MAC and HMAC

29 November 2019 19:00

MESSAGE AUTHENTICATION CODES

also called as "CRYPTOGRAPHIC CHECKSUMS".

Alice — SECURE CHANNEL — Bob (K)

$m' = MAC_K(x)$ ← (x, m) — $m = MAC_K(x)$

check if $m' = m$

PROPERTIES of MACs:

1. Arbitrary Input length
2. Fixed output length
3. Message Authentication: Alice is certain that Bob sent the message.
4. Integrity: Manipulations in transit will be detected by ALICE.
5. Non-Repudiation is NOT given
   - offers no protection if Alice and Bob try to CHEAT each other

MACs from HASH FUNCTIONS:

Basic Idea:

$$m = MAC_K(x) = h(k, x)$$

Q: how exactly do we combine (concatenate) k, x?

(a) $m = h(K \| x)$ → SECRET PREFIX

(aa) $m = h(x \| K)$ → SECRET SUFFIX

SECRET PREFIX MAC's

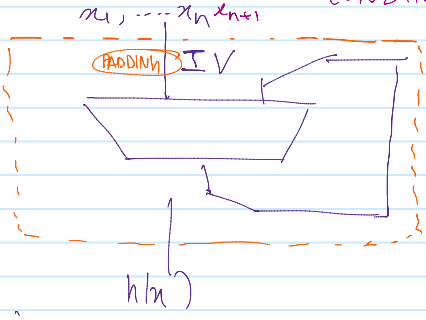
assume

$$X = (x_1 \| x_2 \| \ldots \| x_n)$$

(input width of hash function eg 512 bit)

$$m = h(K \| x) = h(K \| x_1 \| x_2 \| \ldots \| x_n)$$

Most hash functions use MERKLE-DAMGARD CONSTRUCTION



ATTACK:

OSCAR — Bob

(x, m) — $m = h(k \| x_1 \| x_2 \| \ldots \| x_n)$

$x_0 = (x_1, \ldots x_n, x_{n+1})$

↳ generate x_{n+1} on its own

HMAC CONSTRUCTION

→ proposed in 1996

→ widely used in practice eg: SSL/TLS

IDEA: use 2 nested secret prefix MACs.

Roughly,

$$h(K \| h(K \| x))$$

(outer hash ↑, inner hash)

in reality,

$$HMAC_K(x) = h((\bar{K} \oplus opad) \| h(\bar{K} \oplus ipad) \| x)$$

$k^+ \rightarrow$ 000..... 0 1 1 K

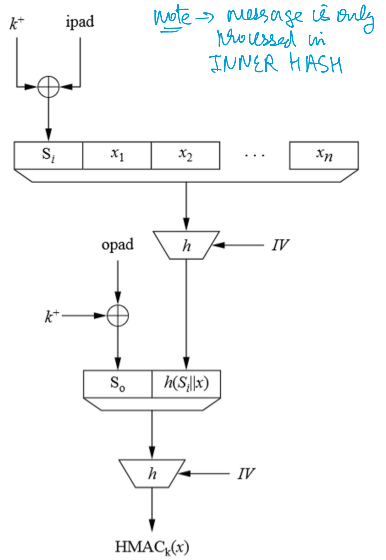
← HASH INPUT LENGTH eg 512 bit

ipad = 0011 0110, ..., 0011 0110

← HASH INPUT LENGTH →

opad = 0101 1100, ..., 0101 1100

← HASH INPUT LENGTH →



$m_0 = h|_{IV=M}(x_{n+1})$

$\downarrow (x_0, m_0)$

$m' = h(K \| x_1 \| \dots \| x_{n+1})$

$m' \stackrel{?}{=} M$

Remark:
Attack does not work if padding with length information is being used.

SECRET SUFFIC MACS:

$m = h(x \| k)$

assume Oscar can find collisions ie
$h(x) = h(x_0)$

$h(x \| k) = h(x_0 \| k) \quad (= m)$

$\Rightarrow$ comparing Brute force effort with collission finding method.

e.g. $h() \rightarrow$ SHA 1 (160 bit output)
$|k| = 128$ bit
↳ we expect attack complexity of 2^{128}.

because of the birthday paradox, collision search takes $\approx \sqrt{2^{160}} = 2^{80}$ steps