AES Mode Choices

OCB vs. Counter Mode with CBC-MAC

Niels Ferguson, MacFergus BV
Russ Housley, RSA Labs
Doug Whiting, HiFn

Introduction

- 802.11i currently specifies AES-OCB for confidentiality and integrity

- Have concerns with this choice
- Highlight issues by comparing to AES Counter (CTR) mode with AES-CBC-MAC

AES CTR with CBC-MAC

- CBC-MAC
  - Over: Length || SA || DA || … || Payload
  - Truncate to 64 bits and append to payload
  - CBC-MAC key derived from encryption key, only single-key required (may be pre-computed or computed on-the-fly)
- Encrypt using AES CTR, using IV to ensure unique counter values

Dimensions of Comparison

- Patent Status
- Size of Implementation
- Power Consumption
- Speed
- Cleartext Integrity Coverage
- Simplicity of Key Management
- Packet Overhead
- Crypto Confidence

Patent Status

- IEEE 802 has long history with patents
  - Bottom line: Avoid patents when there are viable unencumbered alternatives
- No patents on CTR or CBC-MAC
- Three independent IP claimants on OCB
  - All three emphatically believe that their yet-to-be-issued patent(s) cover OCB mode
    - Virgil Gligor, Charanjit Jutla (IBM), and Phil Rogaway
- Fair, non-discriminatory, and non-onerous are subjective (especially after standard is done)

Size of Implementation

- Unlike OCB, AES CTR and CBC-MAC require only encryption operations, *not* decryption
- Software: CTR with CBC-MAC is smaller
  - Cut table size in half (4K bytes vs. 8K bytes)
  - Cut round key table size in half (save 160 bytes)
  - Cut code size in half (roughly)
- Hardware: CTR with CBC-MAC is SMALLER than AES-OCB
  - Silicon area roughly 1.5x to 2x smaller than performing both encrypt and decrypt operations
  - Less than 20K gates for encryption only (fraction of overall ASIC?)

Power Consumption (in Hardware)

- OCB performs roughly half the number of crypto operations as CTR with CBC-MAC
- "Duty cycle" of encryption logic activity @ 40 MHz (assuming gated clocks)
  - ~3% for 802.11b (CTR with CBC-MAC)
  - ~15% for 802.11a (CTR with CBC-MAC)
- Small fraction of gates, small duty cycle, digital vs. analog → power for encryption is "in the noise" (< 1%)

[Power Duty Cycle Computations]

- Assumptions:
  - 10 clocks per 128-bit AES block
  - 40 MHz clock (i.e., 4M AES blocks/sec)
- AES throughput = 512 Mbps
- 802.11b ≈ 6.5 Mbps (max),
  x2 (for CTR with CBC-MAC) ≈ 13 Mbps
- Duty cycle ≈ 13/512 < 3%

Speed

- Most 802.11 implementations of AES will be in hardware
- Hardware: 55 Mbps (or twice that) is very slow for AES, as shown by the duty cycle in previous slide
- Software: OCB is twice the speed of CTR with CBC-MAC
  - OCB “wins” if 1x is fast enough, but 2x is too slow

Cleartext Integrity Coverage

- OCB "nonce stealing" allows integrity protection outside the payload
  - IV plus header fields <= 128 bits
  - Current proposal has reduced IV to 27 bits because of this OCB limitation
  - How would we protect another MAC address?
- CBC-MAC can cover an *arbitrary* amount of cleartext in addition to the payload

Simplicity of Key Management

- OCB uses two keys internally on decrypt
  - Pre-computed or computed on-the-fly
- CTR with CBC-MAC uses two keys
  - Derive CBC-MAC key from CTR key with one encrypt operation (counter = zero)
  - Pre-computed or computed on-the-fly

Packet Overhead

- OCB
  - IV
  - Check value
- CTR with CBC-MAC
  - IV
  - Check value
- Same overhead for same security

Crypto Confidence

- OCB is new
  - In crypto, new is dangerous
  - Some provably secure systems have been broken
    - Proofs can contain subtle errors
    - Proofs are always based on assumptions and a restricted model
- CTR and CBC-MAC are 20+ years old
  - Well studied, no surprises
- OCB and CTR both require care with IVs

Conclusion

- No compelling advantage to OCB
- Please consider unencumbered alternatives