Hi,

Does Strongswan VPN Client on Android version 2.2.1 support the ESPv3 protocol please?

Thanks in advance for your answer,
Kind Regards,
Jean-Luc J

History

#1 - 27.03.2020 09:19 - Tobias Brunner
- Status changed from New to Feedback

Does Strongswan VPN Client on Android version 2.2.1 support the ESPv3 protocol please?

Partially, as not all features are supported (e.g. ESN, or TFC as sender). Why do you ask? Which feature of v3 in particular are you interested in?

#2 - 30.03.2020 09:00 - Jean-Luc Jordan

Hi Tobias,

Thanks for your answer.
I am asking that because I have a requirement for my project about the supported protocol by the used VPN product :
the compliancy with ESPv3 protocol defined in [RFC 4303].
So that's why I need to know what is supported by strongswan product.

From RFC 4303,
"In the new ESP (v3), we make two provisions to better support traffic
flow confidentiality (TFC):
- arbitrary padding after the end of an IP packet
- a discard convention using Next Header = 59"

These 2 features are not supported or just 1 of them.
I assume that answer is valid for Android and Linux (it is a common SW code).

Kind Regards,
Jean-Luc J

#3 - 30.03.2020 10:55 - Tobias Brunner

I assume that answer is valid for Android and Linux (it is a common SW code).

Not at all. On Android (in our app, not when strongSwan is running natively on Android) a custom userland IPsec implementation is used
(souce:src/libipsec), not the one in the Linux kernel.

The Linux kernel fully implements TFC (without generating dummy traffic itself, I think) and is configurable via ttc/ttc_padding option in strongSwan.
However, libipsec only supports it as recipient (i.e. it can process packets with arbitrary padding and it will discard packets with IPPROTO_NONE as
next header), but it can not pad to an arbitrary length/MTU or generate dummy traffic.
Hi Tobias,

Thanks for your answer.

Finally, in my case, the behavior between Linux and Android is the same because strongswan linux configuration includes the option "--enable-kernel-libipsec" that embeds strongswan own IPsec implementation libipsec (source:src/libipsec) as strongswan on Android.

To have a correct picture of the supported ESP VERSION3 on the src/libipsec file, is it possible to answer by YES or NO or PARTIAL on the different ESPV3 features supported by the file src/libipsec please?

Extract of RFC6071
- In IPsec-v2, an SA (Security Association) is uniquely identified by a combination of the SPI (Security Parameters Index), protocol (ESP or AH) and the destination address. In IPsec-v3, a unicast SA is uniquely identified by the SPI and, optionally, by the protocol; a multicast SA is identified by a combination of the SPI and the destination address and, optionally, the source address. [YES/NO/PARTIAL]

- More flexible SPD (Security Policy Database) selectors, including ranges of values and ICMP message types as selectors. [YES/NO/PARTIAL]

- Decorrelated (order-independent) SAD (Security Association Database) replaced the former ordered SAD [YES/NO/PARTIAL]

- Extended sequence numbers (ESNs) were added [YES/NO/PARTIAL]

- Mandatory algorithms defined in standalone document [YES/NO/PARTIAL]

- AH [RFC4302] is mandatory to implement (MUST) in IPsec-v2, optional (MAY) in IPsec-v3 [YES/NO/PARTIAL]

Changes to ESP [RFC4303] include:
- Combined mode algorithms were added, necessitating changes to packet format and processing [YES/NO/PARTIAL]

- NULL authentication, mandatory (MUST) in ESP-v2, is optional (MAY) in ESP-v3 [YES/NO/PARTIAL]

An additional question:
is it necessary to configure in a strongswan file the ESP version number or no need?

Thanks a lot for your support,
Have a nice day,
Kind Regards,
Jean-Luc J

#5 - 06.04.2020 10:01 - Tobias Brunner

because strongswan linux configuration includes the option "--enable-kernel-libipsec"

Please read the warnings etc. on kernel-libipsec.

- In IPsec-v2, an SA (Security Association) is uniquely identified by a combination of the SPI (Security Parameters Index), protocol (ESP or AH) and the destination address. In IPsec-v3, a unicast SA is uniquely identified by the SPI and, optionally, by the protocol; a multicast SA is identified by a combination of the SPI and the destination address and, optionally, the source address. [YES/NO/PARTIAL]

Yes.

- More flexible SPD (Security Policy Database) selectors, including ranges of values and ICMP message types as selectors. [YES/NO/PARTIAL]

Partial, no support for ICMP type/code selectors.

- Decorrelated (order-independent) SAD (Security Association Database) replaced the former ordered SAD [YES/NO/PARTIAL]
No (assuming that's an error in RFC 6071 and they really mean decorrelated SPD, not SAD, because RFC 4301 does not mention any decorrelated SAD).

- Extended sequence numbers (ESNs) were added [YES/NO/PARTIAL]
  No.

- Mandatory algorithms defined in standalone document [YES/NO/PARTIAL]
  Yes, but depends on the loaded plugins.

  - AH [RFC4302] is mandatory to implement (MUST) in IPsec-v2, optional (MAY) in IPsec-v3 [YES/NO/PARTIAL]
  No.

- Combined mode algorithms were added, necessitating changes to packet format and processing [YES/NO/PARTIAL]
  Yes, but again, depends on the loaded plugins.

  - NULL authentication, mandatory (MUST) in ESP-v2, is optional (MAY) in ESP-v3 [YES/NO/PARTIAL]
  No (strongSwan does not support NULL authentication for ESP in general).

  is it necessary to configure in a strongswan file the ESP version number or no need ?

No, there is no such option (ESP is not versioned).

#6 - 07.04.2020 08:21 - Jean-Luc Jordan

Hi Tobias,

Thanks for your answer.
I am little bit confused by that answer
"
- NULL authentication, mandatory (MUST) in ESP-v2, is optional (MAY) in ESP-v3 [YES/NO/PARTIAL]
No (strongSwan does not support NULL authentication for ESP in general)."

For ESP, it is written that Linux 2.6+ kernel supports it.
That means that Linux kernel supports "Null" encryption for ESP but not strongswan in its libipsec source and in its plug-in.
Is it correct ?

Thanks a lot for your support,
Have a nice day,
Kind regards,
Jean-Luc J

#7 - 07.04.2020 09:37 - Tobias Brunner

That means that Linux kernel supports "Null" encryption for ESP but not strongswan in its libipsec source and in its plug-in.
Is it correct ?

No, it's not. NULL encryption is not the same as NULL authentication/integrity, the former is supported by strongSwan and libipsec (if the openssl plugin is loaded), the latter is not.

#8 - 07.04.2020 09:42 - Jean-Luc Jordan

Thanks for your answer
And sorry for my misunderstanding.

You can close that issue.
It is ok for me.

Have a nice day,
Kind regards,
Jean-Luc J

#9 - 07.04.2020 09:44 - Tobias Brunner
- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to No change required