Authenticated Encryption: Combining Authentication with Encryption to get IND-CCA

15-859I
Spring 2003

Motivation

- We have previously shown how to construct a symmetric encryption scheme $\mathcal{SE}$ which is secure against chosen-plaintext attacks, based on the assumption that one-way functions exist.
- We have introduced a provably stronger notion of security: indistinguishability under chosen ciphertext attack.
- Question: How can we construct a system which meets this notion?

Authenticated Encryption

- [BN00] Consider the problem of generically combining message authentication with encryption:
- Develop two notions of authenticated encryption, INT-PTXT and INT-CTXT
- Consider three ways to combine a MAC with an encryption scheme, and determine if the result satisfies INT-PTXT or INT-CTXT
- Show that if $\mathcal{SE}$ satisfies IND-CPA and INT-CTXT it also satisfies IND-CCA.

Punchline

- Let (G,E,D) be a cryptosystem satisfying IND-CPA and let (K,T,V) be a *strongly unforgeable* MAC. Then the cryptosystem SE = (G',E',D') satisfies IND-CCA, where:
- $G'(1^k) = K_e \leftarrow G(1^k)$; $K_m \leftarrow K(1^k)$, (K_e,K_m)
- $E'(K_e,K_m,M)$ = let $c = E(K_e,M)$, $t = T(K_m,c)$, return (c,t)
- $D'(K_e,K_m,(c,t))$ = If $V(K_m,c,t) = 1$ then $D(K_e,c)$, else $\perp$

Definitions: IND-CPA

Let SE = (G,E,D) be a symmetric encryption scheme. Define $LR(b,x_0,x_1) = x_b$ if $|x_0|=|x_1|$, "" otherwise.

$Exp_{A,SE}^{cpa\text{-}b}(k)$ =

Choose $K \leftarrow G(1^k)$

Return $A^{E_K(LR(b,.,.))}(1^k)$.

Define the advantage of A, $Adv_{A,SE}^{cpa}(k)$, by

$Pr[Exp_{A,SE}^{cpa\text{-}1}(k) = 1] - Pr[Exp_{A,SE}^{cpa\text{-}0}(k) = 1]$

And $Insec_{SE}^{cpa}(k,t,q,l) = max_{A|t,q,l}\{Adv_{A,SE}^{cpa}(k)\}$

Definitions: IND-CCA

Let SE=(G,E,D).

Define $Exp_{A,SE}^{cca\text{-}b}(k)$ =

Choose $K \leftarrow G(1^k)$

Return $A^{E_K(LR(b,.,.)),D_K}(1^k)$.

A is not allowed to query D_K on $C \leftarrow E_K(LR(b,.,.))$.

Define the advantage of A, $Adv_{A,SE}^{cca}(k)$, by

$Pr[Exp_{A,SE}^{cca\text{-}1}(k) = 1] - Pr[Exp_{A,SE}^{cca\text{-}0}(k) = 1]$

And $Insec_{SE}^{cca}(k,t,q,l) = max_A\{Adv_{A,SE}^{cca}(k)\}$

Definitions: SUF-CMA

Let MA = (K,T,V) be a MAC.

Define $Exp_{A,MA}^{suf\text{-}cma}(k)$ =

$K \leftarrow K(1^k)$

If $A^{T_K, V_K}(1^k)$ queries $V_K(M,s)$ such that

$V_K(M,s) = 1$ and $T_K(M)$ never returned s

then return 1, else return 0.

Define $Adv_{A,MA}^{cma}(k) = \Pr[Exp_{A,MA}^{cma}(k)=1]$,

$Insec_{MA}^{suf\text{-}cma}(k,t,q,l) = \max_A\{Adv_{A,MA}^{cma}(k)\}$

SUF-CMA vs EUF-CMA

- Notice that this is a bit different from our previous definition of security for a MAC: before A could only win if his message M had not been queried previously. Now he wins if s was never returned by T(M).
- Any stateless, deterministic MAC satisfies SUF-CMA whenever it satisfies EUF-CMA.
- In particular, CBC-MAC extended to arbitrary message spaces satisfies SUF-CMA.

Integrity of Authenticated Encryption

- Authenticated encryption allows the decryption oracle to return the symbol $\perp$ on an invalid ciphertext.
- Intuitively, a scheme has integrity of plaintexts if it is hard to make a valid ciphertext for a new plaintext, given access to an encryption oracle and a validity oracle D_K^* that returns 1 if $D_k(C) = 1$.
- A scheme has integrity of ciphertexts if it is hard to make a new, valid ciphertext.

INT-PTXT

Define $Exp_{A,SE}^{int\text{-}ptxt}(k)$ =

Choose $K \leftarrow G(1^k)$

if $A^{E_K, D^*_K}(1^k)$ queries $D_K^*(C)$ such that:

$D_K(C) = M \neq \perp$ and

$E_K(M)$ was never queried

then return 1, else return 0.

Define $Adv_{A,SE}^{int\text{-}ptxt}(k) = \Pr[Exp_{A,SE}^{int\text{-}ptxt}(k) = 1]$,

$Insec_{SE}^{int\text{-}ptxt}(k,t,q,l) = \max_A\{Adv_{A,SE}^{int\text{-}ptxt}(k)\}$

INT-CTXT

Define $Exp_{A,SE}^{int\text{-}ctxt}(k)$ =

Choose $K \leftarrow G(1^k)$

if $A^{E_K, D^*_K}(1^k)$ queries $D_K^*(C)$ such that:

$D_K(C) = M \neq \perp$ and

E_K never returned C

then return 1, else return 0.

Define $Adv_{A,SE}^{int\text{-}ctxt}(k) = \Pr[Exp_{A,SE}^{int\text{-}ctxt}(k) = 1]$,

$Insec_{SE}^{int\text{-}ctxt}(k,t,q,l) = \max_A\{Adv_{A,SE}^{int\text{-}ctxt}(k)\}$

INT-CTXT $\Rightarrow$ INT-PTXT

Theorem. If SE=(G,E,D) is INT-CTXT secure it is also INT-PTXT secure:

$Insec_{SE}^{int\text{-}ptxt}(k,t,q,l) \leq Insec_{SE}^{int\text{-}ctxt}(k,t,q,l)$

INT-CTXT $\wedge$ IND-CPA $\Rightarrow$ IND-CCA

Theorem: Let SE=(G,E,D) and suppose SE satisfies INT-CTXT and IND-CPA. Then it is secure against chosen-ciphertext attack:

$\mathrm{Insec}_{SE}^{\text{ind-cca}}(k,t,q,l) \le$
$2\mathrm{Insec}_{SE}^{\text{int-ctxt}}(k,t,q,l) + \mathrm{Insec}_{SE}^{\text{ind-cpa}}(k,t,q,l)$

Proof: (idea) Let A be an IND-CCA adversary with high advantage. We will show how to construct an INT-CTXT adversary A_c and an IND-CPA adversary A_p such that at least one also has high advantage.

Adversaries A_c, A_p

- $A_c^{E_K,D_K^*}(1^k)$ =
  - Choose b $\leftarrow$ {0,1}
  - Run $A(1^k)$:
    On query $E(M_0,M_1)$, respond with $E_K(M_b)$
    On query D(C): if $D_K^*(C) = 1$ then stop.
    else respond with $\perp$
- $A_p^{E_K(LR(b,.,.))}(1^k)$ =
  - Run $A(1^k)$ to get b':
    On query $E(M_0,M_1)$, respond with $E_K(LR(b,M_0,M_1))$
    On query D(C) respond with $\perp$
  - Return b'

Proof of IND-CCA Theorem

- For any event X, we use the notation:
  $Pr[X] = Pr[X : b \leftarrow \{0,1\}, \mathrm{Exp}_{A,SE}^{\text{ind-cca-b}}(k)]$
  $Pr_c[X] = Pr[X : \mathrm{Exp}_{A_c,SE}^{\text{int-ctxt}}(k)]$
  $Pr_p[X] = Pr[X : b \leftarrow \{0,1\}, \mathrm{Exp}_{A_p,SE}^{\text{ind-cpa-b}}(k)]$
- Call b' the output of A in $\mathrm{Exp}_{A,SE}^{\text{ind-cca-b}}(k)$.
- Let E be the event that A submits a query C such that $D_K(C) \neq \perp$

Then $\frac{1}{2}\mathrm{Adv}_{A,SE}^{\text{ind-cca}}(k) + \frac{1}{2} = Pr[b'=b]$
$= Pr[b'=b \wedge E] + Pr[b'=b \wedge \neg E]$
$\le Pr[E] + Pr_p[b'=b]$
$= \mathrm{Adv}_{SE,A_c}^{\text{int-ctxt}}(k) + \frac{1}{2}\mathrm{Adv}_{SE,A_p}^{\text{ind-cpa}}(k) + \frac{1}{2}$

IND-CCA $\not\Rightarrow$ INT-PTXT

- Theorem: If there exists a scheme SE = (G,E,D) which satisfies IND-CCA then there exists a scheme SE'=(G',E',D') which satisfies IND-CCA but not INT-PTXT
- Proof: Define G' = G
- $E'_K(M) = 0||E_K(M)$
- $D'_K(b||C)$ = if (b = 0) then $D_K(C)$ else 0
- Adversary $A(1^k)$ = Query $D_K^*(1||0)$.
- $\mathrm{Adv}_{A,SE'}^{\text{int-ptxt}}(k) = 1$.
- But given an oracle for $E_K(LR(b,.,.))$ and one for D_K, we can perfectly simulate same for E_K', D_K'. Thus SE' is IND-CCA secure iff SE is IND-CCA secure.

How to combine a MAC and cipher

- There are several ways we could conceivably compose a MAC (K,T,V) with a cryptoscheme (G,E,D):
- Encrypt-And-Mac: E'(M) = E(M)||T(M)
- Mac-Then-Encrypt: E'(M) = E(M||T(M))
- Encrypt-Then-Mac: E'(M) = E(M)||T(E(M))
- Which is guaranteed to give us IND-CPA? INT-PTXT? INT-CTXT?

Encrypt-and-MAC: IND-CPA?

- Theorem: For any secure, deterministic MAC, Encrypt-and-MAC is not IND-CPA secure.
- Adversary: Query $E_K(LR(b,0,0))$ to get $E_K(0)$, $T_K(0)$. Query $E_K(LR(b,0,1))$. If the tag is the same as the first, guess b = 0, else guess b = 1.
- (If the MAC is secure, then $T_K(0)=T_K(1)$ with only negligible probability)

Encrypt-and-MAC: INT-PTXT?

- Theorem: If MA is SUF-CMA then SE' = Encrypt-then-MAC is INT-PTXT secure:
  $\mathrm{Insec}_{SE'}^{\text{int-ptxt}}(k,t,q,l) \le \mathrm{Insec}_{MA}^{\text{suf-cma}}(k,t,q,l)$.
- Proof: Given a INT-PTXT adversary A for SE', we can simulate SE' given T,V oracles for MA by choosing a key for SE.
- Suppose A succeeds. Then A has produced a valid ciphertext C'=C,t for some message M that was never queried. Thus $V_K(M,t)=1$.
- Thus we succeed in forging MA whenever A succeeds in the INT-PTXT sense.

Encrypt-and-MAC: INT-CTXT?

- Theorem: If there exist SE which is IND-CPA secure and MA which is SUF-CMA, then there exists SE' such that SE' is IND-CPA secure but E&M(SE',MA) is not INT-CTXT secure.
- Proof: SE' = SE except E'(M) = 0||E(M), D'(b||C) = D(C). It is easy to see that SE' is still IND-CPA, but

  $\mathrm{Insec}_{E\&M(SE',MA)}^{\text{int-ctxt}}(k,O(1),1,1) = 1$

  since we can forge a new valid ciphertext by querying E(0) to get 0||C and returning 1||C.

Mac-then-Encrypt: IND-CPA?

- Theorem: If SE is IND-CPA and MA is SUF-CMA then MtE(SE,MA) is IND-CPA:
  $\mathrm{Insec}_{MtE}^{\text{ind-cpa}}(k,t,q,l) \le \mathrm{Insec}_{SE}^{\text{ind-cpa}}(k,t,q,l+qs)$
  where s is the tag length of MA.
- Proof: Given a IND-CPA adversary A for MtE, we construct a IND-CPA adversary B for SE:
  - $B^{LR}(1^k)$: Choose $K \leftarrow MA.K(1^k)$;
    Run A; respond to $LR(M_0, M_1)$ with
    $LR(M_0||T_K(M_0),M_1||T_K(M_1))$
    Return result of A.

  Clearly B has the same advantage as A.

MAC-then-Encrypt: INT-PTXT?

- Theorem: If MA is SUF-CMA secure then MtE(SE,MA) is INT-PTXT secure:
  $\mathrm{Insec}_{MtE}^{\text{int-ptxt}}(k,t,q,l) \le \mathrm{Insec}_{MA}^{\text{suf-cma}}(k,t,q,l)$
- Proof: given a INT-PTXT adversary A, construct a SUF-CMA adversary B for MA:
- $B^{T,V}(1^k)$: Choose $K \leftarrow G(1^k)$

  Run A. On query E(M), send $E_K(M||T(M))$

  On query D*(C), send $V(D_K(C))$

  Clearly if A succeeds in creating A valid ciphertext for an M which was never queried, B succeeds in finding a M,t pair where t was never output by T(M).

Mac-then-Encrypt: INT-CTXT?

- Theorem: If there exist SE satisfying IND-CPA and MA satisfying SUF-CMA, then there exists SE' satisfying IND-CPA such that MtE(SE',MA) is not NM-CPA secure.
- Corollary: Since IND-CPA $\wedge$INT-CTXT$\Rightarrow$IND-CCA $\Rightarrow$ NM-CCA $\Rightarrow$ NM-CPA, we have that MtE is not INT-CTXT secure.
- Proof: SE'=
  - E'(M) = 0||E(M)
  - D'(b||C) = D(C)

Encrypt-then-MAC: IND-CPA?

- Theorem: If SE is IND-CPA secure then EtM(SE,MA) is IND-CPA secure:
  $\mathrm{Insec}_{EtM}^{\text{ind-cpa}}(k,t,q,l) \le \mathrm{Insec}_{SE}^{\text{ind-cpa}}(k,t,q,l)$
- Proof: Given LR oracle for SE, we can perfectly simulate an LR oracle for EtM by choosing a key K, for MA:
  EtM.E(M) = c $\leftarrow$E(M); return c||T(c).
  This simulation will succeed with the same success as an attack on SE.

EtM: INT-CTXT?

- Theorem: If MA is SUF-CMA secure then EtM(SE,MA) is INT-CTXT secure:
  $\mathrm{Insec}_{EtM}^{int\text{-}ctxt}(k,t,q,l) \leq \mathrm{Insec}_{MA}^{suf\text{-}cma}(k,t,q,l+qs)$
  where |SE.E(M)| = |M| + s
- Proof: Given T,V oracles for MA, we perfectly simulate E,D* oracles for EtM by choosing a key K for SE and answering EtM.E(M) by letting c = $SE.E_K(M)$, t = T(c), and returning (c,t). Simulating D*(c,t) by $V(SE.D_K(c),t)$.
- An INT-CTXT adversary A succeeds when it finds a C' such that EtM.D*(C') = 1 and C' was not returned by EtM.E(). But in this case our simulation has also found a (c,t) pair such that V(c,t) = 1 and t was never returned by T(c). So we succeed in the SUF-CMA sense against MA.