

strongSwan - Feature #406

TNC: Speeding up the Attestation process

09.09.2013 18:24 - Pedro Larbig

Status:	Feedback	Start date:	09.09.2013
Priority:	Low	Due date:	
Assignee:	Andreas Steffen	Estimated time:	0.00 hour
Category:			
Target version:			
Resolution:			
Description			
Hello again,			
when playing around with the TNC Attestation plugins I encountered several IKE_SA timeouts since checking the IMA hashes and rebuilding the PCR took quite a lot of time.			
Of course raising the timeout value fixes this error, but still the authentication process is taking a lot of time and sure can be improved.			
The first thing that comes to my mind is the database backend that may be slow?			

History

#1 - 10.09.2013 10:20 - Tobias Brunner

- Assignee set to Andreas Steffen

#2 - 10.09.2013 13:47 - Andreas Steffen

Yeah, you are right. The current SQLite DB interface is quite slow, especially when inserting new reference values. We are trying to improve the insertion speed by using transactions.

For the time being just increase the **charon.half_open_timeout** parameter in strongswan.conf from the 30 seconds default value to about 60-90 seconds. Also if you are doing extensive IMA file measurements, limit the number of Simple Component Evidence Attributes per PA-TNC message via the parameters

```
charon {
  plugins {
    tnccs-20 {
      max_batch_size = 32754
      max_message_size = 32722
    }
  }
}
```

which in my setup does not cause IKE message retransmissions by impatient VPN clients.

BTW - with strongswan-5.1.1 the tnccs-20, tnc-imc, and tnc-impv plugins are going to move to libtnccs, so you have to put any parameters in the libtnccs section:

```
libtnccs {
  plugins {
    ..
  }
}
```

This makes the TNC libraries independent of the charon daemon so that they can be used e.g. with our new lean pt-tls-client.

#3 - 10.09.2013 14:00 - Andreas Steffen

- Status changed from New to Feedback