INTERSECT
Kullanıcı Kimlik Doğrulama ve Onaylama Sistemi

Gülçin ÇİVİ - M. Niyazi ÇEKİÇ

ÖZET

Bu çalışmada, bugünün gelişen bilgisayar teknolojisinin işleyişine uygun ve kullanıcı kimlik bilgilerinin güvenliğini, mevcut yöntemlerden faklı olarak, daha uygun maliyetle ve %100 garantili şekilde sağlamaya yönelik geliştirilen bir ileri seviyede Kullanıcı Kimlik Doğrulama ve Onaylama ” teknolojisi tanıtılmaktadır.

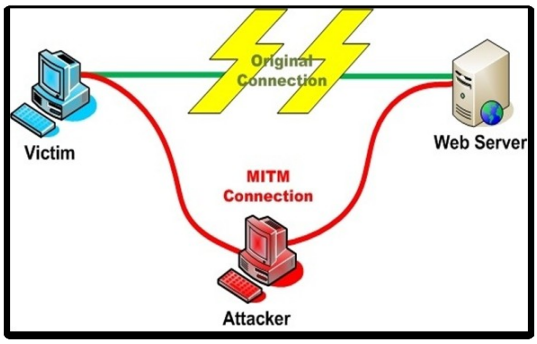
Anahtar kelimeler: Kimlik Doğrulama, İki Faktörlü Doğrulama,

1. Giriş

Gelişen web teknolojisi kişiler ve kurumlar arasında kolay iletişimi mümkün kıldığından kişi/kurum bilgileri üçüncü kişilere açık hale gelmektedir.. Mevcut çözümler, username - password ve/veya OTP(One Time Password) vb key leri aynı bilgisayar sistemi(bilgisayarın internete bağlanırken aldığı IP) üzerinden ilettiği için

- Keylogger ,
- Fake Mail,
- Phishing,
- Virtual keyboard,
- Network sniff,
- Brute Force
- Man in the middle
- Man in the Browser

gibi metodlarla internet üzerinden çalınabilmektedir.
Intersectin tasarımında, bu çalınma yöntemlerinin etkisiz kalması amaçlanmıştır.



2. Mevcut Uygulamalar

Kimlik Doğrulama (Authentication), çok çeşitli yöntemlerle gerçekleştirilmesi mümkün bir süreçtir. Bu süreçte belirleyici olan, kimliği tanıtıcı olarak kabul edilen ve doğrulanmak istenen unsurlar ile bunun için kullanılan faktörlerdir.

Doğrulamada kullanılan faktör adedine göre temel iki ayrım söz konusudur:

- TEK FAKTÖRLÜ Kimlik Doğrulama
- ÇOK FAKTÖRLÜ Kimlik Doğrulama

Kimlik doğrulamada kullanılan faktörlerin kimliğin sahibine göre kategorize edilmesiyle, aşağıdaki şekilde bir sınıflandırma kabul edilmektedir:

1. Kullanıcı Kodu, Şifre, Onay Şifresi gibi BİLİNEN (Known – something you know) şeyler.

2. Banka ve Kredi Kartları, Cep Telefonu SIM Kartı, OTP (One Time Password) Cihazı – Token gibi SAHİP OLUNAN (Own – something you have) şeyler.

3. Ses, Parmak İzi, Retina Deseni ve DNA gibi VARLIĞA AİT (something you are) şeyler varlıkla ilgili unsurlar ise, Karakteristikler ve Biyometrikler olarak ikiye ayrılır. Varlığa ait unsurlar, daha yaygın şekilde, BİYOMETRİK unsurlar olarak anılmaktadır.

Ayrıca, kimlik sahibi ile doğrulayacak taraf arasındaki ilişki esas alındığında, doğrulamaya dayanak olarak çok farklı unsurlar faktör olabilir.

- Anne Kızlık Soyadı kişinin önceden paylaştığı bir bilgidir. Bu bilginin kullanılması, yani önceden belirlenmiş müşteri sırlarını doğrulamak, TANIMA TABANLI bir doğrulama olur.
- Sadece yetkili terminallerden gelen erişim taleplerine izin verilmesi, KONUM TABANLI bir doğrulamadır.
- Erişimlere, zamana endeksleyerek, çeşitli periyotlarla izin verilmesi ise, ZAMAN TABANLI bir doğrulamadır.
- Sağlanmış erişimlerde, önceden tanımlı işlemler ve talimatlar gerçekleştiriliyor olması nedeniyle, kimliğin doğruluğunu varsaymak, HACİM TABANLI bir doğrulamadır.
- Yetki Tanımlama ile kullanıcının yetkilerinden yola çıkılarak erişime izin verilmesi YETKİ TABANLI Kimlik Doğrulama olarak kategorize edilmektedir.

- İşlem yapılan bilişim sisteminin (yaygın olarak PC) kontrolü ya da Yazılım ve/veya Donanım Kontrolü (örneğin tarayıcı, "mac id" bilgileri) ile karar verilmesi ise, SİBERMETRİK bir doğrulama olmaktadır.

İki Faktörlü Doğrulama, iki farklı vesileyle kimliğin doğrulanmasıdır.

Tipik ve yaygın olarak, SAHİP OLUNAN ve BİLİNEN iki unsurun kontrolü ile doğrulama yapılır.

VARLIĞA AİT olan karakteristik ve biyolojik unsurlarla (Biyometriklerle) kimliğin doğrulanması ise, biyometrik okuyucu donanımları, biyolojik verilerin sağlanması, saklanması ve korunmasına ilişkin yüksek maliyetler nedeniyle daha kısıtlı olarak çok özel ve kritik süreçlerde kullanılmaktadır. Yani, biyometrik doğrulamalarda maliyet ile hata payı ters orantılı olmaktadır. Bu yüzden, yaygın ve yoğun şekilde doğrulama gerektiren durumlarda, örneğin internet bankacılığı işlemlerinde, katlanılamaz maliyetler söz konusu olacağından, Biyometriklerle kimlik doğrulama tercih edilmemektedir.

Ayrıca, sır (gizli) olmadıkları (dokunduğumuz her yerde parmak izimizi bırakıyoruz, gözlerimizle her an her yere bakıyoruz), yani kolayca elde edilebilmeleri, rastsal ve yenilenebilir olmadıkları, iptal edilemedikleri için, Biyometrikler, PIN(*) (Personel Identification Number) yani kimliği tanıtıcı, ibraz edici, sabit bir kullanıcı kodu olarak veya adımız soyadımız gibi kullanılmaya çok daha uygundurlar.

Bu arada, PIN ifadesi, dilimizde şifre olarak geçmekte ise de, bu tanımlamalardan da anlaşılacağı gibi, ŞİFRE için doğru ifade PASSWORD (alfabetik) veya PASSCODE (alfa nümerik) olmalıdır.

3. BDDK Tebliği ve İki Faktörlü Kimlik Doğrulama:

İki faktörlü doğrulamada, sahip olunan faktöre ilişkin güç farkını, bankacılık sektöründen örnekleyerek açıklamak durumu çok somutlaştıracaktır.

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından, 14 Eylül 2007' de Resmi Gazete' de yayınlanarak yürürlüğe giren ve 01 Ocak 2010 itibarıyla bankaların yükümlü olduğu, "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" in, İnternet Bankacılığı bölümünde, Kimlik Doğrulama başlığı altında düzenlenen 27. Maddesinin 4. Fıkrasında, "Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir." diyerek iki faktörlü doğrulamayı ifade etmiştir.

Aynı maddede,

"Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık

parola gibi bileşenler kullanılabilir." denilerek, faktörler örneklenmiş ve daha da önemlisi, "sahip olunan" unsur olarak, BDDK tarafından kabul ve tebliğ edilen yöntemler tanımlanmıştır.

Burada, "kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir" ifadesi ile halen bankaların internet şubesi kanalında, kullanıcı/müşteri kimliğini doğrulama amacıyla, en yaygın şekilde kullanılan – aslında tercihe bırakıldığı için, güvenlik algısı gelişmemiş ve farkındalığı tam oluşmamış ortalama internet kullanıcısı müşterilerin "kolay" olduğu için tercih ettiği – banka tarafından üretilip GSM hatlarına (cep telefonlarına), müşterinin abonesi olduğu GSM İşletmecisi firma aracılığı ile Kısa Mesaj Servisi (SMS) mesajı olarak iletilen Tek Kullanımlık Parola'ların (şifre) "müşterinin sahip olduğu" bir unsur olarak kabul edildiği açıkça belirtilmektedir.

Teorik olarak ise, belirtilen yöntemde, GSM hattına, ne kadar "sahip olunduğu" ve o hatta ulaştırılan SMS mesajının (şifre içeren) gerçekten de kimliği doğrulanmaya çalışılan kullanıcı/müşterinin hattına ulaşıp ulaşmadığı konusunda mutlak bir doğruluktan söz etmek mümkün değildir.

4. Tasarlanan teknoloji: INTERSECT

Tasarlanan algoritma ile

- username bir bilgisayar sisteminden,
- password ve/veya OTP vb. key ler(ve/veya Intersect Key ler) başka bir sistemden(bilgisayarların internet e bağlanırken aldığı farklı IP ler üzerinden)

iletilmektedir.

Username in girildiği bilgisayar sistemi

- 3 karakterlik genetik bir kod üretir.

Diğer bir bilgisayar sisteminden

- Üretilen genetik kod ile birlikte password ve/veya OTP vb key ler (ve/veya Intersect Key ler) girilir.

Algoritma, iki farklı bilgisayar sisteminden, **birinin user login işlemi, diğerinin password ve/veya OTP vb (ve/veya Intersect Key) girişi işlemi** yapmak istediğini **çözer.**

İkinci bilgisayar sisteminden girilen **password ve/veya OTP vb key ler (ve/veya Intersect Key ler)**

- ✓ **doğru ise**, user login olunmak istenen birinci bilgisayar sistemi user **a login olma izni verir**,
- ✓ **doğru değil ise user** login olunmak istenen birinci bilgisayar sistemi user a **login olma izni vermez**.

4.1 Intersect Yönteminin Çalışması

INTERSECT Yöntemi, aşağıdaki 3 temel kural altında çalışır:

1. Username ve Password hiçbir zaman aynı network üzerinde bir arada bulunmaz.
2. Username ve passwordun bir araya geldiği tek yer erişilmek istenen server dır. Ancak server'da username ve password eşleşmesi kabul edildiği durumda giriş sağlanır.
3. İki farklı network ve iki farklı bilgisayar sistemi kullanılır.

Herhangi iki network trafiğini takip etmek, mevcut tüm network trafiğini takip etmek anlamına gelir ki bu imkânsız olmasa da çok zordur. Herhangi iki bilgisayar arasında ilişki kurabilmek ise, istatistik olarak imkânsızdır. Bu yüzden, herhangi iki network arasındaki ilişkinin kurulması ve kullanıcı kimlik bilgilerinin ele geçirilmesi imkânsızdır.

4.2 Intersect Kullanım Alanları

- ✓ Tüm Operating System yöneticileri
- ✓ Tüm Web Server yöneticileri
- ✓ Tüm Yazılım geliştiriciler
- ✓ Tüm kurumsal uygulama yazılımı kullanıcıları
- ✓ Tüm kurumsal ve/veya bireysel internet bankacılığı kullanıcıları
- ✓ Tüm ATM kullanıcıları
- ✓ Tüm internet üzerinden kredi kartı ile alışveriş yapan kişi ve kurumlar

Intersect ile güvenle işlem yapabilirler.

Referanslar:

1) http://www.bilgiguvenligi.gov.tr/kimlik-yonetimi/kimlik-dogrulama-faktorler-ve-bilesenleri.html

2) Oracle® Access Manager Integration Guide". Oracle Corporation. August 2007. "[...] the RSA ACE/Server®, which has been renamed to the Authentication Manager."

3) TOTP: Time-based One-time Password Algorithm

4) Sample SecurID Token Emulator with Token Secret Import

5) RSA SecurID SID800 Hardware Authenticator [dead link]

6) http://www.process.com/tcpip/tcpware57docs/User_Guide/ch14.htm#E53E27

7) RSA Security to enable ubiquitous authentication as RSA SecurID(r) technology reaches everyday devices and software;. - M2 Presswire | HighBeam Research: Online Press Releases

8) "Testing Multiple Factors Authentication (OWASP-AT-009)".

9) "Does RSA SecurID have a US gov't-authorized back door?".

10) "Towards a Book on Advances in Cryptovirology, Chapter 10".

11) "Simple Backdoors for RSA key generation".

12) "A Comprehensive Study of Backdoors for RSA Key Generation".

13) ”RSA SecurID Solution Named Best Third-Party Authentication Device by Windows IT Pro Magazine Readers’ Choice 2004". RSA.com. 2004-09-16. Retrieved 2011-06-09.

14) Diodati, Mark (2010). "Road Map: Replacing Passwords with OTP Authentication". Burton Group. "Gartner's expectation is that the hardware OTP form factor will continue to enjoy modest growth while smartphone OTPs will grow and become the default hardware platform over time. ... If the organization does not need the extensive platform support, then OATH-based technology is likely a more cost-effective choice."

15) "Open Letter to RSA Customers".

16) "EMC / RSA 8K filing". Form 8-K. The United States Securities and Exchange Commission. 17 March 2011.

17) Rivner, Uri (1 April 2011). "Anatomy of an Attack". Speaking of Security - The RSA Blog and Podcast.

18) Mills, Elinor (5 April 2011). "Attack on RSA used zero-day Flash exploit in Excel". CNET.

19) Goodin, Dan (24 May 2011). "RSA won't talk? Assume SecurID is broken". The Register.

20) Messmer, Ellen (18 March 2011). "Did hackers nab RSA SecurID's secret sauce?". Network World.

21) Bright, Peter (6 June 2011). "RSA finally comes clean: SecurID is compromised". Ars Technica.

22) Gorman, Siobhan; Tibken, Shara (7 June 2011). "Security 'Tokens' Take Hit". Wall Street Journal.

23) Gorman, Siobhan; Tibken, Shara (7 June 2011). "RSA forced to replace nearly all of its millions of tokens after security breach". News Limited.

24) Mills, Elinor (6 June 2011). "China linked to new breaches tied to RSA". CNet.

25) Leyden, John (27 May 2011). "Lockheed Martin suspends remote access after network 'intrusion'". The Register.