Thoughts Encryption for 50G-EPON

CableLabs

Steve Goeringer | s.goeringer@cablelabs.com

Dr. Massimiliano Pala | m.pala@cablelabs.com

Summary

- We appreciate
  - The need to support backwards compatibility
  - The need for fast resolution
  - The need to leverage existing silicon
- The encryption proposal can move forward
- We have concerns
  - No planned crypto agility
  - Support of next-generation key exchange such as recommend for PQC will be important in 2-5 years
  - No integrity scheme provided for the encrypted payloads
  - The IV coordination scheme looks valid, but also seems very complicated

Questions we were asked to address

- Is there a security basis for choosing zero-overhead or MACSec based encryption?
- Is the approach to IV construction that Glen has developed look good?
- Should we move to 256 bit encryption keys?
- Can an MKA PDU support a custom 16-bit value?
- Can we use the MKA key exchange protocol for multicast LLIDs?
- Can we leverage EAP/EAPOL?

Is there a security basis for choosing zero-overhead or MACSec based encryption?

- Counter/IV size
  - It's our understanding that the MPCP size supported by the legacy zero-overhead approach drove key agreement/negotiation every 68 secs at 10Gpbs rates
  - Key agreement does introduce the potential for failure (though this doesn't seem to have been a problem yet)
  - High frequency key generation provides lots of samples against which cryptanalysts can look for systemic bias
  - It would be better if perfect forward secrecy was supported on longer duration keys – the 200 hour lifetime may be sufficient
  - It's good to have a key rotation period configurable by the operator with a default of something less than a week
- Future support of crypto-agility and PQC
  - There is great uncertainty on the future of cryptography right now
  - Using highly adopted standards such as MACSec may provide a path to future support for crypto-agility that is easier than doing something that is architecture or implementation specific

Does the approach to IV construction proposed by Broadcom look good?

- Yes, the IV construction looks fine
- It may be overly complicated
  - We haven’t done the design work to see if it can be simplified

Should we move to 256 bit encryption keys?

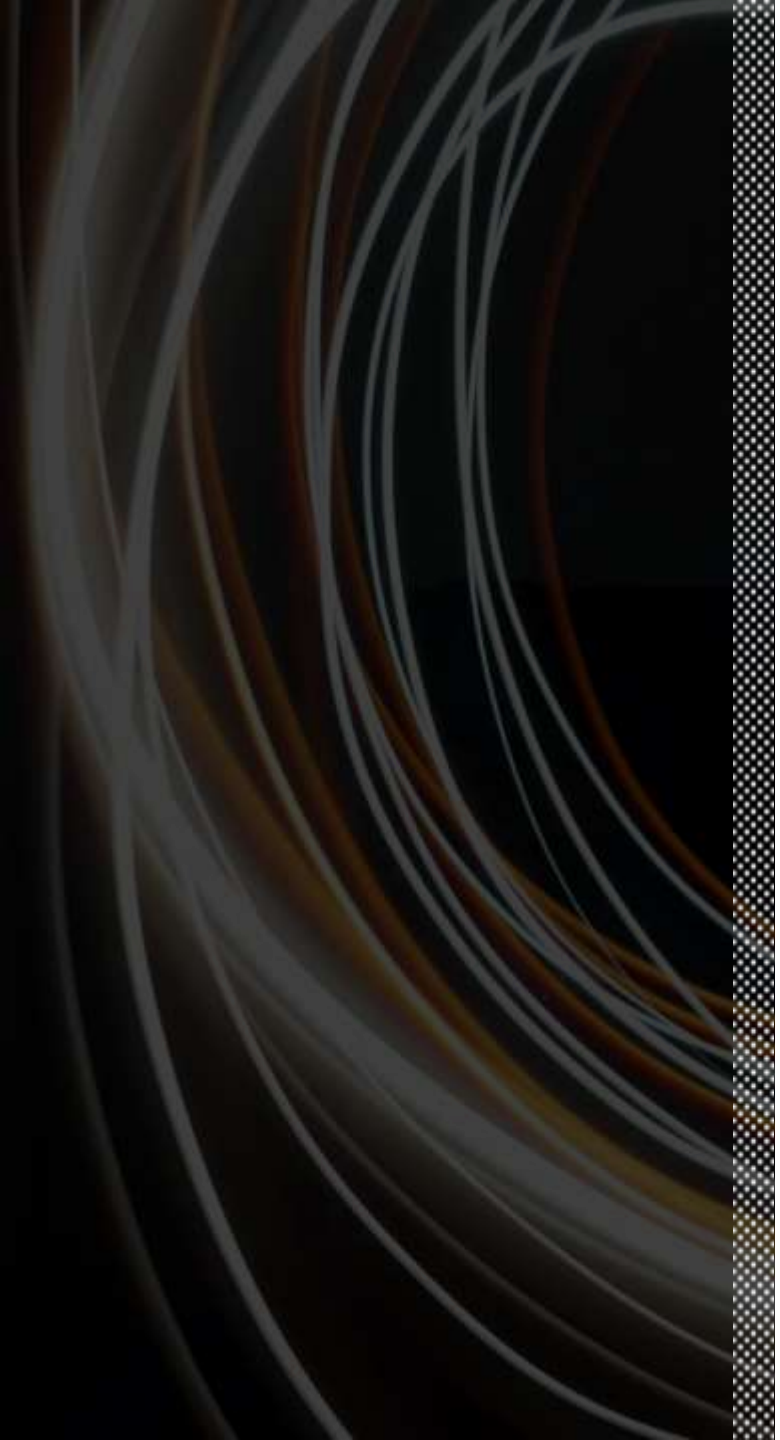
- Yes – but it is a design decision
  - Use IANA/IETF recommended cipher suites of at least 256 security bits
  - It may be prudent to prohibit 128 bit security even though this is still indicated as acceptable by NIST
- Nearly all standards authorities still allow 128 bit encryption keys
  - Integrity inclusion often recommended
  - Key agreement or other factors can lower effective security bits
- Resources
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
  - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile
  - https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-03/EPC342-08%20v11.0%20Guidelines%20on%20Cryptographic%20Algorithms%20Usage%20and%20Key%20Management.pdf
  - https://www.rfc-editor.org/rfc/rfc7696
  - https://www.keylength.com/en/

Questions needing further research

- Can an MKA PDU support a custom 16-bit value?
  - Probably not, but still researching
- Can we use the MKA key exchange protocol for multicast LLIDs?
  - Not sure -- there would be mapping between LLIDs and their associated keys to other values in MKA
    - Perhaps the LLID might map to group Secure Association Keys (SAKs)
  - Key hierarchy for MKA is defined in 6.2 Key Hierarchy
  - There is a notion for group CAs in spec, but these are referring to multi-access LAN
- Can we leverage EAP/EAPOL?
  - Maybe, but the details matter for interoperability
    - EAP-TLS, EAP-FAST, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-AKA, LEAP, PEAP
  - Leverage X.509 certificates?
  - Note that MKPDUs are conveyed by EAPOL PDUs as distinguished by their EAPOL packet type

IEEE 802.1x-2020

- Section 6.2 Key hierarchy
  - Figure 6-3 MKA key hierarchy
- Section 11
  - Figure 11-7 MKPDU parameter set encoding
  - Figure 11-6 EAPOL-MKA packet body with MKPDU format
  - Table 11-7 PKPDU parameter sets



CableLabs®

CableLabs

cablelabs.com