Comments Received on SP 800-57, Part 1

From: stully@qantas.com.au
Date: 5/27/11

I was looking for some best practice security guidance on the rotation period for pre-shared keys for Guest users at an organisation i.e. say when a contractor comes to a building to work on-site that provides wireless access. This may be one-off access for less than a day, or longer (depending on the contract type really). Or it could be guest access for someone giving a presentation to management, that would typically take <2 hours.

Attendees at a conference that publishes guest access to conference material, would be another use case & where I imagine the typical rotation period would be say <5 days i.e. keys generated at the start of the week (Monday morning), & rotated at the end of the week (Friday afternoon).

I think this probably should fit in section 5.3.6 - with both some text, and a line in *Table 1: Recommended cryptoperiods for key types* - but there is nothing there at present

Am I looking in the wrong document (is there a NIST Guest access document?), or is there scope for some guidance to be added in SP 800-57, Part 1 to cover this? Or is it already there, but I have missed the reference?

If this is not covered, could you please add it.

Having said that, does NIST recognise contributors to it's documents anywhere? I could not see it in this document, but I have provided comments to various other bodies, and they do recognise contributors, such as SANS.

Thanks,

Shane.

Shane Tully
SABSA Chartered Architect (SCF) | M.Inst.ISP | M.iapp/ANZ | JP
Senior Enterprise Security Architect | Enterprise Architecture & Consolidation | Architecture Services
Qantas Centre, Building B, Level 8, 203 Coward St, Mascot, New South Wales 2020 Australia

From: Kim Wagner <kwagner@visa.com>
Date: 6/30/11

Section 1 on p.14: The second paragraph says: "This NIST recommendation applies to U.S. government agencies using cryptography for the protection of their sensitive unclassified information. This Recommendation may also be followed, on a voluntary basis, by other organizations that want to implement sound security principles in their computer systems." We would suggest adding: "Other industries may have other standards that apply to specifically to their field of business."

Section 3.2 on p.30: line 4-6 of subsection has two occurrences of "high probability". There probably should only be one.

Section 4.2.5.4 Key Wrapping: The footnote says that "Additional text will be added after a key wrapping publication is completed." We would like to propose that the key wrapping mechanism from X9F6 is considered for inclusion in the key wrapping documentation. A definition can be found in TR-31, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms, Annex A, using key derivation binding method. The key wrap is very simple, based on CBC mode of operation with CMAC for key derivation.

Section 5.3.6, point 1 (Private signature key): We take Private signature key to cover also a CA private key used to sign certificates. As such, for a root CA such as those of Visa or other CAs that have their public keys in Internet browsers, a maximum cryptoperiod of 1-3 years is not realistic. We would expect many 2048-bit keys that are now trusted root CA public keys in Internet browsers to stay there for more than 15 years. The same consideration goes for the Visa CA that issues certificates for chip cards (EMV) world-wide. The public key is loaded into point-of-sale terminals and resides there for many years. Changing it would have great cost and no obvious benefit. Given the length of the keys (1408 and 1984-bit RSA keys) we feel there is no significant risk in keeping those public keys in terminals for e.g. 10 years (and for the 1984-bit key maybe 20 years). Hence, we would welcome some wording taking particularly CAs into account, acknowledging that sometimes CA public and private keys can be used significantly longer than 3 years. Otherwise it looks like the reality of Internet root keys and EMV root keys is not acknowledged.

Section 5.3.6, point 3 (Symmetric authentication keys): The derived Symmetric authentication keys used in EMV are unique per card, and reside on customer chip cards. Typically such a payment card (credit or debit) is issued for 3-5 years, but even 8-year cards exist. The symmetric authentication key cannot be changed "in the field", and hence will be used for 3-8 years. We think that in the balance between cost and security this works well, and would like to see a practice like that reflected better in SP 800-57.

Section 5.3.6, point 4 (Private authentication key): Again the comment relate to EMV chip cards. Each EMV chip card will have an RSA key unique to that card, used for card authentication. As described above, that key will be used for 3-8 years on a typical card,

and again we ask that scenarios like this be reflected better in SP 800-57, since a recommendation of a cryptoperiod of 1-2 years would not work. The card issuers would have to issue every one of their cardholders a new card every year, which is cost prohibitive and seems unnecessary

Section 5.3.6, point 9 (Symmetric master key): In EMV symmetric master keys are used to derive the card specific authentication keys. From the use of the master keys, there are no plaintext-ciphertext pairs exposed (since the ciphertexts would be the derived keys). The extra cost associated with managing a new master key each year would be very large, and actually not feasible. The derived card keys stay in the field for 3-8 years, and the master key used to derive them is still needed throughout their entire lifetime, to validate the authentication from the card. We would like to see a recommendation here regarding cryptoperiod include comments that take scenarios like this into account and mention cryptoperiods significantly longer than 1 year, which is the only recommendation mentioned at this point.
‘

Section 5.6.1, p.61, second paragraph (beginning "Determining the security strength…"): This is a good explanation of the security of 2-key TDEA. However, for implementers of TDEA this important information might be missed, and we suggest that it be put in a note to Table 2, possibly as an extension to footnote 18. This point is important for many financial institutions that may employ 2-key TDEA in a session key mode. Reading SP 800-57 leads them to think they should migrate from 2 to 3-key TDEA prior to 2014 (as per Table 3), whereas in fact, if they realized that 2-key TDEA with their use of it, has an estimated strength of 112 bits, they would realize that it could be used until 2030. This information would allow them to prioritize the application of their limited resources on security issues that require more urgent attention.

Table 3, p.64: We would like to suggest that signatures with message recovery be treated separately from signatures with appendix, since collision resistance is not required in the case of message recovery (as e.g. in EMV).

From: Paul Turner, Paul.Turner@venafi.com
Date: July 12, 2011

- In section 5.3.1 Risk Factors Affecting Cryptoperiods, it should be noted that a risk factor is the turnover of administrators who have had access to the key. For example, most private keys (that correspond to certificates) are stored in software-based keystores today, which enable the private key to be exported and copied. Most organizations experience regular turnover of administrators (e.g. reassigned, terminated, etc.). The turnover of an administrator should trigger replacement of the private key and certificate, however, most organizations are logistically incapable of tracking turnover and proactively changing keys/certs. Consequently, the use of shorter cryptoperiods helps minimize the window that a reassigned or terminated administrator can use a compromised private key for malicious purposes.

- Section 5.5 on page 59. States, "Certain protective measures may be taken in order to minimize the likelihood or consequences of a key compromise. The following procedures are usually involved:" I realize you can't dedicate too much focus to PKI but it may make sense to note that the potential for compromise of a CA signing (private) key and the broad effect that would have warrants establishing a CA compromise response plan (to minimize consequences). On a related note, the earlier numbered items on 58 and 59 do not specifically note a CA signing key as an example, although digital signing keys are noted. It may make sense to note a CA signing key as an example there.

- On page 60 under, "The compromise recovery plan should contain:" it might be good to include one or more of the following:

o An inventory of all cryptographic keys (e.g. location of all certificates to respond to a CA key compromise)

o Education of all appropriate personnel on re-key procedures

o Identification of personnel to support re-key procedures (e.g. help desk)

o Policies that certificate revocation checking be enforced (to minimize the effect of a private key compromise)

o Monitoring and tracking of re-keying operations (so it is clear when all required re-key operations have been completed)

During our discussion in Gaithersburg, I had mentioned that "device" might be mentioned more often in the context of certificates and PKI (i.e. that there appeared to be more focus on user for certificates although device certificates are generally more prevalent on most organizations today). Upon looking at the document again tonight, I am not seeing the sections where I felt that applied. I will take another look when I am a bit more lucid. ;-)]

This is truly an excellent document. I hope these comments are helpful.

Regards,

Paul