strongSwan - Bug #871

make_before_break reauthentication inconsistency...

03.03.2015 23:39 - Luka Logar

Status:	Closed	**Start date:**	03.03.2015
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Affected version:	dr|rc|master	**Resolution:**	Fixed

Description

Hi, I am testing the make_before_break functionality and have found inconsistency (at least I think so) in handling the »old/pre-auth« child sa-s between the initiator and responder.

As can be seen from the statuses below, the initiator keeps the old child sa and also creates the new one, whereas the responder drops the old one and creates the new one.

Initiator pre-reauth:

```
Status of IKE charon daemon (strongSwan 5.3.0dr1, Linux 4.0.0-rc1, i686):
  uptime: 21 hours, since Mar 02 13:18:14 2015
  malloc: sbrk 311296, mmap 0, used 234600, free 76696
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon pkcs11 nonce x509 revocation constraints pem openssl curl kernel-netlink
socket-default stroke updown
Listening IP addresses:
  10.208.0.208
  10.200.0.208
Connections:
      to_bob:  10.200.0.208...10.200.0.209  IKEv2
      to_bob:   local:  [10.200.0.208] uses public key authentication
      to_bob:   remote: [10.200.0.209] uses public key authentication
      to_bob:    crl:   status must be GOOD
      to_bob:   child:  10.0.0.0/24 === 10.209.0.0/24 TUNNEL
Routed Connections:
      to_bob{1}:  ROUTED, TUNNEL, reqid 1
      to_bob{1}:   10.0.0.0/24 === 10.209.0.0/24
Security Associations (1 up, 0 connecting):
      to_bob[6]: ESTABLISHED 2 hours ago, 10.200.0.208[10.200.0.208]...10.200.0.209[10.200.0.209]
      to_bob[6]: IKEv2 SPIs: d04108e79e96b890_i b932253bd6889fc1_r*, public key reauthentication i
n 11 minutes
      to_bob[6]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
      to_bob{715}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c8ed0f4a_i c3639c91_o
      to_bob{715}:  AES_CBC_128/HMAC_SHA2_256_128, 107307 bytes_i (1674 pkts, 1s ago), 102749 byte
s_o (1594 pkts, 1s ago), rekeying in 20 minutes
      to_bob{715}:   10.0.0.0/24 === 10.209.0.0/24
```

Initiator post-reauth:

```
Status of IKE charon daemon (strongSwan 5.3.0dr1, Linux 4.0.0-rc1, i686):
  uptime: 21 hours, since Mar 02 13:18:14 2015
  malloc: sbrk 311296, mmap 0, used 239504, free 71792
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon pkcs11 nonce x509 revocation constraints pem openssl curl kernel-netlink
socket-default stroke updown
Listening IP addresses:
  10.208.0.208
  10.200.0.208
Connections:
      to_bob:  10.200.0.208...10.200.0.209  IKEv2
```

```
      to_bob:   local:  [10.200.0.208] uses public key authentication
      to_bob:   remote: [10.200.0.209] uses public key authentication
      to_bob:    crl:   status must be GOOD
      to_bob:   child:  10.0.0.0/24 === 10.209.0.0/24 TUNNEL
Routed Connections:
      to_bob{1}:  ROUTED, TUNNEL, reqid 1
      to_bob{1}:   10.0.0.0/24 === 10.209.0.0/24
Security Associations (1 up, 0 connecting):
      to_bob[7]: ESTABLISHED 18 seconds ago, 10.200.0.208[10.200.0.208]...10.200.0.209[10.200.0.20
9]
      to_bob[7]: IKEv2 SPIs: 592974bac165dbdd_i b1ce0d010747fb6b_r*, public key reauthentication i
n 2 hours
      to_bob[7]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
      to_bob{715}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c8ed0f4a_i c3639c91_o
      to_bob{715}:  AES_CBC_128/HMAC_SHA2_256_128, 122656 bytes_i (1857 pkts, 1s ago), 113941 byte
s_o (1764 pkts, 1s ago), rekeying in 17 minutes
      to_bob{715}:   10.0.0.0/24 === 10.209.0.0/24
      to_bob{716}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c637cae0_i c39ac310_o
      to_bob{716}:  AES_CBC_128/HMAC_SHA2_256_128, 3684 bytes_i (26 pkts, 1s ago), 2037 bytes_o (2
6 pkts, 1s ago), rekeying in 44 minutes
      to_bob{716}:   10.0.0.0/24 === 10.209.0.0/24
```

Responder pre-reauth:

```
Status of IKE charon daemon (strongSwan 5.3.0dr1, Linux 4.0.0-rc1, i686):
  uptime: 2 hours, since Mar 03 08:17:53 2015
  malloc: sbrk 303104, mmap 0, used 225664, free 77440
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon pkcs11 nonce x509 revocation constraints pem openssl curl kernel-netlink
socket-default stroke updown
Listening IP addresses:
  10.209.0.209
  10.200.0.209
Connections:
    to_alice:  10.200.0.209...10.200.0.208  IKEv2
    to_alice:   local:  [10.200.0.209] uses public key authentication
    to_alice:   remote: [10.200.0.208] uses public key authentication
    to_alice:    crl:   status must be GOOD
    to_alice:   child:  10.209.0.0/24 === 10.0.0.0/24 TUNNEL
Routed Connections:
    to_alice{1}:  ROUTED, TUNNEL, reqid 1
    to_alice{1}:   10.209.0.0/24 === 10.0.0.0/24
Security Associations (1 up, 0 connecting):
    to_alice[1]: ESTABLISHED 2 hours ago, 10.200.0.209[10.200.0.209]...10.200.0.208[10.200.0.208]
    to_alice[1]: IKEv2 SPIs: d04108e79e96b890_i* b932253bd6889fc1_r, public key reauthentication i
n 17 seconds
    to_alice[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
    to_alice{5}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c3639c91_i c8ed0f4a_o
    to_alice{5}:  AES_CBC_128/HMAC_SHA2_256_128, 112150 bytes_i (1739 pkts, 1s ago), 116852 bytes_
o (1826 pkts, 1s ago), rekeying in 18 minutes
    to_alice{5}:   10.209.0.0/24 === 10.0.0.0/24
```

Responder post-reauth:

```
Status of IKE charon daemon (strongSwan 5.3.0dr1, Linux 4.0.0-rc1, i686):
  uptime: 2 hours, since Mar 03 08:17:53 2015
  malloc: sbrk 303104, mmap 0, used 233760, free 69344
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon pkcs11 nonce x509 revocation constraints pem openssl curl kernel-netlink
socket-default stroke updown
Listening IP addresses:
  10.209.0.209
  10.200.0.209
Connections:
    to_alice:  10.200.0.209...10.200.0.208  IKEv2
```

```
    to_alice:   local:  [10.200.0.209] uses public key authentication
    to_alice:   remote: [10.200.0.208] uses public key authentication
    to_alice:    crl:   status must be GOOD
    to_alice:   child:  10.209.0.0/24 === 10.0.0.0/24 TUNNEL
Routed Connections:
    to_alice{1}:  ROUTED, TUNNEL, reqid 1
    to_alice{1}:   10.209.0.0/24 === 10.0.0.0/24
Security Associations (1 up, 0 connecting):
    to_alice[2]: ESTABLISHED 7 seconds ago, 10.200.0.209[10.200.0.209]...10.200.0.208[10.200.0.208
]
    to_alice[2]: IKEv2 SPIs: 592974bac165dbdd_i* b1ce0d010747fb6b_r, public key reauthentication i
n 2 hours
    to_alice[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
    to_alice{6}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c39ac310_i c637cae0_o
    to_alice{6}:  AES_CBC_128/HMAC_SHA2_256_128, 1275 bytes_i (14 pkts, 0s ago), 3025 bytes_o (15
pkts, 0s ago), rekeying in 42 minutes
    to_alice{6}:   10.209.0.0/24 === 10.0.0.0/24
```

The connection keeps working till the next rekey, when the initiator starts (and keeps trying forever) to rekey the non-existent (on the responder side) child sa. There also seem to be some other issues as after a day or so of trying to rekey charon freezes. Unfortunatley I can not give you more details at this time, since I am still discovering what exactly is going on.

Best regards
Luka

Associated revisions

Revision 1a31fe55 - 04.03.2015 11:18 - Martin Willi

ikev2: Don't adopt any CHILD_SA during make-before-break reauthentication

While the comment is rather clear that we should not adopt live CHILD_SAs during reauthentication in IKEv2, the code does nonetheless. Add an additional version check to fix reauthentication if the reauth responder has a replace uniqueids policy.

Fixes #871.

History

#1 - 04.03.2015 11:26 - Martin Willi

- Tracker changed from Issue to Bug

- Category set to libcharon

- Status changed from New to Feedback

- Assignee set to Martin Willi

- Target version set to 5.3.0

- Resolution set to Fixed

Hi Luka,

> [...] the initiator keeps the old child sa and also creates the new one, whereas the responder drops the old one and creates the new one.

Thanks for testing and your bug report. I've tried to reproduce this issue using a configuration very similar to yours, and was successful when using a uniqueids=replace policy. For IKEv1 we must adopt all children to a re-authenticated IKE_SA, but for IKEv2 we certainly must not. As the comment in that code is actually correct it is possible that this is a merge/rebase conflict not properly resolved.

I've addressed this bug with the referenced commit, please let me know if it fixes this issue for you.

Regards
Martin

#2 - 04.03.2015 13:40 - Luka Logar

Hi Martin, the fix seems to be working.

Thanks
Luka

#3 - 04.03.2015 14:56 - Martin Willi

- Status changed from Feedback to Closed

Thanks for your feedback, closing the issue.