YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Secure Remote Password Protokolünün SIP Kimlik Doğrulama Mekanizmasına Uygulanması

Celalettin KILINÇ

FBE, Bilgisayar Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı **:** Yrd. Doç. Dr. A. Gökhan YAVUZ

İstanbul, 2008

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

a, b	Rastgele üretilen ve genel olarak dağıtılmayan geçici özel anahtarlar
A, B	Genel anahtarlar
g	n ile aralarında asal olan “generator” değeri
H	Tek yönlü kıyım (hash) fonksiyonu
K	Oturum anahtarı
n	Hesaplamalarda mod almada kullanılacak büyük asal sayı
P	Kullanıcı şifresi
s	Kullanıcının salt değeri olarak kullanılacak rastgele değer
u	Rastgele seçilen ve açık olarak dağıtılan karıştırıcı değeri
v	Sunucunun şifre doğrulayıcısı
x	Kullanıcının şifresinden ve salt değerinden elde edilen özel anahtar

KISALTMA LİSTESİ

AKE	Asymmetric Key Exchange
DH-EKE	Diffie Hellman Key Exchange
EKE	Encrypted Key Exchange
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPEKE	Strong Password-Only Authenticated Key Exchange
SRP	Secure Remote Password
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
VoIP	Voice Over Internet Protocol

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Internet üzerinden sesli iletişim teknolojileri Internet ile birlikte çok hızlı bir şekilde gelişirken ve uygulama alanları artarken VoIP protokolleri de doğan ihtiyaçları karşılamak için bu gelişime ayak uydurmak zorunda kalmışlardır. İnternet telefon servisleri klasik devre anahtarlamalı telefon servislerinin yerini almak için çok güçlü bir aday olarak görünmektedir. Gelecekte klasik telefon sistemlerinin yerine tamamen Internet tabanlı sistemlerin kullanılabilmesi için Internet tabanlı sistemlerin getirdiği ek servisler ve kolaylıkların yanında güvenlik ve servis kalitesi gibi temel gereklilikleri de en az klasik sistemlerde olduğu kadar sağlaması gerekir. Internet üzerinden verilen telefon servisleri Internet'in sahip olduğu güvenlik riskleri ile doğrudan karşı karşıya gelecektir.

Kullanım alanı gittikçe yaygınlaşan Internet telefon protokollerinden birisi de Session Initiation Protocol (SIP) olarak karşımıza çıkmaktadır. SIP tasarımı itibariyle oldukça basit ve esnek bir protokoldür. Bu yüzden tasarım aşamasında güvenlik ile ilgili geniş ve sağlam önlemler geliştirilmemiştir. Kullanımı arttıkça güvenlik ile ilgili konular daha çok gündeme gelmeye başlamış ve bununla ilgili yapılan çalışma sayısı artmıştır. Bu çalışmalarda ortak amaç protokol güvenliğini artırmak olmakla birlikte dikkat edilmesi gereken bir konu da protokolün basit yapısının bozulmaması ve performans kayıplarının yaşanmamasıdır.

Secure Remote Password protokolü 1998 yılında Stanford Üniversitesi'nde geliştirilmiş anahtar değişim tabanlı bir protokoldür. Kimlik doğrulama için güvenli bir protokol olarak tanımlanmıştır. Bu çalışmada, SIP kimlik doğrulama mekanizmasında yaşanan sıkıntıları gidermek üzere SRP protokolünün kullanılması düşünülmüştür. SRP protokol adımlarının SIP kimlik doğrulama ile benzer olması uygulamayı kolaylaştırmıştır. SRP protokolünün kullanılması ile SIP kimlik doğrulamada önemli bir güvenlik artışı sağlanması hedeflenmektedir.

Bu tezin hazırlanmasındaki katkılarından dolayı ve tezin tüm aşamalarında beni cesaretlendirmesi ve desteklemesi nedeniyle tez danışmanım Yrd. Doç. Dr. Sayın Gökhan Yavuz'a teşekkürü bir borç bilirim. Ayrıca tezimin hazırlık, gerçekleştirme ve yazım aşamasında gösterdikleri anlayış ve kolaylıktan dolayı başta genel müdür Prof. Dr. Levent Arslan olmak üzere tüm Sestek Ses ve İletişim Bilgisayar Teknolojileri A.Ş. çalışanlarına teşekkür ederim.

ÖZET

SIP'in tasarım itibariyle basit bir protokol olması sebebiyle güvenlik anlamında çok sağlam bir yapı geliştirilmemiş, örneğin kimlik doğrulamada doğrudan HTTP'deki güvenlik mekanizması kullanılmıştır. Bu yapı ise sistemi birçok saldırı tehlikesi ile karşı karşıya bırakabilmektedir. Örneğin, kimlik doğrulama sırasında şifrenin doğrudan veya kıyım(hash) fonksiyonundan geçirilmiş hali ile iletişimde kullanılması, sistemi bir sözlük saldırısına açık hale getirmektedir. SIP, VoIP protokolleri arasında önemli bir yere sahiptir. Gelecekte klasik telefon sistemlerinin yerini internet tabanlı sistemlerin alması hedeflenmektedir. Bunun gerçekleşebilmesi için güvenlik ve servis kalitesi olarak daha iyi yerlere ulaşılması gerekmektedir. Tasarım sırasında basit önlemler ile geçiştirilen güvenlik konusu SIP'in kullanım alanı yaygınlaştıkça daha önemli hale gelmiştir ve güvenliğin artırılması ile ilgili yapılan çalışmalar hız kazanmıştır.

Bu çalışmada SIP kimlik doğrulama mekanizması incelenmiş, açıkları ve maruz kalabileceği saldırı tehlikeleri ele alınmıştır. Daha sonra SIP güvenliği ile ilgili yapılan birkaç çalışmaya değinilmiştir. SIP kimlik doğrulama sistemine alternatif olabilecek kimlik doğrulama yöntemleri incelenmiştir. Daha sonra bunlar arasından seçilen SRP protokolünün SIP kimlik doğrulama mekanizmasına uygulaması yapılmıştır.

SRP protokolü kullanılarak, şifre iletişimde hiç kullanılmadan, ön tanımlı matematiksel bağıntılardan yararlanılarak kimlik doğrulama işlemi gerçekleştirilmektedir. Şifrenin düz metin veya kıyım karşılığının iletişimde kullanılmaması sistem güvenliğini önemli derecede artırmaktadır. SIP, yapı itibari ile basit ve esnek bir protokoldür. Protokol üzerinde yapılacak değişiklikler, eklemeler, iyileştirmeler bu basitliği ve esnekliği bozmamalı ve performans kaybına neden olmamalıdır. Güvenlik iyileştirmeleri ile ilgili çalışırken bu konu göz ardı edilmemelidir. Bu çalışmada kullanılan SRP protokolünün çalışma yapısı ile SIP kimlik doğrulama arasındaki paralellik bu konuda bir kolaylık sağlamıştır. Protokolde yapılan küçük değişikliklerle bu iyileştirme gerçekleştirilmiştir.

Anahtar Kelimeler: SIP güvenliği, voip, güvenlik, kimlik doğrulama, secure remote password

ABSTRACT

Session Initiation Protocol (SIP) is a simple and flexible signalling protocol. Because of its simple structure it has not a strict security mechanism. HTTP digest authentication mechanism is used in SIP authentication. This simple security structure can be face a lot of security threats. For example using the plaintext or hash equivalent in communication can cause to a dictionary attack. SIP is the leading protocol used in IP telephony today. By the increasing use of IP telephony and also SIP, features like QoS and security are becoming more and more important. In the future IP based telephony systems are expected to replace the traditional telephony systems. Security and qulity of service issues in IP based telephony systems must be enhanced to do this replacement.

In this study, SIP authentication mechanism is analysed, security threats and possible attacks are investigated, some of the other studies on SIP authenticaiton is placed. After looking at alternative authentication mechanisms to SIP, SRP is choosen as a new authenticaiton in SIP. Applying of SRP in SIP is shown with additional protocol steps and message formats.

By applying SRP on SIP authenticaiton, new authentication mechanism works without sending client passwords neither plaintext nor hashed. Not using the password in communication provides a serious enhancement in the security mechanism of SIP. Modifications on the protocol must not damage this simplicity and it must not cause a noticable effect on performance. While working on security these aspects must not be ommited. In this study, similarity between SRP protocol and SIP authentication provide convenience. This refinement is applied with minor modifications to the original SIP protocol and without noticable impact on the performance.

Keywords: SIP security, voip, security, authentication, secure remote password

1. GİRİŞ

İnternet tabanlı telefon sistemleri geleneksel telefon sistemlerinin yerini daha fazla almaya başladıkça bu sistemlerin getirdiği yeni özellikler ve kolaylıkların yanı sıra eski sistemdeki özellikleri de sürdürebiliyor olması gerekir. Bu özelliklerin en başında servis kalitesi ve güvenlik sayılabilir. PSTN sistemlerde kullanıcıların sahip olduğu sabit bir bant genişliği varken internet tabanlı sistemlerde böyle bir sabit bant genişliği yoktur. Hat yoğunluğuna göre kullanıcılar dinamik değişen bant genişliklerini kullanırlar. Bu bant genişliğinin dinamik kullanılması avantajlı olarak gözükmektedir fakat her halde kullanıcının kullandığı bant genişliğinin belirli bir değerin altına düşmemesi gerekir. Yine geleneksel sistemlerde bu iş için ayrı bir altyapı kullanıldığından güvenlik ayrı bir problem olarak karşımıza çıkmamaktadır. Fakat internet tabanlı sistemlerde internet protokollerinin tehlike oluşturabilecek birçok açığı, eksiği telefon sistemlerinin karşısına bir güvenlik problemi olarak çıkmaktadır.

İnternet tabanlı telefon sistemlerinden bahsedildiğinde temel olarak H323 ve Session Initiation Protocol (SIP) olmak üzere iki protokol karşımıza çıkmaktadır. Bu iki protokolden SIP, yapısının basitliği ile H323'e nazaran daha fazla tercih edilmektedir. SIP bu popülerliği ile gelecekte şu anki sahip olduğu yerden daha fazlasına sahip olacak ve geleneksel telefon servisleri için gerçek bir rakip olacak gibi görünmektedir. Fakat bu rekabet için geleneksel telefon sistemlerinin sağladığı güvenlik ve kalitenin de sağlanması gerekmektedir. Bu yüzden internet tabanlı protokollerde ve özellikle SIP'de ilk tasarım aşamasında çok önemsenmeyen güvenlik konusu önem kazanmaktadır. Bu çalışmada öncelikle SIP'de kullanılan güvenlik sisteminin işleyişi incelenecektir. Daha sonra bu güvenlik yapısının sebep olabileceği tehlikeler üzerinde durulacak ve bu tehlikelere ne gibi çözümler getirilebileceği incelenecektir. Bu çözümler arasından seçilen SRP'nin ne gibi açıkları kapatacağı ve ne gibi iyileştirmeler sağlayacağının üzerinde durulacak ve SIP kimlik doğrulama sürecine nasıl ekleneceği gösterilecektir.

2. SİP ÇALIŞMA YAPISI

SIP; oturum açma, mevcut bir oturumun parametrelerini değiştirmek ve oturumu sonlandırmak için kullanılan bir uygulama katmanı protokolüdür (Rosenberg vd., 2002). Herhangi bir oturum için kullanılabilecek genel amaçlı bir protokol olmasına rağmen asıl kullanım alanını VoIP sistemlerde bulmuştur. Temel olarak HTTP (Fielding vd., 1999) ve SMTP (Postel J. B., 1982)ye benzer. Hatta bunlardaki bazı mesajları kullanır. Metin tabanlı ve bir işaretleşme protokolüdür. SIP çalışma yapısını açıklamak için öncelikle SIP bileşenleri ve mesajlarının açıklanmasına ihtiyaç vardır.

2.1 SIP Bileşenleri

Kullanıcı Etmenleri (User agents)

Kullanıcılar SIP'de uç nokta (endpoint) olarak tanımlanan terminallerdir. Yani bir çağrının başladığı ve sona erdiği uç noktalar olarak tanımlanabilir. Bir kullanıcı çağrı başlatan veya çağrı alan bir terminal olabilir. Kullanıcı, bir istek ile çağrı başlattığı durumda istemci kullanıcı etmeni (User Agent Client - UAC), çağrı kabul ettiği durumda ise sunucu kullanıcı etmeni (User Agent Server - UAS) olarak isimlendirilir. Gerçek hayatta bu terminaller birer IP telefon veya ayrı bir telefon yazılımı olarak karşımıza çıkmaktadırlar.

Vekil (Proxy) Sunucular

Vekil sunucular diğer istemciler adına istekte bulunmak için bazen istemci ve bazen de sunucu rolü oynayan arabirimlerdir. Vekil sunucuların asıl görevi bir anlamda çağrıların yönlendirilmesidir. Ayrıca arama haklarını da kontrol eder. Bir SIP vekil, istek mesajlarını sunucu kullanıcı etmenine, cevap mesajlarını da istemci kullanıcı etmenine iletir Bu mesajları yorumlar ve gerektiğinde bazı bu mesaj üzerinde değişiklik yaparak iletir.

Yönlendirici (Redirect) Sunucular

Aldığı istekler için cevaplar üreten ve istemciyi aradığı adrese yönlendiren sunucu kullanıcı etmenleri olarak tanımlanabilir. Bazı mimarilerde vekil sunucular üzerindeki işlem yükünü hafifletmek için yönlendirici sunuculardan yararlanılabilir.

Kaydedici (Registrar) Sunucular

Kayıt isteklerini kabul eden ve kullanıcı kayıtlarını yapan birimlerdir. SIP kimlik doğrulama mekanizmasında sunucu rolü oynarlar. SIP kullanıcıları kendilerini kaydedici sunuculara

kayıt ederler.

Vekil, yönlendirici ve kaydedici sunucular uygulamada genelde tek bir cihaz üzerinde çalışan yazılımlardır.

2.2 SIP Mesajları

SIP işaretleşmesi kullanıcılar arasındaki istek ve cevap mesajlarından oluşur. Bir SIP mesajı ya istemci tarafından sunucuya yapılan bir istek ya da sunucu tarafından istemciye verilen bir cevaptır (Rosenberg vd., 2002).

2.2.1 İstek Mesajları

SIP istek mesajları Rosenberg vd. (2002) tarafından şu şekilde sıralanır.

INVITE: Yeni bir oturum açmak için veya mevcut bir oturumun parametrelerini değiştirmek için istemci kullanıcı etmeni tarafında üretilen bir mesajdır.

ACK: Oturumun kurulduğu ile ilgili onay mesajıdır.

OPTION: Sunucu bilgilerini almak için gönderilen bir istek mesajıdır.

BYE: Aktif bir oturumu sonlandırır.

CANCEL: Yapılan bir isteği iptal eder.

REGISTER: Kullanıcıların kaydedici sunuculara kayıt olma isteklerini gösteren mesajdır.

2.2.2 Cevap Mesajları

İstek mesajlarına karşılık olarak üretilen mesajlardır. Belirli bir durum kodu ile geri dönerler. Bu durum kodu mesajın önünde yer alır. 100 durum kodlu mesajlar sonlanmamış işlemler için kullanılırken diğer mesajlar her durumda sonlanmış bir işlem sonucunu bildirir. İstek mesajlarının durum kodları ile beraber aşağıdaki gibi gösterilebilir. SIP 2.0 da mesaj kodunun ilk rakamı için 6 değer vardır (Rosenberg vd., 2002).

1xx: Provisional: Bir istek alındığını ve bu isteğin işlenmeye devam edildiğini bildirir.

2xx: Success: İşlem başarılı bir şekilde alındı, anlaşıldı veya işlendi anlamına gelir.

3xx: Redirection: İsteğin tamamlanması için başka işlemlerin de yapılması gerektiğini bildirir.

4xx: Client Error: İsteğin ya söz dizimi olarak bozuk olduğunu veya bu sunucuda

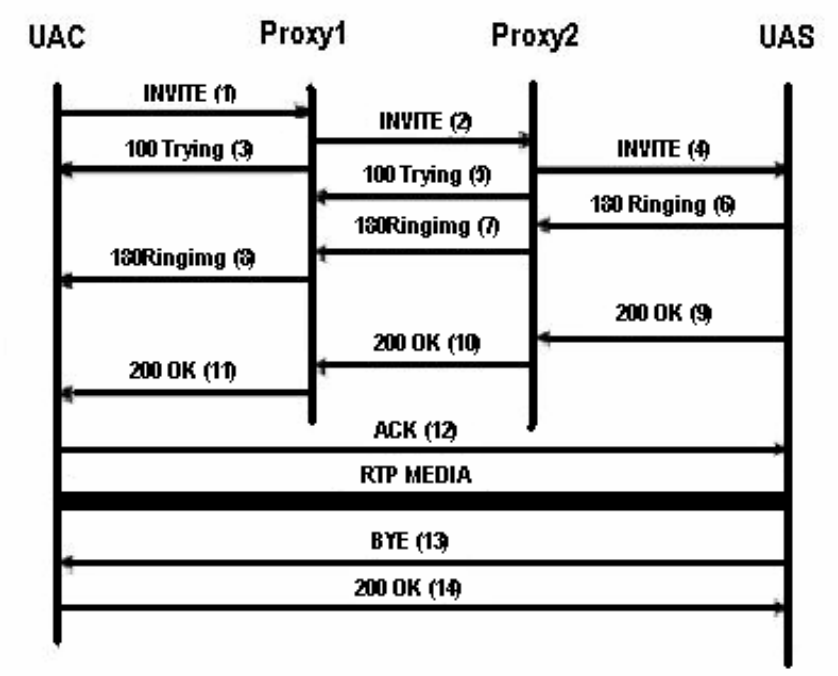
işlenemediğini bildirir.

5xx: Server Error: Doğru bir isteğin bu sunucuda işlenmesinde bir hata oluştuğunu bildirir.

6xx: Global Failure: İsteğin herhangi bir sunucuda yerine getirilemediğini bildirir.

2.3 Çağrı Yapma ve Karşılama

Temel bir SIP arama senaryosu şu şekilde özetlenebilir. Bir kullanıcı etmeni çağrı başlatmak istediğinde yerel olarak konfigüre edilmiş vekil sunucuya bir *INVITE* mesajı gönderir. *INVITE* mesajı aranan kişiyle ile bir çağrı başlatma isteği anlamına gelir. Yerel vekil bu isteği arama yapmak istenilen domaindeki vekil sunucusuna iletir. Buradan aranacak kişiye ulaşan mesaj geçtiği yolda her ulaştığı birim üzerinden geriye *100 Trying* mesajını geri döndürür. Aranan kişi bu isteği kabul ederse *Ringing* mesajı ile geri döner ve ayrıca bir *OK* mesajı gönderir. *OK* mesajı çağrının kabul edildiğini gösterir. Arayan, *OK* mesajını aldığını belirten bir ACK cevap mesajını aranana gönderir. Böylece oturum kurulmuş olur.



Şekil 2-1 SIP de bir çağrı senaryosu

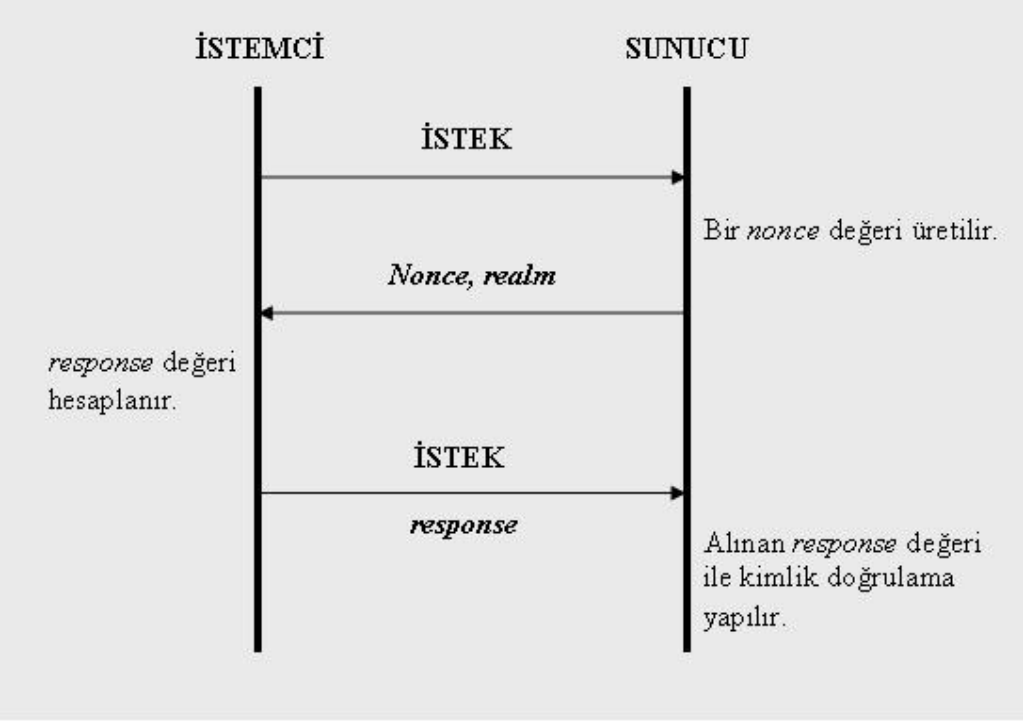
Oturum kurulduktan sonra iki uç arasında çoklu ortam transferi ile görüşme başlar. Bu görüşmeye taraflardan birinin göndereceği *BYE* mesajı son verir. Bu senaryo en basit hali ile Şekil 2-1'de görülmektedir.

3. SIP GÜVENLİĞİ

SIP protokolünün metin tabanlı olması sebebiyle oldukça basit bir yapısı vardır. Bu yapısı ile çalışmada birçok kolaylık ve esneklik sağlamaktadır. Bu esnek ve basit yapının getirilerinin yanı sıra birçok götürüye de sahiptir ve bu götürülerin en belirgini güvenlik açıkları olarak gösterilebilir. SIP içerisinde tasarım aşamasında geliştirilen bir güvenlik mekanizması bulunmaktadır. Bu güvenlik mekanizması temel olarak yapılan bir istek üzerine, isteği yapanın kimliğinin doğrulanmasına dayanır.

3.1 SIP Kimlik Doğrulama

SIP'de kimlik doğrulama için HTTP kimlik doğrulama mekanizması (Franks J. vd., 1999) kullanılmaktadır. Kimlik denetimi, istemcinin kimliğinin doğrulanması ve gönderilen mesajın içeriğinin değiştirilmemiş olması için gereklidir. Bu mekanizma ile istemci kullanıcı etmeni kendini sunucu kullanıcı etmenine, ara bir vekil sunucusuna veya bir kaydedici sunucuya tanıtabilir. SIP kimlik doğrulama mekanizması HTTP Digest kimlik doğrulamadan türetilmiştir. Bilgi istemeye dayalı (challenge-based) bir mekanizmadır. Digest kimlik doğrulamada mesajı gönderenden kimliğini doğrulamasını istenir. Bunun için gönderilen kimlik doğrulama istek mesajı içerisinde bir *nonce* değeri bulunur. Bu değer tek sefer kullanılmak üzere o anda oluşturulmuş bir dizgi (string) değeridir. İstemci ve sunucu ortak bir şifreyi paylaşırlar. İstemci kimlik doğrulama isteğine cevap vermek için bu şifreyi ve sunucudan gelen *nonce* değerini kullanarak bir cevap değeri hesaplar ve bu değer ile tekrar istekte bulunur. Böylece şifre hiçbir zaman metin olarak gönderilmemiş olur. Şekil 3.1'de kimlik doğrulama işlemi temel olarak gösterilmiştir. Burada cevap değeri farklı yöntemler ile hesaplanabilir ama SIP kimlik doğrulamada varsayılan yöntem MD5'tir.



Şekil 3-1 Bilgi istemeye dayalı kimlik doğrulama

İstemci kimlik doğrulama istek mesajı karşılık göndereceği yeni istek mesajında kullanacağı *response* alanını (3.1) eşitliği yardımıyla hesaplar.

$$\begin{aligned} HA1 &= MD5(username : realm : password) \\ HA2 &= MD5(method : digestURI) \\ response &= MD5(HA1 : nonce : HA2) \end{aligned} \qquad (3.1)$$

Bu kimlik denetimi bir çağrı başlatılmak istendiğinde, bir çağrı yönlendirmesi yapılacağında veya bir kayıt işlemi yapılacağında uygulanır. İstemci kullanıcı etmeni düz metin olarak bir istek mesajı göndererek işleme başlar. Bu mesaj çağrı başlatmak için bir *INVITE* mesajı veya *REGISTER* mesajı olabilir. Bu mesajı alan sunucu kullanıcı etmeni, vekil sunucu veya kaydedici sunucu kimlik doğrulamanın gerekli olduğunu anlar ve istekte bulunan istemci kullanıcı etmenine özel bir hata mesajı ile geri döner. Bu mesaj kimlik bilgilerinin istendiği anlamına gelir ve *realm* değeri ile bir *nonce* değerini içerir. Bu mesajı gönderen bir sunucu kullanıcı etmeni ise mesaj bir 401 *Unauthorized* mesajı, eğer bir vekil sunucu ise *407 Proxy Authentication Required* mesajıdır. Kimlik doğrulama sırasında kullanılan *realm* değeri kullanıcının hizmet almaya yetkili olduğu alan adını belirtir.

3.2 Olası Saldırı Tehlikeleri

SIP, internet gibi saldırılara ve tehditlere açık bir sistem üzerinden uygulandığı için birçok tehlike ile karşı karşıyadır. Bir SIP telefon ağında yer alan tüm SIP bileşenleri standart internet saldırılarına hedef olabilirler. Bu tehditler *cevap verme saldırısı, kayıt çalma, sahte istek mesajları, sunucu taklidi ve seçilmiş metin saldırısı* olmak üzere birkaç grupta toplanabilir.

Cevap Verme Saldırısı (Replay Attack)

Cevap verme saldırıları olarak nitelendirilen saldırılar HTTP, SMTP ve güvenlik sistemi bunlardan türeyen SIP gibi iletişimde mesajlaşma kullanan bütün istemci-sunucu sistemleri için ortak bir tehdittir.

Bir cevap verme saldırısı iki SIP biriminin konuşmasını dinleyen üçüncü bir kişi tarafından yapılabilir. Bu üçüncü kişi dinlediği mesajlardan çıkaracağı oturum bilgisi ile doğru birim gibi davranarak oturum açmaya veya mesajlara cevap vermeye başlayabilir. Zaman aşımına uğrayacak bir mesaj belirli zaman aralıklarında tekrarlanabilir. En tehlikeli ve fark edilmesi güç olan cevap verme saldırısı ise saldırganın hedefine varmayan bir mesajı okuyarak buna mesajın hedefi gibi cevap vermesi ile yapılabilir.

Kayıt Çalma (Registration Hijacking)

SIP de güvenlik açıklarından birisi de kayıt bilgilerinin çalınarak sahte kayıt işlemlerinin yapılmasıdır. SIP'de kullanıcı etmenleri kaydedici sunuculara kayıt olurlar. Kayıt çalma saldırısı bu kayıt işlemi sırasında gerçekleştirilebilir. Saldırgan kendisini normal bir kullanıcı gibi göstererek o kullanıcının bilgileri ile kaydedici sunucuya kayıt olabilir. Bu saldırı sonucu kayıt bilgileri çalınan kullanıcıya gelen çağrılar saldırgana yönlenmiş olur.

Bu saldırının uygulanabilir olmasının sebepleri arasında SIP kullanıcılarının kayıt edilmesi sürecinde UDP kullanılmasıdır. UDP sahte paketlerin başkaları tarafında oluşturulmasını kolaylaştırmaktadır. Ayrıca SIP kullanıcıların kayıt edilme sürecinde sağlam bir kimlik doğrulama mekanizması kullanılmamaktadır. Mevcut işlemlerde kullanıcı adı, şifre ve belirli bir zaman etiketi değeri olan *nonce* MD5 kıyım fonksiyonuna tabi tutularak oluşturulan bir cevap değeri kimlik doğrulamada kullanılır. Bu değerin ise saldırganlar tarafından sözlük atakları düzenlenerek elde edilebilme şansı vardır. Kaydedici sunucular gelen bir kayıt isteğinin sahibinin kimliğini *From* başlık alanına bakarak belirlerler. Ancak bu mesaj UDP' nin de sağladığı esneklikle değiştirilebilmekte ve bu kötü niyetli kayıt olma işlemlerine sebep olabilmektedir. Bu saldırı sonucunda saldırgan kullanıcılara gelecek çağrıları karşılayarak bu

çağrılara sahte sesli yanıt anonsları çalabilir veya gelen çağrıya ortak olarak görüşmeyi kaydetme şansı verebilir.

Bu saldırıdan korunmak için bir takım önlemler alınmalıdır. Bunlardan birisi VoIP için konfigüre edilmiş güvenlik duvarlarının kullanılması olabilir. Bu güvenlik duvarları ile kullanıcıların taranması, şifre tahmini için bir sözlük kullanılarak sürekli yapılan kayıt işlemlerinin kayıt altına alınması ve sistem yöneticisinin uyarılması, tüm kimlik doğrulama isteklerinin ve özellikle başarısız olanlarının kaydedilmesi, başarısız kimlik doğrulama isteklerinden sistem yöneticisinin haberdar edilmesi gibi önlemler alınabilir. SIP kaydedici sunucu tarafından sadece bilinen bir kullanıcı listesi için kayıt isteği kabul edilebilir, diğer kayıt mesajları engellenebilir. Daha sağlam şifreler kullanılmalıdır. Genel olarak, belirli bir kurala göre üretilmiş şifreler sözlük saldırıları karşısında zayıf kalabilmektedir. Bu yüzden şifreler sağlam seçilmelidir. Bu saldırıdan korunmanın bir başka yolu da mevcut SIP kimlik doğrulama yönteminden daha sağlam bir kimlik doğrulama yönteminin kullanılmasıdır.

Sahte İstek Mesajları

İstek mesajlarının toplanan bilgilerle sahte bir şekilde hazırlanarak alıcıların kandırılmasıdır. Mesajların başlık ve gövde kısımları değiştirilerek alıcıların başka kişilerle konuştuklarını sanmaları sağlanabilir. En genel olarak üç çeşit sahte mesaj üretilebilir. Sahte bir *INVITE* mesajı üretilerek karşıdaki kişinin başkası ile konuştuğunu sanması sağlanabilir. Bu bir SIP *INVITE* mesajındaki *Via*, *From* ve *Subject* alanları değiştirilerek yapılabilir. Sahte bir *BYE* isteği ile hâlihazırdaki bir konuşma sona erdirilebilir. Sahte bir *BYE* mesajının hazırlanması için önceki mesajlardan oturum ile ilgili belirli parametrelerin elde edilmesi gerekir. Yine hazırlanacak sahte bir *CANCEL* isteği ile gerçek bir *INVITE* mesajı durdurulabilir. Gerçek bir kullanıcı hakkı olmasına rağmen çağrı başlatamayabilir.

Sunucu Taklidi (İmpersonating a Server)

Şimdiye kadar bahsedilen saldırıların hepsi istemci tarafından hazırlanan saldırılardı. Bunlardan başka sunucular taklit edilerek de saldırılar yapılabilir. Örneğin bir kaydedici sunucu taklit edilerek çağrılar kötü niyetli kullanıcı etmenlerine yönlendirilebilir.

Seçilmiş Metin Saldırısı

Bu saldırıda şifreyi çözümlemek isteyen saldırgan kendi metnini şifreleyiciye vererek sonuçları gözler ve böylelikle düz metnin nasıl şifrelendiğini ortaya çıkarmaya çalışır. SIP de *nonce* değerlerinin seçimli olması böyle bir saldırıda saldırganın işini daha da

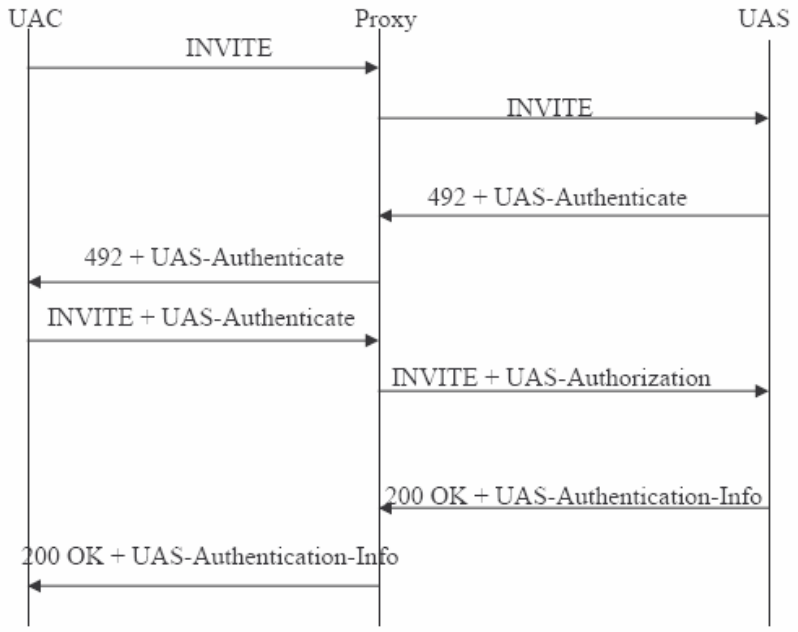
kolaylaştırabilir. Bununla beraber bu saldırının SIP de başarı şansı düşüktür, çünkü SIP de kullanılan digest authentication şu an bilinen en iyi kıyım yöntemi olan MD5 kullanmaktadır.

3.3 SIP Güvenlik Mekanizması için önerilen iyileştirmeler

SIP kimlik doğrulama sisteminin açıklarından kaynaklanabilecek tehlikeleri azaltmak için birkaç yeni kimlik doğrulama mekanizması ortaya atılmıştır.

3.3.1 SIP için Digest Kimlik Doğrulama Üzerine Bir Çalışma

SIP'de kimlik doğrulama istemci kullanıcı etmeni ve iletişimde bulunduğu sunucu arasında gerçekleştirilir. Bu sunucu bir vekil sunucu veya bir yönlendirici sunucu olabilir. Bu çalışmada istemci kullanıcı etmeni ve vekil sunucu arasındakine benzer bir kimlik doğrulma da vekil sunucu ve sunucu kullanıcı etmeni arasına önerilmiştir. Bunun için bu çalışmada çağrı kurulumunun bu son adımı için de digest kimlik doğrulamaya benzer bir mekanizma getirilmesi tasarlanmıştır. Mevcut SIP kimlik doğrulama sisteminde böyle bir yapı olmadığı için gerekli başlık bilgileri ve parametreler de bulunmamaktadır. Bu yüzden yeni başlık alanları ve parametreler tanımlanmıştır. Yeni mesaj olarak *Proxy Authorization Required* mesajına benzer şekilde bir *Proxy Unauthorized* mesajı ve bununla beraber *UAS-Authenticate Response Header, UAS-Authenticate Request Header, UAS-Authenticate-Info* başlık alanları tanımlanmıştır.

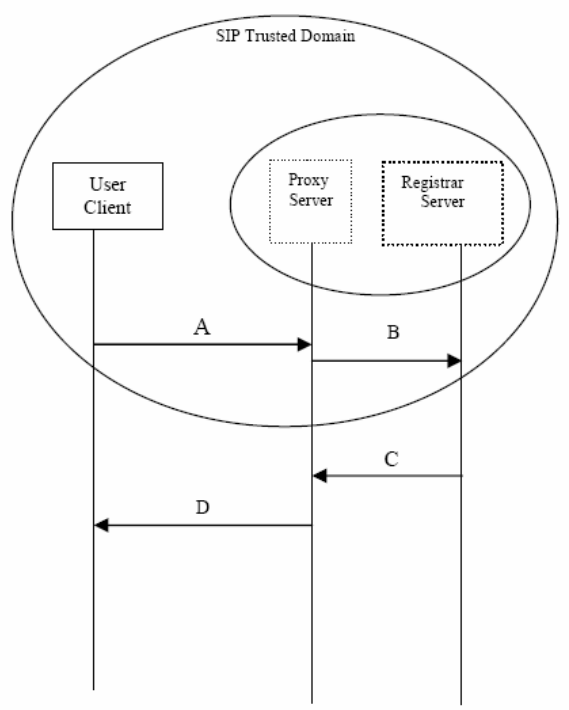


Şekil 3-2 Vekil sunucu-sunucu kullanıcı etmeni kimlik doğrulama(Qi, 2003)

Sistem çalışması şu şekilde özetlenebilir. İstemci kullanıcı etmeninden başlayan bir çağrı ara vekil sunuculardan geçtikten sonra son olarak sunucu kullanıcı etmenine gelir. sunucu kullanıcı etmeni kendisine gelen böyle bir isteğe *Proxy Unauthorized* mesajı ile cevap verir. Bu vekil sunucunun kimliğini sunucu kullanıcı etmenine doğrulatması gerektiği anlamına gelmektedir. Vekil sunucu bu mesajı aldığında *UAS-Authenticate* başlığına bakarak bu başlıkta bulunan *target* ve *route* parametrelerini kontrol eder. Bundan sonra kendi kimlik bilgilerinin de içinde bulunduğu bir mesajla sunucu kullanıcı etmenine geri döner. Bu akış Şekil 3.2'de görülebilir.

3.3.2 VoIP Uygulamalarında İşaretleşmenin Kimlik Doğrulaması

Başka bir kimlik doğrulama yöntemi de Anna Üniveritesi'nden Srinivasan tarafından gerçekleştirilmiştir. Önerdikleri sistem istemcinin vekil sunucuya kimliğinin doğrulatılması üzerine kurulmuştur. Buradaki vekil sunucu domain için bir giden vekil sunucudur. Çağrıyı başlatan istemci vekil sunucu ile iletişimdedir. Vekil sunucu istemcinin kimliğini doğrulamalıdır fakat istemci kayıt işlemini kaydedici sunucu ile yapar. Bu durumda vekil sunucunun kimlik doğrulama işlemini gerçekleştirmek için bu güvenilir SIP domain de kaydedici sunucu ile ek bir işlem yürütmesi gerekmektedir. Böyle bir kimlik doğrulama kaydedici sunucu ve vekil sunucunun güvenilir olması varsayımı ile yapılabilir. Ayrıca bu sunucuların birer genel anahtar sertifikası da olmalıdır.



Şekil 3-3 SIP domainde kimlik doğrulama protokolü akış diyagramı (Srinivasan vd., 2005)

Kullanıcı kendisini kaydedici sunucuya kaydeder ve bu kayıt sırasında kendisine atanmış olan kimlik bilgilerini de gönderir. Kaydedici sunucu bu kayıt isteğini aldığında büyük bir N sayısı üretir ve bu N sayısı ile kullanıcının kimlik bilgilerini kullanarak hesapladığı bir değeri kullanıcıya gönderir. Bu değer kullanıcının şifresidir. Daha sonra kaydedici sunucu kendi kimlik bilgileri ve kullanıcının kimlik bilgileri ve ürettiği N değeri ile bir r değeri hesaplar.

Çağrıyı başlatan istemci kendisini giden vekil sunucuya kaydetmelidir. İstemci kullanıcı etmeni, r değeri ve şifresini kullanarak bir n değeri hesaplar. Ayrıca kayıt işlemi sırasında aldığı şifresini kullanarak rastgele bir R değeri hesaplar. Zaman etiketi ve şifresini kullanarak geçici bir K anahtarı oluşturur ve R, K ile şifrelenir. İstemci kullanıcı etmeni Şekil 3.3'de görülen A istek mesajı ile birlikte n, K ile şifrelenmiş R, kaydedici sunucunun kimliği ve bir zaman etiketi değeri gönderir. Vekil sunucu bu parametreler ile birlikte A isteğini aldığında mesaj içindeki zaman etiketi değeri ile o anki zamanı karşılaştırır ve mesajın kabul edilebilir bir zaman içinde üretilip üretilmediğini kontrol eder. Bundan sonra vekil sunucu kaydedici sunucuya B mesajını göndererek, vekil sertifikası ve aldığı parametreler ile istemci kullanıcı etmeninin kimlik doğrulamasını yapar.

B mesajını alan kaydedici sunucu eğer istemci kullanıcı etmeninin kimliğini doğrulamış ise bir C mesajı ile vekil sunucuya döner. Vekil sunucu istemci kullanıcı etmenine üzerinde ne

kadar geçerliliği olduğu belirtilen geçici bir sertifika gönderir. Daha sonra vekil sunucu sertifikayı oturum anahtarı ile şifreler ve tüm sinyalleşme boyunca bu oturum anahtarı kullanılır. İstemci kullanıcı etmenine şifrelenmiş sertifikayı içeren D mesajını aldığında geçici bir sertifika ve oturum anahtarına sahip olmuş olur.

Burada yürütülen kimlik doğrulama mekanizmasının ayrıntıları ve matematiksel gösterimi yayınlanan makalede (Srinivasan vd., 2005) ele alınmıştır.

3.3.3 SIP İçin Vekil Sunucu Tabanlı Güvenlik

Holger vd. (2007) daha çok çağrı merkezlerindeki güvenlik sorunları için bir sistem tasarlamışlardır. Arama yapan kullanıcıların seslerinin tanınmadığı çağrılarda çağrı yapan kişinin kimliğinin çalınması durumunda kullanıcıya ait kritik bilgilerin de çalınması söz konusu olabilir. Buna en iyi örnek olarak bir bankanın müşterilerinin aradığı çağrı merkezi gösterilebilir. Çağrı merkezinin içerisindeki operatörlere bir sertifika yüklenerek burada bir güvenlik sağlanabilir fakat çağrı merkezlerinde operatörler tek tek ulaşılan kimseler değildirler. Bir çağrı grubu altından erişilirler, ayrıca her operatör için bu sertifikaların yüklenmesi yönetim bakım açısından oldukça zahmetli olacaktır. Holger vd. (2007) bunun için vekil sunucuların bilinen kullanıcılardan gelen mesajları çağrı merkezinin imzasıyla imzalayarak göndermelerini savunmuşlardır. Böylelikle her operatör için ayrı bir kurulum ve bakım gerekmeyecektir.

Bu çözüm önerisinde kendilerinin de belirttiği bir açık söz konusudur. Vekil sunucunun sorumlu olduğu domain içerisinden bu servis kullanılabilecektir. Bu durumda içeriden bu servisi kullanacak İstemci kullanıcı etmenlerinin da kimlik doğrulama işlemine tabi tutulmaları gerekir. Holger vd. (2007) bunun için mevcut SIP kimlik doğrulamasını önermiştir. Bu nedenle bu öneri belirli bir güvenlik artımı sağlasa da mevcut SIP kimlik doğrulama sisteminin açıklarını barındırmaya devam etmektedir.

4. MEVCUT KİMLİK DOĞRULAMA YÖNTEMLERİ

Kimlik doğrulama, bir kişinin veya sistemin olduğunu iddia ettiği kişi veya sistem olduğunun ispatlanmasıdır. Güvenlik ihtiyacı olan tüm sistemler için vazgeçilmez bir özellik olan kimlik doğrulama, bilgisayar sistemlerinde de oldukça önemli yer tutar.

Kimlik doğrulama yöntemleri ya parmak izi veya retina deseni gibi doğrudan kullanıcıyla ilgili olan bir şeye, ya bir akıllı kart gibi sahip olunan bir şeye ya da parola veya pin gibi bilinen bir şeye dayanır. Biz bu çalışmamızda bir parola kullanılarak gerçekleştirilen kimlik doğrulama sistemlerini inceleyeceğiz.

Kullanıcı adı ve şifre ile yapılan kimlik doğrulama sistemlerinde sadece kullanıcıdan gelecek şifreye göre bir doğrulama yapılması pek güvenilir olmayabilir çünkü kullanıcı ile doğrulayıcı arasındaki ağın dinleniyor olma ihtimali ve gelen kimlik bilgilerinin başkaları tarafından değiştiriliyor olma ihtimali vardır. Bu sebeple kullanıcı ve doğrulayıcı arasında daha güvenli yöntemlerin uygulanması gerekir. Kullanıcı adı ve şifre kullanılarak yapılan kimlik doğrulama işlemlerinde düz metin şifreyi gönderip alan protokoller de mevcuttur. Şifrenin metin olarak iletişimde kullanıldığı bir protokol her türlü tehlikeye açık demektir.

Kimlik doğrulama mekanizmalarını incelerken kimliklerini doğrulama istenen kullanıcıları istemci, doğrulayıcıları ise sunucu olarak değerlendirebiliriz. Kimlik doğrulama sistemleri iki kısımda incelenebilir. Birinci kısımda sunucu, istemcinin şifresinin düz metin halini saklar. Bir kimlik doğrulama isteği geldiğinde sakladığı bu şifre ile karşılaştırma yaparak karar verir. Bu tür mekanizmalara düz metin eşlenekli mekanizmalar denir. İkinci olarak sunucunun, istemcinin şifresini direkt olarak saklamadığı, bir dizi matematiksel işlemler sonucu istemciyi doğrulayabileceği bir doğrulayıcı değer sakladığı sistemler sayılabilir. Bu sistemlere ise doğrulayıcı tabanlı sistemler denir.

Doğrulayıcı tabanlı sistemler düz metin eşlenekli sistemlere göre birçok üstünlüğe sahiptir. Şifrelerin düz metin olarak saklandığı sistemlerde şifre veritabanı bir şekilde ele geçtiğinde tüm güvenlik mekanizması devre dışı kalabilir. Güvenli bir iletişim protokolünden beklenen iletişim sırasında kimlik doğrulama işleminde kullanılan değerler ile ilgili dışarı mümkün olduğu kadar az bilginin çıkmasıdır. Doğrulayıcı tabanlı sistemlerde kullanıcı şifresi iletişimde kullanılmaz. Bu, iletişimi dinleyen bir saldırganın sisteme zarar verme ihtimalini oldukça düşürür.

Birçok kimlik doğrulama protokolü olmakla beraber burada düz metin tabanlı ve doğrulayıcı tabanlı birkaç tanesi işlenecektir. Öncellikle bilgi istemeye dayalı (challenge-response) kimlik

doğrulama sistemleri ele alınacak daha sonra EKE ve AKE kullanılarak gerçekleştirilen kimlik doğrulama mekanizmaları incelenecektir.

4.1 Bilgi İstemeye Dayalı Kimlik Doğrulama

En basit anlamda bir kimlik doğrulama istemcinin şifresini sunucuya göndermesi ve sunucunun veritabanında o istemci için sakladığı şifre ile karşılaştırma yaparak istemcinin doğrulamasını yapması şeklinde çalışabilir. Burada istemci şifresini düz metin olarak değil, tek yönlü bir kıyım fonksiyonundan geçmiş olarak sunucuya gönderebilir. Sunucu da veritabanında sakladığı şifreyi yine aynı kıyım fonksiyonundan geçirerek karşılaştırmayı yapar ve kimlik doğrulama işlemini gerçekleştirir. İstemcinin şifresi iletişimde, kıyım fonksiyonundan geçirilmiş olsun veya olmasın, doğrudan kullanıldığı için dinlenme tehlikesi olan ağlarda bu iletişim tehlikelere açıktır.

Bu açığın kapatılması için bilgi istemeye dayalı (chalenge-based) bir mekanizma önerilmiştir. Buna göre istemci sunucuya kimliğini gönderir. Bu kimliği alan sunucu istemciye challenge adı verilen bir mesaj gönderir. İstemci bu challenge mesajı, ilk gönderdiği mesaj (kimlik bilgisi) ve şifresini kullanarak bir cevap değeri hesaplar, sunucuya gönderir. Sunucu tarafında da aynı hesaplama yapılarak karşılaştırma yapılır ve istemcinin kimliği doğrulanır.

Sunucunun challenge mesajı her kimlik doğrulama işlemi için farklı olacağından ağ üzerinde başkası tarafından yakalanan bir cevap değeri sonraki kimlik doğrulama işlemleri için anlamsız olacaktır. Bu şekilde basit bir replay saldırısının önüne geçilmiş olur. Buna rağmen bu şekilde bilgi istemeye dayalı protokoller daha farklı yöntemler ile saldırıya uğrayabilmektedirler. Örneğin başarılı bir kimlik doğrulama işlemini dinleyen saldırgan challenge ve istemci tarafından hesaplanan cevap değerini yakalayabilir. Elde ettiği parametreler ile elde ettiği cevap değerine ulaşıncaya kadar farklı şifreler ile hesaplamalar yaparak şifreyi tahmin etmeye çalışabilir. Bu tür saldırılar sözlük saldırıları olarak adlandırılır. Geçmişte birçok başarılı sözlük saldırısı gerçekleştirilmiştir.

4.2 Encrypted Key Exchange (EKE)

EKE, Diffie ve Hellman'nın (1976) genel anahtar dağıtım sistemi olarak isimlendirdikleri sisteme yapılan bir ekleme ile ortaya çıkmıştır. Bu ekleme ile, kimlik doğrulama ve iletişimde kullanılan verinin dinlenmemesi için, iletişimde gönderilen veriler gizli bir anahtar ile şifrelenmektedir. Gönderilen verinin böyle bir gizli anahtar ile şifrelenmesi iletişimi dinleyen

İstemci		Sunucu
Rasgele bir R_A değeri üretilir. $P(\alpha^{RA} (\text{mod } \beta))$ hesaplanır.	$\rightarrow$ A, $P(\alpha^{RA} (\text{mod } \beta)) \rightarrow$	Rasgele bir R_B değeri üretilir. $P(\alpha^{RA} (\text{mod } \beta))$ hesaplanır. Ortak P şifresi kullanılarak istemciden gelen değer çözülür. $= P^{-1}(P(\alpha^{RA} (\text{mod } \beta)))$ $= \alpha^{RA} (\text{mod } \beta)$ Oturum anahtarı K hesaplanır: $K= (\alpha^{RARB} (\text{mod } \beta)$
P ortak şifresi kullanılarak sunucudan gelen değer çözülür: $= P^{-1}(P(\alpha^{RB} (\text{mod } \beta)))$ $= \alpha^{RB} (\text{mod } \beta)$ Sunucu ile aynı şekilde oturum anahtarı K hesaplanır: $K= (\alpha^{RARB} (\text{mod } \beta)$ Hesaplanan oturum anahtarı ile sunucudan gelen mesaj çözülür: $= K^{-1}(K(challenge_B))$ $= challenge_B$ Rasgele bir $challenge_A$ değeri üretilir. $=K^{-1}(K(challenge_A))$ $= challenge_A$ $challenge_A$ değerinin sunucudan doğru olarak geldiği kontrol edilir.	$\leftarrow P(\alpha^{RB} (\text{mod } \beta)) \leftarrow$ $\leftarrow K(challenge_B) \leftarrow$ $\rightarrow K(challenge_A, challenge_B) \rightarrow$ $\leftarrow K(challenge_A) \leftarrow$	Rasgele bir $challenge_B$ değeri üretilir. $=K^{-1}(K(challenge_A, challenge_B))$ $= challenge_A , challenge_B$ challengeB nin karşı taraftan doğru olarak geldiği kontrol edilir.

Şekil 4-1 EKE çalışma adımları

üçüncü kişilerin kimlik doğrulama sistemi ile ilgili bilgi edinmelerini engeller.

Üstel anahtar değişimi kullanılarak EKE'nin gerçekleştirilmesi Şekil 4.1'de gösterildiği şekilde açıklanabilir. EKE'nin gelişmiş hali olarak bir takım protokoller ortaya çıkmıştır.

Bunlar arasında DH-EKE (Steiner M. vd., 1995) ve SPEKE (Jablon D., 1996) sayılabilir. Bu protokollerde şifreyi ele geçiren saldırganın bu şifreyi kullanarak geçmiş veya sonraki oturumların genel anahtarlarını elde edememesi amaçlanmıştır. Buna *forward secrecy* adı verilmektedir. EKE gerçekten şifre tabanlı kimlik doğrulama protokolleri için oldukça güvenilir ve sağlam bir çözüm olmuştur.

EKE'nin en büyük açık noktası, metin tabanlı şifre kullanan protokollerdeki gibi, istemci ve sunucunun aynı şifreye veya kıyım fonksiyonundan geçirilmiş haline ulaşıyor olmalarıdır. Bunun için yapılan bir çalışma yine Bellovin ve Merritt (1994) tarafından yapılmıştır. Fakat bu çalışmada eklenen özellikler *forward secrecy* özelliğini ortadan kaldırmıştır. EKE'nin bu sorununu ortadan kaldırmak için metin şifre karşılığını özel şifre dosyalarında tutan çalışmalar yapılmıştır. Bu çalışmalarda istemcinin gerçek şifresinin doğrulanması için ek bir anahtar değişimi daha getirilmiştir. Bu işlem EKE'nin bahsedilen sorununu gidermektedir. Bununla birlikte kimlik doğrulama işleminin süresini uzatmakta ve daha fazla hesaplama karmaşıklığı getirmektedir.

4.3 Asymmetric Key Exchange (AKE)

EKE'de olduğu gibi AKE'nin de amacı istemci ve sunucu arasında anahtar değişimleri yapmak ve bu anahtarı kullanarak iki tarafın da belirli bir şifreyi bildiklerini doğrulamaktır. EKE'nin aksine AKE protokol akışında şifreleme kullanmaz. Bunun yerine ön tanımlı matematiksel ilişkilerden yararlanır. Şifrelemenin kullanılmamasının birçok getirisi vardır.

Şifrelemenin kullanılmaması ortak bir şifreleme algoritmasının seçilmesi aşamasını kaldırdığı için protokolde bir sadeleşmeye imkân verir. Şifreleme kullanıldığı durumda şifreleme algoritması sabitlenerek de bu algoritma seçim aşaması kaldırılabilir fakat bu protokolü sadece belirli bir şifreleme algoritmasına bağımlı kılacaktır. Şifreleme kullanıldığı takdirde şifreleme algoritmasındaki herhangi bir açık doğrudan protokolün de bir açığı haline gelecektir. Ayrıca bazı şifreleme algoritmalarının kullanımı ile ilgili yasal kısıtlamalar olabilir. Bu durumda bu algoritmayı kullanan protokoller de lisans gibi konularda bağımlı hale gelecektir. Şifreleme kullanılmaması durumunda bu gibi sorunlar protokolün dışında kalacaktır.

AKE'yi diğer yöntemlerden ayıran bir özelliği daha vardır. EKE gibi protokoller kimlik doğrulama işleminin temelinde önceden tanımlanmış, paylaşılan bir şifreyi kullanırlar. Bu, sunucunun ve istemcinin aynı şifreyi sakladıkları ve kimlik doğrulama işleminde dolaylı olarak bu şifreyi kullandıkları anlamına gelir. Bu şifre hem sunucu ve hem de istemci

tarafından dikkatli bir şekilde korunmalı ve güvenli bir şekilde paylaşılmalıdır. Önceden tanımlanmış bir şifre kullanılmasına karşılık AKE bir "swaped-secret" kavramı tanımlar. Buna göre istemci ve sunucu bir şifre hesaplar. Bu şifreyi tek yönlü bir kıyım fonksiyonundan geçirerek bir doğrulayıcı üretir. Karşı tarafa bu doğrulayıcı gönderilir. Doğrulayıcıyı bir sözlük saldırısından korumak hala önemlidir fakat çalınan bir doğrulayıcı istemciyi taklit etmek için yeterli değildir. Bunun için bu doğrulayıcıya karşılık gelen şifre de gereklidir. Bu tekniğin daha özel bir durumu olarak sadece bir taraf bir şifre üretir ve bir doğrulayıcı hesaplar. Bu durumda başlangıçtaki şifre değişme adımları boyunca kullanıcının şifresi hiç ağa çıkmamış olur. Sadece doğrulayıcı karşı tarafa gönderilir. Bu da sistemin güvenliğini önemli derecede artırır.

Çizelge 4-1 AKE matematiksel ifadeleri (Wu, 1998)

w, x, y, z	Rastgele seçilmiş parametreler
P(x)	Tek yönlü doğrulayıcı üreten fonksiyon
Q(x, y), R(x, y)	Özel ve genel parametreler için "mixing" fonksiyonları
S(x,y)	Oturum anahtarı üretme fonksiyonu
K	Oturum anahtarı

$$(\forall w.x, y, z)$$
$$S(R(P(w), P(x)), Q(y, z)) = S(R(P(y), P(z)), Q(w, z)) \tag{4.1}$$

İstemci		Sunucu
Rasgele bir *x* değeri seçilir.		Rasgele bir *z* değeri seçilir.
	→ *P(x)* →	
	← *P(z)* ←	
Rasgele bir *w* değeri seçilir.	→ *P(w)* →	Oturum anahtarı hesaplanır: K=S(R(P(y), P(z)), Q(w,x))
Oturum anahtarı hesaplanır: K=S(R(P(y), P(z)), Q(w,x))	← *P(y)* ←	Rasgele bir *y* değeri seçilir.

Şekil 4-2 Genel AKE çalışması (Wu, 1998)

AKE'nin doğru çalışması için (4.1) eşitliğinin sağlanması gerekir. Bu eşitlik kendisini kullanan protokolün güvenliği ile ilgili hiçbir şeyi garanti etmez. Bu tamamen P(), Q(), R() ve

S() fonksiyonlarının düzgün seçilmesine bağlıdır. Örneğin, verilen bir P(x) değeri için x'in elde edilmesi yeterince zor olmalıdır.

AKE protokolünün işleyişi Tablo 4-3 de gösterilen adımlarla açıklanabilir. İstemci ve sunucu birer *x* ve *z* rastgele değeri seçerler. Bunlar protokoldeki şifre değerleri olarak kabul edilebilir. İstemci P(x) değerini hesaplayarak sunucuya gönderir. Aynı şekilde sunucu da seçtiği z değeri ile P(z)'yi hesaplayarak istemciye gönderir. Aynı şekilde iki tarafta birer w ve y değerleri seçilir ve P(w) ile P(y) değerleri karşılıklı olarak değişilir. Bu değerler ile (4.1) eşitliğinden yararlanılarak oturum anahtarları hesaplanır. Burada x ve z parametreleri iki taraf tarafından seçilen uzun zamanlı şifrelerdir. w ve y ise her oturumdaki oturum anahtarın değişmesi için geçici olarak seçilen ve oturumdan oturuma değişen değerlerdir.

5. SECURE REMOTE PASSWORD PROTOKOLÜ

AKE ile anahtar değişmeli sistemler için bir matematiksel ifade ortaya konmuştur. Bu ifadenin bir protokol olarak uygulanması için ilgili fonksiyonların doldurulması gerekir. Buradaki P, Q, R ve S fonksiyonlarının gerçeklenerek AKE'nin bir uygulaması gerçekleştirilebilir. Bu uygulamalardan birisi de Secure Remote Password (SRP) protokolüdür.

5.1 Matematiksel Açıklama

SRP protokolünde bütün hesaplamalar sınırlı bir GF(n) alanında yapılır. Diğer bir deyişle büyük bir asal sayı seçilerek yapılacak tüm işlemler bu asal sayıya göre mod alınarak yapılır. Bu durumda P, Q, R ve S fonksiyonlarının tüm giriş ve çıkış parametreleri 0 ile n-1 arasındadır.

Tek yönlü doğrulayıcı fonksiyonu P(), g GF(n)'de bir *generator* olmak üzere, bir üstel fonksiyon olarak seçilir:

$$P(x) = g^{z} \tag{5.1}$$

Q(), R(), S() fonksiyonları ise aşağıdaki gibi seçilir:

$$Q(w,z) = w + ux \tag{5.2}$$

$$R(w,z) = wx^{u} \tag{5.3}$$

$$S(w,z) = w^{x} \tag{5.4}$$

(5.2) ve (5.3) deki eşitliklerde kullanılan u w ve z nin bir fonksiyonudur. (5.1) den (5.2) ye kadar verilen eşitlikler (4.1) de yerine yazıldığında eşitliğin sağlandığı (5.5) de görülmektedir.

$$S(R(g^{w}, g^{x}), Q(y,z)) \cong S(R(g^{y}, g^{z}), Q(w,x))$$

$$S(g^{w} g^{xu}, y + uz) \cong S(g^{y} g^{zu}, w + ux) \tag{5.5}$$

$$g^{(w+ux)(y+uz)} = g^{(y+uz)(w+ux)}$$

5.2 Çalışma Yapısı

Bu bölümde başlangıçtan sonuna kadar adım adım SRP ile nasıl bir kimlik doğrulama yapılacağı incelenecektir. Çizelge 5.1 de SRP nin matematiksel gösterimi için kullanılan parametreler ve ne anlama geldikleri yer almaktadır.

Çizelge 5-1 SRP için matematiksel gösterim (Wu, 1998)

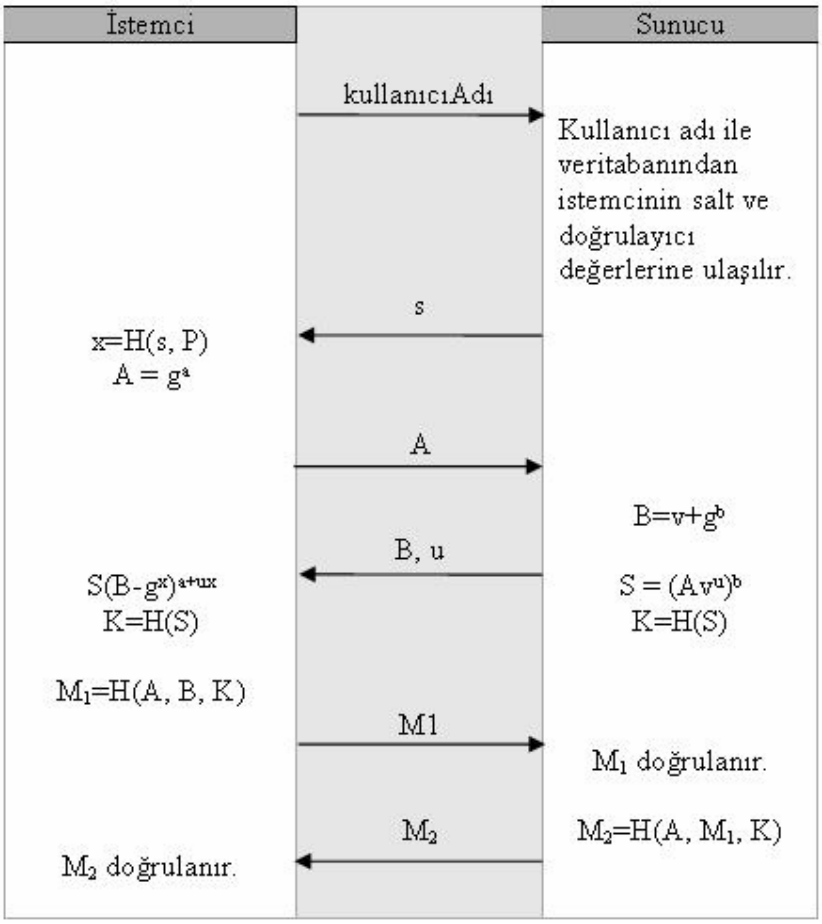
n	Hesaplamalarda mod almada kullanılacak büyük asal sayı
g	n ile aralarında asal olan "*generator*"
s	Kullanıcının *salt* değeri olarak kullanılacak rastgele değer
P	Kullanıcının şifresi
x	Kullanıcının şifresinden ve salt değerinden elde edilen özel anahtar
v	Sunucunun şifre doğrulayıcısı
u	Rastgele seçilen ve açık olarak dağıtılan karıştırıcı değeri
a, b	Rastgele üretilen ve genel olarak dağıtılmayan geçici özel anahtarlar
A, B	Genel anahtarlar
H()	Tek yönlü kıyım fonksiyonu
K	Oturum anahtarı

SRP protokolünün çalışma yapısı bir kimlik doğrulama işlemi üzerinde incelenebilir. İstemci, sunucu ile ortak bir *P* şifresi oluşturmak için rastgele bir *s* salt değeri seçer ve (5.6)'da gösterildiği gibi bununla bir *x* değeri hesaplar. Sunucu ise (5.7)'deki gibi *v* şeklinde bir doğrulayıcı değer hesaplar. Sunucu, istemcinin şifresi için bu doğrulayıcı değeri ve s (salt) değerini saklar.

$$x = H(s, P) \tag{5.6}$$

$$v = g^{x} (\mathrm{mod}\, n) \tag{5.7}$$

Burada x. P şifresinin eşleneği olduğu için kimlik doğrulama adımlarında kullanılmaz. AKE, tıpkı istemci tarafında olduğu gibi sunucunun da bir şifre oluşturmasına ve istemcinin de bu şifrenin doğrulayıcısını saklamasına olanak sağlar. SRP'de bu şifre 0 olarak seçilir ve doğrulayıcı değeri de 1 olur. Böylece sunucu kendi şifresini saklamak yerine sadece istemcinin doğrulayıcısını saklar. İstemci de sunucunun doğrulayıcı değerini saklamak



Şekil 5-1 SRP matematiksel çalışma adımları

zorunda olmayacağından protokol daha basit hale gelmiş olur.

Ortak bir şifre oluşturulduktan sonra sunucu ve istemci bir kimlik doğrulama yapabilir hale gelirler. Bu kimlik doğrulama adımları Şekil 5-1' de görülebilir. Kimlik doğrulama için öncelikle istemci kullanıcı adını sunucuya gönderir. Sunucu kullanıcı adına göre istemci için sakladığı doğrulayıcı ve salt değerlerine ulaşır, salt değerini istemciye gönderir. İstemci, aldığı s ve kendi sakladığı P değeri ile kendi özel anahtarı olan x değerini hesaplar. İstemci 1 ile n arasında rastgele bir *a* değeri üretir ve (5.8)'e göre kendi A genel anahtarını hesaplar. Hesapladığı bu genel anahtarı sunucuya gönderir. Benzer şekilde sunucu da 1 ile n arasında rastgele bir *b* değeri üretir ve (5.9)'e göre kendi B genel anahtarını hesaplar. Sunucu, hesapladığı genel anahtarı, rastgele ürettiği bir *u* değeri ile birlikte istemciye gönderir.

$$A = g^{a} \tag{5.8}$$

$$B = v + g^{b} \tag{5.9}$$

İstemci ve sunucu sahip oldukları değerleri kullanarak (5.10)'daki gibi üstel bir değer hesaplarlar. Eğer istemci genel anahtarını doğru şifreyi kullanarak oluşturmuş ise hesaplanan bu *S* değeri iki tarafta da aynı olmalıdır. İstemci ve sunucuda hesaplanan değerler karşılıklı olarak doğrulanmalıdır. Bunun için hesaplanan oturum anahtarı, *S*, kıyım fonksiyonundan geçirilir. İstemci, kendi genel anahtarı, sunucunun genel anahtarı ve kıyım fonksiyonundan geçirilmiş oturum anahtarını kullanarak (5.11) eşitliğindeki gibi bir M_1 değeri hesaplar ve sunucuya gönderir. Sunucu tarafında da aynı hesaplama yapılarak bu değer doğrulanır. Bu adımdan sonra sunucu da (5.12) eşitliğindeki gibi bir M_2 değeri hesaplayarak istemciye gönderir. Böylece istemci de sunucunun oturum anahtarını doğru hesapladığından emin olur.

$$S = g^{ab+bux} \tag{5.10}$$

$$M_1 = H(A, B, K) \tag{5.11}$$

$$M_2 = H(A, M_1, K) \tag{5.12}$$

SRP protokolü AKE protokolünün özeli bir hali olarak gösterilebilir. AKE'deki protokol akışına kullanıcı adı ve salt değerlerinin değişimi gibi birkaç adım eklenmiştir. Tüm adımlar doğru çalıştığında sonuçta hesaplanan oturum anahtarı iki tarafta da aynı olacaktır. Ortak oturum anahtarı düzgün hesaplandıktan sonra sunucu ve istemci arasında akacak tüm trafik bu anahtar ile şifrelenebilir.

5.3 Olası Saldırılara Karşı Dayanıklılığı

Dikkat edilecek olursa, protokol adımlarında istemci genel anahtarını kendi ürettiği rastgele bir değerin üstel bir fonksiyonu olarak hesaplarken, sunucu buna ek olarak bir de istemcinin şifresi için hesapladığı doğrulayıcıyı kullanmaktadır. Burada kullanılan doğrulayıcı değeri muhtemel bir saldırının önüne geçmek için kullanılmıştır. Örnek bir senaryo ile inceleyerek bu değerin kullanım nedenini daha iyi anlayabiliriz. Saldırgan başarılı bir kimlik doğrulama işlemini dinleyerek bu oturumdan *s* değerini yakalar. Daha sonra sunucu gibi davranarak istemciden kimlik doğrulama yapmasını ister. İstemci kullanıcı adının sunucuya gönderir. Sahte sunucu daha önce yakaladığı s değerini istemciye gönderir. İstemci *A* genel anahtarını hesaplar. Sahte sunucu rastgele *b* ve *u* değerlerini üretir. Kendi *B* genel anahtarını hesaplar, *B* ve *u* değerlerini istemciye gönderir. İstemci aldığı değerler ile oturum anahtarını hesaplar ve sahte sunucuya gönderir. Bu adımdan sonra gerekli değerleri elde eden saldırgan bir ağ veya şifre hatası ile oturumu sonlandırır. Saldırgan şifreyi bulmak için bir *p'* şifresi tahmin eder, bu tahmin değerinden *x'* ve *v'* değerlerini hesaplar. Bu değerleri kullanarak oturum anahtarını

hesaplar ve istemciden elde ettiği oturum anahtarı ile karşılaştırır. Bu işlemi başarılı oluncaya kadar tekrar ederek şifreye ulaşmaya çalışabilir. Sunucunun genel anahtarını hesapladığı adımda doğrulayıcı v değerini kullanması bu açığı ortadan kaldırır çünkü v değeri ağa hiç çıkarılmaz ve başka kimse tarafından bilinmez.

Protokolün güvenliğini artırmak için kullanılan diğer bir parametre de u değeridir. Doğrulayıcı v değerini çalan bir saldırganın kimlik doğrulama denemesini göz önüne alalım. Saldırgan bir şekilde sunucunun ürettiği u değerini öğrenmiş olabilir. Bu durumda akış şu şekilde olacaktır:

1. Saldırgan var olan bir istemcinin kullanıcı adını sunucuya gönderir.
2. Sunucu bu istemci için var olan s değerini saldırgana gönderir.
3. Saldırgan genel anahtarı (5.8) eşitliğinde olduğu gibi normal bir şekilde değil de, (5.13) eşitliğindeki gibi hesaplayarak sunucuya gönderir.

$$A = g^{a} v^{-u} \tag{5.13}$$

4. Sunucu (5.9) da olduğu gibi genel anahtarını hesaplayarak saldırgana gönderir.
5. Saldırgan oturum anahtarını (5.14)'deki gibi hesaplar ve sunucuya gönderir.

$$K = H(B - v)^{a} \bmod n \tag{5.14}$$

6. Hesaplanan bu oturum anahtarı sunucu tarafından onaylanacaktır çünkü sunucu oturum anahtarını (5.15)'deki gibi hesaplamaktadır.

$$S = (Av^{u})^{b} = (g^{a} v^{-u} v^{u})^{b} = g^{ab} \tag{5.15}$$

Böylece saldırgan kendini doğru bir kullanıcı gibi sunucuya göstermeyi başarabilir. Bunu önlemek için sunucu, istemcinin genel anahtarını almadan u değerini oluşturmamalı ve ağa çıkarmamalıdır. Ayrıca u'nun genel sabit bir değer olarak seçilmesinden de kaçınılmalıdır.

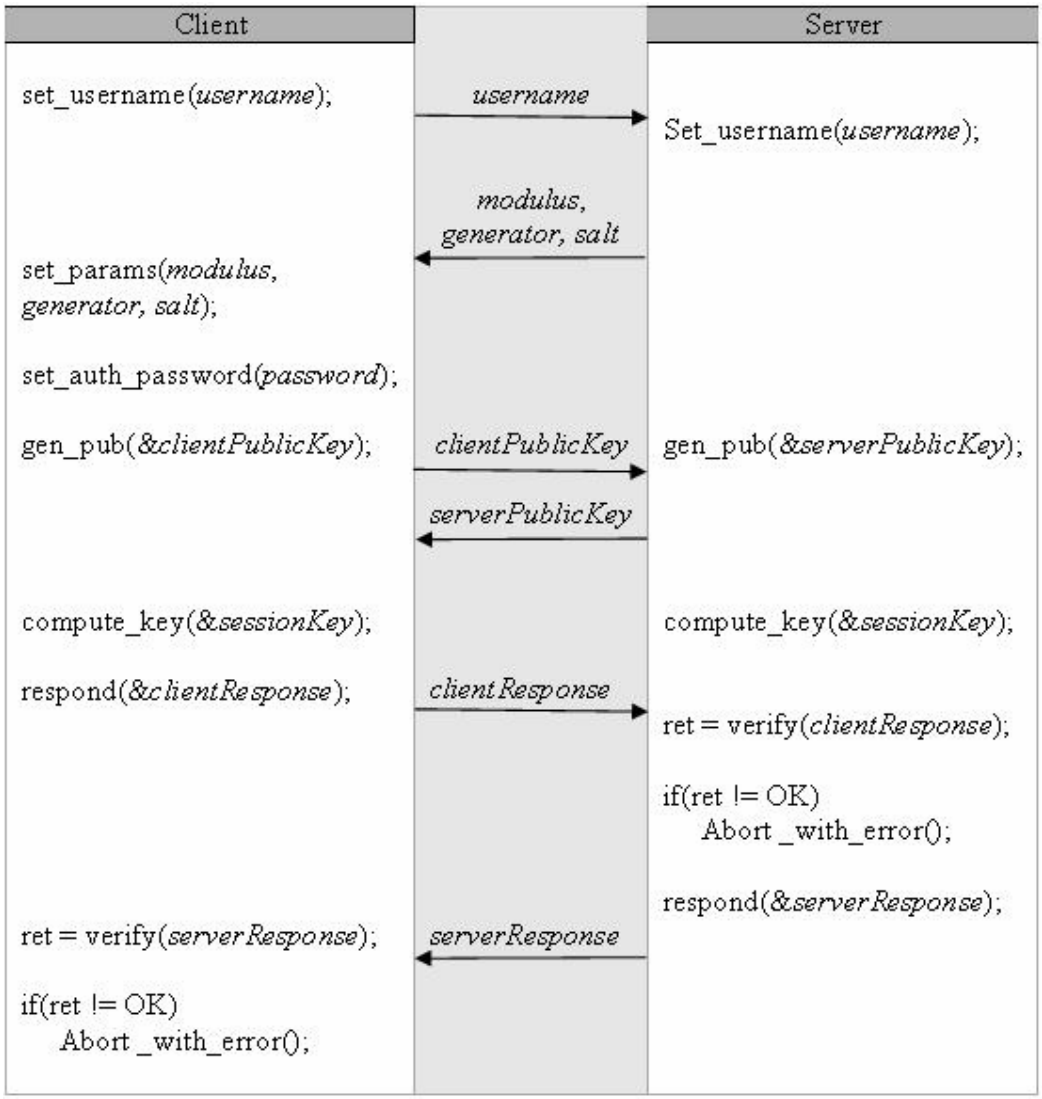
6. SRP'NİN SIP KİMLİK DOĞRULAMADA KULLANILMASI

SIP'in basit yapısı sebebiyle tasarım aşamasında güvenlik ile ilgili sağlam çözümler sunulmamıştır. Bu sebeple bölüm 3.2'de anlatılan saldırılarla karşı karşıya kalabilmektedir. SIP'in kullanım alanı arttıkça ve kullanımı yaygınlaştıkça güvenliğinin artırılması da zorunlu hale gelmiştir. SIP güvenliği ile ilgili düzeltmeler, iyileştirmeler yapılırken dikkat edilmesi gereken en önemli konulardan birisi de protokolün basit yapısının bozulmaması ve performans açısından sisteme aşırı yük getirmemesidir. Bunun için bölüm 3.3'de SIP güvenliğinin iyileştirilmesi ile ilgili yapılan çalışmalardan bahsedilmiştir. Bu çalışmada ise SIP kimlik doğrulama ile ilgili bir iyileştirme gerçekleştirilmeye çalışılacaktır. Bunun için mevcut kimlik doğrulama mekanizmaları incelenmiştir. Bunların avantaj ve dezavantajları 4. bölümde ele alınmış ve bunlardan birisi olan SRP 5. bölümde anlatılmıştır. Bu bölümde ise SRP protokolünün SIP kimlik doğrulama mekanizmasına uygulamasını gerçekleştirmeye çalışılacaktır.

6.1 SRP ve SIP Kimlik Doğrulma Mekanizmasının Karşılaştırılması

SIP kimlik doğrulama mekanizmasından bölüm 3.1'de bahsedilmiştir. Benzer şekilde bölüm 5.1'de SRP matematiksel çalışma adımlarından bahsedilmiştir. SRP protokolünün uygulama olarak kimlik doğrulama aşamaları Şekil 6-1'deki gibi gösterilebilir. Bu aşamalara göre önce istemci tarafından kimlik doğrulama amacıyla sunucuya kullanıcı adı gönderilir. Kullanıcı adını alan sunucu protokol ile ilgili parametreleri istemciye gönderir. İstemci bu parametreler ile genel anahtarını hesaplayarak sunucuya gönderir, aynı şekilde sunucu da genel anahtarını hesaplayarak istemciye gönderir. Bu anahtar değişimi yapıldıktan sonra istemci oturum anahtarını hesaplar ve doğrulatmak amacıyla sunucuya gönderir. Sunucu eğer oturum anahtarı doğru ise istemciye kendi hesapladığı oturum anahtarı ile cevap verir, istemci de bu oturum anahtarı ile sunucunun kimlik doğrulamasını yapar. Böylelikle karşılıklı kimlik doğrulama işlemi tamamlanmış olur.

SRP protokolündeki kimlik doğrulama adımları incelendiğinde mevcut SIP kimlik doğrulama mekanizması ile benzer yönleri görülmektedir. Örneğin SIP kimlik doğrulamada istemci sunucuya bir istek mesajı gönderdiğinde sunucu bu mesaja içinde kimlik doğrulamada kullanılacak *nonce* değeri olan bir *Unauthorized* mesajı ile cevap verir. Benzer şekilde SRP protokolünde de kullanıcı adı ile kimlik doğrulama isteyen bir istemciye yine kimlik doğrulamada kullanılacak parametreler ile cevap verir. Yine SIP kimlik doğrulamada istemci aldığı *nonce* değeri, kullanıcı adı ve şifre ile hesapladığı cevap değeri ile sunucuya tekrar bir



Şekil 6-1 SRP çalışma adımları

istek mesajı gönderir. SRP'de ise bu cevap değeri hesaplanan oturum anahtarı olarak kabul edilebilir. Bu benzerlikler göz önüne alınarak SRP protokolünün SIP kimlik doğrulama mekanizmasına mevcut protokol akışını fazla bozmadan uygulanabileceği söylenebilir. Bunun uygulanması için yine de birkaç yeni alan ve mesaja ihtiyaç vardır.

6.2 Yeni Mesaj ve Mesaj Alanları ile Uygulama

Önceki bölümde anlatıldığı gibi SRP protokolü ve SIP kimlik doğrulama çalışma yapısı anlamında benzerlik göstermektedirler. Bununla beraber SRP protokolünün SIP kimlik doğrulamaya uygulanabilmesi için bazı eklemelere ihtiyaç vardır. Öncelikle SIP istek mesajlarının içinde istemci kimlik bilgisi de bulunmalıdır. SIP'de kullanıcı adı içinde kimlik

bilgileri ve *response* değeri bulunan *REGISTER* mesajı ile gönderilmektedir. Şekil 6-2'de standart bir *REGISTER* mesajı, Şekil 6-3'de ise kimlik bilgileri içeren bir *REGISTER* mesajı

```
REGISTER sip:192.168.10.239 SIP/2.0
Via:SIP/2.0/UDP192.168.10.124:5060; rport;
branch=z9hG4bK68891D628141436 88D27D4FCD6BB6995
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>
Contact: "celalettin" <sip:509@192.168.10.124:5060>
Call-ID: D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26106 REGISTER
Expires: 1800
Max-Forwards: 70
User-Agent: X-Lite release 1103m
Content-Length: 0
```

Şekil 6-2 SIP *REGISTER* mesajı

```
REGISTER sip:192.168.10.239 SIP/2.0
Via:SIP/2.0/UDP192.168.10.124:5060; rport;
branch=z9hG4bKDBB583F9D7D14E149F20BF016CBB9C27
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>
Contact: "celalettin" <sip:509@192.168.10.124:5060>
Call-ID: D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26107 REGISTER
Expires: 1800
Authorization:Digest username="509", realm="192.168.10.239", nonce="6f2aed14",
response="adb953f21385c8db51b10460e0465429", uri="sip:192.168.10.239"
Max-Forwards: 70
User-Agent: X-Lite release 1103m
Content-Length: 0
```

Şekil 6-3 Kimlik bilgileri içeren SIP *REGISTER* mesajı

görülmektedir. SRP protokolünün uygulanabilmesi ve sunucunun istemci için sakladığı bilgilere ulaşabilmesi için kullanıcı adının ilk istek mesajında sunucuya gelmesi gerekir. Bunun için standart *REGISTER* mesajında *Contact* alanına bir parametre daha eklenerek kullanıcı adı ilk *REGISTER* mesajı ile birlikte sunucuya gönderilir. Yeni eklenen mesaj alanı ile birlikte yeni *REGISTER* mesajı Şekil 6-4'deki gibi olacaktır.

```
REGISTER sip:192.168.10.239 SIP/2.0
Via:SIP/2.0/UDP192.168.10.124:5060; rport;
branch=z9hG4bK68891D628141436 88D27D4FCD6BB6995
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>
Contact: "celalettin" <sip:509@192.168.10.124:5060>, username="509"
Call-ID: D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26106 REGISTER
Expires: 1800
Max-Forwards: 70
User-Agent: X-Lite release 1103m
Content-Length: 0
```

Şekil 6-4 SRP ile kullanılacak *REGISTER* mesajı

SIP kimlik doğrulamada istek mesajını alan sunucu istemciye içinde *nonce* değeri bulunan bir Unauthorized mesajı gönderirken, SRP protokolünde kullanıcı adını alan sunucu istemciye SRP parametrelerini göndermektedir. Bu parametrelerin taşınması için Unauthorized mesajı içerisinde yeni bir alan tanımlanmalıdır. Şekil 6-5'de standart SIP *Unauthorized* mesajı görülmektedir. Bu mesaja, SRP parametrelerini taşımak amacıyla "SRP Authenticate" alanı eklenmiştir. Yeni tanımlanan alanla birlikte yeni *Unauthorized* mesajının bir örneği Şekil 6-6'daki gibidir.

```
SIP/2.0 401 Unauthorized
Via:SIP/2.0/UDP192.168.10.124:5060;
branch=z9hG4bK68891D628141436 88D27D4FCD6BB6995
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>;tag=as6f2846e4
Call-ID: D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26106 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:509@192.168.10.239>
WWW-Authenticate: Digest realm="192.168.10.239", nonce="6f2aed14"
Content-Length: 0
```

Şekil 6-5 Standart SIP Unauthorized mesajı

```
SIP/2.0 401 Unauthorized
Via:SIP/2.0/UDP 192.168.10.124:5060;
branch=z9hG4bK68891D628141436 88D27D4FCD6BB6995
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>;tag=as6f2846e4
Contact: celalettin <sip:509@192.168.10.239>;tag=as6f2846e4
Call-ID: D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26106 REGISTER
User-Agent: Asterisk PBX
Content-Length: 0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
WWW-Authenticate: Digest realm="192.168.10.239", nonce="6f2aed14"
SRP_Authenticate: generator="2"
modulus="d4c7f8a2b32c11b8fba9581ec4ba4f1b04215642ef7355e37c0fc0443e
f756ea2c6b8eeb755a1c723027663caa265ef785b8ff6a9b35227a52d86633dbdfc
a43" salt="e0938e9ce880449f2c47"
```

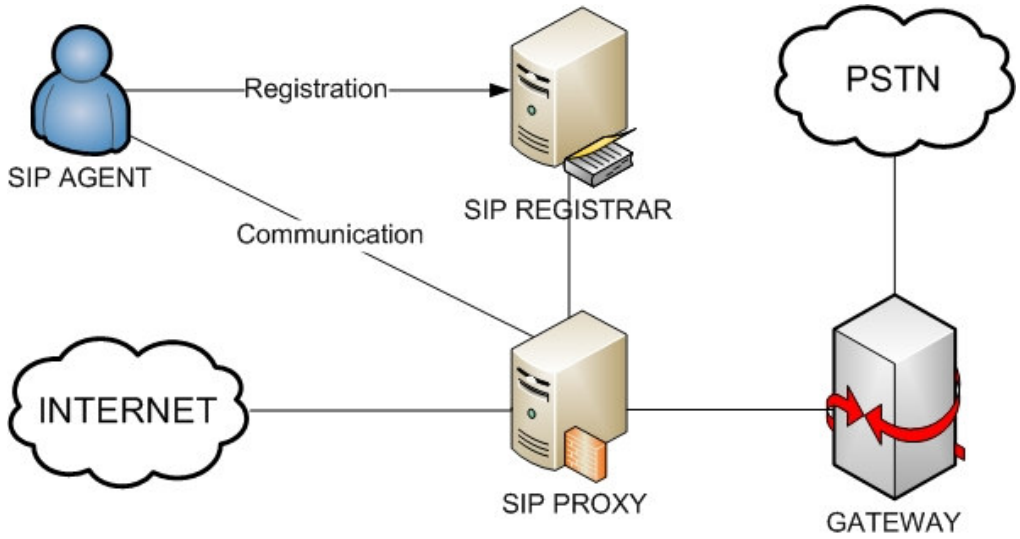
Şekil 6-6 SRP_Authenticate alanı ile yeni Unauthorized mesajı

Unauthorized mesajının içinde SRP parametrelerini alan istemci kendi genel anahtarını oluşturur. Bu genel anahtarın sunucuya gönderilmesi için bir mesaja ihtiyaç vardır. Bu uygulamada, bu iş için *SRPPublicKey* mesajı tanımlanmıştır. Bu mesaj içeriği bir örnek ile Şekil 6-7 de görülebilir. Bu mesaj ile istemci ve sunucu genel anahtarlarını paylaşırlar. Genel anahtar değişiminden sonraki adımda iki tarafta oturum anahtarı hesaplanır. İstemci hesapladığı oturum anahtarı için ürettiği doğrulayıcıyı değeri göndereceği ikinci *REGISTER* mesajının *Authorization* alanında gönderir. Bu yüzden bu işlem için ayrıca bir mesaj veya alan tanımlanmasına gerek yoktur.

```
SRPKey sip:192.168.10.239 SIP/2.0
Via:SIP/2.0/UDP 192.168.10.124:5060; rport;
branch=z9hG4bK68891D628141436 88D27D4FCD6BB6995
From: celalettin <sip:509@192.168.10.239>;tag=657718805
To: celalettin <sip:509@192.168.10.239>
Contact: celalettin <sip:509@192.168.10.239>
Call-ID:D627496D04D24EE392C4D4C6BDFC0A43@192.168.10.239
CSeq: 26106 REGISTER
Expires: 1800
Max-Forwards: 70
User-Agent: X-Lite release 1103m
Content-Length: 0
SRPKey :
5B0880841954B05F7F2B1100F764776B9A68D95F309E6F86537B6CFA297
80FD6D5A1CC883F83795ADEE36C74EB2E85441FE7C0ED694FDF1BD0B
B23A93AC0B3E9
```

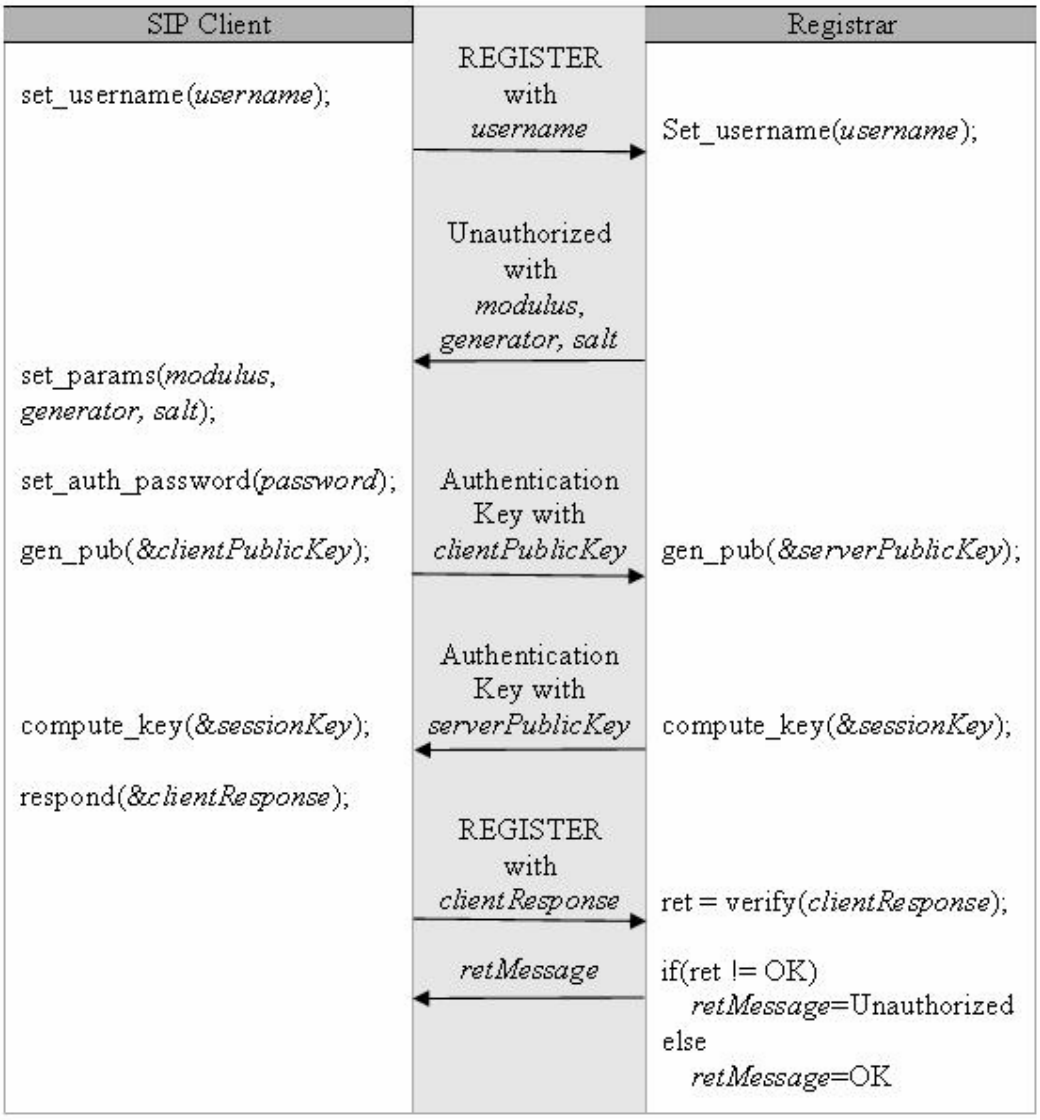
Şekil 6-7 SRPPublicKey mesajı

SRP protokolü ve SIP kimlik doğrulama mekanizması arasındaki benzer yönler incelendikten sonra uygulamaya geçmeden önce tanımlanması gereken mesaj ve mesaj alanları tanımlandı. Bu adımdan sonra Bölüm 6.1'de bahsettiğimiz benzerlikten yararlanarak ve Bölüm 6.2'de tanımladığımız mesaj ve mesaj alanlarını kullanarak yeni kimlik doğrulama prosedürünü gerçekleştirildi. Yeni kimlik doğrulama prosedürü Şekil 6-8'deki SIP agent ile kaydedici sunucu arasındaki işleme uygulandı.



Şekil 6-8 SIP kullanıcı etmeni kayıt işlemi

SRP protokolü ile gerçekleştirilen bir SIP kimlik doğrulama adımları Şekil 6-8'de görülmektedir. Buna göre ilk olarak istemci sunucuya kullanıcı adı ile birlikte bir *REGISTER* mesajı gönderir. *REGISTER* mesajını alan sunucu istemciye içinde SRP parametrelerinin bulunduğu *Unauthorized* mesajı gönderir. İstemci bu parametreler ile genel anahtarını oluşturur ve tanımlanan *SRPKey* mesajı ile genel anahtarını sunucuya iletir. Sunucu da aynı mesajı kullanarak kendi genel anahtarını istemciye iletir. Sunucunun da genel anahtarını alan istemci oturum anahtarını hesaplar. Daha sonra oturum anahtarı için bir doğrulayıcı değer hesaplayarak bunu sunucuya gönderir. Sunucu kendi tarafında hesapladığı oturum anahtarı ile istemciden gelen doğrulayıcı değeri karşılaştırır ve istemcinin kimliğinin doğrulanıp doğrulanmayacağına karar verir. Buna göre ya istemciye *OK* mesajı dönülür ya da tekrar *Unauthorized* mesajı gönderilir. Böylelikle kimlik doğrulama işlemi tamamlanmış olur.



Şekil 6-9 SRP kullanılarak gerçekleştirilen SIP kimlik doğrulama adımları

6.3 Güvenlik Kazanımları

Önceki bölümlerde tartışıldığı gibi SIP güvenlik sistemi çok sağlam bir yapıya sahip olmamakla birçok saldırı tehlikesiyle karşı karşıya kalabilmektedir. Bu saldırı tehlikelerinden birisi de pasif sözlük saldırısı olarak gösterilebilir. Bu saldırı yönteminin kendisine uygulama alanı bulmasının en önemli sebebi SIP kimlik adoğrulama mekanizmasında, iletişim sırasında şifrenin kıyım fonksiyonundan geçirilmiş halinin doğrudan kullanılmasıdır. Güvenli bir ağ protokolünden beklenen, iletişim sırasında taraflar hakkında minimum bilgi sızdırmasıdır.

SRP protokolünde ise şifre veya herhangi bir kıyım eşleneği iletişimde kullanılmamaktadır.

SIP kimlik doğrulamadaki bu açık noktayı gidermek için yaptığımız bu uygulama ile protokolün bu tip sözlük saldırılarına karşı dayanıklılığı oldukça artırılmıştır. Ayrıca kimlik doğrulama sırasında hesaplanan bu oturum anahtarı ile iletişimde gizli kalması istenen bilgiler de şifrelenerek kullanılabilir. Böylece sadece kimlik doğrulama adımı değil protokol akışında ihtiyaç duyulan başka adımlar için de güvenlik artırılabilir.

Daha önce de bahsettiğimiz gibi güvenlik ile ilgili iyileştirmeler yapılırken dikkat edilmesi gereken en önemli konulardan birisi de protokolün basit yapısının bozulmamasıdır. SRP protokolünün, SIP kimlik doğrulama adımları ile örtüşmesi sayesinde protokol üzerinde çok küçük değişiklikler ile bu güvenlik kazanımı sağlanmıştır.

7. SONUÇ

SIP, IP tabanlı telefon sistemlerinde geniş ve gün geçtikçe artan bir uygulama alanına sahiptir. Kullanımının artması SIP'in taşıdığı sorumluluğu da artırmaktadır. SIP protokolü tasarım itibariyle basit ve esnek bir yapıya sahiptir. Bu sebeple ilk aşamada güvenlik ile ilgili çok sağlam tedbirler alınmamıştır. Fakat bugün çalıştığı alanlar ve yüklendiği sorumluluklar itibariyle SIP protokolü güvenlik açısından gözden geçirilmelidir. Internet üzerinde çalışan bir protokol olması sebebiyle Internet'in getirdiği saldırı tehlikeleri SIP için de bir tehdit oluşturmaktadır. Bu sebeple güvenlik konusu SIP için göz ardı edilemez hale gelmiştir.

Bu çalışmada SIP'in kimlik doğrulama mekanizması incelenmiş, açıkları ve karşılaşabileceği saldırı tehlikeleri ortaya konmuştur. Bu konuda şimdiye kadar yapılan çalışmalara değinilmiştir. SIP kimlik doğrulama mekanizmasının iyileştirilmesi ve güvenlik açıklarının giderilmesi için kullanılabilecek kimlik doğrulama yöntemleri üzerinde çalışılmıştır. Bu kimlik doğrulama yöntemlerinden biri olan SRP protokolü üzerinde durulmuş ve SIP kimlik doğrulama ile olan benzerliğine dikkat çekilmiştir. Son olarak SRP protokolünün SIP kimlik doğrulamaya uygulanması gösterilmiş ve bir uygulama ile gerçeklenmiştir.

SRP protokolü ve SIP kimlik doğrulamanın çalışma yapıları arasındaki benzerlik uygulama açısından kolaylık sağlamıştır. Ayrıca bu sayede, iyileştirme yapılırken protokol üzerinde çok az bir değişikliğe ihtiyaç duyulmuştur. Bunun için *SRPKey* adında ek bir SIP mesajı tanımlanmıştır. Standart bir SIP mesajı olan *Unauthorized* mesajının içeriğine *SRP_Authenticate* isimli bir alan eklenmiş ve kimlik doğrulamada kullanılacak SRP parametreleri bu alan içinde gönderilmiştir. Bu durumda her kayıt işleminde sunucu ve istemci arasında ek bir mesaj daha gidip gelecektir. Fakat bu değişiklik ile kimlik doğrulama sürecinde kullanıcı şifrelerinin iletişimde hiç kullanılmaması sağlanacaktır. SIP kimlik doğrulamada SRP protokolünün kullanılması ile SIP güvenliğinde ciddi bir artış sağlanmış olacaktır.

Yeni tasarlanan sistem için bir SIP istemci ve bir SIP sunucudan oluşan bir uygulama hazırlanmıştır. Uygulama C++ dilinde kodlanarak çalışma süreleri incelenmiştir. Digest kimlik doğrulama ve SRP kimlik doğrulama kullanılarak 100'er kez kimlik doğrulama gerçekleştirilmiş ve bu işlem 10 kez tekrar edilmiştir. Bu şekilde kimlik doğrulama için ortalama bir süre elde edilmeye çalışılmıştır. Intel P4 işlemci ve 256 MB hafızaya sahip bir kişisel bilgisayarda yapılan test sonuçları Çizelge 7-1'deki gibidir.

Çizelge 7-1 Digest ve SRP kullanılarak yapılan kimlik doğrulama için çalışma süreleri

Test No	Çalışma Süresi (ms)			
	Digest Kimlik Doğrulama	SRP Kimlik Doğrulama		
1	16687	26125		
2	20687	25032		
3	20531	24500		
4	16031	25969		
5	17891	25718		
6	20437	24594		
7	20718	24281		
8	20657	26844		
9	20516	25688		
10	20532	25985		
Ortalama	19468,7	25473,6	Artış Oranı	0,308439

Eklenen şifreleme ve çözme işlemleri sisteme %30 gibi bir hız kaybı getirmiştir. Bu hız kaybının sebebi gönderilen ve alınan mesaj sayısının her kimlik doğrulama işlemi için iki artması ve SRP protokolünde yapılan şifreleme ve çözme işlemleridir. SIP kimlik doğrulama bir kullanıcı için ilk oturum açtığında ve kullanıcı bilgisi için belirlenen zaman aşımı değeri aşıldığında yapılmaktadır. Bu sebeple bu mekanizmada hızdan daha çok güvenilirlik ön plana çıkmaktadır. Sadece gerekli durumlarda kullanılacak olan kimlik doğrulama işleminde eklenecek bir ek mesaj sistem performansını çok olumsuz etkilemeyecektir. Bu durumda elde edilen güvenlik kazanımı göz önüne alındığında bu hız kaybı kabul edilebilir bir seviyededir.

KAYNAKLAR

Bellovin S.M., Merritt M., “Augmented encrypted key exchange: A password-based protocol secure against dictionary attacs and password file compromise”.1994, AT&T Bell Laboratories

Diffie W., Hellman M. E., “New direcitons in cryptography” IEEE Transactions on Information Theory, vol. IT-11, : 644-654, Kasım 1976

Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., Berners-Lee T., "Hypertext Transfer Protocol", RFC 2616, June 1999

Franks J., Hallam-Baker P., Hostetler J., Lawrence S., Leach P., Luotonen A., Stewart L., “HTTP Authentication: Basic and Digest Access Authentication”, RFC 2617, 1999

Holger S., Chi-Tai D., Franz J. H., (2007), “Proxy-based Security for the Session Initiation Protocol (SIP)”, Second Internatiol Conference on Systems and Networks Communications, IEEE

Jablon D. Strong password-only authenticated key exchange. Computer Communication Review, 26(5):5-26, October 1996.

Postel J. B., "Simple Mail Transfer Protocol", RFC 821, 1982

Qi, Q. (2003), Study of Digest Authentication for Session Initiation Protocol, SITE, University of Ottowa

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Srinivasan R., Vaidehi V., Harish K., LakshmiNarasimhan K., LokeshwerBabu S., Srikanth V. (2005) “Authentication of Signaling in VoIP Applications”, 2005 Asia-Pacific Conference on Communications, 3 - 5 October 2005, , Perth, Western Australia.

Steiner M., Tsudik G., and Waidner M., “Refinement and extension of encrypted key exchange”, ACM Operating Systems Review, 29(3), July 1995.

ÖZGEÇMİŞ

Doğum tarihi	25.05.1983	
Doğum yeri	Zile	
Lise	1998-2000	Manisa Turgutlu Halil Kale Fen Lisesi
	2000-2001	Tokat Gazi Osman Paşa Lisesi
Lisans	2001-2005	Yıldız Üniversitesi Elektrik-Elektronik Fak. Bilgisayar Mühendisliği Bölümü
Yüksek Lisans	2005-2008	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı

Çalıştığı kurumlar

2005-Devam ediyor Sestek Ses ve İletişim Bilgisayar Teknolojileri A.Ş