Lecture 6: Authenticated Encryption

Viet Tung Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.
Agenda

1. AE and Its Security Definitions

2. Failed Ways to Build AE

3. Generic Compositions
So Far

Privacy
- Encryption scheme

Authenticated Encryption
- Achieve **both** of these aims

Authenticity
- MAC

Transfer $5 to account 12345
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

\[ \mathcal{K} \rightarrow K \]

Encrypt

\[ M \rightarrow \mathcal{E} \rightarrow C \]

Decrypt

\[ C \rightarrow \mathcal{D} \rightarrow \begin{cases} M \text{ or } \bot \end{cases} \]

Decryption may reject invalid ciphertexts
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>Initialize()</td>
<td>$K \leftarrow \mathcal{K}$ Return $\mathcal{E}_K(M)$</td>
</tr>
<tr>
<td>Enc$(M)$</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

$C_0 \quad C_1 \quad C_2 \quad C_3$

$M_1 \quad 0^n$

$E_K$ $E_K$ $E_K$

$C_1 \quad C_2 \quad C_3$

$E_K^{-1}$ $E_K^{-1}$

$C_1 \quad C_2$

$M_1 \quad 0^n$
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

\[ \begin{align*}
&\text{Enc} \\
C_0 & \quad C_1 & \quad C_2 & \quad C_3 \\
M & \quad M_1 & \quad h(M_1) \\
C_0 & \quad C_1 & \quad C_2 \\
\end{align*} \]
A Case Study: WEP

Used in IEEE WiFi standard

IV is a part of the ciphertext

```
<table>
<thead>
<tr>
<th>IV</th>
<th>K</th>
<th>RC4</th>
<th>CRC(M)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

\[ M \]

Encode

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

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

CBC

\[ C \]

\[ F_{K_m} \]

\[ T \]
MAC-then-Encrypt

Privacy | Authenticity
---|---
Yes | No

for some bad encryption scheme

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

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

<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

\[ M \rightarrow \mathcal{E}_{K_e} \rightarrow C \]

\[ F_{K_m} \rightarrow T \]

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