Vulnerable MAC CTF Design Proposal and Implementation

Table of contents

1 Introduction

大部分的 MAC 是針對 fixed-length 訊息設計的。然而，有時候，我們需要對不同長度的訊息進行 MAC 驗證。在這種情況下，我們可以做 domain extension。常見的方法是將 message 分段，然後對每個分段進行 HMAC 或 NMAC 驗證。

let π' = (Gen', Mac', Vrfy') be fixed length msg Mac. (n-bits)

let π = (Gen, Mac, Vrfy) be variable length msg Mac. (arbitrary length)

$Gen(n)$: identical to Gen'(n) $\rightarrow$ k $\in \{0,1\}^n$

$Mac(k, m)$: k $\in \{0,1\}^n$, m $\in \{0,1\}^*$

$Vrfy(k, m, t)$: k $\in \{0,1\}^n$, m $\in \{0,1\}^*$, t $\in \{0,1\}^n$

(i) Parse m into d blocks $(m_1, m_2, ...m_d)$ where each of length $\frac{n}{4}$. Note that the last one can be padded by 0s

(ii) choose a uniform r $\in \{0,1\}^{\frac{n}{4}}$

(iii) for i = 1, 2, ... d, $t_i \leftarrow Mac_k$' $(r \parallel l \parallel i \parallel m_i)$, output $t = (r, t_1, ...t_d)$

過程中的 r, l, i 缺一則會使 MAC 變得不安全。

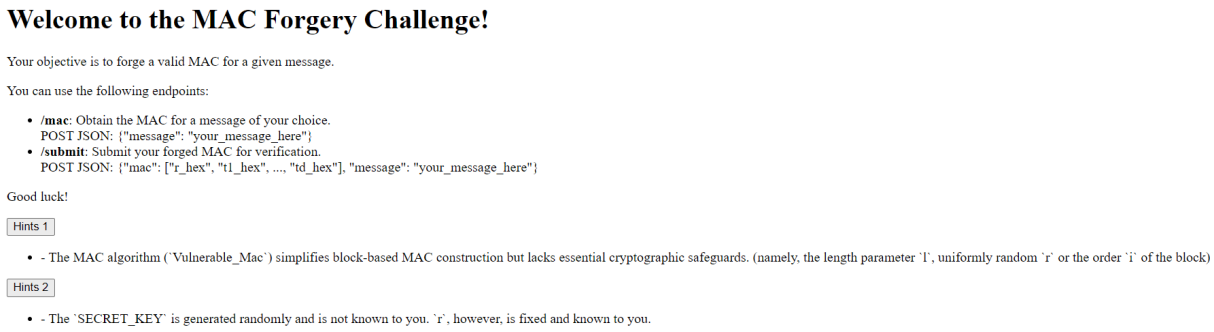
1.1 Goal

利用缺少 r, l 或 i 的產生的漏洞設計 CTF。

2 Implementation

使用者可以訪問一個生成給定訊息的 MAC 的 MAC oracle。該 MAC 是使用一個易受攻擊的 MAC 實現生成的(缺少 l)。使用者可以為尚未向 MAC oracle 查詢的訊息提交偽造的 MAC。如果 MAC 有效，伺服器將回應 flag。否則，伺服器將回應錯誤訊息。在 main page 上，使用者可以選擇性的查看 hint，以幫助他們得到 flag。

2.1 Main Page



Welcome to the MAC Forgery Challenge!

Your objective is to forge a valid MAC for a given message.

You can use the following endpoints:

- **/mac**: Obtain the MAC for a message of your choice.
  POST JSON: {"message": "your_message_here"}
- **/submit**: Submit your forged MAC for verification.
  POST JSON: {"mac": ["r_hex", "t1_hex", ..., "td_hex"], "message": "your_message_here"}

Good luck!

Hints 1

- - The MAC algorithm (`Vulnerable_Mac`) simplifies block-based MAC construction but lacks essential cryptographic safeguards. (namely, the length parameter `l`, uniformly random `r` or the order `i` of the block)

Hints 2

- - The `SECRET_KEY` is generated randomly and is not known to you. `r`, however, is fixed and known to you.

Figure 1: Main Page

2.2 Endpoints

/mac: 使用者可以訪問 MAC oracle 並提交訊息以獲取 MAC。

/submit: 使用者可以提交偽造的 MAC 以獲取 flag。

3 Team Members

110590005 蕭耕宏

112C53035 王煥昇

113C53006 吳仲霖

113598043 張育丞

113598088 李以謙

4 Links

Figure 2: Repository

Figure 3: Demo