YOON- RYU- YOO UZAKTAN KİMLİK DOĞRULAMA YÖNTEMİNİN KRİPTO ANALİZİ

Esma Ergüner Özkoç, Tuncay Ercan
Yaşar Üniversitesi, Mühendislik-Mimarlık Fakültesi, İzmir
esma.erguner@yasar.edu.tr; tuncay.ercan@yasar.edu.tr;

ABSTRACT

Nowadays with the widespread use of Internet resources, remote user authentication has become an important process to provide the security of the different systems. The process determines the identity of a person who is attempting to access the system. Various cryptographic algorithms are used in remote user authentication schemes used in smartcards to provide better security.

In this work, we analyzed remote user authentication scheme proposed by Yoon et al [1].

Key words: Security, Password Authentication, Guessing Attack, Smartcard.

1. GİRİŞ

Uzaktaki bir sistemin kaynaklarına erişim için kullanıcıların giriş izinlerinin olması gerekmektedir. Bu amaçla güvensiz ağlarda kullanılan en basit yöntem; şifreli kimlik doğrulamadır. Bu yöntem ile güvenliğin temel ilkelerinden olan bütünlük ve güvenilirlik sağlanmaktadır. Birçok internet uygulaması, okul sistemleri, özel şirketler, resmi kuruluşlar şifreli kimlik doğrulama yöntemlerini kullanmaktadır. Ancak günümüz koşullarını ele alırsak, sadece şifre ile kimlik doğrulama yapılmasının saldırılara karşı büyük bir hassasiyet yaratacağı açıktır. Bu sebepten dolayı kimlik doğrulama için birçok araştırma yapılmış ve çok sayıda yöntem önerilmiştir.

Kimlik doğrulamanın en çok bilinen ve en kolay uygulanabilen yöntemi, kullanıcının kendi tanıtıcı (ID) bilgisi ve şifresi ile sistemin kaynaklarına erişmesidir. Özetle işlem şu şekilde gerçekleşir; sunumcu tarafında tutulan ID ve şifre tablosunda, kullanıcının girdiği ID aranır; bulunursa girilen şifre ile tablodaki şifre karşılaştırılır, eşleşirse kullanıcıya sistemin kaynaklarına erişim izni verilir. Ancak bu sistemde şifre tablosunun sunumcuda tutulması büyük güvenlik açığı oluşturmaktadır. Milyonlarca kullanıcının olduğu düşünülürse sistemde her defasında kullanıcı ID ve şifresinin aranıyor olması, sistem kaynaklarını etkilemesi sebebiyle tablo kullanmanın ayrı bir dezavantajı olarak ortaya çıkar. Araştırmalar sonucunda bu probleme en iyi çözümün sunumcu tarafında bir doğrulama tablosu tutulmaması olduğuna karar verilmiştir.

Güvenliği sağlamak amacıyla, uzaktan kimlik doğrulama için birçok yöntem geliştirilmiştir. Genel olarak geliştirilen kimlik doğrulama yöntemlerini sınıflandıracak olursak [2];

- Bir şeyler bilerek kimlik doğrulama (örneğin; Şifre)
- Bir şeylere sahip olarak (örneğin; Akıllı kart)
- Bazı karakteristik özellikleri kullanarak (örneğin; Parmak izi)

1.1 Önceki çalışmalar

Sistemin güvenliği bu yöntemler farklı kombinasyonlarla kullanılarak arttırılabilir. Son zamanlarda üzerinde en çok araştırma yapılan kombinasyon, akıllı kart ve şifre kullanarak yapılan kimlik doğrulama yöntemidir. Akıllı kart kullanılmasının amacı, aritmetik işlemleri yapabilmesi ve bazı bilgileri saklayabilmesidir. Ayrıca akıllı kartın sahip olduğu mikroişlemci, RAM, I/O ve ROM ile de sunumcuda ayrı bir tablo tutulmasına gerek kalmamaktadır. Akıllı kart ve şifre kombinasyonu yöntemi ile birçok yöntem geliştirilmiştir [2,3,4,6,9].

Yapılan çalışmalar ile doğrulama için şifre kullanan ideal bir yöntemde olması gereken özellikler belirlenmiştir [2,3]:

1- Sunumcu tarafında herhangi bir şifre veya doğrulama tablosu saklanmamalıdır.
2- Şifre kullanıcı tarafından seçilebilmeli ve istendiği takdirde kolaylıkla değiştirilebilmelidir.
3- Şifre sistem yöneticisi tarafından görülmemelidir.
4- Şifreler düz metin halinde güvenli olmayan ağda iletilmemelidir.
5- Şifre akılda kolay tutulacak uzunlukta olmalıdır.
6- Yöntem hesaplama kolaylığına sahip ve çalışma zamanı konusunda verimli olmalıdır.
7- Kullanıcının yanlış şifre girdiği kolaylıkla tespit edilebilmelidir.
8- İletişimin güvenilirliğini sağlamak için oturum anahtarı üretimi doğrulama fazında olmalıdır.

Ö9- Kullanıcının bağlantı mesajında kısmi kayıpları önlemek amacıyla ID dinamik olarak her bağlantıda değişmelidir.
10-Sunumcunun gizli anahtarının kaybolması veya çalınması durumunda bile kullanılan yöntem güvenilir olmalıdır.

1.2 Notasyon

Şekillerde kullanılan ifadeler Tablo 1.de açıklanmıştır.

PW	Kullanıcı şifresi
ID	Kullanıcının tanımlayıcısı
S	Uzak sistem / sunumcu
h(.)	Tek yönlü özetleme fonksiyonu
$\oplus$	Mantıksal harici veya operasyonu
x	S'nin gizli anahtarı
T_u	Kullanıcının o anki zamanı
T_s	Uzak sistemin o anki zamanı

Yoon, Ryu ve Yoo, Hwang, Lee ve Tang 'ın önerdikleri akıllı kart kullanan uzaktan kimlik doğrulama yönteminin [15] eksik yönlerini gidererek ve yöntemin avantajlı yönlerini aynen alarak yeni bir yöntem önermişlerdir.
Yoon, Ryu ve Yoo'nun Hwang, Lee ve Tang yöntemine ekledikleri güvenlik özellikleri şunlardır[1]:

1.Kullanıcı şifresini özgürce seçip değiştirebilmektedir.
2. Akıllı kart çalınarak uygulanan servis durdurma saldırılarına karşı yöntem güvenlidir.
3. Sunumcunun gizli sayısı (x) çalınsa dahi hesaplanan özet değerleri güvendedir.
4. Sunumcu aldatma saldırılarına karşı yöntem çift taraflı doğrulama (mutual authentication) sağlanılarak korunmaktadır.
5.Kullanıcının girdiği yanlış şifrenin tespiti hızlıdır.
6.Daha önce önerilen yöntemlere kıyasla yöntemin hesaplama maliyeti düşüktür.

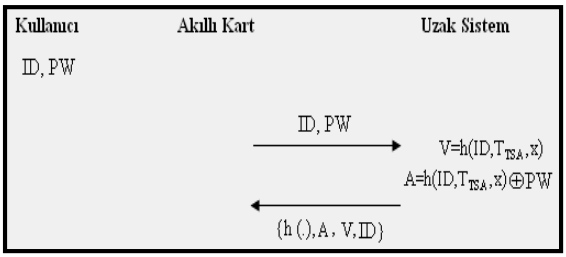
Yoon, Ryu ve Yoo'nun ekledikleri bu özelliklere rağmen yöntemin güvenlik eksiklikleri mevcuttur.
Bu bildiride öncelikle Yoon, Ryu ve Yoo'nun önermiş oldukları akıllı kart kullanan kimlik doğrulama yöntemi detaylı olarak verilecek, sonra yöntemin güvenlik gereksinimleri kripto analizi yapılarak incelenecektir.

2. YOON- RYU- YOON YÖNTEMİ

2004 yılında Yoon, Ryu ve Yoo, Hwang, Lee ve Tang [15]'in geliştirdikleri yöntemin zayıflıklarını gidererek önerdikleri yeni yöntem [1] Kayıt, Bağlantı, Doğrulama ve Şifre değiştirme olmak üzere dört fazdan oluşmaktadır.

2.1 Kayıt Fazı

Her kullanıcı için yalnızca bir kez ve güvenli bir ağ üzerinde gerçekleşen faz şu şekildedir; Kullanıcı PW seçer ve ID ile birlikte güvenli bir kanaldan uzak sisteme iletir. Uzak sistemde V ve A değerleri Şekil 1'deki gibi hesaplandıktan sonra ID, V, h(.) ve A değerleri akıllı karta yazılır.

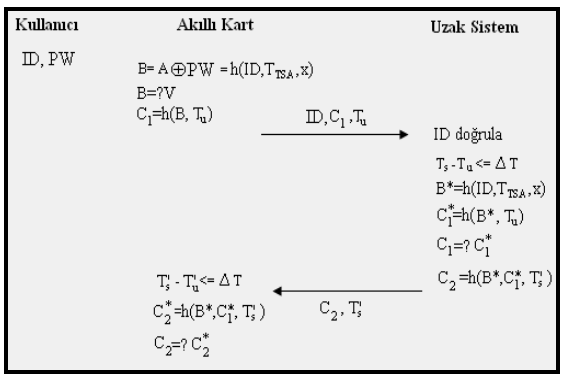


Şekil 1 Yoon Ryu Yoo Yöntemi Kayıt Fazı

Yöntemde kullanılan TSA, Zaman Mührü Otoritesidir, istenildiği anda o anki zamanı sağlamaktadır. Kayıt fazı Şekil 1 de özetlenmiştir. Şekildeki T_{TSA} Zaman mührü otoritesi tarafından sağlanan o anki zamanı temsil etmektedir.

2.2 Bağlantı Fazı

Kullanıcı uzak sisteme bağlanmak istediğinde akıllı kartını kart okuyucuya yerleştirir ve PW ile ID yi sisteme girer. Akıllı kartta B değeri hesaplanır. Hesaplanan B ile daha önceden akıllı karta kaydedilmiş V değeri karşılaştırılır. Eğer aynı ise C_1 hesaplanır. C_1, T_u ve ID'nin uzak sisteme gönderilmesiyle bağlantı fazı sona erer. Bağlantı ve Doğrulama fazı Şekil 2'de birlikte gösterilmektedir.



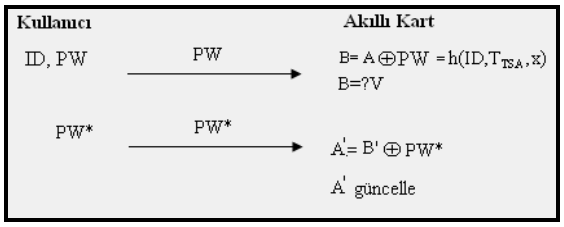
Şekil 2. Yoon Ryu Yoo Yöntemi Bağlantı-Doğrulama Fazı

2.3 Doğrulama Fazı

Bağlantı mesajını (ID, C_1, T_u) alan uzak sistem, önce gönderilen ID'nin istenilen formatta olup olmadığını kontrol eder, istenen formatta ise zamanın makul aralıkta olup olmadığına bakar. Eğer zaman da uygun ise B^* ve C_1^* hesaplanır; Hesaplanan C_1^* ile gönderilen C_1 eşit ise uzak sistem kullanıcıyı doğrulamış olur. Kullanıcının da uzak sistemi doğrulaması için C_2 değeri hesaplanır. Buradaki T_s, uzak sistemin o anki zamanını temsil eder. C_2 ve T_s akıllı karta gönderilir. Burada da önce zaman kontrol edilir ve C_2^* hesaplanır. Eğer hesaplanan değer ile gönderilen değer aynı ise kullanıcı da uzak sistemi doğrular ve böylece çift taraflı doğrulama gerçekleşmiş olur (Mutual Authentication). (Şekil 2)

2.4 Şifre Değiştirme Fazı

Kullanıcı şifresini değiştirmek istediğinde uzaktaki sisteme bağlanmadan akıllı kartta işlem gerçekleştirilir. Kullanıcı akıllı kartını yerleştirdikten sonra PW girer, akıllı kartta B değeri hesaplanır. Hesaplanan B ile kayıtlı V değeri karşılaştırılır eşit ise kullanıcı PW değiştirme hakkına sahiptir. Yeni PW^* girilir. Ve girilen PW^* ile A' değeri hesaplanır. Akıllı karttaki A ile hesaplanan A' yer değiştirilir. Böylece kullanıcı şifresini değiştirmiş olur (Şekil 3).



Şekil 3 Yoon Ryu Yoo Yöntemi Şifre Değiştirme Fazı

3. YOON- RYU- YOO YÖNTEMİNİN KRİPTO ANALİZİ

Önceki bölümde verilen Yoon, Ryu ve Yoo, yöntemi ideal kimlik doğrulama yöntemi özelliklerine göre değerlendirilirse,

—Sunumcu tarafında herhangi bir şifre veya doğrulama tablosu saklanmamaktadır.

—Şifre, kullanıcı tarafından seçilebilmekte ve istendiği takdirde kolaylıkla değiştirilebilmektedir.

—Şifreler düz metin halinde güvenli olmayan ağda iletilmemektedir.

—Şifre akılda kolay tutulacak uzunluktadır.

—Yöntem hesaplama kolaylığına sahip ve çalışma zamanı konusunda verimlidir.

Kayıt Fazı	**Bağlantı Fazı**	**Doğrulama Fazı**	**Şifre değiştirme Fazı**
$1T_h$ $1T_{XOR}$	$1T_h$ $1T_{XOR}$	$4T_h$	$2T_{XOR}$

Tablodaki T_h ve T_{XOR} sırasıyla, özet (hash) fonksiyonu hesaplama zamanı ve XOR işleminin hesaplama zamanını ifade etmektedir.

—Kullanıcının yanlış şifre girdiği uzak sisteme gidilmeden kolaylıkla tespit edilebilmektedir.

—Sunumcunun gizli anahtarının kaybolması veya çalınması durumunda dahi yöntem güvenilirdir.

Yöntemin sağladığı bu özelliklerin yanında ideal bir kimlik doğrulama yönteminde olması gereken fakat Yoon, Ryu ve Yoo, yönteminde bulunmayan özellikler şunlardır;

—Şifre sistem yöneticisi tarafından görülmemelidir. Fakat kayıt fazında kullanıcının girdiği şifre düz metin halinde güvenli ağda sunumcuya iletilmektedir.
—İletişimin güvenilirliğini sağlamak için oturum anahtarı üretimi doğrulama fazında olmalıdır Fakat bu yöntemde oturum anahtarı üretimi yoktur.
—Kullanıcının bağlantı mesajında kısmi kayıpları önlemek amacıyla ID dinamik olarak her bağlantıda değişmelidir. Fakat bu yöntem ID sabittir.
Ayrıca yöntemin çevrimdışı tahmin saldırısı ve akıllı kartın çalınması durumunda servis durdurma saldırısına karşı zayıflıkları mevcuttur.

3.1 Tahmin Saldırıları

İdeal kimlik doğrulama yönteminde olması gereken özelliklerden biri olan şifrenin akılda kolay tutulabilmesi özelliği, saldırganlar için de şifrenin tahminini kolaylaştırmaktadır. Şifrenin tahmini çevrimiçi ve çevrimdışı olmak üzere ikiye ayrılmaktadır. Saldırganın doğru şifreyi bulup sunumcuya erişmek için sisteme sürekli tahmini şifre girmesi yöntemi "çevrimiçi tahmin saldırısı" olarak adlandırılır. Ancak sisteme yanlış şifre girişini sınırlandırılarak bu saldırı için kolaylıkla önlem alınabilmektedir.

Çevrimdışı tahmin saldırılarında ise saldırgan sunumcu ve kullanıcı arasındaki veri değişimi esnasında elde ettiği verileri kullanarak sisteme

bağlanmadan şifreyi tahmin etmeye çalışmaktadır. Bu saldırıdan iki yöntemle korunmak mümkündür: Birincisi kullanıcı ve sunumcu arasındaki mesajlaşmada şifre açıktan gönderilmemelidir. İkincisi ise önemli bilgilerin kaydedildiği akıllı kartın iyi korunmasıdır. Eğer akıllı kart çalınır veya kaybedilirse hafızasındaki bilgiler bazı fiziksel yöntemlerle açığa çıkarılabilir (power consumption). Yoon, Ryu ve Yoo yönteminde kayıt fazında akıllı kartın hafızasına A ve V değerleri kaydedilmektedir. Akıllı kartın kaybolması veya çalınması durumunda ise A ve V değerleri açığa çıkarılabilir.

$V=h(ID, T_{TSA}, x)$

$A=h(ID, T_{TSA}, x) \oplus PW \rightarrow A=V \oplus PW$

Buradan " $PW= A \oplus V$ " kolaylıkla hesaplanabilir. Dolayısıyla bu yöntem akıllı kartın kaybolması veya çalınması durumuna çevrimdışı tahmin saldırılarına karşı açıktır.

3.2 Tekrarlı Gönderme Saldırıları (replay attack)

Saldırgan, kullanıcı sisteme bağlanırken bilgilerini çalabilir ve sonraki bağlantıda bu verileri kullanıp sisteme bağlanabilir. Yoon, Ryu ve Yoo, bu saldırının önüne geçmek için zaman mührü (T_u-T_s) kullanmaktadır. Fakat zaman mührü kullanımı sunumcu ve kullanıcı arasındaki zaman senkronizasyonu problemini doğurur. Bu sebeple genelde zaman mührü yerine tekrarlı gönderme saldırılarından korunmak için tek kullanımlık sayılar (Nonce) tercih edilmektedir.

3.3 Servis Durdurma Saldırıları (Denial of Service Attacks)

Saldırganın kullanıcı bilgilerini yanlış girerek, yasal kullanıcının bir sonraki bağlantısını engelleme servis durdurma saldırısı olarak adlandırılır. Böylece yasal kullanıcının sisteme erişim hakkı engellenmiş olmaktadır.

Yoon, Ryu ve Yoo yönteminde şifre değiştirme fazı uzak sunumcuya bağlanmadan akıllı kart içinde yapılmaktadır. Bu da şifrenin güvensiz ağda iletimini engellediği için güvenliği arttırmaktadır. Yoon, Ryu ve Yoo önerdikleri yöntemin akıllı kartın çalınması veya ifşa edilmesi durumunda bile servis durdurma saldırılarına karşı güvenli olduğunu belirtmiştir. Ancak yöntemde akıllı karta geçici süre erişen saldırgan daha önce açıklanan çevrimdışı tahmin saldırısıyla şifreyi çözebilmektedir. Şifreyi çözen saldırgan kolaylıkla şifreyi değiştirip yasal kullanıcının sisteme girişini engelleyebilmektedir.

6. SONUÇLAR

Bu çalışmada, Yoon, Ryu ve Yoo'nun önerdikleri akıllı kart kullanan uzaktan kimlik doğrulama yöntemi güvenlik açısından incelenmiş, ideal kimlik doğrulama yöntemi özellikleri temel alınarak bütün özellikleriyle değerlendirilmiştir. Son olarak da bu yöntemin çevrimdışı tahmin saldırısı ve servis durdurma saldırılara karşı zayıflıklarından bahsedilmiştir.

Belirtilen eksiklikler ve zayıflıklar giderildiği takdirde yöntem uygulamalar için pratiktir**.**

KAYNAKLAR

[1] R.J. Yoon,, E. K. Ryu, K. Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication schemes". Computers & Security; .vol. 24 p. 50–56. 2004

[2] I.E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," accepted in Journal of Computer and System Sciences, 2005.

[3] C.S Tsai, C.C Lee, M.S Hwang," Password Authentication Schemes: Current Status and Key issues", International Journal of Network security,Vol.3 No.2,PP.101-115, Sept 2005.

[4] I-En Liao, C. C. Lee, and M. S. Hwang, "Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme", IEEE CS Press, pp. 437–440, Seoul, Korea, August 2005.

[5] M. L. Das, A. Saxena and V.P. Gulati,"A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629–631, 2004.

[6] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication schemes," Computers & Security, vol. 24, pp. 50–56, 2005.

[7] Mao Wenbo, "Modern Cryptography Theory and practice." Prentice Hall 2004.

[8] D.E.Denning, G. M. Sacco "Timestamps in Key Distribution Protocols" ACM 1981.

[9] C.C Lee, M.S. Hwang, W.P Yang "A Flexible Remote User Authentication Scheme Using Smart Cards" ACM Operating Systems Review vol. 36, no3, pp. 46-52, 2002.

[10] E.J. Yoon, E.K.Ryu, K.Y.Yoo "Secure User Authentication Scheme Using Hash Function" ACM SIGOPS Operating Systems Review, Vol.38, pp. 62 - 68 April 2004

[11] C.C. Chang, T.C. Wu"Remote password authentication with smart cards", IEE proceedings-e,Vol.138, No 3, May 1991

[12] H.M Sun, "An efficient remote user authentication scheme using smart cards, IEEE

Transactions on Consumer Electronics" Vol. 46.no.4 p. 958–961. 2000.
[13] X.-M. Wang et al. "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards". Computer Standards & Interfaces,doi:10.1016 /j.csi.2006. 11.005. 2006.
[14] Y.Z. Wei, Y.P. "Hu Security Analysis of Timestamp-based Remote User Authentication Scheme Using Smart Cards", Communications, Circuits and Systems Proceedings; Vol. 3, p.1580-1582, 2006.
[15] M.S Hwang., C.C Lee., Y.L. Tang "A simple remote user authentication" .Math Comput Model;36:103-7, 2002