Adding AES-ICM and AES-GCM to OpenCrypto

J. Gurney¹

¹Consultant, @encthenet

12 June 2015 / BSDCan 2015
Why is AES-GCM and AES-ICM Necessary?

- Performance
- Security (AES-NI)
- More complete IPsec cipher mode support
- AES-GCM is an AEAD mode
Why not AES-CBC?

Cipher Block Chaining (CBC) mode encryption

Initialization Vector (IV)

Key

Plaintext

block cipher encryption

Ciphertext

Key

Plaintext

block cipher encryption

Ciphertext

Key

Plaintext

block cipher encryption

Ciphertext
What is AES-GCM?
Multiplication in GF($2^{128}$)

- Addition does not carry:
  \[
  \begin{array}{c|cc}
  + & 0 & 1 \\
  \hline 
  0 & 0 & 1 \\
  1 & 1 & 0 \\
  \end{array}
  \]
  aka XOR or $\oplus$

- $11_b \cdot 11_b = 110_b + 11_b = 101_b$

- Multiplication is otherwise the same, add the reducing factor when value is $\geq 2^{128}$

- Distribution works: $(a + b) \cdot c \equiv a \cdot c + b \cdot c$
Dangers of Side Channel Attacks

- In 2010, Bonan Huang wrote his masters thesis [1] on attacking AES-GCM’s secret authentication value $H$
- Not just GHASH, AES is vulnerable too [2]
- Fixing side channels can bring performance improvements, but usually not
Compromise

- Even intra-cache line accesses have timing variations [3]
- 4-bit lookup is a compromise between performance and side-channel resistance

J. Gurney Adding AES-ICM and AES-GCM
Optimizing Opportunities

- Pipelining: \((((((a \cdot H) + b) \cdot H) + c) \cdot H) + d) \cdot H \equiv a \cdot H^4 + b \cdot H^3 + c \cdot H^2 + d \cdot H$
- Precompute the powers of $H$
- Performance increase even for software, not just AES-NI

J. Gurney
Adding AES-ICM and AES-GCM
AES-NI Avoids Cache Timing Attacks

- AES Instructions
- PCLMULQDQ (Carry-less multiply) instruction – 64x64->128
- Needs work to make a 128x128->128 needed for GHASH
Reviews Are Necessary

- Require nonce to be specified for AES-ICM and AES-GCM
- Found bug in reference code for comparing GCM tags
Testing and Verification Are Too

- tests/sys/opencrypto/runtests
- requires python and nist-kat ports
Thanks

Mike Hamburg
Watson Ladd
For Further Reading

- B. Huang, “Cache-collision timing attacks against AES-GCM.” University of Delaware, 2010. [Link](http://udspace.udel.edu/handle/19716/9765).
