Hi,

I have a running site-to-site tunnel with IKEv2.

BOX[~]# ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.4, Linux 5.4.23, armv7l):
  uptime: 109 seconds, since Apr 22 10:22:42 2020
  malloc: sbrk 200704, mmap 0, used 185344, free 15360
  worker threads: 27 of 32 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aes des sha2 sha3 shal md5 random nonce x509 revocation constraints pubke y pkcs1 pkcs7 pkcs12 pgp dnskey pem openssl fips-prf gmp curve25519 xcbc hmac attr kernel-ne tlink resolve socket-default stroke updown xauth-generic unity
Listening IP addresses:
  192.168.3.3
  fc00:192::3
Connections:
  ipsec$0:  192.168.3.3...192.168.3.28  IKEv2
  ipsec$0:  local:  [C=DE, ST=Bayern, L=Muenchen, O=Garderos, OU=TEST, CN=server, E=server@garderos.com] uses public key authentication
  ipsec$0:  cert:  "C=DE, ST=Bayern, L=Muenchen, O=Garderos, OU=TEST, CN=server, E=server@garderos.com"
  ipsec$0:  remote: uses public key authentication
  ipsec$0:  child:  192.168.4.3/32 === 192.168.4.28/32 TUNNEL
Routed Connections:
  ipsec$0(2):  ROUTED, TUNNEL, reqid 2
  ipsec$0(2):  192.168.4.3/32 === 192.168.4.28/32
Security Associations (1 up, 0 connecting):
  ipsec$0[3]:  ESTABLISHED 30 seconds ago, 192.168.3.3[C=DE, ST=Bayern, L=Muenchen, O=Garderos, OU=TEST, CN=server, E=server@garderos.com]...192.168.3.28[C=DE, ST=Bayern, L=Muenchen, O=Garderos, OU=TEST, CN=client, E=client@garderos.com]
  ipsec$0[3]:  IKEv2 SPIs: 5a804ad67c12d1c4_i* bf7aa17ef8be69f8_r, rekeying in 60 minutes
  ipsec$0[3]:  IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
  ipsec$0(4):  INSTALLED, TUNNEL, reqid 2, ESP SPIs: c61a4fa5_i c4e5ada_o
  ipsec$0(4):  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 50 minutes
  ipsec$0(4):  192.168.4.3/32 === 192.168.4.28/32

How should I switch to using SHA3 for IKE, for example? If I change the configuration from "ike=aes256-sha256-ecp256!" to "ike=aes256-sha3_256-ecp256!", I get this in the logs:

```
Apr 22 10:41:34 BOX info charon [ 4318]: CFG 05 : algorithm 'sha3' not recognized
Apr 22 10:41:34 BOX info charon [ 4318]: CFG 05 : skipped invalid proposal string: aes256-sha3_256-ecp256
```

Thanks for the help!
How should I switch to using SHA3 for IKE, for example?

You can't. The use of SHA-3 has not yet been standardized for use with IKE or ESP (not sure if that ever will happen as AEADs are clearly preferred nowadays), it can only be used for signatures.

Hi Tobias,

thanks for the quick reply!

OpenSSL in the new LTS version 1.1.1 states this as a major feature. If SHA2 gets broken in the future, do you think that SHA3 will get standardized?

OpenSSL in the new LTS version 1.1.1 states this as a major feature.

So?

If SHA2 gets broken in the future, do you think that SHA3 will get standardized?

Just use an AEAD algorithm. As I said, for signatures (in certificates and IKEv2) it can already be used.

hehe, ok :)

Just use an AEAD algorithm.

Yes, I've tested that already and it works fine!

Thank you very much, Tobias!