Lecture 6: Authenticated Encryption

Viet Tung Hoang
1. AE and Its Security Definitions

2. Failed Ways to Build AE

3. Generic Compositions
So Far

Transfer $5 to account 12345

Privacy

Encryption scheme

Authenticated Encryption
Achieve both of these aims

Authenticity

MAC
Authenticated Encryption (AE)

Begin with two **realizations**

1. Authenticity is routinely needed/assumed
2. "Standard" privacy mechanisms don’t provide it

Provide an easier-to-correctly-use abstraction boundary
AE Syntax

Key Gen

$K \xrightarrow{\$} K$

Encrypt

$M \xrightarrow{\$} C$

$K \xrightarrow{}$ Decryption may reject invalid ciphertexts

Decrypt

$C \xrightarrow{}$
Defining Security for AE

- Use Left-or-Right security for privacy

**Auth $\mathcal{E}$**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Initialize()</code></td>
<td>$K \leftarrow \mathcal{K}$</td>
</tr>
<tr>
<td><code>Enc(M)</code></td>
<td>Return $\mathcal{E}_K(M)$</td>
</tr>
<tr>
<td><code>Finalize(C')</code></td>
<td>Return $(\mathcal{D}_K(C') \neq \bot)$</td>
</tr>
</tbody>
</table>

\[
\text{Adv}^{\text{auth}}_{\mathcal{T}}(A) = \Pr[\text{Auth}^A_{\mathcal{E}} \Rightarrow 1]
\]
Agenda

1. AE and Its Security Definitions

2. Failed Ways to Build AE

3. Generic Compositions
Plain Encryption Doesn’t Provide Authenticity

Question: Does CBC provide authenticity?

Answer: No, because any ciphertext has valid decryption
A Bad Fix: CBC with Redundancy

On decryption, verify the decrypted last block is zero.

**Question**: Break the authenticity of this scheme with a single Enc query
An Attack

\[ C_0 \rightarrow M_1 \rightarrow 0^n \rightarrow \text{Enc} \rightarrow C_0 \rightarrow C_1 \rightarrow C_2 \]
Complex Redundancy Doesn’t Help

Some (unkeyed) “redundancy” function, such as checksum

The redundancy is verified upon decryption

**Question:** Break the authenticity of this scheme with a single Enc query
An Attack
A Case Study: WEP

IV is a part of the ciphertext

Used in IEEE WiFi standard

Question: Break the authenticity of this scheme with a single Enc query
An Attack

\[(M \| \text{CRC}(M)) \oplus (M' \| \text{CRC}(M')) = C \oplus C'\]
Agenda

1. AE and Its Security Definitions

2. Failed Ways to Build AE

3. Generic Compositions
Constructing AE: Generic Composition

A good PRF, such as Encrypted CBC-MAC

Privacy-only encryption (such as CTR/CBC)

Compose them to build AE

<table>
<thead>
<tr>
<th>Method</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt-and-MAC</td>
<td>SSH</td>
</tr>
<tr>
<td>MAC-then-Encrypt</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>Encrypt-then-MAC</td>
<td>IPSec</td>
</tr>
</tbody>
</table>
Encrypt-and-MAC: Simple Composition

No privacy: encrypting the same message results in the same tag
No authenticity if one can modify $C$ such that decryption is unchanged.

for some bad encryption scheme
Encrypt-and-MAC in SSH

\[ M \]

Encode

\[ \text{len}(M) || \text{len}(\text{pad}) \]

\[ M \quad \text{pad} \]

CBC

\[ C \]

Privacy | Authenticity
--- | ---
Yes | Yes

\[ F_{K_m} \]

\[ T \]
MAC-then-Encrypt

\[ M \rightarrow F_{K_m} \rightarrow M \rightarrow T \rightarrow E_{K_e} \rightarrow C \]

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Authenticity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

for some bad encryption scheme

No authenticity if one can modify \( C \) such that decryption is unchanged.
MAC-then-Encrypt in SSL

\[ M \xrightarrow{F_{K_m}} M \xrightarrow{T} CBC \xrightarrow{} C \]

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Authenticity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Encrypt-then-MAC

\[ M \xrightarrow{\mathcal{E}_{K_e}} C \xrightarrow{F_{K_m}} T \]

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Authenticity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>