Message Authentication

Sven Laur
University of Tartu
Formal Syntax
Symmetric message authentication

A randomised **key generation algorithm** outputs a secret key $sk \in K$ that must be transferred privately to the sender and to the receiver.

A **keyed hash function** $Mac_{sk} : M \rightarrow T$ takes in a plaintext and outputs a corresponding *digest* (also known as *hash value* or *tag*).

A **verification algorithm** $Ver_{sk} : M \times C \rightarrow \{0, 1\}$ tries to distinguish between altered and original message pairs.

The authentication primitive is **functional** if for all $sk \leftarrow Gen$ and $m \in M$:

$$Ver_{sk}(m, Mac_{sk}(m)) = 1$$
Two main attack types

**Substitution attacks.** An adversary substitutes \((m, t)\) with a different message pair \((\overline{m}, \overline{t})\). An adversary succeeds in *deception* if

\[
\text{Ver}_{sk}(\overline{m}, \overline{t}) = 1 \quad \text{and} \quad m \neq \overline{m}.
\]

**Impersonation attacks.** An adversary tries to create a valid message pair \((\overline{m}, \overline{t})\) without seeing any messages from the sender. An adversary succeeds in *deception* if

\[
\text{Ver}_{sk}(\overline{m}, \overline{t}) = 1.
\]
Maximal resistance against substitutions

For clarity, assume that $\mathcal{M} = \{0, 1\}$, $\mathcal{K} = \{0, 1, 2, 3\}$ and the key is chosen uniformly $sk \leftarrow \mathcal{K}$. Then the keyed hash function can be viewed as a table.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>1</td>
<td>e</td>
<td>f</td>
<td>g</td>
<td>h</td>
</tr>
</tbody>
</table>

If $a$, $b$, $c$ and $d$ are all different, then the pair $(0, t)$ reveals the key $sk$ and substitution becomes trivial. Hence, the optimal layout is following.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>a</td>
<td>a</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>1</td>
<td>a</td>
<td>b</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>
Maximal resistance against impersonation

Again, assume that $\mathcal{M} = \{0, 1\}$, $\mathcal{K} = \{0, 1, 2, 3\}$ and $sk \leftarrow \mathcal{K}$. Then the following keyed hash function achieves maximal impersonation resistance.

$$
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
0 & a & b & c & d \\
1 & a & b & c & d \\
\end{array}
$$

However, this keyed hash function is insecure against substitution attacks.

**Conclusion.** Security against substitution attacks and security against impersonation attacks are contradicting requirements.
Information Theoretical Security
Authentication as hypothesis testing

The procedure $\text{Ver}_{sk}(\cdot)$ must distinguish between two hypotheses.

- $\mathcal{H}_0$: The pair $c = (m, t)$ is created by the sender.
- $\mathcal{H}_1$: The pair $c = (\overline{m}, \overline{t})$ is created by the adversary $\mathcal{A}$.

Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the corresponding distributions of messages.

Since the ratio of false negatives $\Pr[\text{Ver}_{sk}(m, t) = 0]$ must be zero, the optimal verification strategy is the following

$$\text{Ver}_{sk}(c) = 1 \iff c \in \text{supp}(\mathcal{C}_0)$$

To defeat the message authentication primitive, the adversary $\mathcal{A}$ must chose the distribution $\mathcal{C}_1$ such that the ratio of false positives is maximal.
Kullback-Leibler divergence

Let \((p_x)_{x \in \{0,1\}^*}\) and \((q_x)_{x \in \{0,1\}^*}\) be probability distributions corresponding to hypotheses \(\mathcal{H}_0\) and \(\mathcal{H}_1\). Then Kullback-Leibler divergence is defined as

\[
d(p \parallel q) = \sum_{x : p_x > 0} p_x \cdot \log_2 \frac{p_x}{q_x},
\]

Note that Jensen’s inequality assures

\[
-d(p \parallel q) = \sum_{x : p_x > 0} p_x \cdot \log_2 \frac{q_x}{p_x} \leq \log_2 \left( \sum_{x : p_x > 0} q_x \right)
\]

and consequently

\[
\sum_{x : p_x > 0} q_x \geq 2^{-d(p \parallel q)}.
\]
Lower bound on false positives

Fix a target message $\overline{m}$. Then by construction

$$\Pr \left[ \text{Ver}_{sk}(\overline{m}, \overline{t}) = 1 \right] = \sum_{p_{t,sk} > 0} q_{t,sk} \geq 2^{-d(p\|q)}$$

where

$$p_{t,sk} = \Pr \left[ sk \leftarrow \text{Gen} : sk \land \text{The sender creates } \overline{t} \text{ for } \overline{m} \right]$$
$$q_{t,sk} = \Pr \left[ sk \leftarrow \text{Gen} : sk \land \text{The adversary creates } \overline{t} \text{ for } \overline{m} \right]$$
Simplest impersonation attack

Consider the following attack

\[ A_{\overline{m}} \]
\[ \begin{align*} &\overline{sk} \leftarrow \text{Gen} \\ &\overline{t} \leftarrow \text{Mac}_{\overline{sk}}(\overline{m}) \\ &\text{return } (\overline{m}, \overline{t}) \end{align*} \]

Then obviously

\[ \Pr [\overline{t}] = \sum_{\overline{sk}} \Pr [\overline{sk} \leftarrow \text{Gen} : \overline{sk} = \overline{sk}] \cdot \Pr [\overline{t} \leftarrow \text{Mac}_{\overline{sk}}(\overline{m})] \]

is a marginal distribution of \( \overline{t} \) generated by the sender.
Success probability

As \( q_{sk,t} = p_{sk} \cdot p_t \) the Kullback-Leibler divergence can be further simplified

\[
d(p \parallel q) = \sum_{sk,t} p_{t,sk} \cdot \log_2 \frac{p_{t,sk}}{p_{sk} \cdot p_t}
\]

\[
= \sum_{sk,t} p_{t,sk} \cdot \log_2 p_{t,sk} - \sum_{sk,t} p_{t,sk} \log_2 p_{sk} - \sum_{sk,t} p_{t,sk} \cdot \log_2 p_t
\]

\[
= -H(sk, t) + H(sk) + H(t)
\]

and thus

\[
\Pr[\text{Successful impersonation}] \geq 2^{H(sk,t) - H(sk) - H(t)} = 2^{-I(sk:t)}
\]

for a fixed target message \( \overline{m} \).
An obvious substitution attack

To replace $m$ with $\overline{m}$, we can use the following strategy:

$$A(m, t, \overline{m})$$

$$\begin{cases} 
\text{sk}_* \leftarrow \text{argmax} \Pr [\text{sk} \leftarrow \text{Gen} : \text{sk} = \overline{\text{sk}}|m, t] \\
\overline{t} \leftarrow \text{Mac}_{\text{sk}_*}(\overline{m}) \\
\text{return } (\overline{m}, \overline{t}) 
\end{cases}$$

Obviously, the adversary $A$ succeeds if it guesses the key $\text{sk}$

$$\Pr \text{ [Success]} \geq \Pr [\text{sk} \leftarrow \text{Gen} : \text{sk} = \text{sk}_*]$$

$$\geq \sum_t \Pr [t = \text{Mac}_{\text{sk}}(m)] \cdot \max_{\overline{\text{sk}}} \Pr [\text{sk} = \overline{\text{sk}}|t] .$$
Properties of conditional entropy

Note that for any distribution \((p_x)_{x \in \{0,1\}}^\ast\)

\[
H_\infty(X) = -\log_2 \left( \max_{x: p_x > 0} p_x \right) = \min_{x: p_x > 0} \left( -\log_2 p_x \right)
\]

\[
\leq \sum_{x: p_x > 0} p_x \cdot \left( -\log_2 p_x \right) = H(X).
\]

Now for two variables

\[
\sum_y \Pr[y] \cdot \max_x \Pr[x|y] = \sum_y \Pr[y] \cdot 2^{-H_\infty(X|y)} \geq \sum_y \Pr[y] \cdot 2^{-H(X|y)}
\]

\[
\geq 2 \sum_y \Pr[y] \cdot (-H(X|y)) = 2^{-H(X|Y)},
\]

where the second inequality follows from Jensen’s inequality.
Lower bound on success probability

As the success probability of our impersonation attack is

\[
\Pr [\text{Success}] = \Pr [sk \leftarrow \text{Gen} : sk = sk_*]
\]

\[
= \sum_t \Pr [t = \text{Mac}_{sk}(m)] \cdot \max_{sk} \Pr [sk = \overline{sk} | t]
\]

we can rewrite in terms of conditional entropy

\[
\Pr [\text{Success}] \geq 2^{-H(sk | t)}.
\]
Simmons's lower bounds

For any message authentication primitive

\[
\Pr[\text{Successful impersonation}] \geq \max_{m \in \mathcal{M}} \left\{ 2^{-I(\text{sk}:t)} \right\}
\]

\[
\Pr[\text{Successful substitution}] \geq \max_{m \in \mathcal{M}} \left\{ 2^{-H(\text{sk}|t)} \right\}
\]

and thus

\[
\Pr[\text{Successful attack}] \geq \max_{m \in \mathcal{M}} \left\{ 2^{-\min\{I(\text{sk}:t),H(\text{sk}|t)\}} \right\} \geq \max_{m \in \mathcal{M}} \left\{ 2^{-\frac{H(\text{sk})}{2}} \right\}
\]

since \( I(\text{sk} : t) = H(\text{sk}) + H(t) - H(\text{sk}, t) = H(\text{sk}) - H(\text{sk}|t). \)
Examples
Universal hash functions

A universal hash function \( h : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{T} \) is a keyed hash function such that for any two different inputs \( m_0 \neq m_1 \), the corresponding hash values \( h(m_0, k) \) and \( h(m_1, k) \) are independent and have a uniform distribution over \( \mathcal{T} \) when \( k \) is chosen uniformly from \( \mathcal{K} \).

**Corollary.** An authentication protocol that uses a universal hash function \( h \) achieves maximal security against impersonation and substitution attacks

\[
\Pr \left[ \text{Successful deception} \right] \leq \frac{1}{|\mathcal{T}|}
\]

**Example.** A function \( h(m, k_0||k_1) = k_1 \cdot m + k_0 \) is a universal hash function if \( \mathcal{M} = \text{GF}(2^n) \), \( \mathcal{K} = \text{GF}(2^n) \times \text{GF}(2^n) \) and operations are done in \( \text{GF}(2^n) \).
Polynomial message authentication code

Let \( m_1, m_2, \ldots, m_\ell \) be \( n \)-bit blocks of the message and \( k_0, k_1 \in \text{GF}(2^n) \) sub-keys for the hash function. Then we can consider a polynomial

\[
f(x) = m_\ell \cdot x^\ell + m_{\ell-1} \cdot x^{\ell-1} + \cdots + m_1 \cdot x
\]

over \( \text{GF}(2^n) \) and define the hash value as

\[
h(m, k) = f(k_1) + k_0.
\]

If \( k_0 \) is chosen uniformly over \( \text{GF}(2^n) \) then the hash value \( h(m, k) \) is also uniformly distributed over \( \text{GF}(2^n) \):

\[
\Pr[\text{Successful impersonation}] \leq 2^{-n}.
\]
Security against substitution attacks

Let $\mathcal{A}$ be the best substitution strategy. W.l.o.g. we can assume that $\mathcal{A}$ is a deterministic strategy. Consequently, we have to bound the probability

$$\max_{m \in \mathcal{M}} \Pr \left[ k \leftarrow \mathcal{K}, (\overline{m}, \overline{t}) \leftarrow \mathcal{A}(m, h(m, k)) : h(\overline{m}, k) = \overline{t} \land m \neq \overline{m} \right] .$$

Since $\mathcal{A}$ outputs always the same reply for $k \in \mathcal{K}$ such that $h(m, k) = t$, we must find cardinalities of the following sets:

- a set of all relevant keys $\mathcal{K}_{\text{all}} = \{ k \in \mathcal{K} : h(m, k) = t \}$
- a set of good keys $\mathcal{K}_{\text{good}} = \{ k \in \mathcal{K} : h(m, k) = t \land h(\overline{m}, k) = \overline{t} \}.$
Some algebraic properties

For each $m$, $t$ and $k_1$, there exists one and only one value of $k_0$ such that $h(m, k) = t$. Therefore, $|\mathcal{K}_{\text{all}}| = 2^n$ for any $m$ and $t$.

If $h(m, k) = t$ and $h(\overline{m}, k) = \overline{t}$ then

\[
\begin{align*}
  h(m, k) - h(\overline{m}, k) - t + \overline{t} &= 0 \\
  \quad \uparrow \\
  f_m(k_1) - f_{\overline{m}}(k_1) - t + \overline{t} &= 0 \\
  \quad \uparrow \\
  f_{m-\overline{m}}(k_1) - t + \overline{t} &= 0
\end{align*}
\]

This equation has at most $\ell$ solutions $k_1 \in \text{GF}(2^n)$, since degree of $f_{m-\overline{m}}(x)$ is at most $\ell$. Since $k_1$, $m$, $t$ uniquely determine $k_0$, we get $|\mathcal{K}_{\text{good}}| \leq \ell$. 
The corresponding bounds

Hence, we have obtained

$$\Pr \left[ k \leftarrow \mathcal{K} : h(\overline{m}, k) = \overline{t} \mid m \neq \overline{m}, t \right] = \frac{|\mathcal{K}_{\text{good}}|}{|\mathcal{K}_{\text{all}}|} \leq \frac{\ell}{2^n}.$$  

Since

$$\Pr \left[ k \leftarrow \mathcal{K}, (\overline{m}, \overline{t}) \leftarrow A(m, h(m, k)) : h(\overline{m}, k) = \overline{t} \land m \neq \overline{m} \right]$$

$$\leq \sum_{t} \Pr \left[ k \leftarrow \mathcal{K} : h(m, k) = t \right] \cdot \max_{\substack{m \neq m \\overline{t} \in T}} \Pr \left[ h(\overline{m}, k) = \overline{t} \mid m \neq \overline{m}, t \right]$$

$$\leq \sum_{t} \Pr \left[ k \leftarrow \mathcal{K} : h(m, k) = t \right] \cdot \frac{\ell}{2^n} \leq \frac{\ell}{2^n},$$

we also have a success bound on substitution attacks.
Computational Security
Authentication with pseudorandom functions

Consider following authentication primitive:

- secret key $f \leftarrow_u \mathcal{F}_{\text{all}}$ where $\mathcal{F}_{\text{all}} = \{f : \mathcal{M} \to \mathcal{T}\}$;
- authentication code $\text{Mac}_f(m) = f(m)$
- verification procedure $\text{Ver}_f(m, t) = 1 \iff f(m) = t$.

This authentication primitive is $\frac{1}{|\mathcal{T}|}$ secure against impersonation and substitution attacks, since Mac is a universal hash function.

As this construction is practically uninstantiable, we must use $(t, q, \varepsilon)$-pseudorandom function family $\mathcal{F}$ instead of $\mathcal{F}_{\text{all}}$. As a result

$$\Pr[\text{Successful attack}] \leq \frac{1}{|\mathcal{T}|} + \varepsilon$$

against all $t$-time adversaries if $q \geq 1$. 

Formal security definition

A keyed hash function \( h : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{T} \) is a \((t, q, \varepsilon)\)-secure message authentication code if any \( t \)-time adversary \( A \):

\[
\text{Adv}_h^{\text{mac}}(A) = \Pr [G^A = 1] \leq \varepsilon ,
\]

where the security game is following

\[
G^A
\]

\[
\begin{cases}
k \leftarrow_u \mathcal{K} \\
\text{For } i \in \{1, \ldots, q\} \text{ do} \\
\text{[Given } m_i \leftarrow A \text{ send } t_i \leftarrow h(m_i, k) \text{ back to } A] \\
(m, t) \leftarrow A \\
\text{[return } t \overset{?}{=} h(m, k) \land (m, t) \notin \{(m_1, t_1), \ldots, (m_q, t_q)\}] 
\end{cases}
\]
Problems with multiple sessions

All authentication primitives we have considered so far guarantee security if they are used only once. A proper message authentication protocol can handle many messages. Therefore, we use additional mechanisms besides the authentication primitive to assure:

- security against reflection attacks
- message reordering
- interleaving attacks

Corresponding enhancement techniques

- Use nonces to defeat reflection attacks.
- Use message numbering against reordering.
- Stretch secret key using pseudorandom generator.