Sosyal Medya Sitelerinin Kullandıkları Şifre Paketlerine Göre Sınıflandırılması

Mirsat Yeşiltepe, Muhammet Kurulay

***Abstract*— Today use rate of social media is a rapidly increasing. They were categorized due to the variety of tasks undertaken by these sites. Ranking among other sites of social media sites aim in this study and are classified according to their security cipher suite used by various parameters. Thus, the decision will be given to the security mechanisms at various levels should carry the newly created social media sites.**

***Index Terms*— By rating , encryption, protocol, social media sites.**

***Özet*— Günümüzde sosyal medya sitelerinin kullanım oranı artan bir hızla artmaktadır. Bu sitelerin üstlendikleri görevlerin çeşitliliği sebebiyle kategorize edilmişlerdir. Bu çalışmada amaç sosyal medya sitelerinin diğer siteler arasındaki sıralaması ve kendi kullandıkları güvenlik şifre paketlerine göre çeşitli parametrelerle sınıflandırılmaktadır. Böylelikle yeni oluşturulacak sosyal medya sitelerinin taşıması gereken güvenlik mekanizmalarına çeşitli düzeylerde karar verilmeye çalışılacaktır.**

***Anahtar Terimler*— Protokol, reyting, sosyal medya siteleri, şifreleme.**

I. GİRİŞ

BU çalışmada çoğu web uygulamaları tarafından çeşitli nedenlerle kullanılan ve kullanımı artan sosyal medya sitelerinin[1] sahip olduğu güvenlik mekanizmaları incelenmiştir. Bu çalışmada günümüzde en çok kullanıcı sayısına sahip on beş site üzerinden inceleme yapılacaktır. Esas amaç sosyal medya sitelerinin isimleri üzerinden sitelerin karşılaştırılması olmadığından sitelerin isimlerine yer verilmemiştir. Sonraki bölümlerde sosyal medya sitelerinin tüm siteler içindeki sıralaması incelenmiş sonra güvenlik mekanizmaları özet ve özellikleri biçiminde incelenecektir. Sonuç bölümünde ise yeni oluşturulmak istenen sitelerin taşıması gereken güvenlik mekanizmaları parametrelerine karar verilecektir. Tüm test edilen ortamın test tarihi 15 Haziran 2015'tir.

II. SOSYAL MEDYA SİTELERİNİN REYTİNGLERİ

Tablo I'de sosyal medya sitelerinin tüm siteler arasındaki sıralaması üç adet site sıralayıcısı tarafından alınan bilgilere göre elde edilmiştir. Siteler sıralanırken kullanıcı sayısı dikkate alınılmıştır[2].

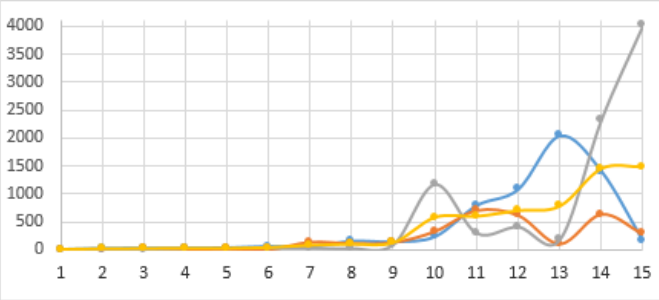
TABLO I
SOSYAL MEDYA SİTELERİNİN TÜM SİTELER ARASINDAKİ SIRALAMASI VE KULLANICI SAYILARI

Site Sırası	Kullanıcı Sayıları	Sıralayıcı 1	Sıralayıcı 2	Sıralayıcı 3
1.	900.000.000	3	3	2
2.	310.000.000	21	8	8
3.	255.000.000	25	19	9
4.	250.000.000	27	13	26
5.	120.000.000	32	28	
6.	110.000.000	55	13	34
7.	100.000.000	49	145	36
8.	80.000.000	150	120	21
9.	65.000.000	138	139	91
10.	42.000.000	231	335	1172
11.	40.000.000	791	701	296
12.	38.000.000	1.082	615	408
13.	37.000.000	2.046	113	179
14.	15.500.000	1407	635	2328
15.	15.000.000	153	285	4022

Tablo I incelendiğinde sosyal medya sitelerinin kullanıcı sayıları ile tüm siteler arasında bir ilişki olduğu fakat bunu kuvvetli bir biçimde olmadığı gözlemlenmiştir. Kullanıcı sayısı azaldıkça sitelerin sıralaması kurallılıktan uzaklaşmaya başlamıştır. Buradan sitelerin sıralaması ile siteyi kullanan kullanıcı sayısı ilk başta sıralamasını belirleyen önemli bir faktör olarak görülürken, sıralama düştükçe bu bağ zayıflamış ve bazende ilişki ortadan kalmıştır. Bundan sonraki bölümlerde bu sıralamada güvenlik mekanizmalarının etkisinin olup olmadığı tartışılacaktır.

Sıralayıcı 1, sıralayıcı 2 ve sıralayıcı 3'ün sosyal medya sitelerini tüm siteler içinde sıralarken hangi parametreleri kullandıklarından çok sitelerin kullandıkları şifreleme paketlerinin güvenlik düzeylerinin hangi sıralayanın daha önem vermiş olabileceği fikri üzerinde durulmuştur.

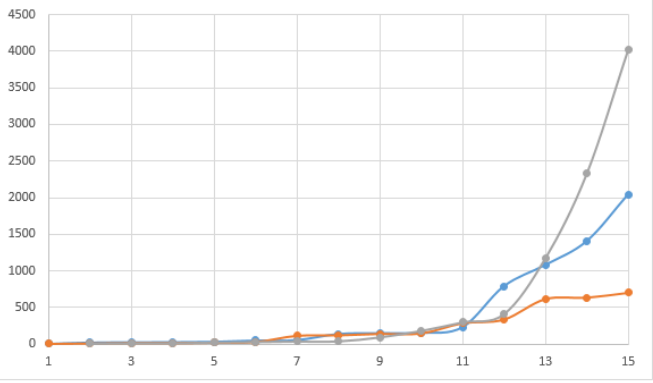
TABLO II
SOSYAL MEDYA SİTELERİNİN TÜM SİTELER ARASINDAKİ SİTELERİN SIRASI



Tablo II'de yatay eksen sitelerin sırasını düşey eksen ilgili sitenin sıralayıcılar tarafından belirlenen sırasını göstermiştir. Mavi renk 1. sıralayıcıyı, turuncu renk ikinci sıralayıcı, gri renk 3. Sıralayıcıyı, sarı renk ise sıralayıcıların ortalamasını göstermiştir.

Tablo II incelendiğinde site sıralayıcıları arasında birinci ve üçüncüsü birbirine uyumlu iken ikinci sıralayıcı diğerlerinden farklı bir eğilim göstermiştir. Fakat sıralayıcıların ortalaması alındığında ise sitelerin sıraları ile kullanıcı sayıları uyumlu olduğu gözlemlenmiştir.

TABLO III
SOSYAL MEDYA SİTELERİNİN TÜM SİTELER ARASINDAKİ SIRALANIŞINDAN BAĞIMSIZ OLARAK SIRALANMASI



Tablo III'de yatay eksen sitelerin sırasını, düşey eksen ilgili sitenin sıralayıcılar tarafından belirlenen sıralaması gösterilmiştir. Burada amaç site sıralayıcılarının kendi içlerindeki uyumunun gösterilmek istenmesidir. Sitelerin reytingleri artan olarak (sitelerin sıralanışından bağımsız olarak) gösterilmiştir. 1. ve 2. site sıralayıcısının 3.'süne göre daha uyumlu oldukları gözlemlenmiştir.

III. SOSYAL MEDYA SİTELERİNİN GÜVENLİK MEKANİZMALARI ÖZETİ

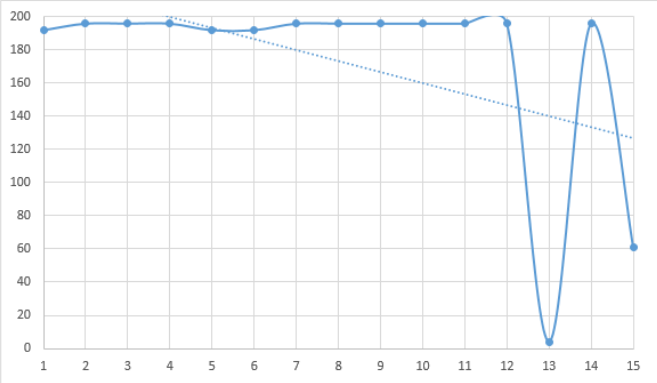
Şifre paketi kavramı kimlik doğrulama, şifreleme, mesaj kimlik doğrulama kodu (MAC), anahtar değişim algoritmalarının Transfer Seviye Güvenlik (TLS), Güvenlik Soket Katmanı (SSL) protokollerinden biri kullanılarak çeşitli güvenlik belirtimlerinin bir bütün olarak açıklamasıdır. Bu sebeple bu kavramı bir bütün olarak düşünülmesi gerekir. Şifre paketleri seviyelerine göre sıralanmıştır[3][6].

TABLO IV
SOSYAL MEDYA SİTELERİNİN ŞİFRE PAKETLERİ

PAKET TANIMLAYICISI	ŞİFRE PAKETİ İSMİ
0x00C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0x00C02B	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0x00C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x000004	SSL_RSA_WITH_RC4_128_MD5
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00003C	TLS_RSA_WITH_AES_128_CBC_SHA256

Tablo IV'de test edilen sosyal medya sitelerinin kullandıkları güvenlik mekanizmalarının kodları ve isimleri verilmiştir[4].

TABLO V
SOSYAL MEDYA SİTELERİNİN ŞİFRE PAKETLERİ GÜVENLİK DÜZEYLERİ



Tablo V'de yatay eksen sitelerin sırasını düşey eksen ilgili sitenin şifre paketinin güvenlik düzeyini gösterilmiştir. Güvenlik düzeyi ile anlatılmak istenen TLS ve SSL protokolünün ilgili şifreleme paketi türünü kaçıncı sırada belirttiğidir. Şifreleme paketleri türleri ilgili protokollerde güvenlik açısında artan düzende sıralanmıştır. Yani şifreleme paketi türü sonra belirtilen (paket tanımlayıcısı yüksek olan) şifreleme paketi bir bütün olarak daha güvenlidir. Sıralama için paket tanımlayıcısının belirttiği binary kod yerine paket sıralayıcı en az olana bir değeri verilerek sıralanmıştır. Test edilen sosyal medya sitelerinin kullandıkları şifre paketlerinin türleri seviyelerine göre listelenmiştir. Paket tanımlayıcıları bir bütün olarak sıralanmıştır. Yani paketin tanımlayıcısının değerinin büyük olması şifreleme paketinin daha güçlü olduğunu gösterir. Tablo incelendiğinde 13. ve 15. site haricinde diğer sitelerin kullandıkları şifre paketlerinin güvenlik düzeylerinin yakın olduğu gözükmüştür. Genel olarak bakıldığında ise eğim çizgisinin aşağı yönlü olduğundan sitelerin kullanıcı sayıları ile şifre paketlerinin genel olarak uyumlu olduğu sonucu çıkarılabilir. 13. sosyal medya sitesinin özel durumu için birinci ve üçüncü sıralayıcının yukardaki duruma uygun sonuçlar içerdiği ikinci sıralayıcının ise bu durumu göz ardı ettiği görülmüştür. Son olarak çıkarılacak durum site reytinginin şifre paketleri ile ilişkisinin olduğudur.

IV. SOSYAL MEDYA SİTELERİNİN GÜVENLİK MEKANİZMALARININ ÖZELLİKLERİ

Bu bölümde isimleri veriler şifre paketlerinin özelliklerine değinilip sitelerin kullanıcı sayılarıyla ilişkili olup olmadığı incelenecektir.

Tablo VI ve tablo VII'da şifreleme paketlerinin içerdiği bilgiler iki guruba ayrılmıştır. Burada amaç şifreleme paketlerinin parçalarının sıralamaya olan etkisini incelemektir. Örneğin 13. Site anahtar değişim algoritması olarak ECDHE, kimlik doğrulama olarak RSA kullanmış, 14. Site ise her iki güvenlik belirtecinde RSA kullanmıştır. Eğer ki sadece şifreleme paketi düzeyinden (genel olarak) incelendiğinde 13. Sitenin güvenlik düzeyi düşük çıkacaktır. Fakat şifreleme paketi bu iki güvenlik düzeyi belirtecine göre incelenirse 13. Site daha yüksek çıkacaktır. Burada amaç güvenlik düzeyi düşük çıkanların kendilerinden düzeltmesi gereken yönleri belirlemeye çalışmaktır. Güvenlik düzeyinin artmasında şifreleme algoritmaların anahtar uzunlukları önemli olmakla birlikte tek başına yeterli değildir. Güvenlik bir bütündür.

TABLO VI
SOSYAL MEDYA SİTELERİNİN ŞİFRE PAKETLERİNİN ÖZELLİKLERİ

	PROTOKOL	ANAHTAR DEĞİŞİM ALGORİTMASI	KİMLİK DOĞRULAMA ALGORİTMASI
1.	TLS	ECDHE	ECDSA
2.	TLS	ECDHE	RSA
3.	TLS	ECDHE	RSA
4.	TLS	ECDHE	RSA
5.	TLS	ECDHE	ECDSA
6.	TLS	ECDHE	RSA
7.	TLS	ECDHE	RSA
8.	TLS	ECDHE	RSA

TABLO VI
SOSYAL MEDYA SİTELERİNİN ŞİFRE PAKETLERİNİN ÖZELLİKLERİNİN ÖZELLİKLERİ (DEVAM)

9.	TLS	ECDHE	RSA
10.	TLS	ECDHE	RSA
11.	TLS	ECDHE	RSA
12.	SSL	RSA	RSA
13.	TLS	ECDHE	RSA
14.	TLS	RSA	RSA
15.	SSL	RSA	RSA

Tablo VI'da test edilen sosyal medya sitelerinin protokol olarak çoğunlukla TLS kullandıkları gözlemlenmiştir. SSL'in iletişimde sertifika uyarı mesajı kullanmaması, sertifika doğrulama mesajı oluşturulabilmesinin mümkün fakat zor bir süreç olması gibi nedenlerden dolayı günümüzde TLS'in kullanımının artması[5] ve bu durumun test edilen sitelerde görülmesi normaldir. Test edilen 12. sosyal medya sitesinin SSL kullanma durumu birinci ve üçüncü site sıralayıcısında önem arz etmekte iken, 15. sosyal medya sitesinin SSL kullanması sadece üçüncü site sıralayıcısında önem arz etmiştir. Genel olarak üçüncü site sıralayıcısı site sıralarının belirlerken kullanılan protokole daha çok ilgilendiği sonucu çıkarılabilir.

Anahtar değişimi algoritmalarının kullanımlarındaki esas amaç iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Test edilen sosyal medya sitelerinin anahtar değişim algoritması olarak çoğunlukla ECDHE kullandıkları, 12. 14. ve 15. Sosyal medya sitelerinin ise RSA kullandıkları gözlemlenmiştir. Test edilen çoğu sitenin ECDHE kullanmasının nedeni bu şifreleme türünün kullanılan şifreleme bit sayısı attığında RSA'ya göre hızının artmasıdır. Diğer bir neden sitelerin yeni teknolojilerle uyumlu olma istediğidir[6]. Bulut ile iletişimde hızın önemi ortada olması ECDHE'nin bir başka tercih nedenidir. RSA kullanan sitelerin bu durumlarının sıralayıcılarında etken olarak en iyi gören üçüncü sıralayıcıdır.

Sunucu kendisindeki bilgi veya siteye erişimi sağlayanın tam olarak kim olduğunu bilmesi gerektiğinde kimlik doğrulama kullanılır. Kimlik doğrulamasında, kullanıcı veya bilgisayar / sunucu veya istemci kimliğini karşı tarafa kanıtlamak zorundadır. Genellikle, bir sunucu tarafından kimlik

doğrulama, kullanıcı adı ve parola kullanımını gerektirir. Test edilen sosyal medya sitelerinin kimlik doğrulaması olarak genellikle RSA kullandıkları, 1. ve 5. sosyal medya sitesinin ise ECDSA kullandığı gözlemlenmiştir. Fakat bu durum site sıralayıcıları için özel bir durum oluşturmamıştır. Anahtar değişimde RSA az kullanılırken kimlik doğrulamada RSA'nın daha yaygın kullanılmasının en önemli nedeni kimlik doğrulama mekanizmasının oluşturulmasındaki zorluktur[9].

TABLO VII
SOSYAL MEDYA SİTELERİNİN ŞİFRE PAKETLERİNİN ÖZELLİKLERİ (DEVAM)

	SİMETRİK ŞİFRELEME ALGORİTMASI	SİMETRİK ŞİFRELEME ANAHTAR UZUNLUĞU	HASH ALGORİTMASI
1.	AES_128_GCM	128	SHA256
2.	AES_128_GCM	128	SHA256
3.	AES_128_GCM	128	SHA256
4.	AES_128_GCM	128	SHA256
5.	AES_128_GCM	128	SHA256
6.	AES_128_GCM	128	SHA256
7.	AES_128_GCM	128	SHA256
8.	AES_128_GCM	128	SHA256
9.	AES_128_GCM	128	SHA256
10.	AES_128_GCM	128	SHA256
11.	AES_128_GCM	128	SHA256
12.	AES_128_GCM	128	SHA256
13.	AES_128_GCM	128	SHA256
14.	AES_128_GCM	128	SHA256
15.	AES_128_GCM	128	SHA256

Test edilen sitelerin simetrik şifreleme algoritması, simetrik şifreleme anahtar uzunluğu ve hash algoritması parametrelerinin aynı olduğu gözlemlenmiştir.

Hash fonksiyonu, değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan algoritma veya alt programdır. Genelde SHA ve MD5 türleri kullanılır. SHA'nın kullanımındaki amaç tek seferde daha çok biti özümseyebilmesidir (hash) [10].

V. SONUÇ

Sosyal medya sitelerinin reytinglerinin belirlenmesinde kullanıcı sayılarının ve şifre paketlerinin ilişkisi vardır. Kullanıcı sayısının fazla olduğu siteler daha güçlü şifreleme paketi tercih etmişlerdir. Fakat sitelerin genel olarak belirli bir seviyedeki şifre paketleriyle çalıştığı gözlemlenmiştir. Elbette ki siteler sıralanırken ortamdaki birçok parametre kullanılmıştır. Fakat şifre paketlerindeki farklılıklardan sitelerin sıralamaması etkilenmiştir. Sitelerin verimli olabilmesi için kendilerine en uygun şifre paketlerinin belirlenip kullanılması gerekir.

Test edilen sosyal medya sitleri genellikle protokol olarak TLS, anahtar değişim algoritması olarak ECDHE, kimlik doğrulama algoritması olarak RSA, simetrik şifreleme algoritması olarak AES_128_GCM, simetrik şifreleme anahtar uzunluğu olarak 128 değerini ve hash algoritması olarak SHA256 kullanılmıştır.

Günümüzde oluşturulmak istenen sosyal medya sitelerinin taşıması gereken en düşük seviyeli şifre paketi TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 iken yapılabilinecek saldırılardan kurtulmak için şu anki sosyal medya sitelerinden daha çok güvenlik mekanizması taşınılması gerektiği düşünülerek ya hash algoritması olarak SHA256 yerine SHA384 kullanarak TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 veya anahtar değişim algoritması olarak ECDH kullanarak TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 şifre paketi kullanılmaları tavsiye edilir. Eğer uzun dönemde kurulacak sitelerin güvenlik mekanizmaları ile mekanizmaların maliyeleri düşünüldüğünde yine bu şifre paketlerinin şu an için kullanılması tavsiye edilebilir. Ama uzun dönemde SSL2 daha uzun dönemde PCT protokollerinin kullanımları düşünülebilir. Bu protokollere uyumlu güvenlik ortamlarına uygun ortamlar yedekte hazır bulundurulabilir. Çünkü günümüzde yapı bilinecek saldırılara karşı sitelerin mümkün olan en kısa sürede yeni ortama adapte olması gerekir. Olmaması durumunda yeni ortam bu site için kalitenin düştüğü bir ortam olacaktır.

KAYNAKLAR

[1] Boyd, Danah. "Why youth (heart) social network sites: The role of networked publics in teenage social life." MacArthur foundation series on digital learning–Youth, identity, and digital media volume (2007): 119-142.

[2] Huyensau, "Top 5 Trendiest Social Networking Sites in 2015", http://www.toplisttips.com/top-5-trendiest-social-networking-sites-update-january-2015/ , 14 Haziran 2015.

[3] Ristic, Ivan. "SSL/TLS Deployment Best Practices." URL https://www. ssllabs. com/downloads/SSL_TLS_Deployment_Best_ Practices_1. 0. pdf (2013).

[4] The Sprawl, "Researchtls and SSL Cipher Suites - Known cipher suites", https://www.thesprawl.org/research/tls-and-ssl-cipher-suites/ , 16 Haziaran 2015.

[5] Rescorla, Eric. SSL and TLS: designing and building secure systems. Vol. 1. Reading: Addison-Wesley, 2001.

[6] Mishra, Vivek. "Cassandra Data Security." Beginning Apache Cassandra Development. Apress, 2014. 61-78.

[7] Nagaraju, Mr S., and Mr B. Latha Parthiban. "An Enhanced Symmetric Role-Based Access Control Using Fingerprint Biometrics for Cloud Governace.".

[8] Çeviri:Mesut Timur -OWASP GUIDE 2.0.1, 2007.

[9] Fu, David E., and Jerome A. Solinas. "IKE and IKEv2 authentication using the elliptic curve digital signature algorithm (ECDSA)." (2007).

[10] Krawczyk, Hugo, Ran Canetti, and Mihir Bellare. "HMAC: Keyed-hashing for message authentication." (1997).