ME Mustafa Erdinç ZORBA

Güvenli Şifre Oluşturma

Merhabalar,

Sizlerinde bildiği gibi milenyum çağının başlaması ile birlikte İnsanlar yavaş yavaş gerçek hayattan sanal hayat'a doğru yol almaya başladı. Özellikle facebook, twitter, youtube gibi siteler ve bunun yanında medyanın da etkisiyle insanlar sosyal hayatını, gerçek hayattan çok sanal ortamda oluşturdukları hayatta yaşıyorlar.

Bu sanal hayatın insan üzerindeki yararlı ve zararlı etkileri şüphesiz ki uzun yıllarca tartışılacaktır ama bizim burada tartışacağımız, irdeleyeceğimiz konu ise zaten içinde bulunduğumuz **sanal dünyada nasıl daha güvenli olabileceğimizdir**.

Şöyle özetlemeye çalışayım:

Bundan yaklaşık 10-15 sene kadar önce İnsanlar kendileri için değerli olan eşyaları veya paralarını sandık dibi, yastık altı gibi yerlerde saklayıp; güvenlik için: güvenli apartmanlar, çelik kapılar hatta alarm sistemi kullanıyorlardı. Şimdi ise bu değerli eşyalarını internet üzerinden sürekli kontrol edebilecekleri, üzerinde işlem yapabilecekleri bankalarda saklıyorlar.

Teknolojinin ve interaktif hayatın bu önlenemez gelişimini takip eden kişiler tabii ki sadece bilinçli tüketiciler değil. Gerek işlerinin azalması gerek ise etrafta çalınacak malzeme bulunamaması nedeniyle hırsızlar da teknolojiye ayak uydurdu ve kendilerini sanal ortama adapte ettiler ve tabii ki hırsızlığın adı da böylelikle "**hackerlik**" olarak değişti :)

Hırsızlar yani artık hacker olarak adlandıracağımız kişiler de bizimle birlikte interaktif ortamı kullandıklarına göre: önceden evimize çelik kapı taktırma işlemini interaktif olarak ta yapmamız gerekmekte.

Peki interaktif çelik kapı nereden bulucaz ?

Nasıl evimizin kapısını açan anahtarımız varsa interaktif dünyada da bizim hesaplarımızın kapısını açan şifrelerimiz var. Bu da demek oluyorki tahmin edilemez veya bulunamaz şifre oluşturursak hackerların karşısına bir nevi çelik kapı koymuş oluruz.

Peki tahmin edilemez, bulunamaz şifre nedir ve nasıl oluşturulur ?

İlk olarak tahmin edilebilir şifre nedir bundan bahsedelim:

Aslında hackerlar da sizinle aynı şeyi düşünür yani; siz nasıl doğum gününüzü (veya son 4 rakamını), cep telefon numaranızı (veya son 4 rakamını), sevdiğinizin adını şifreniz olarak seçiyorsanız hackerlar da sizin bu şekilde şifre oluşturacağınızı tahmin edebilir. (*Bu arada 123456, 123456789 gibi rakamlar topluluğu şifre değildir!* :))

Günümüzde çoğu İnsan unutkan olduğunu, klavye becerisinin yeteri kadar iyi olmadığını bahaneederek yukarıda saydığım gibi şifreleri kullanmaktadırlar peki şifrelerinizi nasıl güçlendirebilirsiniz ?

Bu sorunun cevabı çok basit, size tahmin edilemez şeyleri şifre yapmanızı önermek tabii ki haksızlık olur. Bu yüzden size tahmin edilebilir şeyleri, tahmin edilemeyecek şekilde yazmanızı; rakamlara, karakterlere, sembollere anlamlar yüklemenizi önericem. Bu nasıl olur diyecek olursanız. Şöyle düşünün eminim aramızda küçükken eline hesap makinasını alıp, ters çevirip leblebi yazmayan yoktur.

Hesap makinasında leblebiyi yazarken ne yapıyoruz ?

1837837 rakamlarına basıyoruz otomatik olarak gözümüz 7'yi L, 3'ü E, 8'i B, 1'i ise İ harfi olarak yorumluyor.

Siz de fotoğrafik hafızanızı kullanarak bunu şifrelerinizde kullanabilirsiniz.

Bizim örnek olarak oluşturacağımız şifre "AŞKIM" olsun yani şu anda sizin kullandığınız şifre "AŞKIM" diyelim ve bunu biraz güvenli hale getirelim.

"AŞKIM" tahmin edilebilir veya kullanılabilir bir şifre olmasına rağmen '45K1M' o kadar kadar kolay tahmin edilebilir bir şifre değildir. (4'ü A, 5'i Ş, 1'i I olarak gözünüzde canlandırınız)

Üstelik rakamlara yükleyeceğiniz anlamlar tamamen size kalmış örneğin ben 1'i L olarak tanımlarkensiz kendiniz için I olarak tanımlayabilirsiniz ve bunu sizden başka birinin tahmin edebilme imkanı yok.

Gelin şifrenizi şimdi biraz daha güçlendirelim ve sadece rakamlara değil sembollere de anlam yüklemeye başlayalım.

Örneğin M harfini sembollerle kaç farklı şekilde yapabiliriz hiç düşündünüz mü ?

Benim aklıma gelen ve klavyede yapma zorluğuna göre yazılabilen örnekler aşağıdaki gibi:

|\/| (| karakteri için klavyeden AltGr ve büyük, küçük işaretine \ ters taksim için klavyeden AltGr ve 7 tuşuna normal taksim işareti için ise Shift ile birlikte 7 tuşuna basınız) kabul ediyorum başlangıç düzeyinde bir kullanıcı için yazılması zor ama tahmin edilmesi imkansıza yakın bir karakter.
|v| (| karakteri için klavyeden AltGr ve büyük, küçük işaretine basınız ortadaki karakter küçük v harfidir) Orta düzeyde bir bilgisayar kullanıcısının kullanabileceği ve tahmin edilebilmesi yine imkansıza yakın bir karakter.

lvl (baştaki ve sondaki karakter küçük L harfi ortadaki karakter ise v harfidir) tüm bilgisayar kullanıcıları için kolay kullanılabilir ve tahmin edilebilmesi imkansıza yakın bir karakter.
lvl (baştaki ve sondaki karakter büyük ı harfi ortadaki karakter ise v harfidir) tüm bilgisayar kullanıcıları için kolay kullanılabilir ve tahmin edilebilmesi imkansıza yakın bir karakter.

/-\$K1|\/|
45KI|v|
/-\5KI|\/|

}!45K1M!{ (Basit bir süsleme işlemi)
!}!--/-\$K1|\/|--!{! (Zor bir süsleme işlemi)

Şimdiki şifrem mi ? İnanın üç işçi günde ortalama 10 saat çalışarak üç günde ancak yazabiliyor :)

Tüm bunlara rağmen; aklınıza takılan herhangi bir soru(n) olursa çekinmeden info@merdincz.com adresine mail atabilirsiniz.

Mustafa Erdinç ZORBA
20 May. 2012
info@merdincz.com
www.merdincz.com