strongSwan - Bug #1239

[Android5.0.2 -- Strongswan5.3.3] Can't create IKEv1 SA because NAT-D payloads are not recognized

17.12.2015 02:56 - yeping xing

Status:	Closed	**Start date:**	17.12.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.4.0		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

Hi everyone
I use a smartphone(Andriod 5.0.2) as a client to create a L2TPoverIPsec VPN with a server(using strongswan5.3.3)
The ipsec.conf is like this

```
config setup

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev1
    authby=secret
        aggressive=yes

conn net-net
        type=transport
    left=192.168.0.132
    leftsubnet=0.0.0.0/0
    #leftid=@sun
    leftid=@#313233
    leftfirewall=yes
        right=192.168.0.124
    rightsubnet=0.0.0.0/0
    #rightid=@moon
    #rightid=192.168.0.124
    rightid=@#313233
    auto=add
```

On the phone I created a L2tpOverIPsec VPN.The IPsec identity is "123"
When I use dialed the VPN I found the phone use Aggressive-Mode. Strongswan replied the second message
and the phone never sent the third message.

```
   phone<initiator> ---------------------- strongswan<responder>
    first message ---->
                            <-----         second message
    third messge X
```

I checked the phone's log :

```
E/racoon  (16015): ignore the packet, received unexpecting payload type 20.
```

Type 20 is NAT-D.
In the message.c the payloads order is like this:

```
 [ SA KE No ID NAT-D NAT-D HASH V V V]
```

But in RFC3947 , the order like this:

```
   Initiator                           Responder
   ------------                        ------------
   UDP(500,500) HDR, SA, KE,
       Ni, IDii, VID -->
                                       <-- UDP(500,X) HDR, SA, KE,
                                              Nr, IDir, [CERT, ],
                                              VID, NAT-D, NAT-D,
                                              SIG_R
```

When I modifed the order in message.c, and dailed again,the IKE_SA was established.
The new order: [SA KE No ID V V V NAT-D NAT-D HASH]
So please check the aggressive_r_order in message.c if this is a bug.

Thanks.

Associated revisions

Revision fab4c845 - 07.03.2016 14:13 - Tobias Brunner

ikev1: Send NAT-D payloads after vendor ID payloads in Aggressive Mode messages

Some implementations might otherwise not recognize the NAT-D payload
type. Also moves SIG and HASH payloads last in these messages.

Fixes #1239.

History

#1 - 17.12.2015 09:14 - Tobias Brunner

- File aggressive-nat-d-payload-order.patch added

- Subject changed from [Android5.0.2 -- Strongswan5.3.3]Can't create IKE_SA to [Android5.0.2 -- Strongswan5.3.3] Can't create IKE_SA

- Description updated

- Category set to interoperability

- Status changed from New to Feedback

- Target version set to 5.4.0

While RFC 2409 says

```
Except where otherwise noted, there are no requirements for ISAKMP
payloads in any message to be in any particular order.
```

I guess for some simple clients it could make sense to order the Vendor ID payloads before the NAT-D payloads. Otherwise, such crappy clients might not recognize the NAT-D payloads, which are technically only defined when the appropriate Vendor ID has been received, which, of course, is the case, but clients that parse payloads only sequentially are probably not aware of that.

Patch is attached.

#2 - 07.03.2016 14:16 - Tobias Brunner

- Subject changed from [Android5.0.2 -- Strongswan5.3.3] Can't create IKE_SA to [Android5.0.2 -- Strongswan5.3.3] Can't create IKEv1 SA because NAT-D payloads are not recognized

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

Files

aggressive-nat-d-payload-order.patch	947 Bytes	17.12.2015	Tobias Brunner