Authenticated Encryption

Yan Huang

Credit: Dan Boneh (Stanford, Crypto I)
Story So Far …

- **Confidentiality:** Secure Encryption (CPA-secure)
  - Single Block messages
  - Multi-block messages

- **Integrity:** Message Authentication Code
  - Using secure block cipher
  - Using collision-resistant hashing

Can we achieve **Confidentiality** and **Integrity** at the same time?
Sample tampering attacks

TCP/IP: (highly abstracted)

source machine

TCP/IP stack

destination machine

Bob
port = 25

WWW
port = 80

packet

dest = 80 data
Sample tampering attacks

IPsec: (highly abstracted)

TCP/IP stack

WWW port = 80

data

stuff

k

packets encrypted using key k

dest = 80 data

dest = 25 stuff

Bob port = 25
Reading someone else’s data

Note: attacker obtains decryption of any ciphertext beginning with “dest=25”

Easy to do for CBC with rand. IV (only IV is changed)
The lesson

CPA security cannot guarantee secrecy under active attacks.

Only use one of two modes:

• If message needs integrity but no confidentiality: use a **MAC**

• If message needs both integrity and confidentiality: use **authenticated encryption** modes
The Idea

An authenticated encryption system \((E, D)\)

As usual: \(E: K \times M \rightarrow C\)

but \(D: K \times C \rightarrow M \cup \{\bot\}\)

Security: the system must provide

- semantic security, and
- ciphertext integrity:
  attacker cannot create new ciphertexts that decrypt properly
Ciphertext integrity

Let \((E,D)\) be a cipher with message space \(M\).

Def: \((E,D)\) has **ciphertext integrity** if for all “efficient” \(\mathcal{A}\):

\[
\text{Adv}_{\text{CI}}[\mathcal{A}, E] = \Pr[\text{Chal. outputs 1}] \quad \text{is “negligible.”}
\]

\[
\begin{align*}
\text{Chal.} & \quad k \leftarrow \mathcal{K} \\
\text{Adversary} & \quad \mathcal{A}
\end{align*}
\]

\[
m_1 \in M \quad m_2, \ldots, m_q
\]

\[
c_1 \leftarrow E(k, m_1) \quad c_2, \ldots, c_q
\]

\[
b
\]

\[
\begin{cases}
 b=1 & \text{if } D(k,c) \neq \bot \quad \text{and } c \notin \{c_1, \ldots, c_q\} \\
 b=0 & \text{otherwise}
\end{cases}
\]
Authenticated Encryption

Def: cipher \((E, D)\) provides **authenticated encryption (AE)** if it is

1. semantically secure under CPA, and
2. has ciphertext integrity

Bad example: CBC with rand. IV does not provide AE

- \(D(k, \cdot)\) never outputs \(\bot\), hence adv. easily wins CI game
Implication 1: authenticity

Attacker cannot fool Bob into thinking a message was sent from Alice

\[ m_1, \ldots, m_q \]

\[ c_i = E(k, m_i) \]

Bob knows message is from someone who knows \( k \)

\[ \Rightarrow \text{if } D(k, c) \neq \bot \text{ Bob knows message is from someone who knows } k \]

(but message could be a replay)
Implication 2

Authenticated Encryption \implies

Security against \textbf{Chosen Ciphertext Attacks}
Chosen Ciphertext security -- Definition

For \( b=0,1 \) define \( \text{EXP}(b) \):

\[
\text{Chal.}:
\quad k \leftarrow K
\]

for \( i=1,\ldots,q \):

(1) **CPA query:**
\[
\begin{align*}
& m_{i,0}, m_{i,1} \in M : |m_{i,0}| = |m_{i,1}| \\
& c_i \leftarrow E(k, m_{i,b})
\end{align*}
\]

(2) **CCA query:**
\[
\begin{align*}
& c_i \in C : c_i \notin \{c_1, \ldots, c_{i-1}\} \\
& m_i = D(k, c_i)
\end{align*}
\]

\( E \) is CCA secure if for all “efficient” \( \mathcal{A} \):

\[
\text{Adv}_{\text{CCA}}[\mathcal{A},E] = |\Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1]| 	ext{ is “negligible.”}
\]
Combining MAC and Enc (CCA)

Encryption key \( k_E \).

MAC key = \( k_I \)

Option 1: (SSL)

\[
\text{msg m} \quad \rightarrow \quad \text{msg m} \quad \rightarrow \quad \text{tag}
\]

\[
E(k_E, m) \quad \rightarrow \quad \text{tag}
\]

E(k_E, m\|\text{tag})

Option 2: (IPsec)

Option 3: (SSH)

Always correct
Standards (at a high level)

- **GCM**: CTR mode encryption then CW-MAC
  (accelerated via Intel’s PCLMULQDQ instruction)

- **CCM**: CBC-MAC then CTR mode encryption (802.11i)

- **EAX**: CTR mode encryption then CMAC

All support AEAD: (auth. enc. with associated data). All are nonce-based.
An example API (OpenSSL)

```c
int AES_GCM_Init(AES_GCM_CTX *ain,
                 unsigned char *nonce, unsigned long noncelen,
                 unsigned char *key, unsigned int klen )

int AES_GCM_EncryptUpdate(AES_GCM_CTX *a,
                           unsigned char *aad, unsigned long aadlen,
                           unsigned char *data, unsigned long datalen,
                           unsigned char *out, unsigned long *outlen)
```
OCB: a direct construction from a PRP

More efficient authenticated encryption: one $E()$ op. per block.

$$m[0] \oplus P(N,k,0) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow P(N,k,0) \rightarrow \oplus \rightarrow c[0]$$

$$m[1] \oplus P(N,k,1) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow P(N,k,1) \rightarrow \oplus \rightarrow c[1]$$

$$m[2] \oplus P(N,k,2) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow P(N,k,2) \rightarrow \oplus \rightarrow c[2]$$

$$m[3] \oplus P(N,k,3) \rightarrow \oplus \rightarrow E(k, \cdot) \rightarrow P(N,k,3) \rightarrow \oplus \rightarrow c[3]$$

checksum $\oplus$ $\oplus$ $\oplus$ $\oplus$

auth $\oplus$

$c[4]$
802.11b WEP: how not to do it

Previously discussed problems:
- two time pad and related PRG seeds
Active attacks

**Fact:** CRC is linear, i.e. \( \forall m, p : \text{CRC}(m \oplus p) = \text{CRC}(m) \oplus \text{F}(p) \)

WEP ciphertext:

attacker:

\[
\begin{array}{c}
\text{IV} \quad \text{dest-port = 80} \quad \text{data} \quad | \quad \text{CRC} \oplus \\
\quad 000 \ldots .00 \ldots XX\ldots 0000 \ldots \quad | \quad \text{F}(XX)
\end{array}
\]

\(XX = 25 \oplus 80\)

Upon decryption: CRC is valid, but ciphertext is changed !!