Authenticated Encryption

Chanathip Namprempre

Computer Science
Reed College

Agenda: Authenticated Encryption

1. Authenticity is often necessary even when all you care about is privacy.
   1.1 Attack against CBC (TCP/IP)
   1.2 Attack against CTR with checksum (a remote terminal application)
   1.3 Side-channel attack against non-atomic decryption (SSH BPP)
2. Authenticated Encryption is the answer.
3. Generic composition: GCM, CCM, EAX
4. Handcrafted construction: OCB
5. Generic composition: caveats

Encryption alone often is not enough to get privacy: Case 1

TCP/IP uses CBC with random IV.

1. Usually webserver listens on port 80.
2. Suppose an attacker A listens on port 25.
3. Suppose client uses IPsec to encrypt data for webserver.
4. If the client only uses encryption to send M, the packet can be modified by an attacker so that it can get M on port 25.

Client uses CBC with random IV to send M to port 80:

$$C \leftarrow (IV, \mathrm{CBC}_K(IV,\ \text{dest} = 80 \,\|M))$$

A can change C to

$$C' \leftarrow \big(IV', \mathrm{CBC}_K(IV,\ \text{dest} = 80 \,\|M)\big)$$

where

$$IV' = IV \oplus (\ldots 80 \ldots) \oplus (\ldots 25 \ldots)$$

Encryption alone often is not enough to get privacy: Case 1

To see that this attack works, try computing $M[0] = D_K(C[0]) \oplus IV$.

You can change the decryption to be whatever you want by manipulating IV.

CBC with random IV is IND-CPA but still isn't enough to ensure privacy!

Encryption alone often is not enough to get privacy: Case 2

Adding checksum to CTR mode is not enough to get authenticity.

Consider a remote terminal application. Suppose each keystroke is encrypted with CTR mode.

TCP/IP packet:

$$\boxed{\text{IP hdr} \,\|\, \text{TCP hdr} \,\|\quad T \quad\|\quad M \quad}$$

where T is a 16-bit checksum and M is a 1-byte keystroke.

Encryption alone often is not enough to get privacy: Case 2

TCP/IP packet: T is a 16-bit checksum and M is a 1-byte keystroke.

$$\boxed{\text{IP hdr} \parallel \text{TCP hdr} \parallel \quad T \quad \parallel \quad M \quad}$$

Attack:

1. Try for many t and s,
   1.1 submit to the server

   $$\boxed{\text{IP hdr} \parallel \text{TCP hdr} \parallel \quad \oplus\, t \quad \parallel \quad \oplus\, s \quad}$$

   1.2 Watch the server whether it says the packet was valid.
2. Collect many equations of the form:

   $$\text{checksum}(\text{hdr}, M) \oplus t = \text{checksum}(\text{hdr}, M \oplus s)$$

3. For some checksum, it is easy to compute M.

Encryption alone often is not enough to get privacy: Case 3

Attacking SSH Binary Packet Protocol

Weaknesses

1. Packet length is encrypted but is used immediately after decryption but before the MAC is verified.
2. Decryption is non-atomic.

Authenticated Encryption is Needed!
Integrity of Ciphertext

Subroutines

Subroutine `Initialize`
$K \xleftarrow{\$} \mathsf{KG}$; $S \leftarrow \emptyset$; win $\leftarrow$ false

Subroutine $\texttt{Enc}(M)$
$C \xleftarrow{\$} \mathsf{Enc}(K, M)$; $S \leftarrow S \cup \{C\}$
Return C

Subroutine $\texttt{Vf}(C)$
$M \leftarrow \mathsf{Dec}(K, C)$
If $M \neq \perp$ and $C \notin S$ then win = true
If $M = \perp$ then return 0 else return 1

Subroutine `Finalize`
Return win

Experiment

Experiment $\mathbf{Exp}_{\mathsf{AE}}^{\text{int-ctxt}}(A)$

`Initialize`
$d \xleftarrow{\$} A^{\texttt{Enc},\texttt{Vf}}$
Return `Finalize`

We define the **int-ctxt advantage** of an adversary A mounting an attack against integrity of ciphertexts of AE as

$$\mathbf{Adv}_{\mathsf{AE}}^{\text{int-ctxt}}(A) = \Pr\left[\,\mathbf{Exp}_{\mathsf{AE}}^{\text{int-ctxt}}(A) \Rightarrow \text{true}\,\right] .$$

Authenticated Encryption

Authenticated Encryption

$\mathsf{AE} = \mathsf{IND\text{-}CPA} \wedge \mathsf{INT\text{-}CTXT}$

Syntax is slight different from that of encryption also.

Generic composition

Generic composition methods

Encrypt-and-MAC, Encrypt-then-MAC, MAC-then-encrypt

In practice,

- SSL uses MtE.
- IPsec uses EtM.
- SSH uses E&M.

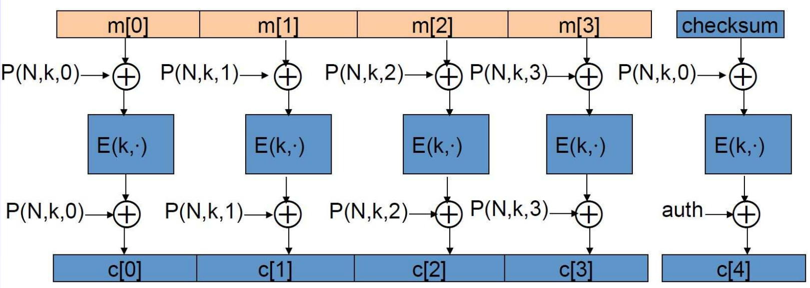
AE schemes in practice

- GCM (EtM): CTR$ then CW-MAC
- CCM (MtE): CBC-MAC then CTR (802.11i)
- EAX (EtM): CTR then CMAC

All are nonce-based and supports AEAD. All are endorsed by NIST.

AE schemes in practice (cont.)

OCB is a dedicated AE scheme constructed from PRP.
One application of PRP per block rather than two.



Generic composition: caveats

It is not as simple as Encrypt-then-MAC being the "best" composition method!