This ballot modifies the “Network and Certificate System Security Requirements” based on Version 1.3.

(Each CA or Delegated Third Party SHALL)

(...)

**Insert as new Section 1(h)**

Ensure that the CA’s security policies encompass a change management process, following the principles of documentation, approval and testing, and to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems follow said change management process;

**Remove from Section 3(a)**

Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems;

**Insert as new Section 3(a)**

Implement a System under the control of CA or Delegated Third Party that continuously monitors, detects, and alerts personnel to any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems unless the change has been authorized through a change management process. The CA or Delegated Third Party shall respond to the alert and initiate a plan of action within at most twenty-four (24) hours.
Effective date

The changes introduced by this Ballot take effect on 1 October 2020. Earlier adoption is permitted.

--- MOTION ENDS ---

*** WARNING ***: USE AT YOUR OWN RISK. THE REDLINE BELOW IS NOT THE OFFICIAL VERSION OF THE CHANGES (CABF Bylaws, Section 2.4(a)):

A comparison of the changes can be found at:
https://github.com/cabforum/documents/compare/16a5a9b...neildunbar:8ec37e8?diff=split

This ballot proposes a Final Maintenance Guideline.

The procedure for approval of this ballot is as follows:

Discussion (7+ days)

Start Time: 2020-03-09 17:00:00 UTC
End Time: 2020-03-16 17:00:00 UTC

Vote for approval (7 days)

Start Time: 2020-03-16 17:00:00 UTC
End Time: 2020-03-23 17:00:00 UTC