Boston Key Party CTF 2014 Crypto 200 MITM II: Electric Boogaloo

Mon, 03 March 2014 in crypto,
0 Comments

BKPCTF , MITM

這題還滿簡單的
解法就是題目名稱 = =
可是不知道為什麼很少人解出來
可能是太晚出來被大家忽略吧 0.0

題目敘述如下：

> *Chisa and Arisu are trying to tell each other two halves of a very important secret! They think they're safe, because they know how cryptography works---but can you learn their terrible, terrible secret? They're available as services at 54.186.6.201:12346 and 54.186.6.201:12345 respectively.*
> *http://bostonkeyparty.net/challenges/mitm2-632e4ecc332baba0943a0c6471dec2c6.tar.bz2*

附檔是環境的 source code
分析後發現目標會有以下行為：

1. 接收 username 並檢查是不是對方名稱 如果錯誤則結束
2. 生成 secretkey 和 publickey ，將 publickey 傳送給對方
3. 接收對方的 publickey，用自己的 secretkey 和 對方的 publickey 生成 aeskey
4. 將 CHECK 中的奇數(或偶數)字元以 aeskey 加密後傳送給對方
5. 用 aeskey 解密訊息，並檢查收到的 CHECK 是否正確，如果有錯誤則結束
6. 用 aeskey 加密 flag，並傳送給對方，以及解密對方傳來的 flag

MITM attack 簡單的說就是
原本是 A ⟷ B 之間傳遞訊息
變成 A ⟷ C ⟷ B 由 C 攔截後並轉送訊息
因為接收 publickey 之後沒有確認來源 (所以需要數位簽章)
所以我們可以在中間攔截並偽造 publickey

所以這題的解法為：

1. 向雙方送正確的 username，アリスです 和 千佐だよ
2. 生成 fake secret key (fseckey) and public key (fpubkey)，並傳送 fpubkey 給雙方
3. 用接收到的 pubkeyA & pubkeyB 和 fseckey 生成 aeskeyA & aeskeyB
4. 用 aeskeyA 解密 A 傳來的 CHECK，並以 aeskeyB 加密傳送給 B
5. 用 aeskeyB 解密 B 傳來的 CHECK，並以 aeskeyA 加密傳送給 A
6. 用 aeskeyA & aeskeyB 解密 flag

Powered by Pelican.
Theme mg by Luca Chiricozzi.