WebRTC Tabanlı Artırılmış Güvenli İletişim
WebRTC Based Augmented Secure Communication

Cengiz Toğay[1] ve Albert Levi[2]
[1]Bilgisayar Mühendisliği Bölümü, Uludağ Üniversitesi, Bursa, Türkiye
ctogay@uludag.edu.tr
[2]Bilgisayar Bilimi ve Mühendisliği Programı, Sabancı Üniversitesi, İstanbul, Türkiye
levi@sabanciuniv.edu

***Özetçe*— Sunulan çalışmada uçtan-uca WebRTC tabanlı güvenli iletişimin sağlanmasına yönelik bir yöntem önerilmektedir. Sunulan yöntemde, standart WebRTC sinyalleşmesinde yer alan anahtar takasına yönelik parametrelerin, akıllı kart üzerinde çalışacak açık anahtar tabanlı kriptografi yöntemleri ile güvenli bir şekilde aktarılması sağlanmaktadır. Geliştirilen yöntem gerçek ortamda denenmiş ve fizibilitesi görülmüştür.**

Anahtar Kelimeler — WebRTC; akıllı kartlar, RSA, güvenli iletişim.

***Abstract*— In the presented study, a method is proposed for WebRTC based secure communication. In the proposed method, some parameters related with key exchange in standard WebRTC signaling are transferred in a secure way with applying public key cryptography methods over smartcards. The method is applied in real environment and feasible results are obtained.**

Keywords — WebRTC; smart cards, RSA, secure communication

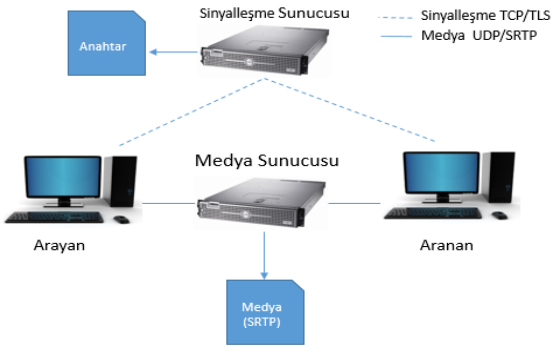
I. GİRİŞ

Internet ve sosyal iletişim platformlarının yaygınlaşmasına bağlı olarak mobil ve masaüstü ortamlarında, IP tabanlı sesli ve görüntülü iletişim önem kazanmaktadır. Web Real Time Communication (WebRTC) [1], [2], bu ihtiyacın karşılanmasına yönelik olarak ortaya çıkmıştır. WebRTC, Özellikle Web ortamında tarayıcılar üzerinde herhangi eklenti ya da kurulum gerektirmeksizin sesli ve görüntülü iletişimin yanı sıra veri kanalı üzerinden ekran, dosya, resim vb. paylaşımına olanak sağlamaktadır. Sunulan platform, sadece medyanın (ses, görüntü ve veri) uçlar arasında iletişimini güvenli bir şekilde sağlamayı hedeflemektedir. Bu kapsamda, tarayıcıların içerisinde bulunan WebRTC platformu temelde:

- ses ve görüntü birimlerinden medyayı almak ve sunma işlemlerini yerine getirmek üzere zengin kodek desteği ile ses ve görüntü motorları,
- medyanın güvenli aktarılması için Secure Real Time Protocol (SRTP) ile uyumlu kütüphane,
- medyanın aktarılmasında kullanılan ses, görüntü ve veri kanallarının tek bir kanal içerisinden ya da ayrı ayrı kanallar üzerinden aktarılmasını sağlayan kütüphane,
- Network Address Translation (NAT) arkası cihazlara erişim probleminin çözülmesine yönelik olarak Traversal Using Relays around NAT (TURN) [3] ve Interactive Connectivity Establishment (ICE)[4] protokollerini gerçekleştiren kütüphanelerden oluşmaktadır.

WebRTC'de bir çağrının kurulabilmesi için temelde offer (talep), answer (cevap) ve ICE candidate (ICE adayları) mesajlarının uçlar arasında aktarılması gerekmektedir.

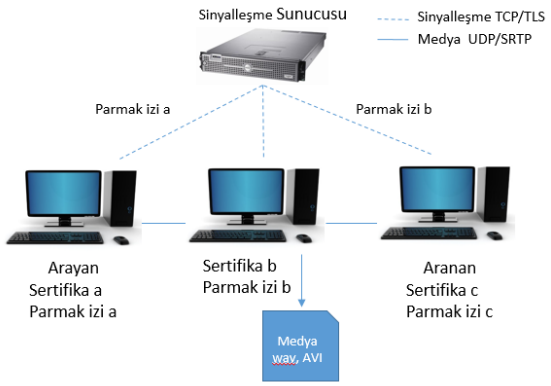
Meydanın şifrelenerek aktarılmasında kullanılacak olan anahtarın iletilmesinde Session Description Protocol (SDP) Security Descriptions for Media Streams (SDES) [5] ve DTLS [6] olmak üzere iki standart yöntem kullanılmaktadır. SDES'de medyanın şifrelenmesinde kullanılan anahtar açık bir şekilde talep ya da cevap mesajının içerisinde yer alır. Güvenlik açısından bu yöntemde, Şekil 1'de gösterildiği üzere uçlar arasında sinyalleşmeyi sağlayan sunucunun açık bir şekilde yer alan anahtarı elde etme imkanı vardır. Dolayısıyla uçlar arasındaki iletişime ait şifreli medyanın saklanması ve sonrasında medya içeriğinin elde edilmesi mümkündür.



Şekil 1. SDES ile dinleme

978-1-5090-1679-2/16/$31.00 ©2016 IEEE

Datagram Transport Layer Security (DTLS) [6] yönteminde talep ve cevap mesajlarının içerisinde WebRTC tarafından oluşturulan bir sertifikaya ait kriptografik parmak izi yer alır. Tüm sinyalleşme aktivitelerinin tamamlanmasının ardından uçlara ait WebRTC kütüphaneleri medya kanalları üzerinden kendilerine aktarılan parmak izleri ile karşı tarafın sertifikasını doğrular ve sonrasında anahtar takasını gerçekleştirirler. Ancak, Şekil 2'de gösterildiği üzere, araya girecek olan bir uygulamaya ait bir parmak izi ile (parmak izi b), SDP mesajlarında orijinali (parmak izi a) ile değiştirmek sureti ile araya girilebilme imkanı bulunmaktadır.



Şekil 2. DTLS ile dinleme

Talep ya da Cevap mesajları Session Description Protocol (SDP) [7] paketini içerir. SDP paketinde temelde aşağıda örnek olarak listelenmiş bilgiler yer alır:

- ICE paketlerinin doğrulanması için ice-ufrag ve ice-pwd kullanılır. ICE paketleri istemcilere ulaşılması için gerekli tüm IP ve port ikililerini içermektedir. İstemciler kendilerine gelen IP adaylarına ulaşırken doğrulama amacı ile ice-ufrag ve pwd bilgisine ihtiyaç duyulur.

  a=ice-ufrag:Yb3012SK07BeS/JQ\r\n

  a=ice-pwd:f+av4QC/V9Vq1rrLcpaAgsLw\r\n

- Ses ve video kodekleri SDP paketlerinde öncelik sırası belirtilerek iletilir.

  m=audio 9 UDP/TLS/RTP/SAVPF 103 104 9 0 8 126

  a=rtpmap:103 ISAC/16000

  m=video 9 UDP/TLS/RTP/SAVPF 101 100 116 117 96\r\n

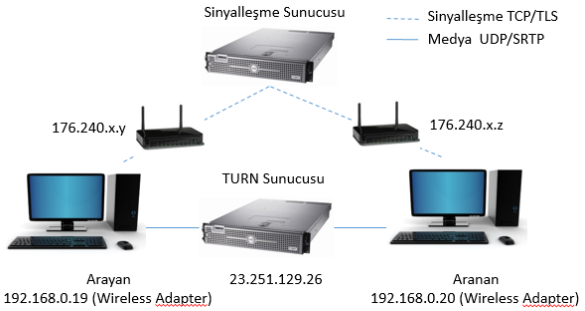
  a=rtpmap:101 VP9/90000

- Medyanın şifrelenmesinde kullanılmak üzere eğer SDES ise base64 ile paketlenmiş anahtar

  a=crypto:1 AES_CM_256_HMAC_SHA1_80 inline:DiCiznXB3stobwz7zPmILYMT+MbIVqBDdXnnY8Fjc9FqXyNW/VewzOK+zZnCYr34

  DTLS ise kullanılacak sertifikaya ait parmak izi

  a=fingerprint:sha-256 36:6B:91:49:A2:3D:3A:2E:D6:00:36:97:93:B2:90:34:CB:4B:E3:60:48:C7:CC:4C:1C:78:C2:30:F7:A4:CE:C2 yer almaktadır.



Şekil 3. İletişim network mimarisi

Şekil 3'de bir çağrı gerçekleştirecek iki istemci, istemcilerin bağlı oldukları bir sinyalleşme sunucusu, medyanın yönlendirilmesi için TURN sunucusu ve NAT cihazları yer almaktadır. İstemciler ile sunucu arasında standart bir TCP soket bağlantısı, WebSocket, XMPP (Extensible Messaging and Presence Protocol) ve Long polling gibi protokoller kullanılabilir. WebRTC, sinyalleşme kanalının nasıl olması gerektiği ile ilgili herhangi bir sınırlandırma getirmemektedir. Çağrının başlatılması için SDP paketinin yanı sıra IP adaylarına (yerel IP, NAT IP ve Relay IP) ihtiyaç bulunmaktadır. IP adayları ICE-candidate [4] olarak aktarılır. TURN sunucusu özellikle NAT arkasındaki cihazların arasındaki iletişimin sağlamasında kullanılan SRTP paketleri için Relay sunucusu görevini görmektedir. Aşağıda Şekil 3 ile uyumlu olmak üzere arayan tarafa ait ICE candidate adresleri aşağıda listelenmiştir.

1. Yerel IP: "candidate:678820566 1 udp 2122129151 **192.168.0.19 61191** typ host generation 0"
2. NAT IP: "candidate:3731194626 1 udp 1685921535 **176.240.x.y 46035** typ srflx raddr 192.168.0.19 rport 61191 generation 0"
3. TURN IP: "candidate:49227043 1 udp 41754367 **23.251.129.26 52601** typ relay raddr 176.240.x.y rport 46035 generation 0"

RTP paketlerinin şifrelenerek SRTP paketleri elde edilmesinde kullanılan algoritmaların standartlara uygunluğu sağlanmalıdır. WebRTC platformunda standart olarak şifreleme için AES 128 ve veri bütünlüğü için HMAC-SHA1 algoritmaları kullanılmaktadır.

978-1-5090-1679-2/16/$31.00 ©2016 IEEE

II. ÖNERİLEN YAKLAŞIM

İnternet ortamında kişiler arasındaki iletişimin mahremiyeti önem kazanmaktadır. Sunucuya güvenilen ortamda sadece **yasal dinleme** kapsamındaki iletişim SDES ya da DTLS olmasına bakılmaksızın medyanın içeriğinin elde edilmesi imkanı olduğu görülmektedir. Güvenliğin daha önem kazandığı durumlarda sunucunun arada olmasına rağmen iletişimin içeriğini öğrenememesi beklenmektedir

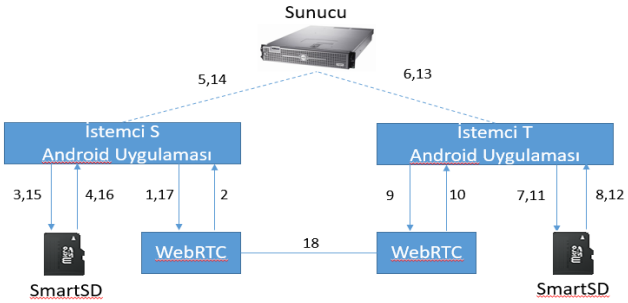
Medyanın şifrelenmesinde kullanılan anahtar uzunluğu kadar rastgele olması da önemlidir. Cihazlarda rastgele anahtar üretiminde kaynak olarak klavye, fare, mikrofon vb. donanımlardan elde edilen girişlerden faydalanılmaktadır. Ancak, üretilen her sayının gerçek rastgele (standartlara uygun) üretiminde problemler bulunmaktadır.

Arayan ve aranan tarafın karşıdakini doğrulaması ve güvenli anahtar veya anahtarın kriptografik parmak izinin aktarımına ihtiyaç bulunmaktadır. Kullanılan en yaygın yöntem sertifika tabanlı şifreleme/doğrulamadır. Burada kullanılacak çözümün kimin tarafından kullanılacağına ve ihtiyaç duyulan güvenlik seviyesine bağlı olarak değişkenlik göstermektedir. Güvenli bir şekilde gönderilmek istenen veri, karşı tarafın sertifikasında yer alan açık anahtar ile şifrelenir ve kendi özel anahtarı ile şifrelenerek karşı tarafa gönderilir. Karşı tarafa ait açık anahtarın herkes tarafından bilinmesi sağlanmalıdır. Yöntemlerden bir tanesi otoritelerce imzalanmış ve açık anahtar bilgisini içeren sertifikaların kullanılmasıdır. Sertifikaların doğrulanması cihazda gerçekleştirilir. Sertifika tabanlı güvenlik ile ilgili bilinen bazı ataklar aşağıda listelenmiştir:

1. Sertifikalar cihazda otoritelere ait kök sertifikaları ile doğrulanmaktadır. Hedef cihaza saldıracak kişiye ait bir kök sertifikasının yüklenmesi durumunda bir başkasına ait oluşturulan sertifika ile araya girilmesi imkanı bulunmaktadır. Hedef istemci gelen sertifikayı daha önce yüklenmiş olan sahte kök sertifika üzerinden doğrular.
2. Sertifikanın cihazın kendisinde bulunmasının bir sakıncası, Nisan 2014'de yayınlanan OpenSSL'deki heartbleed [8] atağına benzer bir atakta sertifikaya ait özel anahtarın elde edilebilme olasılığı bulunmaktadır.
3. Bilinen ve 2009'da ortaya çıkarılan bir diğer atak ise "Null Character Attack" isimli ataktır. https://X.com sitesine yapılan erişimlerde araya girmek için, herhangi bir otoriteden "https://X.com**0**atak.com ait bir sertifika alınır. Site ile aynı içeriğe sahip bir sahte site üzerinden kullanıcıya ait kullanıcı adı ve şifre elde edilebilme olasılığı bulunmaktadır.
4. Kullanıcıya ait özel anahtarın cihazda saklanması güvenlik açısından riskler oluşturmaktadır. Eğer cihazın belleğinde yer alan veya basit bir şifre ile korunan bir dosyada yazan özel anahtar elde edilecek olursa daha önceki iletişim içeriği elde edilebilir.

Uçtan-uca güvenli WebRTC iletişiminde iki temel unsur bulunmaktadır; bunlar sinyalleşme ve medya kanallarıdır. Medya kanalında SRTP üzerinden şifreli medya içeriğinin güvenli aktığı varsayılmaktadır. SRTP güvenliğini arttırmak üzere AES 256, TripleDES, SHA 256/512 veya farklı algoritmalar kullanılabilir. Algoritmaların standartlara uygunluğu ve yan kanal ataklara karşı güvenliği araştırılabilir. Bu tip çalışmalar bu bildirinin kapsamı dışında değerlendirilmektedir. Dolayısı ile sadece sinyalleşme kanalında, kullanılacak anahtarların oluşturulması ve taraflarca belirlenmesinin güvenliğinin sağlanması çalışmanın temel amacını oluşturmaktadır. SDES ve DTLS'de, SDP paketinin içinde yer alan bilginin ("a=crypto:" veya "a=fingerprint:" terimlerine ait içeriğin) güvenli bir şekilde aktarılması gerekmektedir.

Şekil 4. Güvenli iletişim akış diyagramı



No	Açıklama
1	WebRTC'den talep (offer) SDP paketi istenir
2	Talep SDP paketi elde edilir. SDP paketinde yer alan "a=crypto" ile başlayan satırın içeriği İstemci T'nin akıllı kartına ait açık anahtar ile şifrelenerek X elde edilir.
3	X, özel anahtar ile imzalanmak üzere akıllı karta gönderilir
4	Y imzası elde edilir.
5	SDP paketinde yer alan "a=crypto" terimi silinir. SDP, X ve Y sunucuya gönderilir.
6	Sunucu; SDP, X ve Y metinlerini istemci T ye gönderir.
7	Y metni, İstemci S'nin daha önceden bilinen açık anahtarı ile doğrulanır ve X çözülmek üzere akıllı karta gönderilir
8	Madde 2'de şifrelenmiş olan "a=crypto" içeriği elde edilir ve SDP paketine tekrar eklenir.
9	Elde edilen talep SDP paketi WebRTC'ye iletilir ve cevap SDP paketi istenir.
10	Cevap SDP paketi elde edilir. SDP paketinde yer alan "a=crypto" ile başlayan satırın içeriği İstemci S'nin akıllı kartına ait açık anahtar ile şifrelenerek X^i elde edilir.
11	X^i, özel anahtar ile imzalanmak üzere akıllı karta gönderilir
12	Y^i imzası elde edilir.
13	SDP paketinde yer alan "a=crypto" terimi silinir. SDP, X^i ve Y^i sunucuya gönderilir.
14	Sunucu; SDP, X^i ve Y metinlerini istemci S ye gönderir.
15	Y^i metni, İstemci T'nin daha önceden bilinen açık anahtarı ile doğrulanır ve X^i çözülmek üzere akıllı karta gönderilir
16	Madde 10'da şifrelenmiş olan "a=crypto" içeriği elde edilir ve SDP paketine tekrar eklenir.
17	Elde edilen talep SDP paketi WebRTC'ye iletilir.

Tablo 1. Akış diyagramı açıklamaları

978-1-5090-1679-2/16/$31.00 ©2016 IEEE

Sunulan çalışmada mevcut akıllı kartlar tarafından desteklenmesi nedeni ile açık anahtar tabanlı kriptosistem olarak RSA[9] tercih edilmiştir. Şekil 4 ve Tablo 1'de akıllı kart kullanan anahtar takası ve güvenli iletişime ait akış diyagramları sunulmaktadır. Diyagramda ICE candidate mesajları gösterilmemiştir.

Önerilen yöntemin uygulanması amacı ile bir Android uygulaması ve cihazlarda SDkart yuvasına takılabilen SmartSD kartları kullanılmıştır. Standart akıllı kartlar microUSB yuvasına takılabilen kart okuyucu ile aynı şekilde kullanılabilmektedirler. Önerdiğimiz yöntemde, anahtar takasında açık anahtar tabanlı kriptografi operasyonlarının gerçekleştirilmesi için akıllı kartlar kullanılmaktadır. Akıllı kartların tercih edilmesindeki temel nedenler aşağıda sıralanmıştır:

- özel anahtarın hiçbir zaman kartın dışına çıkmaması ve dolayısı ile elde edilemeyecek olması,
- PIN/PUK ve yan ataklara karşı korumalı olması
- taşınabilir olması,
- kapalı bir sistem olması nedeniyle herhangi sertifika otoritesine ihtiyaç duyulmaması,
- gerçek rastgele anahtar üretimi için özel donanımın yer almasıdır.

III. TARTIŞMA VE SONUÇ

WebRTC tabanlı sesli ve görüntülü iletişimin yanı sıra bir veri (dosya, resim vb.) paylaşımı sırasında uçtan uca güvenli iletişimin sağlanmasına yönelik olarak anahtar takası için bir yöntem sunulmaktadır. Sunulan yöntem, Android işletim sistemine sahip mobil cihazlarda uygulanmıştır. Yapılan çalışmada:

- Cihazda yer alan bir trojan ya da doğrudan işletim sisteminden kaynaklı bir açık olmadığı,
- Akıllı kart ve akıllı karta ait PIN bilgisinin güvenliğinin sağlandığı,
- WebRTC platformunda yer alan dışarıdan iletişim imkanı bulunan kütüphanelerinin yan ataklara karşı güvenli olduğu varsayılmaktadır.

Bölüm 3'de sunulan yöntemde SDES için geçerli olan "a=crypto" ile başlayan anahtar için uyguladığımız yöntemi DTLS için geçerli olan "a=fingerprint" içeriğine de uygulanabilir.

Akıllı kart ve PIN bilgisinin elde edilmesi durumunda daha önceden saklanan medya ve SDP paketleri ile medyanın içeriği elde edilebilir. Bu nedenle oturum bazlı anahtar takas yöntemleri ele alınabilir.

Sunulan yöntem RSA tabanlı bir yaklaşım kullanılmıştır ve minimum RSA 2048 bit kullanılması tavsiye edilmektedir. Bir çağrının başlatılması için gerekli zamanın minimuma çekilmesi amacı ile bazı RSA 2048 bit operasyonları doğrudan cihazda gerçekleştirilmektedir. Örnek olarak, Tablo 1'de yer alan madde 2'de "a=crypto" ile başlayan satırın içeriği cihazda şifrelenmektedir. LG Nexus 5 için Tablo 2'deki değerler ölçülmüştür. Tablo 2'de gösterildiği üzere performans açısından sadece özel anahtar odaklı işlemler (imzalama ve çözme) operasyonları kartta, açık anahtar odaklı işlemleri (doğrulama ve şifreleme) cihazda gerçekleştirilmektedir.

Açıklama	Süre (ms)
Akıllı kart imzalama	1570
Android uygulamasında doğrulama	14
Android uygulamasında şifreleme	4
Akıllı kart çözme	1698

Tablo 2. RSA operasyon süreleri

RSA operasyonları için kullanıcılar iletişim kuracakları kullanıcılara ait açık anahtarları daha önceden cihaz ya da akıllı kartlarına aktarmış olmalıdırlar. Cihazda saklanması durumunda açık (cihazın işletim sistemi değiştirilmiş) sertifikaların değişmesine dolayısı ile araya girilmesine olanak sağlamaktadır. Açık anahtarlar doğrudan kartın içerisinde güvenli bir şekilde saklanabilir (istenirse kartın içerisinde tanımlı ve değiştirilemez olarak tanımlanabilir) ancak bu durumda kartın bellek miktarına bağlı olarak sınırlı (yaklaşık 100) sayıda olmaktadır. Bu şekilde sertifika otoritelerine olan bağımlılık ortadan kalkmaktadır.

IV. BİLGİLENDİRME

Bu bildiride sunulan çalışma, TÜBİTAK tarafından desteklenen ve Netaş bünyesinde geliştirilen 1130066 nolu proje kapsamında yapılan araştırma ve geliştirme çalışmalarının bir sonucu olarak ortaya çıkmıştır.

KAYNAKÇA

[1] A. Bergkvist, D. Burnett, C. Jennings, and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers," *WebRTC 1.0: Real-time Communication Between Browsers*, Sep-2013. .

[2] S. Loreto and S. Pietro Romano, "Real-time communications in the web: Issues, achievements, and ongoing standardization efforts," *IEEE Internet Comput.*, vol. 16, no. 5, pp. 68–73, 2012.

[3] R. Mahy, P. Matthews, and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," 2010.

[4] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," 2010.

[5] F. Andreasen, M. Baugher, and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," RFC Editor, RFC 4568, Jul. 2006.

[6] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC Editor, RFC 6347, Jan. 2012.

[7] M. Handley, V. Jacobson, and C. Perkins, "SDP: Session Description Protocol," RFC Editor, RFC 4566, Jul. 2006.

[8] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson, "The Matter of Heartbleed," in *Proceedings of the 2014 Conference on Internet Measurement Conference*, New York, NY, USA, 2014, pp. 475–488.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Commun ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

978-1-5090-1679-2/16/$31.00 ©2016 IEEE