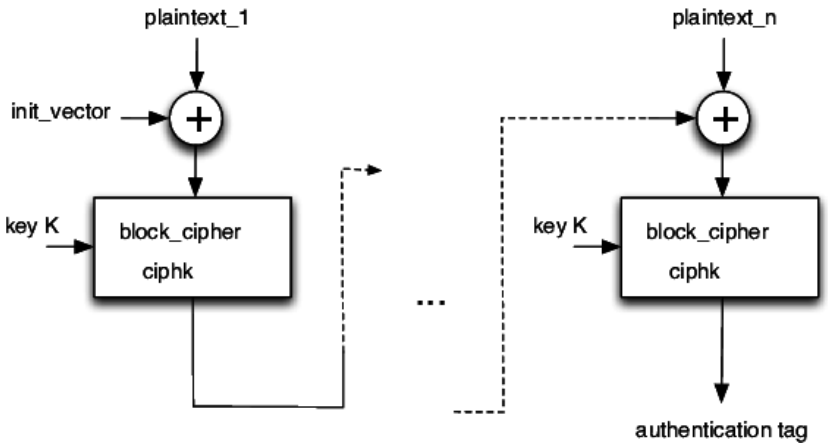
Universidade do Minho
Escola de Engenharia

Criptografia

TP4



João Miguel da Silva Alves (83624)

Paulo Jorge Alves (84480)

MESTRADO INTEGRADO EM ENGENHARIA BIOMÉDICA

INFORMÁTICA MÉDICA 2020/2021

1. Ataque ao CBC-MAC utilizando um IV aleatório

O protocolo CBC-MAC pode ser enfraquecido se em vez de se usar um valor fixo para o IV, usualmente uma string de zeros, torná-lo um valor aleatório. Isto acontece, uma vez que o resultado que vai utilizado na primeira block-cipher corresponde ao valor do XOR entre o IV aleatório e o primeiro bloco da mensagem. Desta forma, se numa primeira situação temos um determinado bloco de mensagem que ao fazer XOR com um determinado IV obtém-se um valor que vai entrar na block-cipher. No entanto, como esta cifra por blocos é determinística, logo se conseguirmos encontrar para outro determinado IV, um diferente primeiro bloco de mensagem que ao fazer XOR com esse IV obtém-se um valor igual ao da primeira situação. Por esse motivo, o resultado que a block-cipher irá retornar corresponde ao mesmo valor que na primeira situação e, por sua vez, o valor da tag final é também o mesmo. Portanto, conseguimos obter uma nova mensagem que corresponde à primeira, mas com o primeiro bloco de mensagem diferente e uma tag válida para essa mesma mensagem.

Exemplo:

$m1 = 0^n$ e IV1 = 011, então

F_k (m1 $\oplus$ IV1) = F_k (0^n $\oplus$ 011) = F_k (011)

m2 = 010 e IV2 = 001, então

F_k (m2 $\oplus$ IV2) = F_k (010 $\oplus$ 001) = F_k (011)

Por este motivo deve-se usar o IV como uma string de zeros, uma vez que assim torna-se impossível para o atacante realizar este ataque, já que não consegue forjar uma nova mensagem cujo XOR com o IV dê o mesmo que o numa outra mensagem.

Este ataque é o que se encontra implementado no ficheiro em anexo.

2. Ataque ao CBC-MAC utilizando como tag todos os blocos do criptograma

O CBC-MAC pode também ser enfraquecido se em vez de se retornar apenas a tag como o último bloco, retornar como tag todos os blocos do criptograma. Isto acontece, uma vez que o atacante, já que vai receber o resultado proveniente de todos os blocos, irá obter informações relevantes sobre esses e dessa forma, consegue forjar através de uma simples combinação entre eles uma nova mensagem com um tag válida, forjando, assim, o CBC-MAC.

Exemplo:

Imaginemos um ataque CPA, em que o adversário envia três mensagens (m1, m2, m3) e obtém as correspondentes três tags (t1, t2, t3).

Agora, envia outras três mensagens (m1, m2', m3'), obtendo as correspondentes três tags (t1, t2', t3').

Numa outra situação, envia outras três mensagens (t2' $\oplus$ m3'', m2'', m3''), obtendo como tags (E_k(t2' $\oplus$ m3''), t2'', t3'').

Neste momento, o adversário consegue forjar três mensagens, como: m1, m2' e m3'' e irá receber como tags os valores: t1, t2' e E_k(t2' $\oplus$ m3''), que corresponde a uma tag válida para esta mensagem. Desta forma, o adversário conseguiu forjar uma nova tag para uma nova mensagem, tornando, assim, o CBC-MAC inseguro.