Authenticated Encryption Requirements

David McGrew
mcgrew@cisco.com

Directions in Authenticated Ciphers, 2012

Many desirable attributes

- High security
- Computationally cheap
- Low latency
- Compact in software and/or hardware
- Re-use existing cryptographic components
- Randomized (no nonce)
- Misuse resistance
- Side channel resistance
- Forward security
- Postquantum
- Key agility
- Beyond birthday bound security
- Message length hiding

Domains of use

	message size	data rates	goals
Links	40 to 2000 bytes	0.6 to 100 Gbit	low latency
Internet	40 to 2000 bytes	1 to 10 Mbit	
Low power wireless	1 to 100 bytes	20 to 250 Kbits	low expansion compact
Data at rest	512 to 4096 bytes	400 Mbit	randomized?

AEAD in standards

AES-CCM	**802.11i**, **802.15**, **ESP**, **TLS** protocols
AES-GCM	**802.1AE (MACsec)**, **INCITS Fibre Channel (FC-SP)**, **IKE**, **ESP**, **TLS**, SSH, and SRTP, **P1619.1** and **LTO-4** tape storage; **Suite B**
AES-OCB	802.11i
Camellia-GCM	TLS
ARIA-GCM	TLS
SEED-GCM	TLS

Issues

CCM

- Pre-encryption plaintext buffering

Issues

CCM

- Pre-encryption plaintext buffering
    - but short messages used in practice

Issues

CCM

- Pre-encryption plaintext buffering
    - but short messages used in practice
- **Serialized**

Issues

CCM

- Pre-encryption plaintext buffering
  - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages

Issues

CCM

- Pre-encryption plaintext buffering
  - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages
  - but short messages used in practice

Issues

CCM

- Pre-encryption plaintext buffering
  - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages
  - but short messages used in practice
- Nonce hashing imperfect

Issues

CCM

- Pre-encryption plaintext buffering
    - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages
    - but short messages used in practice
- Nonce hashing imperfect
    - but unused in practice

Issues

CCM

- Pre-encryption plaintext buffering
  - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages
  - but short messages used in practice
- Nonce hashing imperfect
  - but unused in practice
- **Compact software implementations difficult**

Issues

CCM

- Pre-encryption plaintext buffering
  - but short messages used in practice
- **Serialized**

GCM

- Authentication weaker for longer messages
  - but short messages used in practice
- Nonce hashing imperfect
  - but unused in practice
- **Compact software implementations difficult**
- **Nonce re-use, short tags**

GCM

$$
\begin{aligned}
Y_0 &= \begin{cases} IV \| 0^{31}1 & \text{if } \mathrm{len}(IV) = w - 32 \\ \mathrm{GHASH}(H, \{\}, IV) & \text{otherwise.} \end{cases} \\
Y_i &= \mathrm{incr}(Y_{i-1}) \text{ for } i = 1, \ldots, n \\
C_i &= P_i \oplus E(K, Y_i) \text{ for } i = 1, \ldots, n-1 \\
C_n^* &= P_n^* \oplus \mathrm{MSB}_u(E(K, Y_n)) \\
T &= \mathrm{MSB}_t(\mathrm{GHASH}(H, A, C) \oplus E(K, Y_0)) \\
H &= E(K, 0^w)
\end{aligned}
$$

GCM evolution?

$$
\begin{aligned}
Y_0 &= \begin{cases} IV \| 0^{31}1 & \text{if } \mathrm{len}(IV) = w - 32 \\ \mathrm{GHASH}(H, \{\}, IV) & \text{otherwise.} \end{cases} \\
Y_i &= \mathrm{incr}(Y_{i-1}) \text{ for } i = 1, \ldots, n \\
C_i &= P_i \oplus E(K, Y_i) \text{ for } i = 1, \ldots, n-1 \\
C_n^* &= P_n^* \oplus \mathrm{MSB}_u(E(K, Y_n)) \\
T &= \mathrm{MSB}_t(\mathbf{HASH}(\mathbf{E}(K, Y_0), A, C))
\end{aligned}
$$

- per-packet hash key secure against nonce reuse, short authentication tags

GCM evolution?

$$
\begin{aligned}
Y_0 &= \begin{cases} IV \| 0^{31}1 & \text{if } \mathrm{len}(IV) = w - 32 \\ \mathrm{GHASH}(H, \{\}, IV) & \text{otherwise.} \end{cases} \\
Y_i &= \mathrm{incr}(Y_{i-1}) \text{ for } i = 1, \ldots, n \\
C_i &= P_i \oplus E(K, Y_i) \text{ for } i = 1, \ldots, n-1 \\
C_n^* &= P_n^* \oplus \mathrm{MSB}_u(E(K, Y_n)) \\
T &= \mathrm{MSB}_t(\mathbf{HASH}(\mathbf{E}(K, Y_0), A, C))
\end{aligned}
$$

- per-packet hash key secure against nonce reuse, short authentication tags
- **HASH** can be software friendly (e.g. [RWB]) or **E**-based

GCM evolution?

$$
\begin{aligned}
Y_0 &= \begin{cases} IV \| 0^{31}1 & \text{if } \mathrm{len}(IV) = w - 32 \\ \mathrm{GHASH}(H, \{\}, IV) & \text{otherwise.} \end{cases} \\
Y_i &= \mathrm{incr}(Y_{i-1}) \text{ for } i = 1, \ldots, n \\
C_i &= P_i \oplus E(K, Y_i) \text{ for } i = 1, \ldots, n-1 \\
C_n^* &= P_n^* \oplus \mathrm{MSB}_u(E(K, Y_n)) \\
T &= \mathrm{MSB}_t(\mathbf{HASH}(\mathbf{E}(K, Y_0), A, C))
\end{aligned}
$$

- per-packet hash key secure against nonce reuse, short authentication tags
- **HASH** can be software friendly (e.g. [RWB]) or **E**-based

Broadens applicability, but may not address all domains

Recommendations

Recommendations

- Encourage exploration of design space

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use
    - Low power wireless

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use
    - Low power wireless
- Document requirements within each domain

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements
  - Side channel resistance

Recommendations

- Encourage exploration of design space
- Avoid over focus on performance, compactness, . . .
- Identify domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements
  - Side channel resistance
  - Available royalty-free worldwide