MKA pending PN exhaustion

Mick Seaman

MKA (the MACsec Key Agreement protocol) supports key rollover from one SAK to its successor without interruption to MACsec connectivity. While the current rollover specification[1] is accurate, it is inconsistent as to when SAK information moves from the "Latest" to "Old" fields. This note summarizes an interoperability issue with regard to detecting pending PN exhaustion first raised by Brian Weis, and proposes resolution along the lines discussed in the Security TG.

1. Current specification

Clause 9.8 "SAK generation, distribution, and selection" says[2]:

The Key Server observes the Lowest Acceptable PN (LLPN) for the Latest Key in use, as transmitted by each CA member, and distributes a fresh SAK whenever a participant advertises an LKI that matches the KI of the key currently being distributed and an LLPN that equals or exceeds the constant PendingPNExhaustion. PendingPNExhaustion is 0xC000 0000.

Clause 9.10.2 "MKPDU application data" says[3]:

Each CA member encodes the following information in every MKPDU transmitted, for both the latest (most recent) AN in use or about to be used, and the old (prior) AN:

Figure 12-2, the CP state machine, specifies (in state RETIRE) that, following deletion of SAs using a prior SAK (not the one most recently distributed):

```
oki = lki; lki = 0; otx = ltx; orx = lrx; ltx = lrx = FALSE;
```

i.e. the "Latest Key" information sent in MKPDUs is transferred to the "Old Key" information. The state machine then remains in RETIRE until a newSAK is distributed or there is a change in connectivity (chgdConnect) that needs to be signaled to the user of the secure connectivity provided by the Controlled Port by blipping controlledPortEnabled (link down/link up). RETIRE is entered after transmission begins with a new SAK, with a short delay to allow the other CA participants to enable their transmitters as well.

2. The issue

For most of the time that an SA is in use (according to the CP state machine) its parameters will be those for the "Old Key" while the "Latest Key" parameters will be unused. This means that the clause 9.8 text quoted above is directing the reader to the LLPN field, where is should be referencing the OLPN field.

Unfortunately a possible alternative interpretation is that the clause 9.8 text is correct, and that the state machine should transfer the "Latest Key" parameters to the "Old Key" parameters as a first step in the RECEIVE state (and not make the transfer in RETIRE at all) having also taken care to initialize the "Old Key" parameters to unused in the CHANGE state.

A further sophisticated if unhelpful interpretation also exists. Since the actions for individual states are defined as being performed atomically with respect to cooperating machines (instantaneous operation being unnecessary as well as unrealistic), and implementations that delay the Latest" to "Old" transfer could claim to be strictly conformant.

Adoption of either alternative interpretation leads to the interoperability issue.

3. Proposed resolution

Given the desirability of interoperability and the usual resistance to significant implementation change (reimplementing an already modified CP machine probably counts), a clarification or change to the specification that achieves interoperability with existing implementations following any of the interpretations outlined above is desirable. This can be achieved by being permissive on receive: it is the most recently distributed SAK that is of interest, whether the parameters for that SAK are being received in the Latest Key field or the Old Key field.

This approach also avoids making any changes to the CP state machine. Changing state machines is an error-prone activity and it is by no means guaranteed that such changes would be the same as those made in

[1] References to the current specification are to IEEE Std 802.1X-2010 as amended by 802.1Xbx-2014.

[2] 802.1X-2010 9.8 third paragraph, first full paragraph on page 70. Unmodified by 802.1Xbx-2014 and P802.1Xck/D1.1.

[3] 802.1X-2010 9.10.1 first paragraph, on page 72. Unmodified by 802.1Xbx-2014 and P802.1Xck/D1.1.

any implementation relying on the current clause 9.8 text for justification.

The proposed changes follow, in the style appropriate to an amendment, for inclusion in P802.1Xck. <Cross-references> to be substituted/updated are shown in angle brackets.

A number of possibly subtle points have also been addressed in the changed text:

1) The test for pending PN exhaustion only applies if XPN is not being used. With XPN, exhaustion is not credible (at least not before current implementations are obsolete and the standard has been revised:-).

2) The most recent SAK is not necessarily being distributed at present. It is possible that the conditions for distributing a fresh key have not been met for recent MKPDUs, while conditions that proscribe distribution of the most recent key apply. There is also little or no point in continuing to distribute a key if it has already been received by all CA members (though that is not explicitly spelt out in the standard)—another reason for not specifying the most recent SAK as the one “currently being distributed”.

3) There are constraints on newSAK generation and distribution, and it should be clear that these are not over-ridden by the pending exhaustion condition—they are unlikely to persist, and if they do some break in connectivity is inevitable in any case.

4) The ‘In Service’ flags mentioned in 9.10.1 were never actually needed/used in the encoding.

4. Proposed changes

Change the first sentence of the third paragraph of 9.8 as follows:

If the Current Cipher Suite is not using extended packet numbering, t~~T~~he Key Server observes the Key Identifier and Lowest Acceptable PN ~~(LLPN) for the Latest Key~~ for the most recent SAK in use, as transmitted by each CA member (the LKI and LLPN if LRX is true, and the OKI and OLPN otherwise, <9.10.1>), and distributes a fresh SAK (subject to the constraints specified in <9.5> and this clause) if that Key Identifier ~~whenever a participant advertises an LKI that~~ matches the KI of the key ~~currently being~~ most recently distributed and ~~an LLPN~~ that Lowest Acceptable PN equals or exceeds the constant PendingPNExhaustion.

Change the first paragraph of 9.10.1 as follows:

Each CA member encodes the following information in every MKPDU transmitted, for ~~both~~ the latest ~~(most recent) AN in use or about to be used,~~ and the old ~~(prior)~~ AN:

Change the second paragraph of 9.10.1 as follows:

A fixed format encoding is ~~supported by an ‘In Service’ flag, indicating that the fields for the respective SA are being~~ used. For convenience, these fields can be identified by the names and acronyms ~~Latest In Service/Old In Service (LIS/OIS),~~ Latest AN, Old AN (LAN, OAN), Latest Key Identifier/Old Key Identifier (LKI/OKI), Lowest Acceptable PN for the Latest Key/Lowest Acceptable PN for the Old Key (LLPN/OLPN), Latest Receiving/Old Receiving (LRX/ORX), Latest Transmitting/Old Transmitting (LTX/OTX).