strongSwan - Issue #2184

configuration with multiple RSA keys

08.12.2016 18:58 - Petre Rodan

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.5.0	**Resolution:**	

Description

problem description:

once I introduce the last 6 lines in the responder's config (the ikev2-internal conn profile), all the users that try to connect into the native_xauth_rsa_ikev1 conn profile are unable to establish a tunnel. if those last 6 configuration lines get removed from ipsec.conf then the native_xauth_rsa_ikev1 conn works again properly.

the server seems to send out apigen_server.crt instead of wildcard.cg-dialup.net.crt in the 'native_xauth_rsa_ikev1' conn, and thus the xauth+rsa ikev1 clients never get passed the CONNECTING stage.

so my question is this:

is this configuration in some way invalid from strongswan's perspective - especially can strongswan support two different profiles (ikev2-wildcard and ikev2-internal) that use different RSA keys in the same time?

responder conf:

```
config setup
    uniqueids = no

conn l2tp_psk
    fragmentation=yes
    authby=psk
    type=transport
    left=194.54.80.110
    leftsubnet=%dynamic[udp/l2tp]
    right=%any
    rightsubnet=%dynamic[udp/%any]
    dpdaction=clear
    dpddelay=5s
    dpdtimeout=20s
    auto=add

conn native_xauth_rsa_ikev1
    keyexchange=ikev1
    fragmentation=yes
    left=%defaultroute
    leftsubnet=0.0.0.0/0
    leftcert=wildcard.cg-dialup.net.crt
    leftid=@*.cg-dialup.net
    leftupdown="/opt/bin/updown_c ipsec_native"
    leftauth=pubkey
    right=%any
    rightsourceip=10.235.0.0/16
    rightauth=pubkey
    rightauth2=xauth-eap
    rightdns=194.187.251.67,185.93.180.131
    dpdaction=clear
    dpddelay=30s
    dpdtimeout=10m
    auto=add
    ikelifetime=40m
```

```
    lifetime=40m
    margintime=2m

conn native_xauth_psk_ikev1
    keyexchange=ikev1
    authby=xauthpsk
    fragmentation=yes
    left=%defaultroute
    leftsubnet=0.0.0.0/0
    leftid=@*.cg-dialup.net
    leftauth=psk
    leftupdown="/opt/bin/updown_c ipsec_native"
    right=%any
    rightsourceip=10.238.0.0/16
    rightdns=194.187.251.67,185.93.180.131
    rightauth=psk
    rightauth2=xauth-eap
    dpdaction=clear
    dpddelay=5s
    dpdtimeout=20s
    auto=add

conn ikev2-base
    keyexchange=ikev2
    fragmentation=yes
    left=%defaultroute
    leftsubnet=0.0.0.0/0
    leftauth=pubkey
    leftsendcert=always
    leftupdown="/opt/bin/updown_c ipsec_native"
    right=%any
    rightdns=194.187.251.67,185.93.180.131
    rightauth=eap-radius
    rightsendcert=never
    eap_identity=%any
    esp=aes256-sha256,aes256-sha1,3des-sha1!
    dpdaction=clear
    dpddelay=10

conn ikev2-wildcard
    also=ikev2-base
    leftid=@*.cg-dialup.net
    leftcert=wildcard.cg-dialup.net.crt
    rightsourceip=10.239.0.0/16
    auto=add

conn ikev2-internal
    also=ikev2-base
    leftid=@nikolaev-s01-i04.cg-dialup.net
    leftcert=apigen_server.crt
    rightsourceip=10.240.0.0/16
    auto=add
```

strongswan 5.3.5 was used and a 4.6.4 kernel.

we are no longer using this configuration since this bug was discovered. we decided to drop support for the ikev1+rsa+xauth profile - but the bug and my question still stands since adding those last 6 lines do still seem to have a negative impact on the number of users that are able to use our ipsec services. and we are using strongswan 5.5.0 now on the servers.

History

#1 - 09.12.2016 11:15 - Tobias Brunner

- Description updated

- Category set to configuration

- Status changed from New to Feedback

> especially can strongswan support two different profiles (ikev2-wildcard and ikev2-internal) that use different RSA keys in the same time?

Yes, but since the config is selected based on the IPs and identities when the first IKE_AUTH message is received the clients have to e.g. send a particular responder identity (IDr, *leftid* in the server config), or initiator identity (IDi, *rightid* in the server config), or connect to (or from) different IPs to allow the server to select the "right" config.

#2 - 09.12.2016 13:22 - Petre Rodan

I confirm that conn profile selection was done via "remote id" in ios initiators and rightid in linux clients.

I can 100% vouch for the setup presented above to fail for clients that were trying to use native_xauth_rsa_ikev1 (all using the ios initiator) if the ikev2-internal conn profile was present. so I think there is clearly either a misconfiguration in the ipsec.conf above or a bug in the server code.

we dropped the native_xauth_rsa_ikev1 profile entirely due to this.

we did an A/B test with 300 servers that have the ikev2-internal profile and 300 that don't have it. we seem to end up with 10% less users on the servers that have that profile enabled. problem is that we cannot reproduce any kind of connection problem with the set of servers that have that critical profile present. this result will be re-checked during next week.

production servers have a no-logs policy which makes debugging even more difficult.

do you have any clues of what hidden consequences can the extra 6 lines have in the config?

#3 - 09.12.2016 15:09 - Tobias Brunner

> I can 100% vouch for the setup presented above to fail for clients that were trying to use native_xauth_rsa_ikev1 (all using the ios initiator) if the ikev2-internal conn profile was present.

Failed how? Please be more specific and provide logs.

> do you have any clues of what hidden consequences can the extra 6 lines have in the config?

An additional certificate is loaded (the config itself shouldn't be relevant as it is for a different IKE version).

#4 - 13.12.2016 13:55 - Petre Rodan

Tobias Brunner wrote:

> > I can 100% vouch for the setup presented above to fail for clients that were trying to use native_xauth_rsa_ikev1 (all using the ios initiator) if the ikev2-internal conn profile was present.
>
> Failed how? Please be more specific and provide logs.

we have all strongswan logging disabled on all the servers, so we can detect errors only based on statistical data (number of users successfully connected in a given time frame). after I enabled those 6 extra lines, zero (from about 200) unique users were able to connect via the ikev1+rsa+xauth profile . the only log snippet I was able to generate is this one:

```
charon: 16[NET] received packet: from 41.78.195.35[57584] to 194.54.80.110[4500] (1280 bytes)
charon: 16[ENC] parsed ID_PROT request 0 [ FRAG(1) ]
charon: 16[ENC] received fragment #1, waiting for complete IKE message
charon: 10[NET] received packet: from 41.78.195.35[57584] to 194.54.80.110[4500] (532 bytes)
charon: 10[ENC] parsed ID_PROT request 0 [ FRAG(2/2) ]
charon: 10[ENC] received fragment #2, reassembling fragmented IKE message
charon: 10[NET] received packet: from 41.78.195.35[57584] to 194.54.80.110[4500] (1740 bytes)
charon: 10[ENC] parsed ID_PROT request 0 [ ID CERT SIG CERTREQ N (INITIAL_CONTACT) ]
charon: 10[IKE] ignoring certificate request without data
charon: 10[IKE] received end entity cert "C=RO, L=Bucharest, O=C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CENSO
RED, E=webmaster@cyberghostvpn.com"
charon: 10[CFG] looking for XAuthInitRSA peer configs matching 194.54.80.110...41.78.195.35[C=RO, L=Bucharest,
 O=CyberGhost S.R.L, CN=CENSORED, E=webmaster@cyberghostvpn.com]
charon: 10[CFG] selected peer config "native_xauth_rsa_ikev1"
charon: 10[CFG]   using certificate "C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CENSORED, E=webmaster@cyberghos
tvpn.com"
charon: 10[CFG]   using trusted ca certificate "C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CyberGhost Root CA,
E=webmaster@cyberghostvpn.com"
charon: 10[CFG] checking certificate status of "C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CENSORED, E=webmaste
```

```
r@cyberghostvpn.com"
charon: 10[CFG] certificate status is not available
charon: 10[CFG]   reached self-signed root ca with a path length of 0
charon: 10[IKE] authentication of 'C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CENSORED, E=webmaster@cyberghostv
pn.com' with RSA_EMSA_PKCS1_NULL successful
charon: 10[IKE] authentication of '*.cg-dialup.net' (myself) successful
charon: 10[IKE] sending end entity cert "C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CyberGhost VPN Server Nikol
aev-S01-I04, E=webmaster@cyberghostvpn.com"
charon: 10[ENC] generating ID_PROT response 0 [ ID CERT SIG ]
charon: 10[ENC] splitting IKE message with length of 1644 bytes into 4 fragments
charon: 10[ENC] generating ID_PROT response 0 [ FRAG(1) ]
charon: 10[ENC] generating ID_PROT response 0 [ FRAG(2) ]
charon: 10[ENC] generating ID_PROT response 0 [ FRAG(3) ]
charon: 10[ENC] generating ID_PROT response 0 [ FRAG(4/4) ]
charon: 10[NET] sending packet: from 194.54.80.110[4500] to 41.78.195.35[57584] (544 bytes)
charon: 10[NET] sending packet: from 194.54.80.110[4500] to 41.78.195.35[57584] (544 bytes)
charon: 10[NET] sending packet: from 194.54.80.110[4500] to 41.78.195.35[57584] (544 bytes)
charon: 10[NET] sending packet: from 194.54.80.110[4500] to 41.78.195.35[57584] (156 bytes)
charon: 10[ENC] generating TRANSACTION request 3726557570 [ HASH CPRQ(X_USER X_PWD) ]
[connection progress never goes beyond this point. the tunnel is not established]
```

"sending end entity cert" above is sending the wrong certificate toward the user.
instead of sending out the 'wildcard.cg-dialup.net.crt' certificate as per ipsec.conf it is sending 'apigen_server.crt'.

```
nikolaev-s01-i04 ~ # openssl x509 -in /etc/ipsec.d/certs/wildcard.cg-dialup.net.crt -text | grep -E "(Subject:
)|(Issuer:)"
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation S
ecure Server CA
        Subject: OU=Domain Control Validated, OU=COMODO SSL Wildcard, CN=*.cg-dialup.net

nikolaev-s01-i04 ~ # openssl x509 -in /etc/ipsec.d/certs/apigen_server.crt -text | grep -E "(Subject:)|(Issuer
:)"
        Issuer: C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CyberGhost Root CA/emailAddress=webmaster@cyberghost
vpn.com
        Subject: C=RO, L=Bucharest, O=CyberGhost S.R.L, CN=CyberGhost VPN Server Nikolaev-S01-I04/emailAddress
=webmaster@cyberghostvpn.com
```

it is true that the client certs are signed by our in-house CA, but inside the conf strongswan was expected to send the COMODO signed cert (wildcard.cg-dialup.net.crt) for that ikev1 profile, not the in-house server cert (apigen_server.crt).

> do you have any clues of what hidden consequences can the extra 6 lines have in the config?

> An additional certificate is loaded (the config itself shouldn't be relevant as it is for a different IKE version).

please see above. unfortunately we can no longer replicate the issue above since both the client and server have been reconfigured to no longer use the ikev1+rsa+xauth profile, but maybe you can still locate where the bug is, since it might break similar setups.

#5 - 13.12.2016 18:21 - Tobias Brunner

My guess is that since both certificates, presumably, match the identity you configured (*leftid=@*.cg-dialup.net*) the wrong certificate gets selected. That is, both have a *subjectAltName* extension that matches that identity so a lookup based on it could be ambiguous. This is probably related to #1077 (whose fix was actually reverted by 904f93f65562fef).

#6 - 14.12.2016 05:49 - Petre Rodan

the SANs look like this:

for apigen_server.crt:

```
            X509v3 Subject Alternative Name:
                IP Address:194.54.80.110, DNS:nikolaev-s01-i04.cg-dialup.net
```

for wildcard.cg-dialup.net.crt:

```
            X509v3 Subject Alternative Name:
                DNS:*.cg-dialup.net, DNS:cg-dialup.net
```

why would be a certificate with an explicit DNS SAN like nikolaev-s01-i04.cg-dialup.net picked in a profile where leftid=@*.cg-dialup.net is expected?

and I specified the exact certificate filename as leftcert= in ipsec.conf in all conn profiles in order to disambiguate any such errors, is this information

overridden by leftid=?

#7 - 14.12.2016 11:46 - Tobias Brunner

> why would be a certificate with an explicit DNS SAN like nikolaev-s01-i04.cg-dialup.net picked in a profile where leftid=@*.cg-dialup.net is expected?

The wildcard identity *.cg-dialup.net matches both SANs (that's the whole point of such a wildcard i.e. that any subdomain of cg-dialup.net is matched). It is usually not used in *leftid* but rather in *rightid* to match clients with a matching identity. Technically, the wildcard SAN is not interpreted as such but literally as * subdomain of cg-dialup.net, but that's also matched by the wildcard identity.

> and I specified the exact certificate filename as leftcert= in ipsec.conf in all conn profiles in order to disambiguate any such errors, is this information overridden by leftid=?

For IKEv1 it currently is. The fact that the config explicitly references a certificate is basically ignored as far as I can tell.

#8 - 14.12.2016 13:09 - Petre Rodan

Tobias Brunner wrote:

> > why would be a certificate with an explicit DNS SAN like nikolaev-s01-i04.cg-dialup.net picked in a profile where leftid=@*.cg-dialup.net is expected?
>
> The wildcard identity *.cg-dialup.net matches both SANs (that's the whole point of such a wildcard i.e. that any subdomain of cg-dialup.net is matched).

I see. I was hoping leftid would match only the exact strings provided and not 'expand' the wildcard.

> It is usually not used in *leftid* but rather in *rightid* to match clients with a matching identity.

we have this strange setup because of two reasons:
- iOS clients had to connect to our vpn service without importing any new CA cert into the OS (wildcard cert)
- strongswan initiators were unable to connect to our own strongswan servers if the certificate used on the server contains a wildcard domain in the CN/SAN. this is why the last 6 lines and the in-house signed certificate were added.

> Technically, the wildcard SAN is not interpreted as such but literally as * subdomain of cg-dialup.net, but that's also matched by the wildcard identity.

fortunately for the current ikev2 profiles the cert seems to be selected properly, maybe due to the fact that leftcert takes precedence.

> > and I specified the exact certificate filename as leftcert= in ipsec.conf in all conn profiles in order to disambiguate any such errors, is this information overridden by leftid=?
>
> For IKEv1 it currently is. The fact that the config explicitly references a certificate is basically ignored as far as I can tell.

please tell me it's not ignored for ikev2. pretty please with a cherry on top? :)