PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5812 di Mercoledì 19 marzo 2025

Cosa è un MAC?

Continuando nell'analisi dei preziosi documenti messi a disposizione dalla agenzia per la cybersicurezza nazionale, passiamo ad analizzare cosa sono i codici di autenticazione di messaggi, nel quadro delle linee guida per le funzioni crittografiche.

Quando ognuno di noi riceve un messaggio elettronico, si preoccupa, oppure dovrebbe preoccuparsi, di verificare due aspetti fondamentali:

- che il messaggio elettronico sia stato effettivamente spedito da chi dichiara di averlo spedito,
- che il contenuto del messaggio elettronico non sia stato alterato.

Nell'ambito crittografico, lo strumento che garantisce l'autenticazione di un messaggio viene chiamato con l'acronimo MAC (message authentication code, oppure codice di autenticazione del messaggio).

Si tratta di due funzioni separate, che però possono essere risolte con un applicativo integrato. Appare evidente che l'applicativo deve essere debitamente protetto da attacchi illeciti, in quanto questi attacchi potrebbero compromettere in modo significativo la validità del messaggio, a livello di contenuto e di mittente.

Pubblicità

Ecco il motivo per cui l'agenzia per la cybersicurezza nazionale ha messo a disposizione questo manuale, che offre indicazioni sui migliori algoritmi da utilizzare per la generazione di MAC.

La garanzia di identità del mittente viene assicurata dell'utilizzo di una chiave segreta condivisa: il mittente, usando la chiave, genera un MAC, che viene inviato congiuntamente al messaggio stesso. Il destinatario, partendo dal messaggio e dalla chiave segreta conosciuta, genere un altro MAC e lo confronta con quello ricevuto. Se i due MAC coincidono, viene garantita l'identità del mittente. Lo stesso applicativo consente evidentemente di verificare anche l'integrità del messaggio e mette in evidenza possibili alterazioni.

L'esperienza ha mostrato che le principali tipologie di attacco, cui i MAC sono soggetti, sono legate alla contraffazione, cioè alla generazione di un MAC valido per un messaggio, anche senza essere in possesso della chiave segreta. Perché l'attaccante possa portare a termine questa tipologia di attacco, egli deve avere a disposizione un certo numero di messaggi, dai quali potrebbe estrarre le informazioni necessarie per individuare la chiave segreta e creare un MAC.

Un'altra tipologia di attacco, alquanto più rozza, ma spesso efficace, permette all'attaccante di contraffare un MAC in forma casuale, provando ad autenticare il messaggio con esso (attacco per forza bruta).

Successivamente il manuale passa ad illustrare gli algoritmi raccomandati, che sono i seguenti:

- HMAC (Hash-based Message Authentication Code)
- CMAC (Cipher-based Message Authentication Code)
- GMAC (Galois Message Authentication Code).

Non ci addentriamo nell'analisi di questi algoritmi, in quanto il manuale è tanto sintetico, quanto chiaro.

Nel paragrafo conclusivo, la ACN raccomanda, per raggiungere un adeguato livello di sicurezza, di utilizzare una chiave segreta di almeno 128 bit, in modo da rendere particolarmente difficile la individuazione e la duplicazione. Solo in casi particolari può essere consentito l'utilizzo di una chiave di lunghezza inferiore.

Come di consueto, il manuale è accompagnato da una ricchissima bibliografia, che permette ai lettori di approfondire temi specifici.

Agenzia per la Cybersicurezza Nazionale - Linee Guida Funzioni Crittografiche - Codici di Autenticazione di Messaggi (MAC)

Adalberto Biasiotti

Leggi gli articoli con le altre linee guida:

Cybersicurezza: Linee guida funzioni criptografiche
I computer quantistici: un aiuto ed una minaccia
Cybersicurezza: Linee guida conservazione delle password
Cybersicurezza: Linee guida Cifrari a Blocchi

Licenza Creative Commons