Report for Network Security Working Group

22nd June, 2018

Introduction

The Network Security Working Group was chartered to examine the current state of the Network and Certificate Systems Security Requirements (NCSSRs) document currently produced by the CA/B Forum, to form a view as to:

1. Whether the current documents still form a good basis for auditing CAs, in order to ensure that their computer and network security controls merit widespread public trust.
2. Whether newer, or alternative security standards might better fit the bill, essentially replacing the current NCSSRs. If such standards are suitable, stipulate why they are a better fit. If no standards are found to be better, then to state which standards were examined and why they are not better.
3. If the NCSSRs are found to be deficient, whether it would be better to simply remove the document as the basis for audit; or to attempt to improve the NCSSRs so that their guidelines represent a more up to date and practical rule set.

The work product of the Working Group is this document.

The background for the reexamination is that the structures which underpin the computing infrastructure for many CAs has changed considerably since the NCSSRs inception, notably:

1. Virtual instances are now a commonplace artifact of most infrastructures, but they carry their own security considerations (both positive and negative) which the traditional bare metal instances do not.
2. Cloud computing services are now integral parts of many CA's deployments. While such architectures are covered in the BRs via the Delegated Third Party provisions, there are no explicit security guidelines laying down what cloud architectures pose acceptable versus unacceptable risk.
3. Co-located data processing facilities are also commonplace, but few, if any, explicit rules exist regarding the appropriate setup and operations of hardware deployed into collocated facilities, especially when considering the most sensitive of CA assets (Root CA infrastructures).
4. General consensus on what represents good operational security has changed over the years. A typical example given is the periodic rotation of passwords. Once considered a fundamental piece of good security design, expert consensus now argues strongly against such rules.
5. General consensus on the threat landscape has also changed. Things like firmware based threats using USB devices as vectors is something which

has moved from theoretical risk to a significant real-world threat. Against such threats, many of the traditional anti-virus solutions may do little to defend.

6. Multi-factor authentication is now becoming both standardized and mainstream, whereas only a few years ago, it was somewhat esoteric, bespoke and difficult to consider as a security primitive.

We note, more generally, that the NCSSRs are a set of best practices combined with some illustrative controls mapped to the very specific purpose of maintaining a publicly trusted CA, thus any putative replacement must be viewed through that prism: how do we translate security principles into security policies which then underpin security standards and practices?

Evaluations

The group has covered the following standards/frameworks as alternatives to the NCSSRs:

Center for Information Security (CIS) Controls

Acting as a set of controls which drives compliance documentation for various schemes, the working group examined how the CIS Control s(V7) might map to CA specific areas which might then be auditable under the relevant WebTrust or ETSI schedules.

The group's consensus was that there was significant overlap in subject material between the NCSSRs and the CIS controls, but that the effort to turn them into a set of best CA practice documents would not be practical within the timeframes which we could reasonably expect to see for document production.

ISO 27K Frameworks

The other main contender for the replacement of the NCSSRs was the ISO 27000 series of documents. While certainly comprehensive, it is certain that the framework covers virtually all areas of concern which might affect a CA (or indeed, any other operator within a computer security space).

But driving those high level principles into a series of practical measures which CAs should deploy would have been a workload which would have taken a very long time; and might have turned into a "boiling the ocean" effort.

Conclusion

Over the past year, the working group has reached the following conclusions:

1. The existing NCSSRs are somewhat outdated, having not been significantly updated while the computing and threat landscape has changed.
2. However, returning to a world where no coherent standards are available for CA Network and System Security is highly undesirable, therefore having **some** relevant documentation to act as a minimal security standard is the preference of the working group.

3. While other, worthy, security standards exist, none of them fit the somewhat unusual security postures which CAs adopt in order to maintain public trust. As such, while we are content to include some of their recommendations going forward, wholesale replacement of the NCSSRs with another security standard does not recommend itself to the membership of the working group
4. The NCSSRs are, however, unique in that they are custom built to address the issues specifically and uniquely discovered in a CA environment. As such, it is our opinion that they can be improved, that they should be updated and that, with the approval of the CA/B Forum, further work on such updating should be carried out. It is our belief that a renewed NCSSR document would serve CAs, auditors and browsers in giving a state of the art set of rules for the deployment and operation of CAs computing infrastructures.

Some work which was already done in terms of NCSSR evolution was to conduct a risk assessment based approach to the controls surrounding Root CA hardware and software deployment. This was presented in Face to Face meetings to a generally positive reception. Presumably this approach could be extended in future deliberations.

Given the new governance structure of the CA/B Forum, we recommend that a new working group is chartered to carry on the work of the old one. Until such a charter is constructed and approved, the activities of the working group should continue as a subcommittee of the Server Certificate Working Group, after July 3, 2018.