Ataque por fuerza bruta

Ataque por fuerza bruta

En criptografía, se denomina ataque de fuerza bruta a la procedimiento mediante el cual se recupera una clave probando todas las combinaciones posibles.

Los factores determinantes del costo de realizar un ataque de fuerza bruta son la longitud de la clave y el juego de caracteres utilizados en ella.

Fuente: https://www.piqsels.com/en/public-domain-photo-fpvab

¿Qué tan difícil es descifrar una contraseña?

El sitio web WordPress Engine realizó un análisis de dos conjuntos de datos sobre contraseñas, uno que se publicó en foro ruso de BitCoin y otro publicado por el consultor de seguridad Mark Burnett que incluye más de 10 millones de contraseñas en toda la web.

1) 123456
2) password
3) 12345678
4) qwerty
8) 111111
11) 123123
13) abc123

Fuente: https://wpengine.com/resources/passwords-unmasked-infographic/

¿Qué tan difícil es descifrar una contraseña?

Considerando una longitud entre 3 y 8 caracteres, solo letras minúsculas más números:

$36^3 + 36^4 + 36^5 + 36^6 + 36^7 + 36^8 \sim 3$ billones de opciones

Considerando una longitud de 15 y sumándole las letras mayúsculas junto con los caracteres #, $, %, &, /, *, -, ., _ y @ tenemos

$73^{15} \sim 9E27$ opciones

¿Cómo es una contraseña segura?

Hasta mediados de los 70's se pensaba que una clave de 56 bits era segura (2^{56} ~ 7E16 opciones)

En la actualidad, el estándar es el uso de claves de 128 y hasta 256 bits (2^{128} ~ 3E38 y 2^{128} ~ 1E77 opciones)

Hay un argumento físico que indica que una clave de 128 bits es segura contra un ataque de fuerza bruta: el límite de Landauer, el cual define un límite inferior de *kT*Ln(2)* para la energía requerida para realizar un cómputo siendo *T* la temperatura del dispositivo en Kelvins y *k* la constante de Boltzmann.

El solo recorrido por el espacio de búsqueda requeriría ~262.7 TWh (0.1% de la producción mundial anual)