International Journal of Scientific and Technological Research
ISSN 2422-8702 (Online)
Vol 1, No.10, 2015

The User Login with the Constantly Changing Password Depending On Algorithm and Detection of Illegal Logins

Mustafa Ali Akca
Department Of Computer Education & Instructional Technology, Faculty of Education,
Süleyman Demirel University, Isparta, Turkey
E-mail: mustafaakca@sdu.edu.tr

Abstract
Computer programs and web applications are often used in our daily lives. In many fields such as E-mail services, e-government services, social nets or education necessities etc. people always live involved in these technologies. With the increasing of these services from computer some of the security problems come out. In information Technologies security of personal information, closing it to the access of foreign people is the most important requirement. Because of this reason some security precautions were wanted the user to take, such as obligatory password choice, password entry with the screen keyboard. But these methods are not trustable as much as old days, with the development of some applications which can not be identified with anti-virus softwares and with the entry of user name and password screen display can be taken. Nowadays although some institutions, such as banks use single-use password-generating devices or SMS verification service for 3D protection. But it can not be used by a number of other organizations because it is costly In Our study a solution has sought to this problem by creating a dynamic password and successful results were obtained. In database user password was not saved with character values it was saved with the character generated algorithms which were determined by the users and every user should enter with a new password in every entry. So if the password is stolen, this password will be invalid for the other trial.

Key words: Generating dynamic password, screen keyword, detection of illegal logins

Algoritmaya Bağlı Sürekli Değişen Parola İle Kullanıcı Girişi ve Geçersiz Giriş Yapanların Tespiti

Özet
Bilgisayar programları ve web uygulamaları günlük yaşantımızda oldukça sık kullanılmaktadır. E-posta hizmetleri, e-devlet, sosyal ağlar, iş ya da eğitim ihtiyaçları vb. birçok alanda insanlar sürekli bu teknolojilerle iç içe yaşamaktadır. Bilgisayar üzerinden erişilen bu tür hizmetlerin artmasıyla birlikte bazı güvenlik sorunları ve ihtiyaçları da ortaya çıkmıştır. Bilişim teknolojilerinde kişisel bilgilerin korunması yabancı kişilerin erişimine kapatılması kişinin en önemli ihtiyacıdır. Bu sebepten dolayı kullanıcıya zorunlu güçlü parola seçtirme, ekran klavyesi ile şifre girişi gibi bazı güvenlik önlemleri alınması istenmiştir. Ancak ekranı izleyen kullanıcı adı ve şifre gibi bilgiler girildiği anda ekran görüntüsü de alabilen ve anti virüs yazılımları tarafından tespit edilemeyen bazı uygulamaların geliştirilmesiyle bu yöntemlerde artık eskisi kadar güvenli olmamaya başlamıştır. Şuan bankalar gibi bazı kurumlar 3D koruma için SMS doğrulama hizmeti ya da tek kullanımlık şifre üreten cihazlar kullansa da birçok diğer kuruluş için bu yöntem masraflı olduğu için tercih edilememektedir. Çalışmamızda bu soruna dinamik şifre oluşturma ile çözüm aranmış ve başarılı sonuçlar elde edilmiştir. Veri tabanına kullanıcının şifresi, karakter değerleri ile değil, o karakteri oluşturan kullanıcının belirlediği algoritmalar ile saklanmakta ve her kullanıcı girişinde oluşan yeni şifre ile giriş yapılmaktadır. Bu sayede kullanıcı şifresini çaldırsa bile o şifre bir sonraki girişte geçersiz olacaktır.

Anahtar kelimeler: Dinamik şifre oluşturma, ekran klavyesi, geçersiz girişlerin tespiti

1. Giriş

Günümüzde teknolojinin hızla gelişmesi ile birlikte bilgisayar programları ve web tabanlı uygulamalar her geçen gün insan hayatının bir parçası olmaya devam etmektedir. Kişisel kullanım ya da iş ihtiyaçları için her gün insanlar birçok program ya da web uygulaması kullanmakta bu tür sistemlerle sürekli iletişimini devam ettirmektedirler.

Bilgisayar ve web uygulamalarının insan hayatına önemli ölçüde yerleşmesinden dolayı bu uygulamaların güvenliği de önem kazanmıştır. Bilişim teknolojilerinde kullanıcılarının güvenliğin sağlamasındaki amaç insanları tehdit ve tehlikelere karşı korumak ve öncesinde gerekli tedbirlerin alınmasını sağlamaktır [1]. Kişileri korumak için geliştirilen sistemlerdeki temel amaç veriyi sadece ait olan kişiye sunmak ve verilerin yabancı kişilere erişimini kapatmaktır [2]. Bu tür verilerin kaydedilmesi ve daha sonra kullanıcıya açılması aşamasında kullanıcı adı ve şifre kombinasyonuna bağlı güvenlik yöntemleri kullanılır. Bu tür güvenlik sistemlerine bilgi temelli kimliklendirme denir [3]. Bilgi temelli kimliklendirme kullanılırken öncesinde kişiye bir kullanıcı adı ve şifre tahsis edilip daha sonra veriye erişme aşamasında bu bilgiler sorulur. Kullanıcı adı ve şifre veri tabanındaki ile aynı ise kullanıcı bilgiyi görür. Bu tür bilgi erişimlerinde kullanıcının tahmin edilmesi zor şifreler seçmesi kullanıcı açısından güvenliği biraz daha artırabilmektedir. Fakat kendi haline bırakılan (kontrolsüz parola seçimine izin verilen) kullanıcıların doğal olarak hatırlanması kolay ve kısa parolalar seçtikleri bilinmektedir [4]. Kullanıcıların parola seçimlerinde zayıf parola seçmemeleri ve onları daha güçlü parolalara yönlendirmek için bazı çalışmalar yapılmıştır [5-7]. Ancak her ne kadar güvenli bir parola oluşturulsa bile bu sistemlerin en belirgin eksiği şifrenin başka bir kullanıcı tarafından klavye takibi ile kaydedilmesi ve diğer kişilere ulaştırılabilmesidir [8]. Keylogger ismi verilen ve kullanıcının klavyeden girdiği verileri kaydedip başka kullanıcılara gönderebilen birçok yazılım bulunmaktadır. Ayrıca bu yazılımların, programlama araçlarıyla kolayca geliştirilebildiği için güncel anti virüs programları tarafından bile tanınmadığı öne sürülmektedir [9]. Günümüzde bankalar ve bazı kurumlar bu tür şifre çalınmalarına önlem olarak 3D doğrulama olarak da isimlendirdikleri SMS doğrulama özelliğini kullansa da hem teknik olarak hem de maliyet olarak şuan diğer birçok web uygulaması sahipleri yâda geliştiricileri tarafından çok fazla tercih edilmemektedir. Son dönemlerde bazı sitelerin girişlerinde yer alan ve işletim sistemlerinde içerisinde bir araç olarak da bulunan ekran klavyeleri bu soruna bir süre çözüm olmuştur. Ancak klavyeden veri girişi olmasa bile fareyi takip eden ve fare tıklanmalarına göre ekran görüntüsü kaydeden yani şifreleri ekran klavyesinden girilse bile tespit edebilen bazı yazılımlar geliştirilmiştir. Bu sebepten dolayı artık ekran klavyesi ile girişlerde eskisi kadar güven sağlamamaya başlamıştır [10].

Çalışmamızda web uygulamalarının bu tür sorunlarına yeni bir çözüm önerisi sunulmuştur. Mevcut kullanıcı adı ve şifre girişlerine yapılacak küçük düzenlemeler ile kullanıcının kendi belirlediği algoritmaya bağlı olarak sürekli değişen dinamik şifreler oluşturulmuş hiçbir ek donanım ya da yazılım masrafı olmadan yeni bir güvenli giriş sayfası oluşturulmuş ve başarıyla test edilmiştir.

2. Metodoloji

2.1. Kullanıcıların dinamik şifre oluşturabilmesi için algoritma belirlemesi

Bu sistemde kullanıcılar kendilerine ait şifreleri veri tabanına doğrudan kaydetmezler. Çünkü şifrelerin hepsi değişkendir ve anlık olarak değişebilir. Bu sebepten dolayı şifre değil, şifreyi oluşturan algoritma veri tabanına kaydedilir. Hem zamanla hem de lokasyonla değişen şifre türetmek için tarih, saat ve IP adreslerine bağlı bazı bilgiler alınarak ve çeşitli düzenlemelerden geçerek kullanıcıya sunulmuştur. Kullanıcı bu veriler üzerinden şifresini oluşturmaya başlar. Kullanıcının dinamik şifresine ekleyebileceği veriler Tablo 1'de yer almaktadır.

Tablo 1'de görüldüğü gibi kullanıcı dinamik şifresini oluştururken 12 farklı ve sürekli değişen bir bilgi ekleyebilir. Kullanıcılar bu bilgilerin tamamını kullanabilecekleri gibi, soldan ya da sağdan kesilmiş hallerini ya da herhangi bir matematiksel işleme uğramış hallerini kullanabilirler. Örneğin şifresindeki sabit kısmın "sifrem" olduğunu düşünürsek ve şifrenin sonuna saat bilgisinin eklenmesini istersek şifre sadece içinde bulunan saat için geçerli olmuş olacaktır. Yani kişi sisteme girmek istediğinde şuan ki saatin 20.46 olduğunu düşünürsek şifre olarak "sifrem20" yazmalıdır. Bu şifre başkaları tarafından çalınsa bile 1 saat sonra bu şifre otomatik olarak değişeceği için 21.00 da geçerli olmayacaktır. Aynı şekilde eğer kullanıcı şifresinin sonuna dakika bilgisini eklerse o şifre sadece o dakika için geçerli olacak ve o şifreyi çalan kişi 1 dakika sonra bile sisteme girmeye çalışsa başarısız olacaktır.

Bununla ilgili aşağıda bir takım örnekler yer almaktadır;

Tablo 1: Kullanıcının şifresine ekleyebileceği değişkenler ve kısaltmaları

	Değişkenler	Kısaltmaları
1	Yıl	Y
2	Ay	A
3	Ayın İsmi	AN
4	Gün	G
5	Günün İsmi	GN
6	Saat	S
7	Dakika	D
8	Saniye	SA
9	IP Adresinin ilk okteti	IP1
10	IP Adresinin ikinci okteti	IP2
11	IP Adresinin üçüncü okteti	IP3
12	IP Adresinin dördüncü okteti	IP4

İstek 1: Şifremin sabit kısmı "ahmet" olsun. Sabit kısımdan önce gün isminin ilk harfi olsun.
Veri tabanına kaydedilen şifre : "[GN,SOL1]ahmet".

İstek 2: Şifremin sabit kısmı "demir" olsun. Sabit kısmından hemen sonra IP adresimin üçüncü okteti yer alsın.
Veri tabanına kaydedilen şifre : "demir[IP3]"

İstek 3: Şifremde sabit kısım olmasın. Başlangıçta IP Adresimin ilk oktetinin matematiksel olarak 5 fazlası ile saniye bilgisinin 2 katı olsun.
Veri tabanına kaydedilen şifre : "[IP]+5[SA]*2"

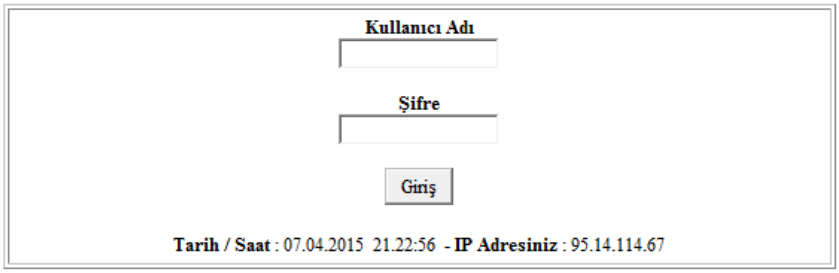
Bu üç örnekte de görüldüğü gibi veri tabanına sabit bir şifre kaydedilmemektir. İlk örnekteki kullanıcı sisteme girmek istediğinde parola kutucuğuna içinde bulunduğu gün çarşamba ise "Çahmet" yazmalıdır. Eğer perşembe günü sisteme girmek isterse "Pahmet" yazmalıdır. Dolayısı ile ahmetin şifresini çalan bir hırsız Çarşamba dışındaki günlerde sisteme "Çahmet" şifresi ile sisteme giriş yapmak istese giremeyecektir.
İkinci örnekte kullanıcının IP adresinin 83.123.78.33 olduğunu düşünürsek kullanıcının parola kutusuna yazması gereken şifresi "demir78" olacaktır. Kullanıcının bu şifresini keylogger ile çalan bir hacker kendi bilgisayarından girerken "demir78" şifresini denediğinde IP adresi farklı olduğu için yine başarısız olacaktır.
Üçüncü örnek, ilk iki örneğe göre biraz daha karmaşık ve güvenlidir. Kullanıcının IP adresinin 83.123.78.33 olduğunu düşünürsek ve şuan saatin 20.42:26 olduğunu varsayarsak kullanıcının şifresi IP adresinin üçüncü oktenin 5 fazlası yani (78+5) ile saniye bilgisinin ikiyle çarpılmış halinin (26*2) yan yana yazılması olacaktır. Yukarda varsaydığımız bilgilere göre bu şifre 8352'dir. Kullanıcının şifresini çalan hacker bu şifreyi çalsa bile bu şifreyle tekrar girebilme ihtimali yok denecek kadar azdır. Saniye bilgisinin yer aldığı şifreli girişlerde, kullanıcıya o anki sunucu saatinin gösterilmesi gerekmektedir. Kullanıcı saati ile sunucu saati arasındaki zaman farkı sorun oluşturabilir.
Şekil 1'de görülen kullanıcı şifre belirleme ekranında kişiler şifrelerine eklemek istedikleri bilgileri seçmektedirler. Bu aşamada ilk olarak eğer şifrelerinin sabit bir kısmı var ise onu yazıp kaydederler. Sonraki aşamada sabit kısma ek olarak Tablo 1'deki değişkenleri doğrudan ya da matematiksel işleme tabi tutarak şifrelerin sol ya da sağ kısımlarına ekleyebilirler. Kullanıcı isterse bu 12 değişkenin biri ya da bir kaçını şifresine ekleyebileceği gibi hepsini de şifresinde kullanabilir.

Şifrenizin Sabit Kısmı		Sabit Kısmı Kaydet

Değişkenler	Doğrudan Kullanım	Matematiksel İşleme Yap
Yıl	Soluna Ekle | Sağına Ekle	-50*5 Ekle
Ay	Soluna Ekle | Sağına Ekle	Ekle
Ayın İsmi	Soluna Ekle | Sağına Ekle	Ekle
Gün	Soluna Ekle | Sağına Ekle	Ekle
Günün İsmi	Soluna Ekle | Sağına Ekle	Ekle
Saat	Soluna Ekle | Sağına Ekle	Ekle
Dakika	Soluna Ekle | Sağına Ekle	Ekle
Saniye	Soluna Ekle | Sağına Ekle	Ekle
IP Adresinin ilk okteti	Soluna Ekle | Sağına Ekle	Ekle
IP Adresinin ikinci okteti	Soluna Ekle | Sağına Ekle	Ekle
IP Adresinin üçüncü okteti	Soluna Ekle | Sağına Ekle	Ekle
IP Adresinin dördüncü okteti	Soluna Ekle | Sağına Ekle	Ekle

Şekil 1: Kullanıcının şifre algoritması belirleme sayfası

2.2. Kullanıcı Giriş Ekranı



Şekil 2: Kullanıcı giriş ekranı

Şekil 2'de görüldüğü gibi kullanıcı giriş yaparken sunucuya ait tarih ve saat bilgisi ile kullanıcının IP adresi bilgileri de gösterilmektedir. Kullanıcı eğer dinamik şifresinde bu değerlerden birini kullandıysa bu ekrana bakarak dinamik şifresini yazar ve giriş butonuna tıklar.

2.3. Oluşturulan Şifrelerin Kaydedilmesi ve Geçersiz Girişlerin Tespiti

Çalışmanın bu aşamasında oluşturulan her dinamik şifre ile yapılan başarılı giriş sonunda o anki şifre veri tabanına tarih ve saat bilgisi ile kaydedilmektedir. Bu kayıttaki amaç, eğer son giriş yapılan bilgisayarda bir keylogger var ise bu şifre ile ne zaman ve hangi IP'den giriş yaptığını tespit etmektir. Örneğin bir kullanıcının dinamik şifresinin "23bulut325" olduğunu ve bu şifre ile 07.04.2015 21.35.55 tarihinde sisteme giriş yaptığını düşünelim. Başarılı girişten sonra bu şifre kaydedilip arşivlenir. Eğer o bilgisayardaki keylogger yardımı ile bu şifre başka birine ulaştırıldıysa ve bu şifre ile tekrar girilmek istenirse kullanıcıya daha sonraki girişte bir uyarı verilir. Bu uyarıda kullanıcının hangi tarihte oluşturduğu şifre ile giriş yapılmak istendiği gösterilir. Dolayısı ile kullanıcı sürekli kullandığı birkaç farklı bilgisayar arasından hangisinde bir keylogger var tespit etmiş olur. Ayrıca geçersiz girişi yapmaya çalışan kişinin IP adresi kaydedilir ve sonraki başarılı girişte kullanıcıya gösterilir. Bu sayede geçeriz giriş yapmaya çalışan kullanıcının IP adresini de öğrenmiş olur.

3. Sonuçlar

Çalışma tasarlanmadan önce literatürde kullanıcı adı ve şifre kombinasyonuna bağlı girişlerde uygulanan güvenlik önlemleri hakkında detaylı bir araştırma yapılmıştır. Bu araştırmalarda yukarıdaki bölümlerde de bahsettiğimiz kullanılmakta olan güvenlik önlemleri hem maliyet hem de eksikleri açısından incelenmiş, onlara ek bir çözüm üretilmeye çalışılmıştır. Geliştirilen sistem yazılımsal açıdan çok karmaşık olmayıp tüm geliştiriciler tarafından mevcut bilgisayar programlarına ya da web uygulamalarına eklenebilir. Herhangi ek bir donanım ihtiyacı olmadığı için de maliyeti yoktur. Ayrıca kullanıcılar açısından da bazı kolaylıklar sağlamaktır. Kullanıcıya onun da unutabileceği karmakarışık ve uzun şifreler seçmesini istetmektense basit ama sürekli değişen bir şifreyle daha güvenli bir ortam girişi sağlanmış olmaktadır. Bunun yanında sistemde yer alan geçersiz girişlerin kaydedilmesi ile kullanıcı internete bağlandığı ortamdaki bilgisayarın güvenli olup olmadığını, keylogger yüklü olup olmadığını tespit etmiş olacaktır. Ayrıca izinsiz giriş yapmaya çalışan kullanıcının IP adresini öğrenebilecektir

Kaynaklar

[1] Canbek, G., Sağıroğlu, Ş., "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme", Gazi Üniversitesi Politeknik Dergisi, 9.3 (2006).

[2] Aydın, Ü. A., Acartürk, C., "Kullanılabilir Güvenlik ve Grafik Şifreler", Türkiyede İnternet Konferansı. 2012.

[3] Özkaya, N., Sağıroğlu, Ş., "Açık Anahtar Altyapısı ve Biyometrik Sistemler", I. Ulusal Elektronik İmza Sempozyumu, 7¬8 Aralık 2006, s.283-290, Ankara, Türkiye.

[4] Korkmaz, İ., "Bilgisayar sistemlerinde parola güvenliği üzerine bir araştırma", Ege Üniversitesi Fen Bilimleri Enstitüsü, 2006.

[5] Bergadano, F., Crispo, B., Ruflo, G., "High Dictionary Compression for Proactive Password Checking", ACM Transactions on Information and System Security, 1(1):3-25, 1998.

[6] Stallings, W., "Cryptography and Network Security,Pearson Education, Inc., New Jersey, 2003.

[7] Blundo C., D'Arco P., De Santis, A., Galdi C.,"HYPPOCRATES: a new proactive password checker", The Journal of Systems and Software, 71:163-175, 2004.

[8] Şamlı, R., Yüksel, M.E., "Biyometrik güvenlik sistemleri", Akademik Bilişim'09 (2009): 11-13.

[9] Canbek G, Sağıroğlu, Ş., "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Müh. Mim. Fak. Dergisi 22.1 (2007): 121-136.

[10] Anonim,2012, https://www.youtube.com/watch?v=9SQd5vIPc1U Son Erişim : 07.04.2015