مهدی علی خاصی 9530483

:: 12.3

We study two methods for integrity protection with encryption.
1. Assume we apply a technique for combined encryption and integrity protection in which a ciphertext c is computed as
$c = e_k(x \| h(x))$
where h() is a hash function. This technique is not suited for encryption with stream ciphers if the attacker knows the whole plaintext x. Explain exactly how an active attacker can now replace x by an arbitrary x' of his/her choosing and compute c' such that the receiver will verify the message correctly. Assume that x and x' are of equal length. Will this attack work too if the encryption is done with a one-time pad?

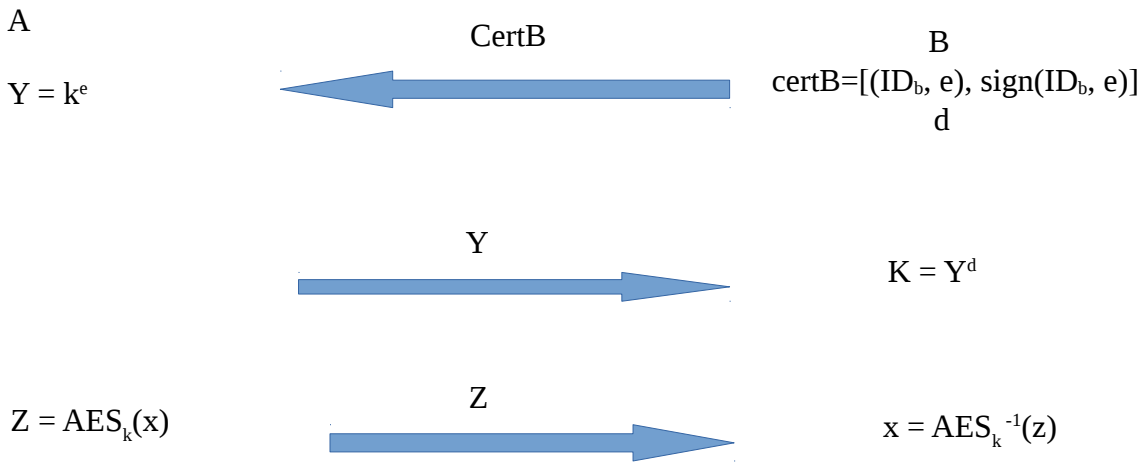
چون حمله کننده متن اصلی x را می داند، میتواند کلید را به راحتی از روی c استخراج کند. برای مثال اگر $e_k = x \text{ xor } k$ بنابراین از روی c و با محاسبه ی $c \text{ xor } (x\|h(x))$ میتواند k را به دست بیاورد. (چون x را دارد میتواند h(x) را به راحتی محاسبه کند)
حال با داشتن k میتواند یک متن دلخواه x' انتخاب کرده و h(x') ر امحاسبه کند و نهایتاً با استفاده از k بیاید و c' جدید را محاسبه کند و آن را برای فرد ارسال کند.

حتی اگر با one-time pad نیز این عمل انجام شده باشد چنین حمله ای به شخص active attack میتواند رخ دهد

2. Is the attack still applicable if the checksum is computed using a keyed hash function such as a MAC:
$c = e_{k1}(x \| MAC_{k2}(x))$
Assume that e() is a stream cipher as above.

خیر. زیرا با داشتن x تنها میتوان کلید k1 را استخراج کرد(مشابه بالا) و چون کلید k2 را ندارد نمیتواند به محاسبه ی MAC(x) بپردازد و نمیتواند با xor کردن دوباره قسمت انتهایی کلید k1 را استخراج کند. (با فرض اینکه طول x برابر L باشد میتواند L بیت اول k1 را استراج کند ولی نمیتواند بیت‌های بعدی k1 را استخراج کند)

::13.9
.1
1Mbit/s * 2 * 60 * 60 = 7200 Mbit = 900 Mbyte = 0.9 Gbyte
2. اگر کاربر بتواند در 10 دقیقه یک کلید را پیدا کند پس در 30 روز میتواند
30 * 24 * 60 / 10 = 4320
کلید را پیدا کند. پس یک فیلم 2 ساعته باید بیش تر از 4320 کلید مختلف داشته باشد
2 * 60 * 60 / 4320 = 1.6 sec
پس حداقل هر 1.6 ثانیه باید یک کلید جدید تنظیم شود


A
CertB
B
Y = k^e
certB=[(ID_b, e), sign(ID_b, e)]
d
Y
K = Y^d
Z
Z = AES_k(x)
x = AES_k^-1(z)