Practical Challenges with AES-GCM

and the need for a new mode and wide-block cipher

Panos Kampanakis, Matt Campagna, Eric Crocket, Adam Petcher

Amazon Web Services (AWS)

Agenda

AES-GCM challenges

- IVs
- PRP limits
- Key / Context Commitment

- Solution Properties
  - New wide-block cipher
  - New Mode

Agenda

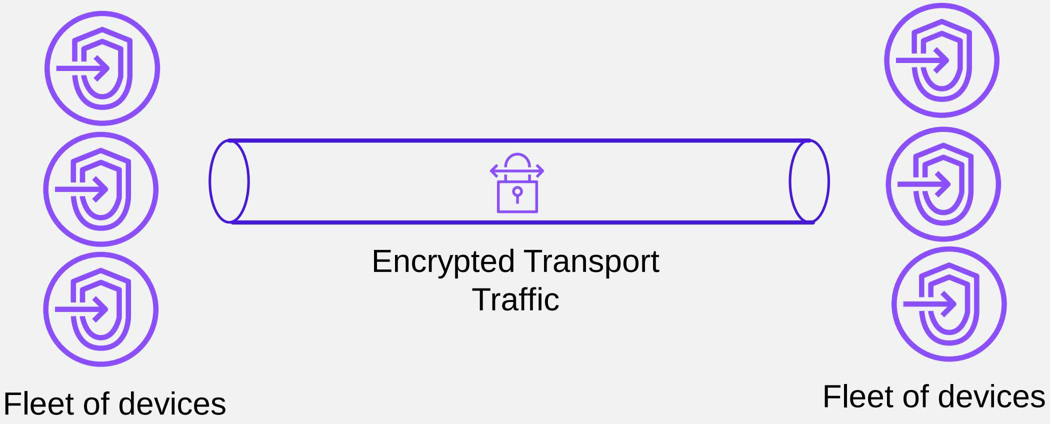
AES-GCM challenges

- IVs
- PRP limits
- Key / Context Commitment

- Solution Properties
  - New wide-block cipher
  - New Mode

Random IVs and the 2^{32} invocation limit

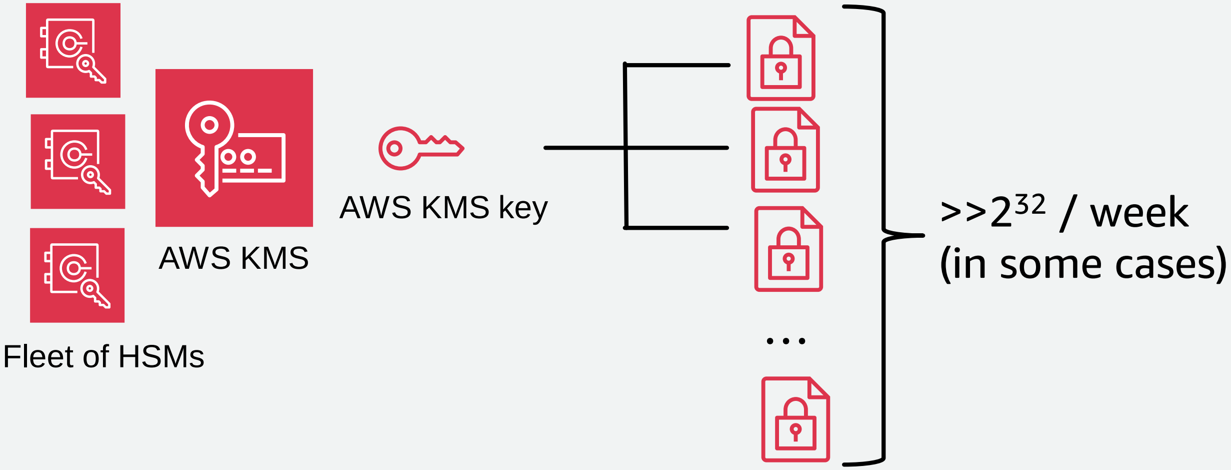
High-volume Transport Encryption for virtualized networks



Distributed transport encryption can collectively encrypt ~2^{32} messages in 2 seconds.

Re-keying every 2 seconds is not practical.

High-volume AWS KMS Encryption

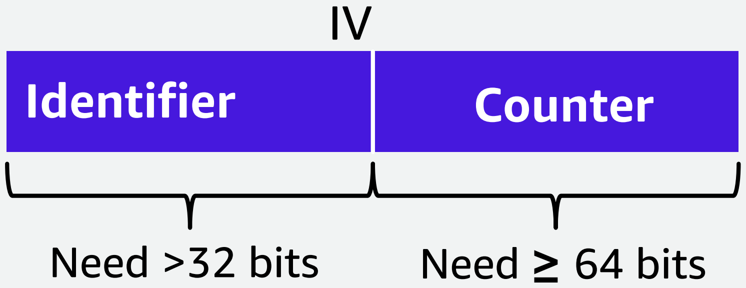


AWS Key Management Service (AWS KMS) key sometimes can encrypt 2^{32} plaintexts / week.

Rekeying weekly and managing AWS keys for thousands of accounts annually adds overhead.

Deterministic 96-bit IVs

Transport Encryption deterministic IV challenges



IV

Identifier | Counter

Need >32 bits

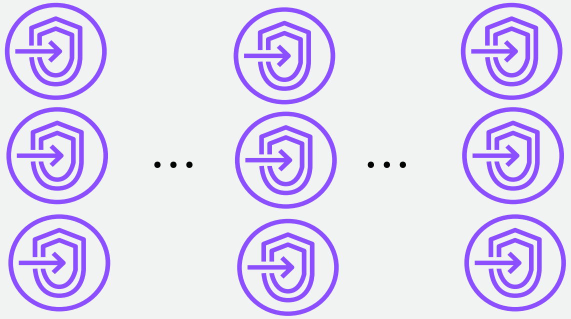
Need ≥ 64 bits

Support for large # of identifiers limits the counter size which means less messages per key.

Unique identifiers in distributed systems add complexity.

We prefer random IVs.

Transport Encryption FIPS challenges

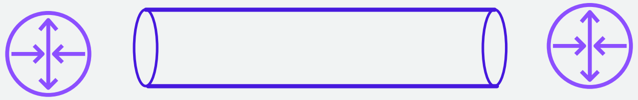


IV uniqueness proof, reuse checks, zeroization in distributed, zero-downtime systems has challenges.

Efficient counter management adds complexity.

We prefer random IVs.

Fabric Encryption performance challenges



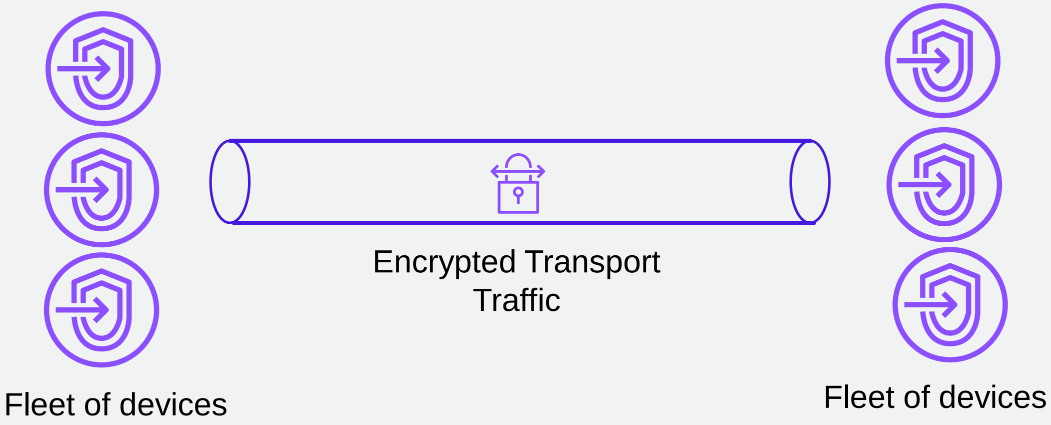
OTN / FlexO

- ~80KB frames = 5,000 AES blocks.
- 100x Gbps speeds
- AES-GCM can be slow for 5,000 AES blocks at 400Gbps speeds.

Block # limits (2^{64} (SP800-38D) or $2^{34.5}$ (RFC8446))

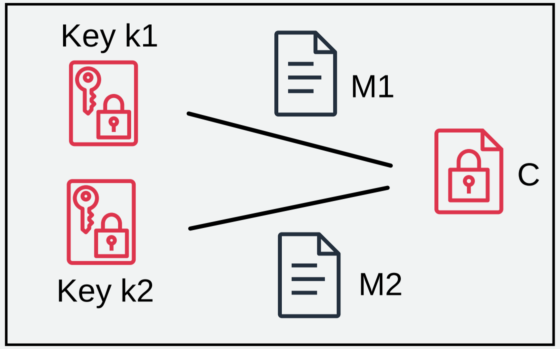
TRANSPORT ENCRYPTION

Distributed encryption systems could collectively encrypt ~2^{64} blocks in 2 weeks.



Key / Context Commitment

HTTPS://IA.CR/2020/1456



- Without key commitment, C could be decrypted to M1 or M2 depending on the data decryption key used.

AWS Encryption SDK

- This issue affected AWS client-side envelope encryption
- It was addressed in 2020 with explicit KeyIds.

Agenda

AES-GCM challenges

- IVs
- PRP limits
- Key / Context Commitment

- Solution Properties
  - New wide-block cipher
  - New Mode

Solution Properties

NEW WIDE-BLOCK CIPHER AND MODE

- Performance
- 256-bit block width (to avoid the 2^{64} block # limit)
- Ability to encrypt (at least) 2^{64} or (ideally) 2^{92} messages with random IVs
- Minimum 2^{-64} {key, IV} collision probability for 2^{64} messages or 2^{-32} for 2^{112} messages.
- A key / context commitment option for robustness
- An IV misuse-resistance option

Solution – 1. New Cipher

Properties

- Can reuse, or build new efficient hardware from existing architectures

Candidates

- Rijndael-256
- Based on other PRPs

Solution – 2. New Mode

Candidates

- OCB mode
- AEGIS-128L
- New stream cipher and authenticator. More in the literature…

Off topic:

Quantum-safe asymmetric encryption to replace RSA-OAEP in SP 800-56B.

Hint: PQ HPKE , hpke-xyber768d00 ☺

Thank you!

Panos
Kampanakis

kpanos@amazon.com