T.C. SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM465 - KRİPTOLOJİYE GİRİŞ

BRUTE FORCE ATTACK

Hazırlayan

ERBİL NAS

B151210053

İçindekiler

Brute Force Attack nedir?

Brute Force Attack (kısaca “brute force”, Türkçesiyle “kaba kuvvet saldırısı”), özünde deneme ve yanılma metoduna dayanan ve şifrelenmiş bir veriye ulaşabilmek için kullanılan kriptoloji algoritmasıdır. Bu algoritmanın yaygın olarak kullanıldığı uygulamalar, şifreleri ve şifreleme için kullanılan anahtarları (encryption keys) ele geçirmek için yapılan uygulamalardır. Ayrıca API anahtarlarına ve SSH log’larına erişmek için de brute force saldırılarının kullanıldığı görülmüştür.

Günümüzde brute force algoritmasını, diğer sık kullanılan şifre kırma algoritmalarından ayıran en önemli farklılığı ise kompleks ya da entellektüel bir stratejiye dayanmıyor olmasıdır. Brute force algoritması, doğru kombinasyonu bulana dek bütün olasılıkları dener, dener ve dener. Bunu bir hırsızın, kilitli bir kasayı açabilmek için her şifreyi tek tek denemesine benzetebiliriz.

```
#define EOS '\0'

void BF(char *x, int m, char *y, int n) {
  char *yb;
  /* Searching */
  for (yb = y; *y != EOS; ++y)
    if (memcmp(x, y, m) == 0)
      OUTPUT(y - yb);
}
```

Brute force saldırısı için kullanılan örnek bir kod parçası

Şifreleme anahtarı (encryption key) nedir?

Şifreleme anahtarı, verilerin karıştırılması ve şifrelenmesi için oluşturulan rastgele bir bit dizisidir. Şifreleme anahtarların tasarlanması, her bir anahtarın önceden kestirilemez ve benzersiz olmasını sağlayabilmek için hazırlanan algoritmalar ile sağlanmıştır. Bu şekilde oluşturulan anahtarlar ne kadar uzun olursa, şifreleme kodunu kırmak da o kadar zor olmaktadır. Ayrıca kullanılan şifreleme yazılımlarının türüne veya işlevine göre, şifreleme ya da şifresini çözmek işlemlerini gerçekleştirebilmek için bir şifreleme anahtarı kullanılır.

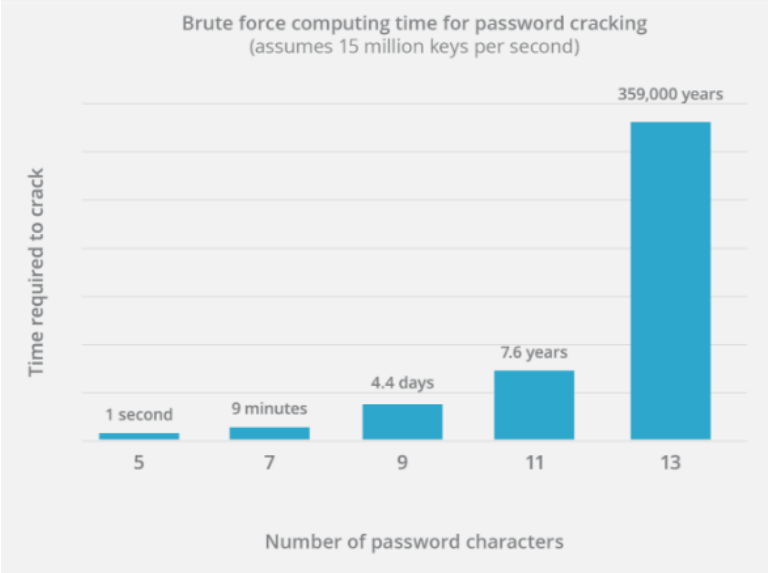
Daha uzun bir şifreleme anahtarının, kısa olanından daha güvenli olduğunu söyleyebiliriz. Örneğin, 128-bit şifreleme anahtarında, bir brute force saldırısının denemesi gereken 2^{128} farklı olası kombinasyon vardır. Bu sayı, 256-bit şifreleme için 2^{128} kat daha fazla olacaktır. (Kombinasyon sayısı 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456) Yüksek bit şifreleme anahtarları, mevcut brute force saldırılarına karşı etkisiz olduğunu varsaydığımız için, kullanıcı bilgileri toplayan tüm web hizmetlerinin 256-bit şifreleme anahtarlarını kullanarak, verileri ve iletişimleri şifrelemesi önerilir.

Brute Force Attack'ın güçlü ve zayıf yönleri

Brute force algoritmasının en büyük avantajı, göreceli olarak uygulamasının basit olması ve uygulamak için yeterli zamanın sağlanması durumunda her zaman işe yaramalarıdır. Günlük hayatımızda kullanılan her şifre tabanlı sistem ve şifreleme anahtarı, brute force saldırısı kullanılarak kırılabilir. Aynı zamanda brute force'a dayanarak bir sisteme girme süresinin ölçülmesi, sistemin sağladığı güvenlik düzeyini anlayabilmek için de oldukça yararlı bir ölçüm yöntemidir. Brute force algoritmasının güçlü yönlerini bu şekilde sıralayabiliriz.

Brute force'un zayıf kaldığı kısımlara gelecek olursak, algoritmanın oldukça yavaş işlemesi en başta gelecektir. Brute force saldırıları çok yavaştırlar, çünkü amaçlarına ulaşana kadar her karakter kombinasyonundan geçmek zorundadırlar. Bu zorluk, doğru kombinasyondaki karakter sayısının artmasıyla doğru orantılı olarak artmaktadır. Örneğin, dört karakterden oluşan bir parolayı brute force kullanarak ele geçirmek, üç karakterli bir parolayı ele geçirmekten daha zordur ancak beş karakterli bir paroladan da kolay olacaktır.

Diyelim ki, elimizde alphanumeric olarak sekiz karakterden oluşan bir şifremiz var. Brute force algoritmasını kullanarak bu şifreyi ele geçirmek ne kadar sürer, hesaplayalım. İngilizce alfabede 26 karakter bulunmaktadır. Harflerin büyük ve küçük olma olasılığını (26*2 = 52) ve numeric olan karakterleri de (0'dan 9'a kadar) hesabımıza katarsak, elimizde 62 karakterlik bir tablo bulunur. Sekiz karakterden oluşan bir şifreyi kırabilmek için denenmesi gereken kombinasyon sayısı, 62^8'den 2.1834011×10^{14} (yaklaşık olarak 218 trilyon) bulunur. Bir saniye içerisinde bir kombinasyonu denediğimizi varsayalım. En kötü ihtimali düşünecek olursak, 218 trilyon saniye, yani yaklaşık 7 milyon yılda bu şifreyi çözmüş oluruz.



Brute force ile şifrelerin kırılması için gereken süreler

Özetlemek gerekirse, karakter sayısı belli bir noktanın üzerinde olmaya başladığı zaman, brute force'un doğru kombinasyona ulaşıp şifreyi ele geçirmesi de gerçekçiliğini kaybetmeye başlıyor. Ele geçirmek istenen şifrenin uzunluğu ve karmaşıklığı yeterince fazlaysa, brute force'u kullanarak bu şifreyi çözebilmek günler, aylar ve hatta yıllar alabilir. Günümüz kriptoloji sistemlerinde kullanılan uzun şifreler ve şifreleme anahtarları da, brute force'un başarılı olabilme ihtimalini düşürmektedir.

Brute Force saldırılarına karşı korunma yöntemleri

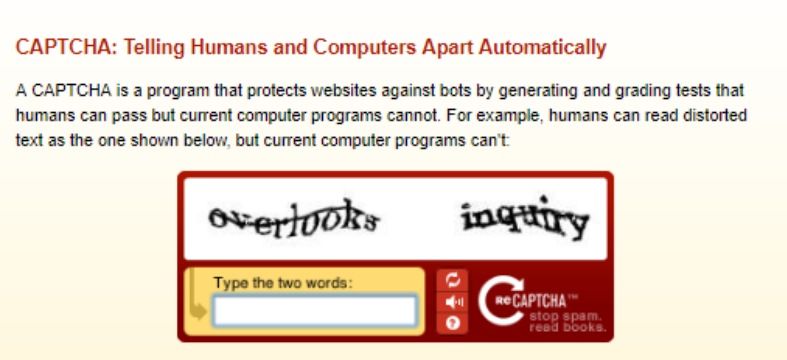
- **Daha Uzun Şifreler:** Brute force saldırılarına karşı koyabilmek için atılması gereken ilk adım, daha uzun şifrelerin kullanılmasıdır. Günümüzde birçok web sitesi ve platform, kullanıcıların belirli bir uzunlukta şifre seçmesini (minimum 8 karakter) zorunlu kılmaktadır.

- **Daha Kompleks Şifreler:** Bir başka önemli adım ise, daha kompleks şifreler oluşturmaktır. Kullandığımız platformlarda "qwerty" ya da "şifre123456" gibi çözülmesi kolay şifrelerin, kullanıcılar tarafında kullanılması önerilmez. Bunların yerinee büyük ve küçük harflerden oluşan, ayrıca sayı ve özel karakterler içermesi kimi zaman zorunlu kılınan şifrelerin seçilmesi gerekir. Bir şifrenin komplekslliği ne kadar artarsa kırılması da o kadar zorlaşır.

Şifrenizin ne kadar sürede kırılabileceğini hesaplayan bir web sitesi

- **Sınırlı Giriş Denemesi:** Basit ama oldukça güçlü bir diğer yöntem ise, kullanıcının giriş denemesine sınırlandırma getirmektir. Örneğin, bir web sitesi sahibi olarak web sitenize beş başarısız giriş denemesi yapılıyorsa, daha fazla girişimde bulunmayı durdurmak için giriş yapmaya çalışan IP adresini belli bir süre boyunca engellenebilir.

- **CAPTCHA Kullanımı:** Günümüzde, bir çok web sitesi ve platformda CAPTCHA yaygın olarak kullanılmaktadır. Resimde yazan kelimleri doğru girmeden sizi web sitesi ya da platformun asıl içeriğine yönlendirmeyen CAPTCHA, bu sayede botların ve özellikle brute force saldırısını gerçekleştiren otomatik komut dosyalarının çalıştırılması da engellemektedir.



Örnek bir CAPTCHA

- **İki Aşamalı Doğrulama:** İki aşamalı doğrulama (Two Factor Authentication ya da kısaca 2FA), şifrelerini başarıyla giren kullanıcılara hesaplara erişebilmeleri için, bir uygulama ya da SMS yolu ile gönderilen altı haneli bir kod ile gerçekleşir. Bu kod her 60 saniyede bir yenilenir ve bir önceki kod geçersiz hale gelir. Bu sebeple, brute force saldırısı sonucu şifre ele geçirilmiş olsa bile doğrulama kodu bilinmediği ve sürekli değişken olduğu için kullanıcıların verilerine ulaşılamaz.

- **Sınırlı IP Adresine Erişim İzni:** Web sitelerindeki trafik yönlendirmesini sağlayan .htaccess dosyasından, sadece seçili IP adreslerine web sitesine erişim izni vererek ya da sadece belirli IP adreslerini yasaklayarak brute force saldırıları engellenebilir.

```
<Files /wp-login>

order deny,allow

allow from IP1

allow from IP2

deny from all

</Files>


```

.htaccess üzerinden IP yetkilendirmesi

Diğer Brute Force Attack uygulamaları

- **Dictionary Attack:** Brute force'un bir başka formu olarak da bilinen dictionary attack (Türkçesiyle "sözlük saldırısı") ise, belirli bir sözlükteki her kelimeyi kullanarak ya da sıklıkla kullanılan şifreleri teker teker deneyerek ele geçirmek istediği şifreye ulaşmaya çalışan bir algoritmadır. Çoğu kullanıcının, sık kullanılan ya da tahmin edilebilen kelimeler ile şifreler oluşturduğu bilindiği için, dictionary attack'ın brute force'dan daha başarılı olduğu rahatlıkla söylenebilir. Ancak dictionary attack yöntemi, çok sözcüklü şifreler kullanan ya da içerisinde büyük harf, sayı ve özel karakter bulunan şifrelerin olduğu sistemlerde etkili bir biçimde çalışmamaktadır.

  Diyelim ki, Ali'nin şifresi "avcı2" ve Ayşe, Ali'nin şifresi öğrenebilmek için dictionary attack yöntemini kullanıyor ve bu sözlükte geçen her kelimeyi kullanıyor. Eğer ki, "avcı2" Ayşe'nin kullandığı sözlüğün içinde varsa artık Ayşe, belirli bir denemenin ardından Ali'nin şifresini kırmış olacak. Ancak Ali'nin şifresi "ahiuhf23fg23tg8902g" olsaydı, Ali'nin şifresinin içinde anlamlı kelimeler ya da sık kullanılan şifreler bulunmadığı için Ayşe'nin sözlüğünde Ali'nin şifresi bulunmayacaktı ve Ali'nin verileri güvende olacaktı.

- **Reverse Brute-Force Attack:** Her algoritmanın normal ve tersine bir işleyiş düzeni olduğu gibi, brute force algoritmasının da tersine işleyişi bulunmaktadır. Tersine bir brute force saldırısında, genellikle sık kullanılan tek bir şifre, birden çok kullanıcı adına veya şifrelenmiş veriye karşı teste tabi tutulur ve bu işlem başka seçilmiş şifreler için de tekrarlanabilir. Brute force saldırısını gerçekleştiren saldırgan, genellikle belirli bir kullanıcıyı hedeflemez. Tersine brute force saldırıları kullanarak sıklıkla kullanılan şifreleri belirleyebilir ve kullanıcılara daha iyi bir şifreleme politikası sağlamak için kullanılabilir.

Kaynakça

https://www.techopedia.com/definition/18091/brute-force-attack

https://www.techopedia.com/definition/1774/dictionary-attack

https://www.cloudflare.com/learning/security/threats/brute-force-attack/

https://www.techopedia.com/definition/25403/encryption-key

https://www.cloudways.com/blog/what-is-brute-force-attack/

http://bilgisayarkavramlari.sadievrenseker.com/2008/12/28/kaba-kuvvet-algloritmasi-brute-force-attack/

http://www-igm.univ-mlv.fr/~lecroq/string/node3.html

http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvRGljdGlvbmFyeV9hdHRhY2s

http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvQnJ1dGUtZm9yY2VfYXR0YWNr

http://www.captcha.net

https://learncryptography.com/attack-vectors/dictionary-attack