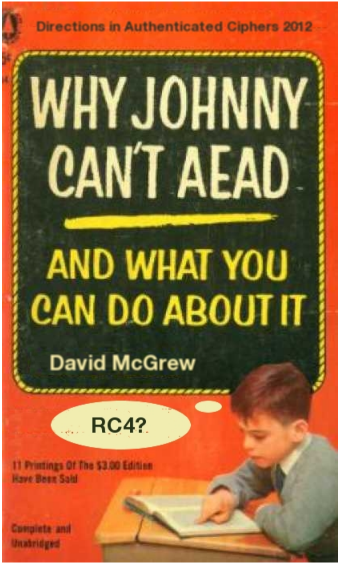
Authenticated Encryption in Practice

mcgrew@cisco.com



Outline

1. History
2. Interface
   - Nonces and misuse resistance
3. AEAD in standards
   - Issues
4. AEAD in security architectures
   - Security
5. Desiderata
   - Desiderata
6. Conclusions

Timeline

	Algorithms	Standards
1999	IAPCBC	
2000	IACBC, AE	
2001	OCB, AEAD	
2002	CCM	802.11
2003		
2004	GCM	802.1
2005		IPsec
2006		FC-SP, 1619.1, LTO-4
2007		
2008		RFC5116
2009	SIV	TLSv1.2, IKE, XMLsec, SSH
2010		
2011	OCBv3	
2012	CBC+HMAC	SRTP, *JOSE*

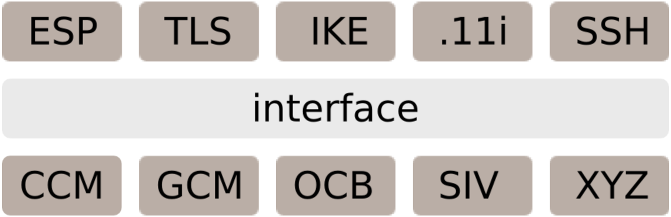
Internet Assigned Name Authority (IANA) Registry

Numeric ID	Name	Reference
1	AEAD_AES_128_GCM	RFC5116
2	AEAD_AES_256_GCM	RFC5116
3	AEAD_AES_128_CCM	RFC5116
4	AEAD_AES_256_CCM	RFC5116
5	AEAD_AES_128_GCM_8	RFC5282
6	AEAD_AES_256_GCM_8	RFC5282
7	AEAD_AES_128_GCM_12	RFC5282
8	AEAD_AES_256_GCM_12	RFC5282
9	AEAD_AES_128_CCM_SHORT	RFC5282
10	AEAD_AES_256_CCM_SHORT	RFC5282
11	AEAD_AES_128_CCM_SHORT_8	RFC5282
12	AEAD_AES_256_CCM_SHORT_8	RFC5282
13	AEAD_AES_128_CCM_SHORT_12	RFC5282
14	AEAD_AES_256_CCM_SHORT_12	RFC5282
15	AEAD_AES_SIV_CMAC_256	RFC5297
16	AEAD_AES_SIV_CMAC_384	RFC5297
17	AEAD_AES_SIV_CMAC_512	RFC5297
18	AEAD_AES_128_CCM_8	RFC6655
19	AEAD_AES_256_CCM_8	RFC6655
20-32767	Unassigned	
32768-65535	Reserved for Private Use	

Observations

- AEAD initially adopted at link layer
- AEAD broadly used in point-to-point encryption
- All IANA algorithms use PRF : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$
  - Camellia, SEED, ARIA not represented
  - Could define companion registry of PRP/PRF functions

RFC 5116 interface



RFC 5116 interface

Inputs

- Key K

RFC 5116 interface

Inputs

- Key K
- Nonce N (authenticated)

RFC 5116 interface

Inputs

- Key K
- Nonce N (authenticated)
- Associated data A (authenticated)

RFC 5116 interface

Inputs

- Key K
- Nonce N (authenticated)
- Associated data A (authenticated)
- Plaintext P (encrypted and authenticated)

RFC 5116 interface

Inputs

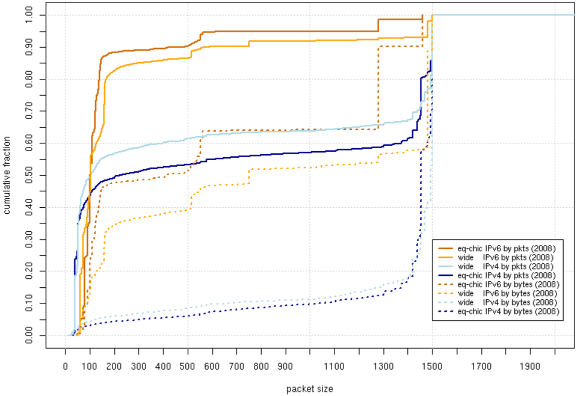
- Key K
- Nonce N (authenticated)
- Associated data A (authenticated)
- Plaintext P (encrypted and authenticated)

Outputs

- Authenticated ciphertext C

IMIX

IPv4 and IPv6 cumulative packet distributions, 2008



Source: CAIDA

Typical parameter sizes

		P	A	N	t
6LoWPAN	802.15.4	0 - 87	5 - 14	13	4, 8
WiFi	802.11i	1 - 2296	22 - 30	13	8
MACsec	802.1AE	0 - 1500	16+	12	16
ESP	RFC4303	40 - 2048 [32M]	8, 12	12	16
TLS	RFC5246	1 - 2048 [16K]	13	12	16
SRTP	RFC3711	20,80,1500	12+	12	4, 10

Deterministic nonces

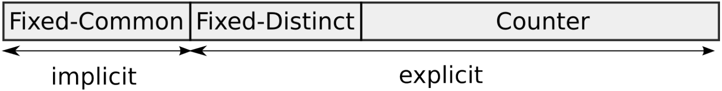
Recommended format

Fixed	Counter

Deterministic nonces

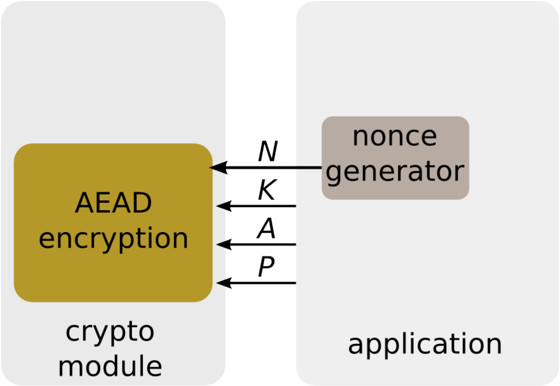
Recommended format

Partially implicit format

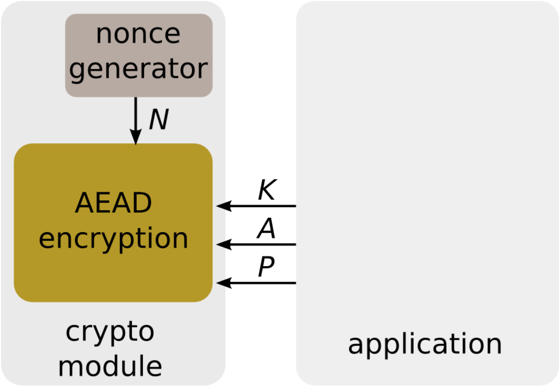


`draft-mcgrew-iv-gen`

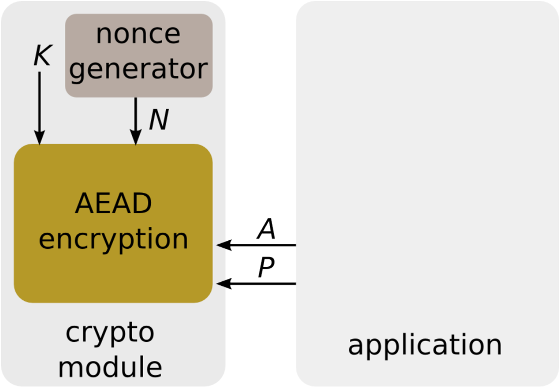
`aead_encrypt(K, N, A, P)`



```
aead_encrypt(K, A, P)
```



```
aead_encrypt(key_id, A, P)
```



Internal nonce generation

Observation

Any nonce-based AEAD scheme can be made into a misuse resistant AEAD scheme by incorporating nonce generation

- Puts burden of correctness on crypto implementer, not crypto caller
- Implementations of internal nonce schemes can be validated

Internal nonce generation

Observation

Any nonce-based AEAD scheme can be made into a misuse resistant AEAD scheme by incorporating nonce generation

- Puts burden of correctness on crypto implementer, not crypto caller
- Implementations of internal nonce schemes can be validated

Implication

An AEAD scheme incorporating nonce generation can provide a nonce as an output

- Anti-replay protection service can be provided to the user

AEAD RFCs

RFC 6367 Addition of the Camellia Cipher Suites to TLS, Informational, 2011.

RFC 6209 Addition of the ARIA Cipher Suites to TLS, Informational, 2011.

RFC 6054 Using Counter Modes with ESP and AH to Protect Group Traffic, Standards Track, 2010.

RFC 5647 AES Galois Counter Mode for the SSH Protocol, Informational, 2009.

RFC 5487 Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES GCM, Standards Track, 2009.

RFC 5297 Synthetic Initialization Vector (SIV) Authenticated Encryption Using AES, Informational, 2008.

RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES GCM, Informational, 2008.

RFC 5288 AES GCM Cipher Suites for TLS, Standards Track, 2008.

RFC 5282 Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, Standards Track, 2008.

RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, Standards Track, 2008.

RFC 5116 An Interface and Algorithms for Authenticated Encryption, Standards Track, 2008.

Lessons

- Most protocols fine with deterministic nonces
  - Algorithms that work without deterministic nonces needed for other applications

Lessons

- Most protocols fine with deterministic nonces
  - Algorithms that work without deterministic nonces needed for other applications
- Contiguous authentication with discontiguous encryption
  - Awkward, but not impossible

Lessons

- Most protocols fine with deterministic nonces
  - Algorithms that work without deterministic nonces needed for other applications
- Contiguous authentication with discontiguous encryption
  - Awkward, but not impossible
- Global ciphers
  - Camellia, ARIA, SEED, . . .

Lessons

- Most protocols fine with deterministic nonces
    - Algorithms that work without deterministic nonces needed for other applications
- Contiguous authentication with discontiguous encryption
    - Awkward, but not impossible
- Global ciphers
    - Camellia, ARIA, SEED, . . .
- No way to separate authentication from confidentiality
    - This is a goal, not a problem!

Lessons

- Most protocols fine with deterministic nonces
  - Algorithms that work without deterministic nonces needed for other applications
- Contiguous authentication with discontiguous encryption
  - Awkward, but not impossible
- Global ciphers
  - Camellia, ARIA, SEED, . . .
- No way to separate authentication from confidentiality
  - This is a goal, not a problem!
  - May be desirable for protocols to have ability to provide symmetric authentication in addition to AEAD (but I doubt it)

Optional or mandatory?

TLS v 1.2 example

```
struct {
          ContentType type;
          ProtocolVersion version;
          uint16 length;
          select (SecurityParameters.cipher_type) {
              case stream: GenericStreamCipher;
              case block:  GenericBlockCipher;
              case aead:   GenericAEADCipher;
          } fragment;
      } TLSCiphertext;
```

Optional or mandatory?

TLS v 1.2 example

```
struct {
          ContentType type;
          ProtocolVersion version;
          uint16 length;
          select (SecurityParameters.cipher_type) {
              case stream: GenericStreamCipher;
              case block:  GenericBlockCipher;
              case aead:   GenericAEADCipher;
          } fragment;
      } TLSCiphertext;
```

Authenticated Encryption with AES-CBC and HMAC-SHA

`draft-mcgrew-aead-aes-cbc-hmac-sha2-00.txt`
(joint work with Kenny Paterson)

Storage encryption

Specialty ciphers (without authentication)

- Disk block encryption (EME2, XCB, XTS)
- Format-preserving encryption
- File and file system encryption

Storage encryption

Specialty ciphers (without authentication)

- Disk block encryption (EME2, XCB, XTS)
- Format-preserving encryption
- File and file system encryption

Needed: standard(s) for AEAD storage

- Security improvements for disk, file, filesystem
- Motivation: network/cloud separates storage from owner
- Existing AEAD algorithms suitable?

Traditional security goals

Inside AEAD

- Confidentiality
- Authenticity

Outside AEAD

- Anti-replay protection
- Forward security
- Message length hiding
- Frequent rekeying

Achievable security goals

Inside AEAD

- Confidentiality
- Authenticity
- Anti-replay protection
- Forward security

Outside AEAD

- Message length hiding
- Frequent rekeying

Forward security

$$C_i = E(K_i, P_i, A_i)$$

$$K_i = \begin{cases} K & \text{if } i = 0 \\ \mathrm{PRF}(K_{i-1}) & \text{otherwise} \end{cases}$$

One-way chain of per-message keys: $K_0 \rightarrow K_1 \rightarrow K_2 \rightarrow \ldots$

Easy to use above reliable transport (TLS, SSH)

[BY03] *Forward-Security in Private-Key Cryptography*

Side channel attacks

Attacker can touch device

- Cryptographic tamper resistance
- Needed to build trustworthy systems

Attacker can run co-resident software

- Virtual machine or process
- Applicable in cloud computing

Multiple Forgery Attacks [MF05]

$$E(F) = \text{expected number of forgeries}$$
$$q = \text{number of queries} \ll 2^t/l, \ll 2^{b/2}$$
$$b = \text{bits in block}$$
$$l = \text{blocks in message}$$
$$t = \text{bits in tag}$$

$$E(F_{\text{Ideal}}) \approx q\,2^{-t}$$
$$E(F_{\text{GCM}}) \approx q^2\,\frac{l+1}{2}2^{-t}$$
$$E(F_{\text{Chained}}) \approx q^3\,\frac{1}{6}2^{-b}$$

Multiple Forgery Attacks [MF05]

$l = 128, t = 128$

$$E(F_{\text{Ideal}}) \approx q\,2^{-128}$$
$$E(F_{\text{AES-GCM}}) \approx q^2\,2^{-122}$$
$$E(F_{\text{AES-CMAC}}) \approx q^3\,2^{-125}$$
$$E(F_{\text{HMAC-MD5}}) \approx q^3\,2^{-125}$$
$$E(F_{\text{HMAC-SHA1}}) \approx q^3\,2^{-157}$$

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	nonce?

AES Criteria

- Security
- Computational efficiency on a variety of software and hardware platforms, including smart cards
- Flexibility and simplicity
- Availability royalty-free worldwide
- Capability of handling key sizes of 128, 192, and 256 bits

Non-security

- Computationally cheap
- Low latency
- Compact in software and/or hardware
- Re-use existing cryptographic components
- Avoid deterministic nonce
- Key agility

Security

- Strength against cryptanalysis
- Side channel resistance
- Misuse resistance
- Message length hiding
- Forward security
- Postquantum
- Beyond birthday bound security

Conclusions

- Encourage exploration of design space

Conclusions

- Encourage exploration of design space
- Identify new domains of use

Conclusions

- Encourage exploration of design space
- Identify new domains of use
  - Low power wireless

Conclusions

- Encourage exploration of design space
- Identify new domains of use
  - Low power wireless
- Document requirements within each domain

Conclusions

- Encourage exploration of design space
- Identify new domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements

Conclusions

- Encourage exploration of design space
- Identify new domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements
  - Side channel resistance

Conclusions

- Encourage exploration of design space
- Identify new domains of use
  - Low power wireless
- Document requirements within each domain
- Identify critical requirements
  - Side channel resistance
  - Available royalty-free worldwide

Conclusions

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

Conclusions

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

Thank You

mcgrew@cisco.com