strongSwan - Bug #193

Race condition between acquire jobs and Mobike update while switching WLANs

16.05.2012 08:41 - Nitin Verma

Status:	Assigned	**Start date:**	16.05.2012
Priority:	High	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:			
Affected version:	4.6.2	**Resolution:**	

Description

Hi,

I installed and build strongSwan on my Android device and I have been trying to switch my device between 2 WLANs requiring tunnel setup on WLAN_2 but not on WLAN_1. Following diagram explains my setup. Generally the transition is smooth between the WLANs but occasionally, I encounter some mobike related issues while switching from WLAN_1 to WLAN_2.

Android device: strongSwan client. Configuring the virtual IP in ipsec.conf as 192.168.3.3
AP: WLAN_1: subnet 192.168.2.0/24: for which traffic needs to go in clear text
AP: WLAN_2: subnet 192.168.3.0/24: for which traffic needs to be encrypted
strongSwan server: IP 192.168.1.154
Traffic: ICMP packets to server 192.168.1.154

To make it possible I used the following ipsec.conf at device:

```
config setup
      plutostart=no
      charondebug="knl 3, cfg 2, ike 2, chd 2, mgr 2, dmn 2"

conn %default
      ikelifetime=60m
      keylife=20m
      keyexchange=ikev2
      installpolicy=no
      reauth=no

conn android
      left=%any
      leftid="abc"
      leftauth=eap
      leftsourceip=192.168.3.3
      eap_identity=deepika
      right=192.168.1.154
      rightid=192.168.1.154
      rightauth=pubkey
      reqid=1
      auto=route
```

I am manually adding security policies using:

```
ip xfrm policy add dir out src 192.168.3.3/32 dst 192.168.1.154/32 proto
any priority 1000 tmpl src 192.168.3.3 dst 192.168.1.154 proto esp mode
tunnel reqid 1 level required
ip xfrm policy add dir in src 192.168.1.154/32 dst 192.168.3.3/32 proto any
priority 1000 tmpl src 192.168.1.154 dst 192.168.3.3 proto esp mode tunnel
reqid 1 level required
```

```
ip xfrm policy add dir fwd src 192.168.1.154/32 dst 192.168.3.3/32 proto
any priority 1000 tmpl src 192.168.1.154 dst 192.168.3.3 proto esp mode
tunnel reqid 1 level required
```

Following are the logs of a successful transition from WLAN_1 to WLAN_2::

```
05-09 15:15:36.531: INFO/charon(16016): 03[KNL] 192.168.2.221 disappeared
from wlan0
05-09 15:15:36.539: INFO/charon(16016): 03[KNL] fe80::a20b:baff:fec3:cf31
disappeared from wlan0
05-09 15:15:36.632: INFO/charon(16016): 14[IKE] old path is not available
anymore, try to find another
05-09 15:15:36.632: INFO/charon(16016): 14[IKE] no route found to reach
192.168.1.154, MOBIKE update deferred
05-09 15:15:40.312: INFO/charon(16016): 03[KNL] 192.168.3.3 appeared on
wlan0
05-09 15:15:40.406: INFO/charon(16016): 09[IKE] old path is not available
anymore, try to find another
05-09 15:15:40.406: INFO/charon(16016): 09[IKE] *requesting address change
using MOBIKE*
05-09 15:15:40.406: INFO/charon(16016): 09[ENC] generating INFORMATIONAL
request 63 [ ]
05-09 15:15:40.414: INFO/charon(16016): 09[IKE] checking original path
192.168.3.3[4500] - 192.168.1.154[4500]
05-09 15:15:40.414: INFO/charon(16016): 09[NET] sending packet: from
192.168.3.3[4500] to 192.168.1.154[4500]
05-09 15:15:40.429: INFO/charon(16016): 13[NET] received packet: from
192.168.1.154[4500] to 192.168.3.3[4500]
05-09 15:15:40.429: INFO/charon(16016): 13[ENC] parsed INFORMATIONAL
response 63 [ ]
05-09 15:15:40.460: INFO/charon(16016): 02[KNL] *creating acquire job for
policy 192.168.3.3/32[1/8] === 192.168.1.154/32[1] with reqid {1}*
05-09 15:15:40.500: INFO/charon(16016): 03[KNL] fe80::a20b:baff:fec3:cf31
appeared on wlan0
05-09 15:15:40.601: INFO/charon(16016): 13[ENC] generating INFORMATIONAL
request 64 [ N(UPD_SA_ADDR) N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2)
N(NO_ADD_ADDR) ]
05-09 15:15:40.601: INFO/charon(16016): 13[NET] sending packet: from
192.168.3.3[4500] to 192.168.1.154[4500]
05-09 15:15:40.617: INFO/charon(16016): 08[IKE] sending address list update
using MOBIKE
05-09 15:15:40.750: INFO/charon(16016): 15[NET] received packet: from
192.168.1.154[4500] to 192.168.3.3[4500]
05-09 15:15:40.750: INFO/charon(16016): 15[ENC] parsed INFORMATIONAL
response 64 [ N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) ]
05-09 15:15:40.750: INFO/charon(16016): 15[IKE] establishing CHILD_SA
android{1}
05-09 15:15:40.765: INFO/charon(16016): 15[ENC] generating CREATE_CHILD_SA
request 65 [ SA No TSi TSr ]
05-09 15:15:40.765: INFO/charon(16016): 15[NET] sending packet: from
192.168.3.3[4500] to 192.168.1.154[4500]
05-09 15:15:41.046: INFO/charon(16016): 14[NET] received packet: from
192.168.1.154[4500] to 192.168.3.3[4500]
05-09 15:15:41.046: INFO/charon(16016): 14[ENC] parsed CREATE_CHILD_SA
response 65 [ SA No TSi TSr ]
05-09 15:15:41.085: INFO/charon(16016): 14[IKE] CHILD_SA android{1}
established with SPIs cd7bd6f2_i c2f459fa_o and TS 192.168.3.3/32 ===
192.168.1.154/32
05-09 15:15:41.085: INFO/charon(16016): 14[ENC] generating INFORMATIONAL
request 66 [ N(NO_ADD_ADDR) ]
05-09 15:15:41.085: INFO/charon(16016): 14[NET] sending packet: from
192.168.3.3[4500] to 192.168.1.154[4500]
05-09 15:15:41.195: INFO/charon(16016): 10[NET] received packet: from
192.168.1.154[4500] to 192.168.3.3[4500]
05-09 15:15:41.195: INFO/charon(16016): 10[ENC] parsed INFORMATIONAL
response 66 [ ]
```

Following are the logs of a unsuccessful transition from WLAN_1 to WLAN_2 (traffic halts in this case)::

```
05-09 15:16:55.843: INFO/charon(16016): 03[KNL] 192.168.2.221 disappeared
from wlan0
05-09 15:16:55.851: INFO/charon(16016): 03[KNL] fe80::a20b:baff:fec3:cf31
disappeared from wlan0
05-09 15:16:55.945: INFO/charon(16016): 10[IKE] old path is not available
anymore, try to find another
05-09 15:16:55.945: INFO/charon(16016): 10[IKE] no route found to reach
192.168.1.154, MOBIKE update deferred
05-09 15:16:56.187: INFO/charon(16016): 13[IKE] sending keep alive
05-09 15:16:56.187: INFO/charon(16016): 13[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:16:56.187: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:16:59.429: INFO/charon(16016): 03[KNL] fe80::a20b:baff:fec3:cf31
appeared on wlan0
05-09 15:16:59.531: INFO/charon(16016): 07[IKE] old path is not available
anymore, try to find another
05-09 15:16:59.531: INFO/charon(16016): 07[IKE] *no route found to reach
192.168.1.154, MOBIKE update deferred*
05-09 15:16:59.546: INFO/charon(16016): 03[KNL] 192.168.3.3 appeared on
wlan0
05-09 15:16:59.609: INFO/charon(16016): 02[KNL] *creating acquire job for
policy 192.168.3.3/32[1/8] === 192.168.1.154/32[1] with reqid {1}*
05-09 15:16:59.609: INFO/charon(16016): 08[IKE] establishing CHILD_SA
android{1}
05-09 15:16:59.625: INFO/charon(16016): 08[ENC] generating CREATE_CHILD_SA
request 70 [ SA No TSi TSr ]
05-09 15:16:59.632: INFO/charon(16016): 08[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:16:59.632: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:16:59.640: INFO/charon(16016): 16[IKE] old path is not available
anymore, try to find another
05-09 15:16:59.640: INFO/charon(16016): 16[IKE] requesting address change
using MOBIKE
05-09 15:17:00.023: INFO/charon(16016): 15[IKE] old path is not available
anymore, try to find another
05-09 15:17:00.023: INFO/charon(16016): 15[IKE] requesting address change
using MOBIKE
05-09 15:17:03.640: INFO/charon(16016): 09[IKE] retransmit 1 of request
with message ID 70
05-09 15:17:03.640: INFO/charon(16016): 09[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:17:03.640: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:17:10.843: INFO/charon(16016): 10[IKE] retransmit 2 of request
with message ID 70
05-09 15:17:10.843: INFO/charon(16016): 10[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:17:10.843: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:17:23.804: INFO/charon(16016): 12[IKE] retransmit 3 of request
with message ID 70
05-09 15:17:23.804: INFO/charon(16016): 12[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:17:23.804: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:17:44.210: INFO/charon(16016): 08[IKE] sending keep alive
05-09 15:17:44.210: INFO/charon(16016): 08[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:17:44.218: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:17:47.140: INFO/charon(16016): 14[IKE] retransmit 4 of request
with message ID 70
```

```
05-09 15:17:47.140: INFO/charon(16016): 14[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:17:47.140: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:18:07.234: INFO/charon(16016): 11[IKE] sending keep alive
05-09 15:18:07.234: INFO/charon(16016): 11[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:18:07.234: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:18:27.250: INFO/charon(16016): 15[IKE] sending keep alive
05-09 15:18:27.250: INFO/charon(16016): 15[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:18:27.257: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:18:29.125: INFO/charon(16016): 09[IKE] retransmit 5 of request
with message ID 70
05-09 15:18:29.125: INFO/charon(16016): 09[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:18:29.125: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:18:49.281: INFO/charon(16016): 13[IKE] sending keep alive
05-09 15:18:49.281: INFO/charon(16016): 13[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:18:49.281: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:19:01.656: INFO/charon(16016): 02[KNL] creating rekey job for ESP
CHILD_SA with SPI cf645ae7 and reqid {1}
05-09 15:19:09.289: INFO/charon(16016): 07[IKE] sending keep alive
05-09 15:19:09.289: INFO/charon(16016): 07[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:19:09.289: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:19:29.304: INFO/charon(16016): 08[IKE] sending keep alive
05-09 15:19:29.304: INFO/charon(16016): 08[NET] sending packet: from
192.168.2.221[4500] to 192.168.1.154[4500]
05-09 15:19:29.304: INFO/charon(16016): 05[NET] error writing to socket:
Invalid argument
05-09 15:19:30.757: INFO/charon(16016): 02[KNL] creating rekey job for ESP
CHILD_SA with SPI c2f459fa and reqid {1}
05-09 15:19:44.632: INFO/charon(16016): 02[KNL] creating delete job for ESP
CHILD_SA with SPI cae8bd23 and reqid {1}
05-09 15:19:44.718: INFO/charon(16016): 11[IKE] giving up after 5
retransmits
05-09 15:19:44.718: INFO/charon(16016): 11[KNL] received netlink error: No
such process (3)
05-09 15:19:44.718: INFO/charon(16016): 11[KNL] unable to delete SAD entry
with SPI cae8bd23
05-09 15:19:44.750: INFO/charon(16016): 03[KNL] 192.168.3.3 disappeared
from wlan0
```

From the logs it can be inferred that in successful case, mobike successfully updates the address before charon tries to acquire job for policy to set up new SAs.However, in unsuccessful case address update through mobike could not take place before charon tries to acquire job for policy. It seems like some race condition is occurring.

I guess lowering the value of timer tv_usec of function "fire_roam_event" might avoid this condition upto an extent. I am not sure what other impacts it will further leave.

Thanks and regards,
Nitin

History

#1 - 16.05.2012 12:18 - Tobias Brunner

- Description updated

- Status changed from New to Assigned

- Assignee changed from Nitin Verma to Tobias Brunner

Yes, this is an issue if the acquire event is handled before the address update (roam event). In that case the CREATE_CHILD_SA exchange is sent with the old endpoints and the roam event has no effect on that.

You could try to lower the time in *fire_roam_event* but that will probably not always work and could result in superfluous roam events (which is not *really* a problem, but still).

I guess the proper solution would be to somehow abort the current exchange (CREATE_CHILD_SA or whatever) in case of a roam event that results in the notion that the current path is not available anymore. Then do a MOBIKE update and if that worked continue with the previous exchange.

Files

log_charon.txt	70.7 KB	16.05.2012	Nitin Verma