Parola Güvenliliğine Yeni Bir Yaklaşim

Taymaz R.FARSHİ [1] Mir Mohammad Reza ALAVI MILANI [2] Orhan KESEMEN[3]

[2]Karadeniz Üniversitesi, Bilgisayar Mühendisliği Bölümü, Trabzon

[1,3]Karadeniz Üniversitesi, İstatistik ve Bilgisayar Bilimleri Bölümü, Trabzon

[1]e-posta: farshi@ktu.edu.tr, [2] e-posta: milani@ktu.edu.tr, [3] e-posta: okesemen@gmail.com

Özet: Erişim denetim sistemleri yasal kullanıcıların kimliğini doğrulamak ve sisteme erişen kötü niyetli olanları önlemek için çeşitli yöntemler üzerinden güvenliğini sağlarlar. Çoğunlukla sistemlerde kullanıcı adı-şifre (username-password) yönteminden yararlanırlar. Bu teknoloji, uzaktan kimlik doğrulama uygulamaları için de-facto standardın oluşturdu. Bir kullanıcı adı-şifre tabanlı sistemlerde, sadece gerçek kullanıcılar kendi kimlik bilgilerin bildiğini varsayılmaktadır. Ancak, bugünkü çağın sosyal ağları ve modern hesaplama cihazlarında, bu tür sistemlerin kırması yaygın bir olay haline gelmiştir. Bu çalışmada, yeni bir kere kullanım şifre (OTP[1]) metodu geliştirerek parola tabanli uygulamaların güvenliliğini, bir cep telefon teknolojisininden yararlanarak artmaktadır.

Anahtar: Parola, kullanıcı adı-şifre, Kimlik doğrulama, Bir kere kullanım şifre.

A New Approach To The Safety Of Password

Abstract: Access control systems rely on a variety of methods for authenticating legitimate users and preventing malicious ones from accessing the system. The most commonly used system is a simple username and password approach. This technology has been the de-facto standard for remote authentication applications. A username-password based system assumes that only the genuine users know their own credentials. However, breaching this type of system has become a common occurrence in today's age of social networks and modern computational devices. In this paper, we proposed a one-time password scheme that improved the security of password-based applications by incorporating mobile technique into the password.

Keywords: Password, Username-Password, Authentication, One Time Password.

1. Giriş

Günümüzde teknoloji ve bilgisayar destekli sistemlerin hızla gelişmesi giderek artmaktadır. Bu gelişmeler nedeniyle sistemlere bağlantilar her gün öncesinden daha fazla ihtiyac duyulur. Özellikle bu sistemlerin web üzerinde olmasından , internet güvenliğinin önemi daha artmaktadır. Son dönemlerde internet güvenlik çalışmaları gündemde. Bu çalışmalar çeşitli yaklaşımlar üzerinden yapılmıştır[3]. Örneğin görsel şifreler yaklaşımlar [4,5,6,10], el cihazlı şifreleme[8], cep telefonlarda görsel şifreleme[9], bir kere kullanım şifreler [11,12] . Ayrıca bazi çalışmalar kloviye analisler üzerinden yapılmıştır[13]. Tüm çalışmalara ragmen, bu tür aktiviteler yenilgiye uğramaktadır[7]. Toplum genelde güçsüz (waek) paroları [1] çeşitli amaclar için seçirler. Ortalama olarak kişi başi 25 parola korumak zorundalar [2].

Bu çalışma aşağıdaki gibi yapılandırılmıştır. 2. Bölümde, Fiziksel adresler ve cep telefonların IMEI kodları tartışılmıştır. 3. Bölümde önerilen yöntem, algoritması ve avantajları bahs edilmiştir. 4. Bölümde yapılan deneysel uygulama açıklanmıştır. 5. bölüm sonuçlar konusunda yapılmıştır.

2. Fiziksel Adresi

Bilgisayarlar arasında ağ üzerinden haberleşmeler yapılmaktadır. Ağ bağlantılar genelde ağ kartlarını kullanırlar. Böylece sistemlerde , her bilgisayar için özel bir ağ kartı vardır. Ağ kartları haberleşme sırasında önemli görev taşımaktadır. Ayrıca ağ üzerindeki herhangi bir bilgisayar ya cep telefonu, belirli şekillerde tanımlanmalı. Ağ kartlar, bilgisayarları bir birinden ayırması için kullanılır. Sistemlerde her bilgisayara özel, bir fiziksel adres göz önünde bulundurulur. Bu adresler ağ kartında MAC adres olarak adlandırılır.

[1] One Time Password

MAC Adresi 6 bayt (48 bit) uzunluğa sahipdir. Eğer üreticiler Belirli bir kriter olmadan ağ kartlarını adreslendirilirseler , Elbette adres arasında bir konfilikasyon olacaktır. Dolaysıyla, adresler benzersizler ve her kart için özel bir adres uygulanmıştır.

2.1. Telefon IMEI[1] kodu

Cep telefonlarında MAC adresine benzer bir düzenek kullanılır. Bu mekanızma IMEI olarak adlandırılmıştır. IMEI, 15 basamaklı ve benzersiz bir koddur. Bu kod GSM gezgin telefonlarında, şebekede bulunması için kullanılır. Bazı LAN ağlarda MAC adreslerde başlangıç ve son adres ünvanında bile kullanılır. Ancak GSM ağlarında bu kod hiç bir zaman böyle kkullanılmaz.her simkart kayıtı ile IMEI ağ için İD kayıdı kısmında (Equipment Identity register = EIR) kayd edilir ve gönderilir. Cep telefonların çoğunluğunda *#06# arayışı ile cep telefonların kendisi ile gösterilir. Ayrıca genelde pil altında cep telefon cihazının gövdesinde bile kazılmıştır. Bir IMEI kodu dört kısımdan oluşur, ve her sektör bir boşluk (space) aracılığı ile, örneği AAAAAA BB CCCCCC gibi ayrılır.aşağıdaki tablo 1, IMEI'ın rakamını oluşturmasını göstermektedir.

Rakam Sayısı	6	2	6	1
Anlam	TAC	FAC	SNR	SP

Tablo 1. İMEİ'ni oluşturan tablo

İlk altı basamak (Type Approval code) (AAAAAA) TAC adlanır.bu altı basamağın üretıcı ülkeni temsil etmektedir. Mesela 35 kodu finlandya ülkesi ile ilgilidir.

Sonraki iki rakam (BB) fabrika kodu (Final Assembly Code) üretici fabrikanın göstergesidir.

Sonraki altı rakam (CCCCCC) kodu SNR ya cihazın seryal numarasıdır.sonuncu rakam SP ya spair kodudur, ve genellikle sıfır değerlenir ve kullanışsızdır.

Her kayıtlı IMEI kodu EIR'da üç sınıflandırmadan oluşur.ve her IMEI kodları bir sınıf içinde bulunur

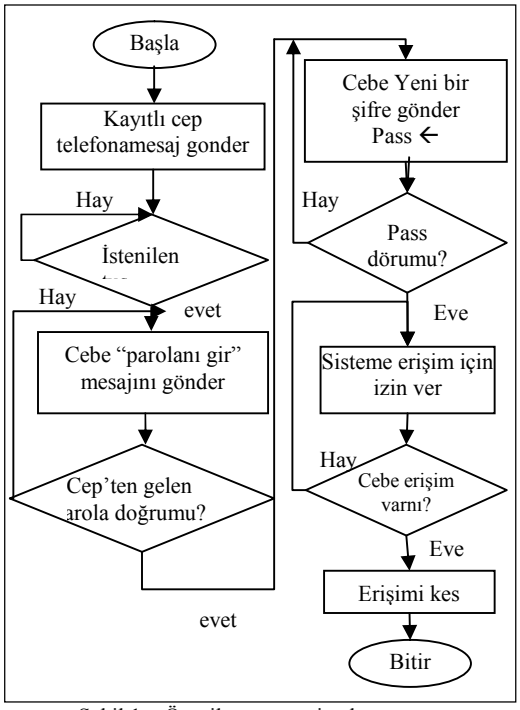
- Beyaz :bir izinli IMEI.
- Gıri : bir IMEI göz altına alınır (genellikle yeni giren cihazlar ve telekom kurumunda kayıtlı olmayanlar bu sınıfta olmaktadırlar).
- Siyah : bir izinsiz IMEI ve tıkanık (genellikle çalınmış ya izinsiz olanlar bu sınıfta bulunmaktadırlar)

3. Önerilen Yöntem

Bu çalışmada, web siteleri ve ya her hangi programların güvenliğini dahada çok sağlamak için, bir yeni yöntem önerilmiştir. Bu yöntemde, cep telefonların IMEI numaraların kullanarak güvenlik işlemleri gerçekleştirilmiştir.

Bu yöntemde, kullanıcı istenilen site (/program) başlattığı zaman, site (/program) tarafından, öncecden kayıt olduğu cep telefonu tespit edilir ve cep telefona bir mesaj gönderilir. Bu esnada kullanıcı, cep telefonundan istenilen tuşa basarak siteye (/programa) cevap verir.bu iletişimin ardından site (/program) tarafından, bir yeni mesaj gönderilir, ve kullanıcı telefon üzerinden kendi parolasın girir. Site (/program) doğru parolanı aldığında yeni ve bir kere kullanılan şifre (OTP) kullanıcının telefonuna gönderir. Böylece kullanıcı OTP şifresin siteye (/programa) girerek, siteye (/programa) erişebilir.

Kullanıcının cep telefonu erişimli olduğuna kadar site (/program), kullanıcıya açıktır. Ancak cep telefon bilgisayardan uzaklaştığında ve ya başka nedenlerle site (/program) tarafından erişilemez hale geldığı zaman, kullanıcı ve site (/program) arasında bağlantı kesilecek. Önerilen yöntemin akış diyagramı aşağıda gösterilmektedir.Önerilen yöntemin akış şeması Şekil 1'de gösterilmektedir:



Şekil 1 – Önerilen yöntemin akış şeması

3.1. Önerilen Yöntemin Algoritması

Önerilen yöntemin algoritması tablo 2'de gösterilmiştir :

```
timer -> start
search device
if device found
    while(er < 4)
       code=button autentication code
       if code==true
```

[1] International Mobile Equipment Identity

```
            pass_generator()
        else
            er++
           if err==4 return
        end
    end
else
    continue
end
pass_generator()
generate new password
    send to mobile via bluetooth
    while(error <4 )
        if pass=true
            system=open()
        else
            error++
            if error==4 return
        end
    end
end
```

Tablo 2. Önerilen yöntemin algoritması

3.2. Önerilen Yöntemin Avantajları

Bu yöntem haker programlarına özellikle keyloger'lere çok dayanaklıdır, zira her seferinde yeni bir şifre oluşup, gönderilir ve programda kullanılır. Başka bir tarafdan kullanıcı, şifre ezberleme zorunda değil ve istediği zaman cep telefon üzerinden yeni şifreler elde edilir.

4. Deneysel Uygulama

Bu yöntemi pratik olarak bir çelik fabrikasında uyguladık.öyleki bir üretim yönetmeni denetim yapmak için sürekli odasından çıkıp ve bilgisayarından uzaklaşıyordu, bu arada bazen sistemden çıkış yapmasını unutuyordu, ve her hangi biri odaya girip ve bilgisayarda sisteme erişe biliyordu, ancak bizim kullandığımız yöntem bu sıkıntıya karşı geldi ve kullanıcı bilgisayar başında olmadıkca sisteme erişim kesiliyor. Kullancı bilgisayara yaklaşırken yeni şifre kullancıya gönderilecektir ve böylece sisteme erişim yapılması sağlanıyor.sisteme erişim sadece kullancının cep telefonu bilgisayara yakınken sağlanıyor ve eğer boyle olmassa hiç bir turlu sisteme giriş yapılamaz. Var sayalım kullanıcı cep telefonunu kayb etdi, bu durumda kullanıcı guvenlilik sorulara cevap verdikden sonra yeni telefonunun IMEI ardresini sisteme ekliyor ve ağer isterse eski telefonunun adresini kaldırıa bilir ,yada sistem yoneticisi kullanıcının yeni IMEI adresini ekliyor.

5. Sonuç

Bu çalışmada, şifre güvenliliğine yeni bir yaklaşım önerilmiştir. Bu yöntemde , bir mekanizma ile kullanıcının aktif olup olmadığını test edir ve aktif değilse veya daha doğrusu bilgisayardan uzak ise, otomatik olarak sisteme erişim kesilir. Dolayısıyla, otorizesiz kullanıcılar siteye girip ve değişimler yapabilmezler. Bu işlemleri gerçekleştirmek için, cep telefonların İMEİ kodların kullanarak, kullanıcı ve programlar arasında bağlantı kurulur. Ayrıca, bu yöntemde kullanıcı her zaman yeni şifreleri otomatik olarak sistemden elde edip ve sistemde kullanır. Yapılan çalışma pratik olarak bir ortamda uygulanmış, yararlı ve elverişli olması belirlendi.

6. Kaynakça

[1] D. Florêncio and C. Herley, "A large-scale study of web e password habits," in Proc. World Wide Web Conf. (WWW'07), Banff, Alberta, Canada, May 2007.

[2] D. Florêncio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?," in Proc. USENIX Workshop on Hot Topics in Security (HotSec'07), Boston, MA, Aug. 2007.

[3] Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA, 2002.

[4] L. D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. 35, pp. 19, 2002.

[5] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[6] S. Akula, V. Devisetty, "Image based registration and authentication system," Midwest Instruction and Computing Symposium (2004).

[7] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[8] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

[9] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[10] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.

[11] Khaled Alghathbar, Hanan Mahmoud "Noisy Password Scheme: A New One Time Password System," 22nd IEEE Canadian Conference on Electrical and Computer Engineering , Canada May 3-6, 2009.

[12] N. Haller, "The S/KEY one-time password system," in *Proc. Network and Distributed System Security Symp. (NDSS'94)*, San Diego, CA, Feb. 1994.

[13] S. Shepherd, "Continuous Authentication by Analysis of Keyboard Typing Characteristics", IEEE Conf. on Security and Detection, European Convention, pages 111–114, 1995.