TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

POPÜLER GÜVENLİ MESAJLAŞMA UYGULAMALARINDA KİMLİK DOĞRULAMA VE ŞİFRELEME ANAHTARININ DEĞİŞMESİ İLE KULLANICI ETKİLEŞİMİ

YÜKSEK LİSANS TEZİ

Gamze AKMAN

Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Güvenliği

Tez Danışmanı: Prof. Dr. Ali Aydın SELÇUK

NİSAN 2018

Fen Bilimleri Enstitüsü Onayı

……..
Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

…….
Prof. Dr. Oğuz ERGİN
Anabilim Dalı Başkan V.

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 151111031 numaralı Yüksek Lisans Öğrencisi **Gamze AKMAN**'ın ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"POPÜLER GÜVENLİ MESAJLAŞMA UYGULAMALARINDA KİMLİK DOĞRULAMA VE ŞİFRELEME ANAHTARININ DEĞİŞMESİ İLE KULLANICI ETKİLEŞİMİ"** başlıklı tezi **03.04.2018** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

Tez Danışmanı : **Prof. Dr. Ali Aydın SELÇUK** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

Jüri Üyeleri : **Doç. Dr. Ahmet Burak CAN (Başkan)** .....
Hacettepe Üniversitesi

Doç. Dr. Osman ABUL .....
TOBB Ekonomi ve Teknoloji Üniversitesi

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

.

Gamze AKMAN

ÖZET

Yüksek Lisans Tezi

POPÜLER GÜVENLİ MESAJLAŞMA UYGULAMALARINDA KİMLİK DOĞRULAMA VE ŞİFRELEME ANAHTARININ DEĞİŞMESİ İLE KULLANICI ETKİLEŞİMİ

Gamze AKMAN

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Güvenliği

Danışman: Prof. Dr. Ali Aydın SELÇUK

Tarih: Nisan 2018

Günümüzde, anlık mesajlaşma uygulamalarının popülaritesinin artması, bazı güvenlik önlemlerini beraberinde getirmiştir. Bu güvenlik önlemlerinden bir tanesi kullanıcıların yapması gereken kimlik doğrulama etkinliğidir. Anlık mesajlaşma uygulamalarında kimlik doğrulaması, kişinin doğru kişiyle mesajlaştığını doğrulaması demektir. Bugüne kadar yapılan çalışmalarda kullanıcılar kimlik doğrulaması etkinliklerinde tam olarak başarı sağlayamamaktadırlar. Bundan dolayı dört popüler anlık mesajlaşma uygulamasında kimlik doğrulama anahtarının kontrol edilmesi ve kimlik doğrulama anahtarının değişmesi ile kullanıcı etkileşimi çalışmasını iki farklı grupta toplam 66 katılımcı eşliğinde yapılmıştır. İlk grupta bulunan katılımcılar bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılardan oluşmaktadır. İkinci gruptaki katılımcılar bilgi güvenliği dersi öğrencilerinden oluşmaktadır. İlk aşamada katılımcılardan kimlik doğrulama anahtarlarını karşılaştırmaları beklenmiştir. İkinci aşamada ise kimlik doğrulama anahtarı değiştiği zaman kullanıcıların bu durumu nasıl değerlendirdikleri

araştırılmıştır. Elde edilen sonuçlara göre, katılımcıların kimlik doğrulaması yapması gerektiğini bilmelerine rağmen kimlik doğrulama işlemini göz ardı edebildikleri gözlemlenmiştir.

Anahtar Kelimeler: Güvenli sohbet, Kimlik doğrulama, Kullanılabilir güvenlik, Kullanıcı çalışması, Mesaj şifreleme, Aradaki adam saldırısı, Uçtan uca şifreleme.

ABSTRACT

Master of Science

USER INTERACTION WITH CHANGE OF AUTHENTICATION AND ENCRYPTION KEY IN POPULAR INSTANT MESSAGING APPLICATIONS

Gamze AKMAN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Engineering
Information Security

Supervisor: Prof. Dr. Ali Aydın SELÇUK

Date: April 2018

Nowadays, the increasing popularity of instant messaging applications has introduced some security measures. One of these security measures is the authentication activity that users need to make. Authentication in instant messaging applications means verifying that someone is messaging with the right person. In studies conducted to date, users are not able to achieve full success in authentication activities. Therefore, in the four popular instant messaging applications, checking the authentication key and changing the authentication key and user interaction were performed in a total of 66 participants in two different groups. Participants in the first group consisted of participants who worked in the information sector and did not have information security knowledge. Participants in the second group consist of students with information security lessons. In the first phase participants were expected to compare the authentication keys. In the second stage, when the authentication key was changed, users were investigated how they evaluated this situation. According to the results obtained, it is observed that the participants may ignore the authentication process although they know that they need to authenticate.

Keywords: Secure chat, Authentication, Security available, User activity, Message encryption, Man-in-the-middle attack, End to end encryption.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Prof. Dr. Ali Aydın SELÇUK'a, öğrenim bursu sağladığı için TOBB Ekonomi ve Teknoloji Üniversitesi'ne, kıymetli tecrübelerinden faydalandığım Bilgisayar Mühendisliği Bölümü öğretim üyelerine ve destekleriyle her zaman yanımda olan aileme ve arkadaşlarıma çok teşekkür ederim.

İÇİNDEKİLER

ŞEKİL LİSTESİ

Sayfa

KISALTMALAR

E2E : End to End of Encryption
MITM : Man-in-the-middle
SUS : System Usability Scale
UKS : An Unknown Key-Share
QUIS : Questionnaire for User Interface Satisfaction
CSUQ : Computer System Usability Qustionnaire
KDF : Key Derivation Function
X3DH : Extended Triple Diffie-Hellman

1. GİRİŞ

İlk SMS 1992 yılında gönderilmiştir ve 2012 yılında SMS en çok kullanılan mesajlaşma uygulaması haline gelmiştir. Zamanla teknolojinin yaygınlaşması ve erişilebilirliğinin artmasının getirdiği avantajlarla SMS yerini anlık mesajlaşma uygulamalarına bırakmıştır [1].

Popülerliği zamanla artan anlık mesajlaşma uygulamaları bir takım güvenlik problemlerini beraberinde getirmektedir. Uygulamalar hayatta kalabilmek ve kullanıcı beklentilerini karşılamak için kendilerini geliştirmelidirler. Son zamanlarda artan güvenlik problemlerinden dolayı popüler anlık mesajlaşma uygulamalarına bir takım güvenlik önlemleri eklenmiştir.

Anlık mesajlaşma uygulamalarındaki güvenlik problemlerinden bir tanesi aradaki adam saldırısıdır ((Man-in-the-Middle Attack) MITM). Aradaki adam saldırısı bir ağ üzerinde iletişimde olan iki bilgisayarın arasına girerek verileri yakalayan veya verileri değiştiren saldırı yöntemidir. Anlık mesajlaşma uygulamalarında saldırgan aradaki adam saldırısı (MITM) yaparak mesajları yakalayabilir. Eğer mesajlar açık metin halinde gönderiliyorsa saldırgan açık mesajları yakalayarak yorumlayabilir. Aradaki adam saldırısını engellemek için uçtan uca şifreleme yöntemi (end to end encryption (E2E)) kullanılır. Uçtan uca şifreleme (end to end encryption (E2E)) yönteminde amaç iki kişi arasında yapılan iletişime üçüncü bir kişinin erişmesini engellemektir. İletişimde olan iki tarafta ilgili anahtarlar bulunur. İlgili anahtarla şifrelenmiş mesaj diğer ilgili anahtar ile çözümlenip anlaşılır hale getirilir. Arada mesajı yakalayan bir üçüncü kişi anahtara sahip olmadığı için mesajı çözümleyemez. Elinde anlamsız bir bilgi olmuş olur. Bu sayede aradaki adam saldırısı (MITM) engellenmiş olur. İletişimde olan tarafların şifreli mesaj gönderip güvende olabilmeleri için anahtarlarını değiştirmeleri ve güvenli bir gizli anahtar oluşturmaları gerekebilmektedir. Diffie Hellman bu işlemleri sağlayan bir anahtar değişim protokolüdür. Kullanıcaların ortak anahtarları sayesinde Diffie Hellman protokolü gizli anahtar üretimini sağlar. Kullanıcılar bu anahtarları kullanarak

verilerini şifreleyebilirler. Aradaki adam saldırısıyla saldırgan Diffie Hellman anahtar değişimi protokolünü kullanıyorsa gizli anahtarı elde edemez; gizli anahtarı elde edemeyince mesajları çözümleyip yorumlayamaz.

Anlık mesajlaşma uygulamalarındaki güvenlik problemlerinden bir tanesi de kullanıcıların yapması gereken kimlik doğrulama etkinliğidir. Anlık mesajlaşma uygulamalarında kimlik doğrulaması yapmak demek kişinin doğru kişiyle mesajlaştığını doğrulaması demektir. Günümüzdeki anlık mesajlaşma uygulamalarında kimlik doğrulama etkinliği kullanıcılar tarafından manuel olarak gerçekleştirilmektedir.

Yaptığımız çalışmada Viber, Telegram, Signal ve Google Allo anlık mesajlaşma uygulamalarında;

1. Kimlik doğrulama anahtarı karşılıklı nasıl kontrol edilir?
2. Kimlik doğrulama anahtarının değiştirildiği nasıl anlaşılır?

sorularının cevaplanması amaçlanmıştır.

Kimlik doğrulama çalışması ise iki ayrı grup ile gerçekleştirilmiştir.

1. Birinci grupta bulunan katılımcılar bilişim sektöründe çalışan fakat bilgi güvenliği üzerine bilgisi olmayan 18 katılımcıdan oluşmaktadır.
2. İkinci gruptaki katılımcılar ise bilgi güvenliği dersini alan 48 üniversite öğrencisinden oluşmaktadır.

Bu tez çalışması şu şekilde oluşturulmuştur: Popüler uçtan uca şifreleme yöntemini kullanan dört güvenli anlık mesajlaşma uygulaması seçilmiştir. Bu seçilen uygulamalar Viber, Telegram, Signal ve Google Allo uygulamalarıdır. Çalışmanın 1. bölümünde literatür taraması yapılmıştır. Çalışmanın 2. bölümünde Viber, Telegram, Signal ve Google Allo uygulamalarının tanıtımı yapılmış, dört anlık mesajlaşma uygulamasında mesajlaşma anahtarının nasıl değiştirilebileceği anlatılmış; mesaj şifreleme anahtarı değiştiği zaman kullanıcıların bunu nasıl anlayabileceği resimlerle açıklanmış ve bu uygulamanın uçtan uca şifreleme için kullandıkları protokollerin Diffie Hellman anahtar algoritması ile ilişkisi açıklanmış; 3. bölümünde Viber, Telegram, Signal ve Google Allo uygulamalarının kullandıkları şifreleme anahtarı değiştirildiği zaman kullanıcının bu durumu nasıl öğrendiğine ilişkin bir araştırma

çalışması yapılmış; 5. bölümde bu yapılan araştırma çalışmasının sonuçları analiz edilip, yorumlanmıştır.

1.1. Literatür Taraması

Anlık mesajlaşma uygulamalarının günden güne yaygınlaşmasından dolayı literatürde anlık mesajlaşma uygulamalarını, anlık mesajlaşma uygulamalarının güvenilirliğini, anlık mesajlaşma uygulamalarının açıklıklarını içeren çeşitli çalışmalar bulunmaktadır. Anlık mesajlaşma uygulamalarındaki açıklıkları kapatmak için veya güvenli mesajlaşmayı sağlamak için uygulamalara günden güne yeni eklentiler gelmektedir. Bu eklentiler ise uygulamaların daha karmaşık olmasına neden olmaktadır.

Frosch ve arkadaşları [2] Signal protokolünün öncülü olan TextSecure protokolünü ayrıntılı olarak tanımlamışlar ve protokolün analizini gerçekleştirmişlerdir. Analiz sonuçlarına göre TextSecure protokolü bilinmeyen anahtar paylaşımı (an unknown key share (UKS)) [3] saldırılarına açıktır. Frosch ve arkadaşları bu saldırıya karşı öneriler sunmuşlardır. Signal mesajlaşma protokolü uçtan uca şifreleme sağlayan bir güvenlik protokolüdür. Whatsapp, Facebook Messenger ve Google Allo gibi popüler anlık mesajlaşma uygulamaları Signal mesajlaşma protokolünü kullanmaktadır. Gordon ve arkadaşları [4] 2017 yılında Signal mesajlaşma protokolünün güvenlik analizi çalışmasını yapmışlardır. Yapılan çalışmada Signal mesajlaşma protokolünde büyük bir güvenlik problemi bulunamamıştır.

Bir diğer güvenli anlık mesajlaşma uygulaması olan Telegram uygulaması MTProto protokolünü kullanmaktadır. Telegram MTProto protokolü gibi anlık mesajlaşma protokolleri, verilerin uçtan uca güvenliğini sağlarlar. MTProto protokolü tasarımcıları tarafından ayrıntılı olarak açıklanmasına rağmen, bu protokol hem performans kusurları içerir hem aradaki adam saldırılarına duyarlıdır. Telegram MTProto protokolünün geliştirilmesi için 2015 yılında çalışmalar yapılmış [5] ve bu protokolü daha güvenli ve verimli hale getirebilmek için bazı güvenlik önlemleri sunulmuştur. Lee ve arkadaşları [6] 2017 yılında Telegram uygulamasının kullandığı MTProto protokolünün güvenlik araştırma çalışmasını yapmışlardır. MTProto protokolünde kriptografik ilkelerde bazı zayıflıklar bulmuşlar ona rağmen algoritmasının iyi tasarlanmış olduğunu belirtmişlerdir.

Anlık mesajlaşma uygulamalarının güvenilirliğini, uygulamaların açıklıklarını içeren çalışmaların yanı sıra uygulamaların kullanılabilirliğini de içeren çalışmalar bulunmaktadır. Brooke tarafından 1996 yılında geliştirilmiş sistem kullanılabilirlik ölçeği (SUS) sistemin hızlı bir şekilde kullanılabilirliğini ölçmek için kullanılmaktadır [7, 8].

2004 yılında Tullis [9] ve arkadaşları iki internet sitesinin kullanılabilirliğini değerlendirmek için 123 katılımcı ile beraber 5 farklı anket çalışması yürütmüşlerdir. 5 anket çalışması; sistem kullanılabilirlik ölçeği (SUS), kullanıcı arayüzü kullanılabilirlik anketi (Questionnaire for User Interface Satisfaction (QUIS)) [10], bilgisayar sistemi kullanılabilirlik anketi (Computer system Usability Qustionnaire (CSUQ)) [11], Microsoft'un ürün reaksiyon kartlarından uyarlanan kelimeler anketi ve Tullis'in kendi oluşturduğu anketten oluşmaktadır. İki internet sitesi ise aynı özelliğe sahip finans internet siteleridir. Katılımcılardan iki sitede de aynı görevleri yapmaları beklenmiştir. Bu görevleri tamamlayan katılımcılar ölçekleri doldurmuşlardır. Tullis ve arkadaşlarının yaptıkları bu değerlendirmeler sonucunda SUS ölçeğinin kullanılırlığının diğer ölçeklerden daha yüksek olduğu ortaya çıkmıştır.

1999 yılında Whitten ve Tygar [12] PGP 5.0 uygulamasında bir kullanıcı çalışması yapmışlardır. PGP 5.0 iyi bir arayüze sahip olmasına rağmen; çoğu bilgisayar kullanıcısı için güvenli mesajlaşma yapmakda yeterli olmadığı ortaya çıkarılmış ve etkin güvenlik için kullanıcı arayüzü tasarımının açık bir problem olduğu hipotezlerine araştırma sonuçları destek vermiştir.

Sistem kullanılabilirlik ölçeğini kullanarak e-mail mesajlaşması üzerine Ruoti ve arkadaşları [13] bir çalışma yapmışlardır. Burada çıkan sonuçlara göre sistemin güvenli mesajlaşmayı nasıl sağlayacağına dair öğreticilerin bulunması sistemin daha çok tercih edilme sebeplerinden bir tanesidir.

Fahl ve arkadaşlarının [14] 2012 yılında yaptıkları çalışmada güvenli olmayan Facebook mesajlaşması için eklenti güvenlik çalışması yapılmıştır. Otomatik anahtar yönetimi, manuel anahtar yönetimi ile otomatik şifreleme, manuel şifreleme kombinasyonlarını kullanarak dört farklı arayüz oluşturulmuş ve kullanıcıların bu arayüzleri kullanarak şifreli mesaj göndermeleri istenmiştir. Kullanıcılar otomatik

anahtar yönetimini ve otomatik şifrelemeyi daha kullanışlı bulmuşlar fakat karmaşık şifreleme mekanizmalarının kullanılması kullanıcıları daha güvende hissettirmiştir.

Ruoti ve Roberts [15] yedi farklı web kimlik doğrulama sistemi için bir kullanılabilirlik çalışması yapmışlardır. Amaçları hangi uygulamanın kullanılabilirliğinin en iyi olduğunu ortaya çıkartmaktır. Yedi tane web kimlik doğrulama özelliğine sahip uygulama dört ayrı özellik altında gruplandırılmıştır. Bu özellikler birleşik tek oturum açma özelliği, e-posta tabanlı tek oturum açma özelliği, kağıt ile QR kod taratma özelliği ve son olarak da akıllı telefon ile QR kod taratma özellikleridir. Birleşik tek oturum açma özelliğini kullanan uygulamalarında sorumluluk tek bir kimlik sağlayıcısındadır. İnternet siteleri kullanıcı adlarını ve parolaları muhafaza etmek yerine internet sitelerini kullanan kullanıcıların kimliğini doğrulamak için bu kimlik sağlayıcısına güvenir. Birleşik tek oturum açma özelliğini kullanan Google OAuth 2.0 [16], Facebook Connect ve Mozilla Persona [17] uygulamaları araştırmada kullanılan üç uygulamadır. Google ve Facebook kullanıcıları için kişisel bilgileri depolamalarından dolayı, kullanıcıların her iki sistemi de kişisel bilgilerinin sızdırılacağı korkusuyla reddetmeleri de göz önüne alınmış [18] ve üçüncü bir uygulama olan ve kullanıcıların kişisel bilgilerini saklamayan birleşik tek oturum açma sistemi olan Mozilla Persona uygulaması da araştırmada kullanılmıştır. E-posta tabanlı tek oturum açma özelliği, kimlik doğrulama sorumluluğunu tek bir ögeye bağlamaz. Kullanıcılar, e-posta gönderme veya alma yeteneklerini göstererek kimliklerini kanıtlar. Bu grup için ise geliştirdikleri basit kimlik doğrulama [19] ve Hatchet uygulamalarını kullanmışlardır. WebTicket [20] ve Snap2Pass [21] sistemleri ise QR kodları kullanarak kimlik doğrulama işlemlerini yaparlar. WebTicket uygulaması kağıttan QR kod okur, Snap2Pass uygulaması ise akıllı telefon ile QR kod okur. Bu uygulamalar kullanılarak yapılan çalışmada şeffaflığın kullanılabilirliği artırdığı fakat güven eksikliğine yol açtığı ortaya çıkmıştır. Ruotini ve arkadaşlarının yaptıkları bu çalışmada katılımcılar en fazla birleşik tek oturum açma özellikli uygulamaları ve akıllı telefon ile QR kod okutmalı uygulamayı kullanışlı bulmuşlardır.

Sutikno ve arkadaşları [22] 2016 yılında Whatsapp, Viber ve Telegram anlık mesajlaşma uygulamalarının özelliklerini karşılaştırmışlar ve Whatsapp anlık

mesajlaşma uygulamasının dünyadaki akıllı telefon kullanıcıları tarafından en fazla kullanılan mesajlaşma uygulaması olduğunu, ikinci sırada Viber uygulamasının kullanıldığını ve üçüncü sırada ise Telegram uygulamasının kullanıldığını bildirmişlerdir.

Tan ve arkadaşlarının [23] yaptıkları çalışmada şifreleme anahtarı tiplerini karşılaştırmışlardır. Bu yapılan çalışmada 8 tip şifreleme anahtarı kullanılmıştır. Bunlar 16 tabanlı sayı sistemi formatı, rakam formatı, kelime formatı, cümle formatı, harf formatı, ssh formatı, unicorn formatı ve vash formatlarıdır. Ssh, unicorn ve vash formatları görsel şifreleme anahtarlarıdır. Kullanıcılara bu tiplerde şifreleme anahtarları gösterilerek doğrulamaları beklenmiştir. Kullanıcılar görsel formatlarda diğer formatlara oranla daha başarısız olmaktadırlar.

Schroder ve arkadaşları [24] Signal uygulamasının güvenliğini ve kullanılabilirliğini analiz etmek için kullanıcı araştırma çalışması yapmışlardır. Signal protokolü üzerindeki kullanıcıların şifreleme anahtarlarındaki farklılıkları tespit edip edememelerini araştırmışlardır. Araştırma sonuçları kullanıcıların çoğunluğunun, anahtarlarını doğru bir şekilde karşılaştırma konusunda başarısız olduğunu göstermektedir. Bu nedenle, kullanıcıların günümüzün güvenli mesajlaşma uygulamalarının temel altyapısına yönelik saldırılara maruz kalma olasılığı yüksektir.

Vaziripour ve arkadaşlarının [25] yaptıkları çalışmada kullanıcılara Facebook Messenger, Whatsapp ve Viber uygulamaları kullandırılmıştır. Kullanıcıların güvenli mesajlaşma uygulamalarında kimlik doğrulama yöntemini bulmalarını incelemek için iki aşamalı bir araştırma çalışması yapılmıştır. İlk aşamada kullanıcılara karşılıklı olarak mesajlaşılan kişinin doğru kişi olduğunun doğrulaması beklenmiştir. Bu işlemin nasıl yapılacağı kullanıcılara ilk aşamada açıklanmamıştır. Kullanıcıların çok az bir kısmı bu aşamada başarılı olabilmişlerdir. İkinci aşamada ise 6 sayfalık kolay anlaşılır bir slayt sunulmuştur. Burada kimlik doğrulamanın önemli olduğu belirtilmiştir ve bir anahtar sayesinde doğrulama yapılabileceği bilgisi verilmiştir. Kullanıcılar bilgilendirildikten sonra kimlik doğrulama başarısı daha artmıştır. Bu kimlik doğrulama işlemlerinin sıradan, bilişim sektörüyle ilgisi olmayan, kullanıcıların çok fazla dikkat etmediği gözlemlenmiştir. Kimlik doğrulama işlemi uzun olduğu için göz ardı edilebildiği ortaya çıkarılmıştır. Viber uygulamasında telefon çağrısı ile doğrulama yapıldığı için kimlik doğrulama işlemi başarısının daha

yüksek olduğu söylenmektedir. Anahtarların uzun olduğu için gözle doğrulama işleminin pek pratik olmadığı QR kod okutmanın ise daha başarılı olduğu belirtilmiştir.

Güvenli anlık mesajlaşma uygulamaları yalnızca bire bir sohbet olanağı sunmaz. Bu uygulamalar grup mesajlaşmayı da desteklemektedir. Bu güne kadar yapılan araştırmaların büyük bir kısmı bire bir mesajlaşma güvenliğine dayanmaktadır. Rosler ve arkadaşları [26] Signal, Whatsapp ve Threema uygulamalarında grup mesajlaşma güvenliğini analiz etmişlerdir.

Şimdiye kadar yapılan araştırmalarda iletişim kuran tarafların, güvenli iletişim kanalını kurmadan önce birbirlerinin şifreleme anahtarlarını öğrenmeleri ve doğrulamaları gerektiği belirtilmiştir. Birçok güvenli mesajlaşma uygulaması, kullanıcıların manuel güven oluşturmasını beklemektedir. Bazı güvenli iletişim uygulamaları da kullanıcıların adına otomatik olarak anahtar yönetimi ve güven tahsis etmeyi ele alır; ancak bu, servis sağlayıcılarının, kullanıcıların şifreleme anahtarlarını değiştirip mesajlarına erişimine olanak sağlar. Kullanıcıların manuel anahtar doğrulamasını gerçekleştirmede sorun yaşadıkları diğer çalışmalarda ortaya çıkarılmıştır. Tüm bu durumlara önlem olarak da CONIKS'de [27] otomatik anahtar yönetim sistemi açıklanmıştır. CONIKS çalışmasında şifreleme anahtarının yönetimi kullanıcı sayesinde olmamakta, otomatik bir şekilde gerçekleşmektedir. CONIKS'den aradaki adam saldırılarını (MITM) güvenilir bir şekilde tespit etmesi ve önlemesi beklenmektedir.

CONIKS ve Sertifika Şeffaflığından [28] gelen bilgiler birleştirilip geliştirilerek Anahtar Şeffaflığı [29] çalışması halen devam eden bir çalışmadır. Anahtar Şeffaflık, kullanıcıların manuel anahtar doğrulamasını gerçekleştirme gereksinimini ortadan kaldıran, CONIKS ve Sertifika Şeffaflığından esinlenen bir stilde denetlenebilen önemli bir yapıdır. Kötü niyetli bir sunucu, yapıdan otomatik olarak bulunabilen kalıcı bir iz bırakmadan bir kullanıcının anahtarlarını ekleyemez, kaldıramaz ve yerini değiştiremez.

1.2. Sistem Kullanılabilirlik Ölçeği

Sistem Kullanılabilirlik Ölçeği (system usability scale (SUS)) [7, 8], 1986 yılında Brooke tarafından kullanılabilirlik değerlendirmesi yapmak amacıyla geliştirilmiş bir ölçektir. Sistem kullanılabilirlik ölçeğinin önemli bazı özellikleri aşağıda verilmiştir:

- Kullanımı basit bir ölçektir.
- Ölçümü hızlı yapılabilmektedir.
- Sonuçları basit ve hızlı bir şekilde yorumlanıp analiz edilebilmektedir

Ölçeği doldurmadan önce kullanıcılara araştırılan sistem kullandırılır. Kullanıcı sistemi kullandıktan hemen sınra ölçek kullanıcıya verilir. Kullanıcıdan ölçeği çok düşünmeden, hızlı bir şekilde doldurması beklenir. Kullanıcı bütün soruları cevaplamalıdır. Eğer kullanıcının soru hakkında cevabı yoksa ortadaki seçeneği (Kararsızım) seçmesi beklenir.

Sistem kullanılabilirlik ölçeği 10 sorudan oluşmaktadır. Bu 10 soru aşağıda verilmiştir:

1. Bu sistemi sık sık kullanmak isterim.
2. Sistemi gereksiz derecede karmaşık buldum.
3. Sistemin kullanımının kolay olduğunu düşündüm.
4. Bu sistemi kullanabilmek için teknik bir kişinin desteğine ihtiyacım olacağını düşünüyorum.
5. Bu sistemdeki çeşitli işlevlerin iyi entegre olduğunu düşünüyorum.
6. Bu sistemde tutarsızlığın çok fazla olduğunu düşündüm.
7. Çoğu kişinin bu sistemi çok hızlı bir şekilde kullanmayı öğreneceğini düşünüyorum.
8. Sistemi çok hantal buldum.
9. Sistemi kullanarak kendimi çok güvende hissettim.
10. Bu sisteme başlamadan önce çok şey öğrenmeliydim.

Kullanıcılar bu soruları 5 farklı şekilde yanıtlayabilirler. Verdikleri her bir yanıtın puan değeri vardır. Verebilecekleri yanıta karşılık gelen puan değerleri aşağıda verilmiştir:

- Kesinlikle Katılmıyorum (1 puan)
- Katılmıyorum (2 puan)
- Kararsızım (3 puan)
- Katılıyorum (4 puan)
- Kesinlikle Katılıyorum (5 puan)

Verilen cevaplara göre sistemin kullanışlı olup olmadığı hesaplanır. Tek soru numarasına sahip sistem kullanılabilirlik ölçeği sorularından (1, 3, 5, 7 ve 9 numaralı sorulardan) bir çıkarılır; çift numaraya sahip soruların (2, 4, 6, 8 ve 10 numaralı sorular) cevapları ise beşten çıkartılarak tüm sonuçlar toplanır. Çıkan sonuç iki buçuk ile çarpılarak yüzdelik sonuç elde edilir. Tüm bu işlemler sonrasında 0 ile 100 puan arasında sistem kullanılabilirlik ölçeği puanı elde edilmiş olur.

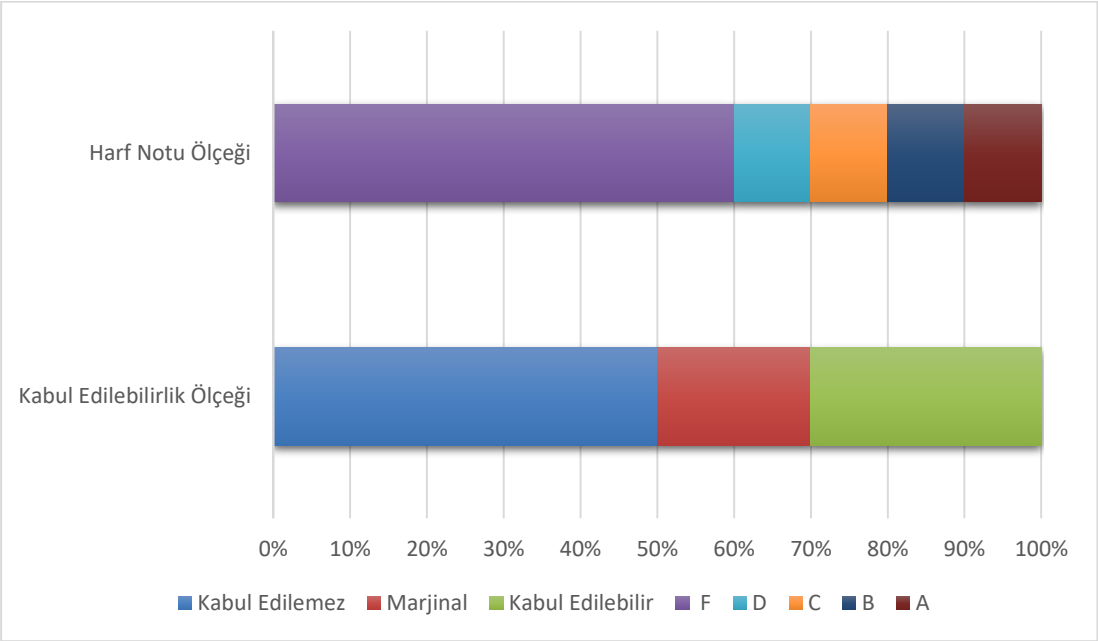
Sistem kullanılabilirlik ölçeğinin daha iyi yorumlanabilmesi için Bangor ve arkadaşları [30] sistem kullanılabilirlik ölçeğini; sıfat ölçeği, üniversite harf notları ölçeği ve kabul edilebilirlik aralığı ölçekleriyle ilişkilendirmişlerdir. Sıfat değerlendirme ölçeği tek sorudan oluşmaktadır. Cevap olarak ise Şekil 1.1'deki seçeneklerden biri seçilebilmektedir. Bir sistemin değerlendirilmesi tek sorudan oluştuğu zaman yeteri kadar analiz edilemediği düşünüldüğü için sıfat değerlendirme ölçeği bir sistemi değerlendirirken tek başına kullanılması yeterli gelmemektedir.

En Kötü	Çok Kötü	Kötü	Kabul Edilebilir/Tamam	İyi	Çok İyi	En iyi
☐	☐	☐	☐	☐	☐	☐

Şekil 1.1: Sıfat değerlendirme ölçeği.

Bangor ve arkadaşları üniversite sınav notlarını sistem kullanılabilirlik ölçeği ile ilişkilendirmişlerdir. Buna göre 90-100 puan arası A, 80-89 puan arası B, 70-79 puan arası C, 60-69 puan arası D ve 0-59 puan arası F harf notuna karşılık gelmektedir. Bangor ve arkadaşlarının kullandığı 3. ölçek ise kabul edilebilirlik ölçeğidir. Bu ölçeğe göre geleneksel sistemde 70 puanı geçmek demektir. Eğer ortalama puan 70 ise sistem kabul edilebilir. 50-70 puan arası marjinaldir (değişken). 50 puan altı ise

kabul edilemez. Şekil 1.2'de harf notu ölçeği, kabul edilebilirlik ölçeği ve sistem kullanılabilirlik ölçeği puanları ile ilişkilendirilmesi görülmektedir.



Şekil 1.2 : Harf notu ölçeği, kabul edilebilirlik ölçeği ve sistem kullanılabilirlik ölçeği puanları ile ilişkilendirilmesi.

2. POPÜLER ANLIK MESAJLAŞMA UYGULAMALARI VE KULLANDIKLARI ANAHTAR DEĞİŞİM PROTOKOLLERİ

Viber [31], Telegram [32], Signal [33] ve Google Allo [34] uçtan uca şifreleme uygulamasını kullanan popüler anlık mesajlaşma uygulamalarından bazılarıdır. Signal, Viber, ve Google Allo uygulamaları Signal protokolünü kullanır. Telegram uygulaması ise MTProto protokolünü kullanır. Uygulamalar uçtan uca şifreleme için farklı protokoller kullanmalarına rağmen anahtar değişim problemini çözen Diffie Hellman protokolünü kullanmaktadırlar.

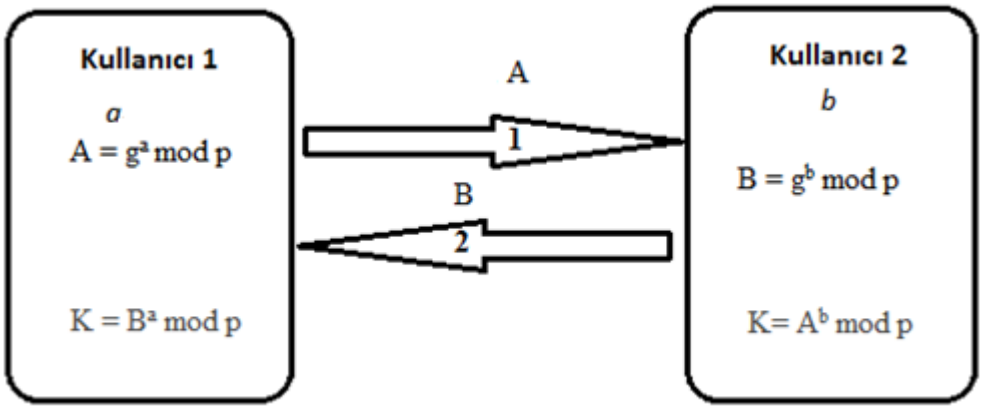
Anahtar değişim problemini ortadan kaldıran Diffie Hellman protokolü, Diffie Hellman protokolü ile Signal ve MTProto protokolleri arasındaki ilişki, Diffie Hellman protokolünde aradaki adam saldırısı ve Viber, Telegram, Signal ve Google Allo anlık mesajlaşma uygulamaları aşağıdaki başlıklarda ayrıntılı olarak açıklanmaktadır.

2.1. Diffie Hellman Protokolü

Diffie Hellman 1976 yılında Whitfield Diffie ve Martin Hellman [35] tarafından anahtar değişimi problemini gidermek için önerilmiştir. Diffie Hellman algoritması güvensiz bir iletişim kanalında karşılıklı haberleşen iki tarafın ortak bir gizli anahtar oluşturmasını sağlar. Oluşturulan gizli anahtar kullanılarak ağ üzerinden gizli iletişim sağlanabilmektedir.

Diffie Hellman anahtar değişimi algoritmasında Kullanıcı 1 a gizli anahtarına sahiptir. Kullanıcı 2 ise b gizli anahtarlarına sahiptir. Kullanıcı 1 ve Kullanıcı 2 p ve g açık anahtarları üzerine anlaşır. Kullanıcı 1 (g^a mod p) hesaplamasını yapar ve sonucu Kullanıcı 2 ye gönderir. Kullanıcı 2 ise (g^b mod p) hesaplamasını yapar ve sonucu Kullanıcı 1'e gönderir. Kullanıcı 1, Kullanıcı 1'e gelen (g^b mod p) sonucuyla kendi özel anahtarını işleme sokar ve $(g^b \text{ mod } p)^a$ sonucunu elde eder. Kullanıcı 2, Kullanıcı 2'ye gelen (g^a mod p) ile kendi özel anahtarını işleme sokar ve $(g^a \text{ mod } p)^b$ sonucunu elde eder. Kullanıcı 1 ve Kullanıcı 2 de aynı sonuçlar oluştuğu için ortak bir anahtar oluşmuş olur. Diffie Hellman çalışma mantığı ($g^{ab} = g^{ba}$) matematiksel

gerçeğine dayanmaktadır. Diffie Hellman anahtar değişim algoritması Şekil 2.1' de gösterilmiştir.



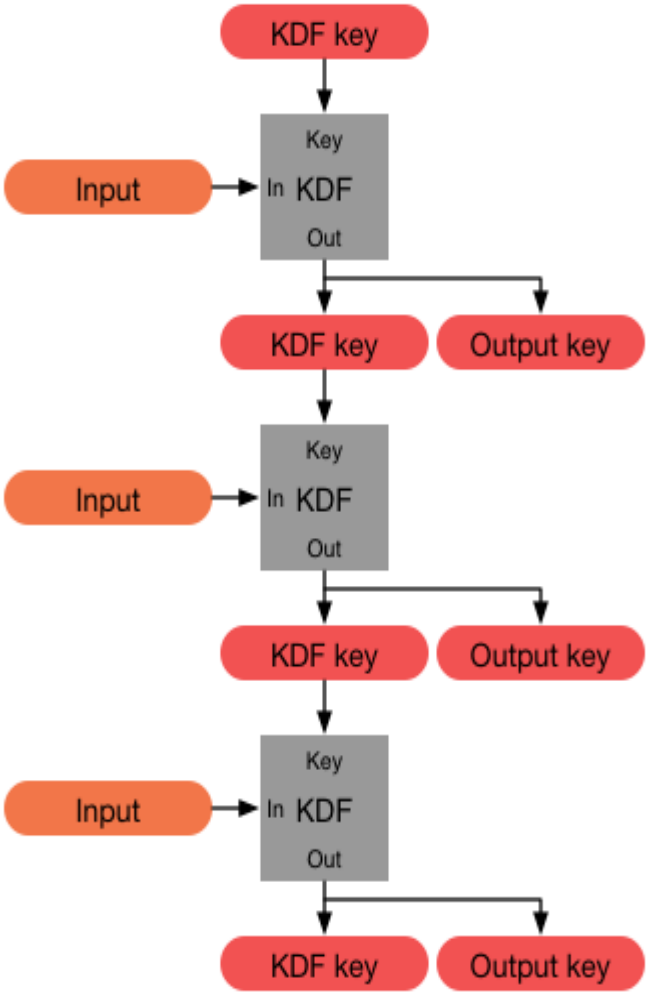
Şekil 2.1 : Diffie-Hellman anahtar değişim algoritması.

Kullanıcılar kendi özel anahtarları açık bir şekilde karşıya iletmedikleri için özel anahtarlarını saklamış olurlar ve tüm bu işlemler sonucunda gizli bir anahtar elde edilmiş olunur. Yani a ve b özel anahtarları güvensiz iletişim kanalında açık şekilde bulunmamaktadır. Kullanıcılar bu özel anahtarı mesajlarını şifreleme de kullanabilirler. Aradaki saldırgan elde ettiği bilgilerle bu ortak anahtarı oluşturamaz çünkü Kullanıcı 1 ve Kullanıcı 2'nin özel anahtarına sahip değildir. Saldırgan anahtara sahip olamadığı için de mesajları çözümleyemez.

Signal, son yıllarda Whatsapp [36] gibi en popüler anlık mesajlaşma uygulamalarında uçtan uca şifreleme sağlayan bir protokoldür. Araştırma çalışmasında kullanılan Viber, Signal ve Google Allo uygulamaları da Signal protokolünü kullanmaktadır. Double Ratchet algoritması Signal protokolünde kullanılan anahtar yönetim algoritmasıdır. Double Ratchet algoritmasının 3 temel adımı vardır. Bu adımlar anahtar türetme fonksiyon zincirleri (key derivation function (KDF) chains), simetrik anahtar (symmetric key ratchet) ve Diffie Helmann adımlarıdır [37].

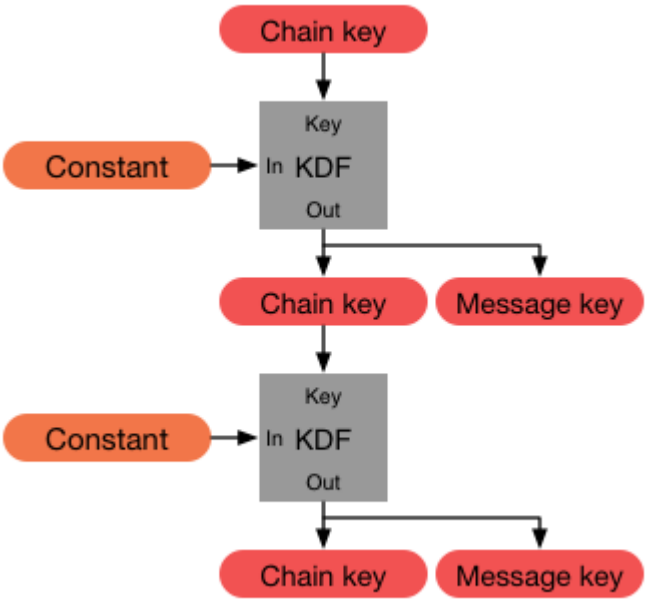
Anahtar türetme fonksiyonu, parola gibi gizli bir değerden belirli formatlarda gizli anahtar türetmeyi sağlar. Anahtar türetme fonksiyonunun çıkışının bir kısmı bir çıkış anahtarı olarak kullanıldığında KDF zinciri kullanılır ve bir kısmı daha sonra başka bir giriş ile kullanılabilen KDF anahtarını değiştirmek için kullanılır. Signal

protokolü dokümanından alınan Şekil 2.2 üç girdiyi işleyen ve üç çıkış anahtarı üreten bir anahtar türetme fonksiyonu zincirini göstermektedir [37].



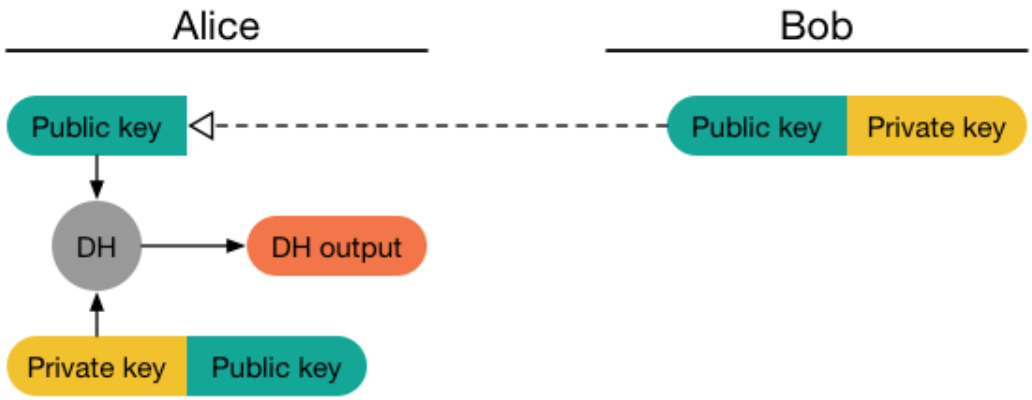
Şekil 2.2 : Signal protokolünde anahtar türetme fonksiyonu zinciri.

Kullanıcılar için bir kök zinciri, bir gönderici zinciri ve bir alıcı zinciri olmak üzere üç tane KDF zinciri oluşturulmaktadır. Gönderen ve alan zincirler her mesajın gönderildiği ve alındığı sırada ilerler. Simetrik anahtar adımında çıkış anahtarları mesajların şifrelenmesi için ve mesajların şifresini çözmek için kullanılır. Yani mesaj anahtarları, gönderen ve alan KDF zincirlerinden gelen çıkış anahtarlarıdır; bu çıkış anahtarlarına zincir anahtarı denilmektedir. Her şifrelenecek mesajın bir mesaj anahtarı vardır. Signal protokolü dokümanından alınan Şekil 2.3 belirli bir zincir anahtarından bir sonraki zincir anahtarını ve mesaj anahtarını hesaplama işlemini göstermektedir [37].



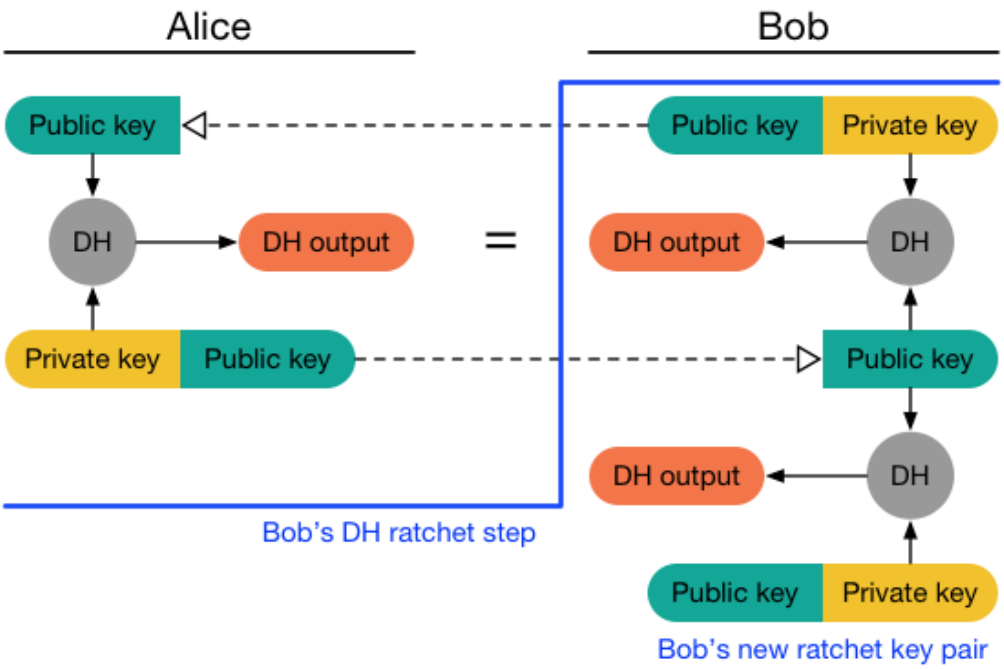
Şekil 2.3 : Signal protokolünde mesaj anahtarı oluşturma zinciri.

Bir saldırgan, iletişimde olan taraflardan birinin gönderici ve alıcı zincirlerini ele geçirirse, bundan sonra ağdaki mesajlara erişebilir. Bu mesajların şifrelerini çözebilir. Bunu önlemek için Signal protokolünde Diffie Hellman protokolü kullanılmaktadır. Signal protokolünde Diffie Hellman adımı anlatılırken Kullanıcı 1 ve Kullanıcı 2 dokümanda Alice ve Bob olarak tanımlanmıştır. Alice ve Bob'un bir özel bir de genel anahtarı vardır. Diffie Hellman'ın başlatma işleminin bir parçası olarak Alice, özel anahtarı ve Bob'un genel anahtarı arasında bir Diffie Hellman hesaplaması gerçekleştirir. Bu işlem Signal dokümanından alınan Şekil 2.4' te gösterilmektedir[37].



Şekil 2.4 : Signal protokolünde Diffie Hellman anahtar üretimi.

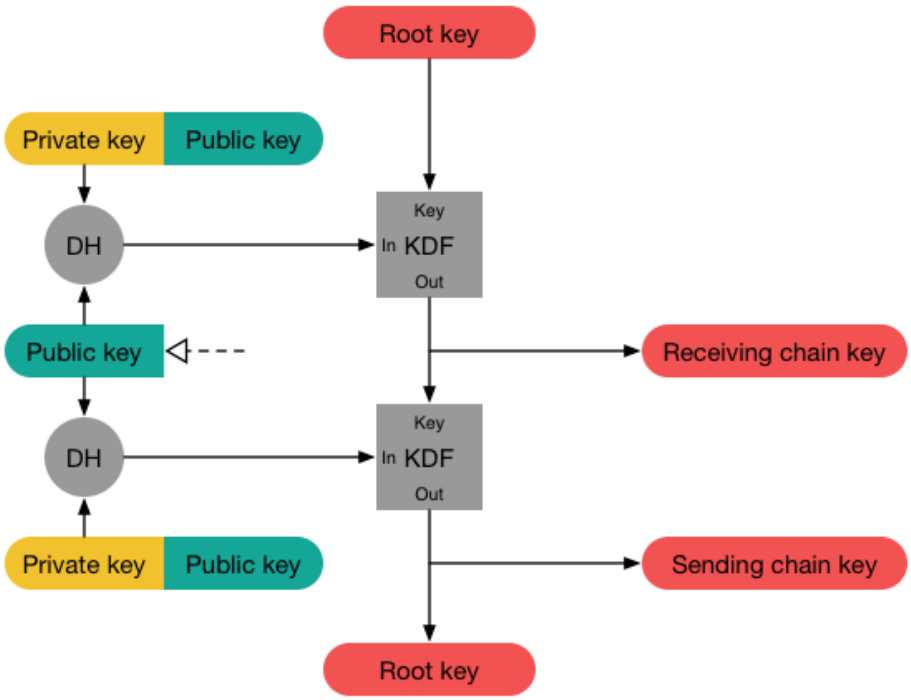
Bob da Alice'in genel anahtarı ve kendi özel anahtarı arasındaki Diffie Hellman çıkışını hesaplar ve bu Alice'in ilk Diffie Hellman çıkışına eşittir. Bob daha sonra anahtar çiftini değiştirir ve yeni bir Diffie Hellman çıktısı hesaplar. Bu işlem Signal dokümanından alınan Şekil 2.5' te gösterilmektedir [37].



Şekil 2.5 : Signal protokolünde anahtar değiştirilip tekrar Diffie Hellman hesaplaması.

Alice ve Bob, Diffie Hellman sonuçlarını kontrol edip yeni anahtar çiftleri oluşturarak Şekil 2.5'teki gibi yeni Diffie Hellman sonuçları çıkarmaya devam ederler.

Zincir anahtarlarına doğrudan Diffie Hellman çıkışlarını dahil etmek yerine, Diffie Hellman çıkışları bir kök zincirinde KDF girişleri olarak kullanılır ve kök zincirinden gelen KDF çıkışları gönderme ve alma zincirleri olarak kullanılır. Diffie Hellman hesaplamalarının sonuçları türetilmiş anahtarlara karıştırılır, böylece daha sonraki sonuçlar daha önceki sonuçlardan hesaplanamaz. Bu sayede anahtar güvenliği sağlanmış olur. Bu işlem Signal dokümanından alınan Şekil 2.6' da gösterilmektedir [37].

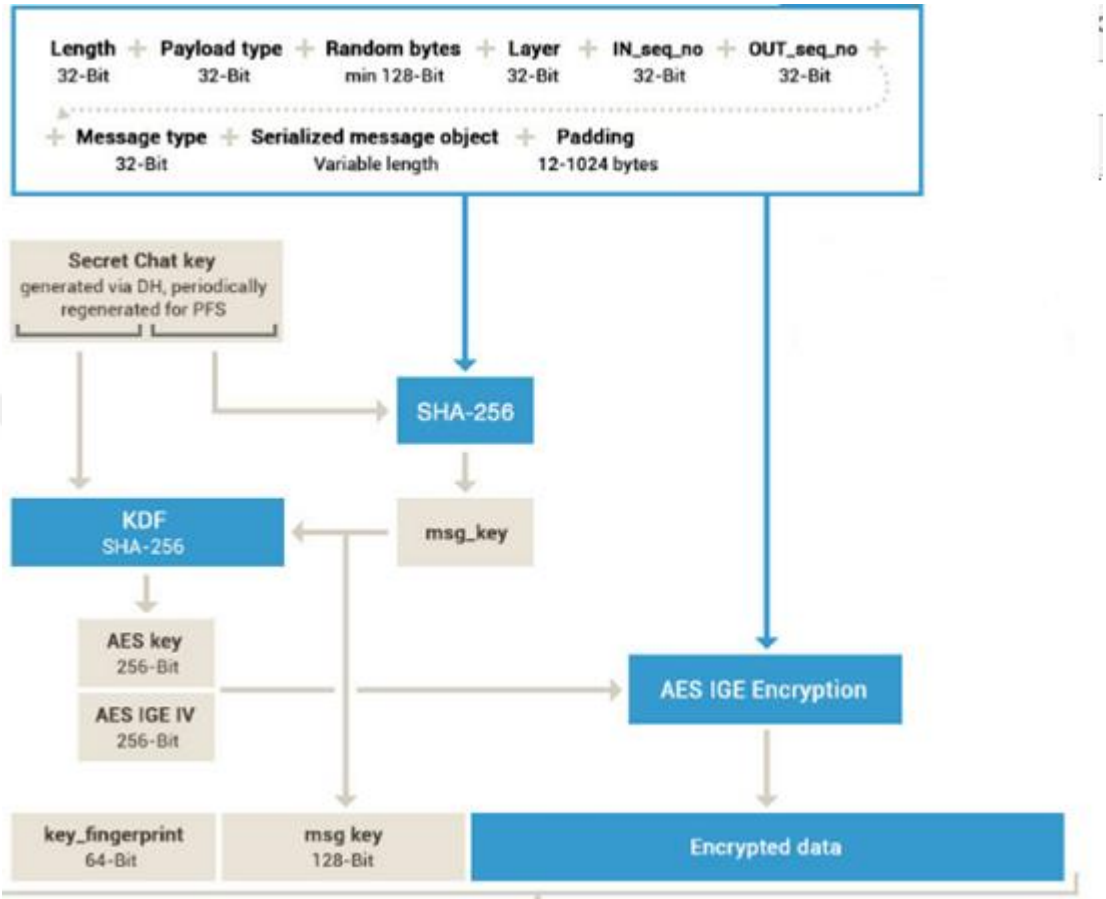


Şekil 2.6 : Signal Protokolünde Diffie Hellman sonuçları ile KDF sonuçlarının işleme sokularak zincir anahtarların elde edilmesi.

Signal protokolünde Diffie Hellman algoritmasının bir türü olan genişletilmiş üçlü Diffie Hellman(Extended Triple Diffie-Hellman (X3DH)) algoritması kullanılmaktadır [38]. Genişletilmiş üçlü Diffie Hellman algoritması, Diffie Hellman algortiması gibi birbirini karşılıklı olarak doğrulayan iki taraf arasında paylaşılan bir gizli anahtar oluşturmaya dayanır ve ileri gizlilik sağlar. Genişletilmiş üçlü Diffie Hellman bir kullanıcının çevrimdışı olduğu zaman, diğer kullanıcının şifrelenmiş verileri çevrimdışı kullanıcıya göndermesine olanak sağlar. Bunun için de çevrimdışı olan kullanıcının sunucuyla bazı bilgileri paylaşması gerekmektedir. Kullanıcıların genişletilmiş üçlü Diffie Hellman anahtar anlaşmasından önce taraflar kimliği doğrulanmış bazı kanallar aracılığıyla kimlik genel anahtarlarını manuel olarak veya bir QR kodu tarayarak karşılaştırabilirler. Bu sayede karşısındaki kişinin doğru kişi olduğunu ispatlamış olurlar [38].

Telegram uygulamasında ise diğer üç uygulamadan farklı olarak MTProto protokolü kullanılmaktadır. MTProto protokolü de Signal protokolü gibi uçtan uca şifreleme olanağı sağlamaktadır. MTProto gizli sohbetleri sağlamak için bir takım güvenlik eklentilerini kullanır. Kullanılan güvenlik eklentileri Telegram sayfasından alınan

MTProto protokolünü açıklayan Şekil 2.7' de gösterilmektedir [39]. MTProto protokolünde Diffie Hellman anahtar değişimi algoritması Signal uygulamasında olduğu gibi mesajı şifreleyen anahtarı oluşturmakta ve bir yetkilendirme anahtarı oluşturmada kullanılmaktadır [40].



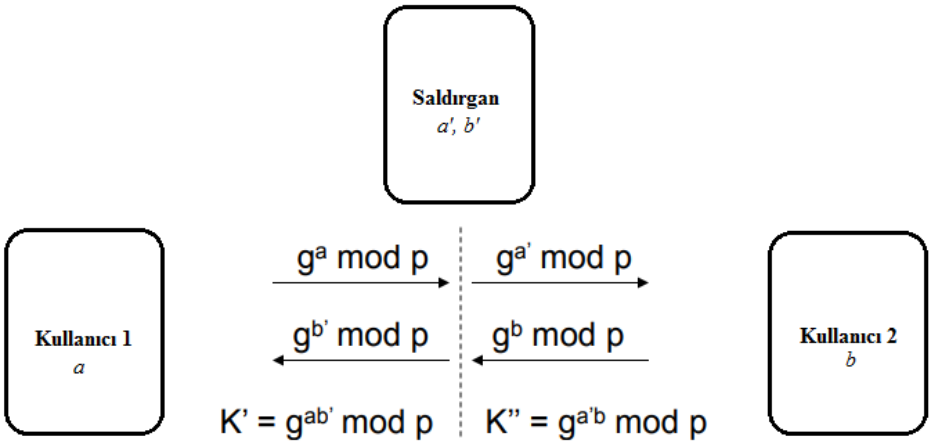
Şekil 2.7 : MTProto protokolünün kullandığı kriptografik birimler.

2.1.1. Diffie Hellman protokolü ve aradaki adam saldırısı

Aradaki adam saldırısı bir ağ üzerinde iletişimde olan iki bilgisayarın arasına girerek verileri yakalayan veya verileri değiştiren saldırı yöntemidir. Bu saldırıdaki amaç Kullanıcı 1 ve Kullanıcı 2 arasındaki trafiğe hakim olmaktır. Diffie Hellman protokolü kullanılan uygulamalarda saldırgan aradaki adam saldırısını kullanıcıların özel anahtarlarına müdahale ederek gerçekleştirebilir. Kullanıcı 1 a özel anahtarına sahiptir. Kullanıcı 2 ise b özel anahtarına sahiptir. Kullanıcı 1 ve Kullanıcı 2 haberleşmesini dinleyen saldırgan kullanıcıların a ve b özel anahtarlarını dinlediği trafikten elde edemez. Çünkü bu anahtarlar sadece kullanıcıların kendilerinde

bulunur. Kullanıcı 1 Kullanıcı 2'nin özel anahtarına sahip değildir; Kullanıcı 2 de Kullanıcı 1'in özel anahtarına sahip değildir.

Diffie Hellman protokolü kullanan uygulamalarda aradaki adam saldırısı yapmak isteyen saldırgan iletişim kanalı arasına yerleşir ve hem Kullanıcı 1 hem de Kullanıcı 2'yi diğer tarafa taklit eder. Kullanıcı 1 için sahte a' anahtarı, Kullanıcı 2 için de sahte b' anahtarı kullanır. Kullanıcı 1'in hesapladığı (g^a mod p) değerini manipüle ederek ($g^{a'}$mod p) değerini kullanıcı 2 ye gönderir. Kullanıcı 2'nin hesapladığı (g^b mod p) değerini manipüle ederek de ($g^{b'}$ mod p) değerini Kullanıcı1'e gönderir. Kullanıcı 1 gelen ($g^{b'}$ mod p) değerini kendi özel anahtarı ile işleme sokar ve ($g^{b'a}$ mod p) değerini elde eder. Kullanıcı 2 ise gelen sonucu kendi özel anahtarı ile işleme sokarak ($g^{a'b}$ mod p) sonucunu elde eder. $g^{a'b}$ sonucu ile $g^{ab'}$ sonuçları birbirine eşit olmadığı için ortak anahtar oluşmamış olur. Yani saldırgan Kullanıcı 1 ve Kullanıcı 2'nin anahtarlarını değiştirerek yeni oluşan ortak anahtarı elde edemez. Anahtarları değiştirmeye çalışan aradaki saldırganın ortak anahtarı elde edememesi Şekil 2.8'de gösterilmiştir.



Şekil 2.8 : Anahtarları değiştirmeye çalışan aradaki saldırganın ortak anahtarı Diffie Hellman protokolünden dolayı elde edememesi.

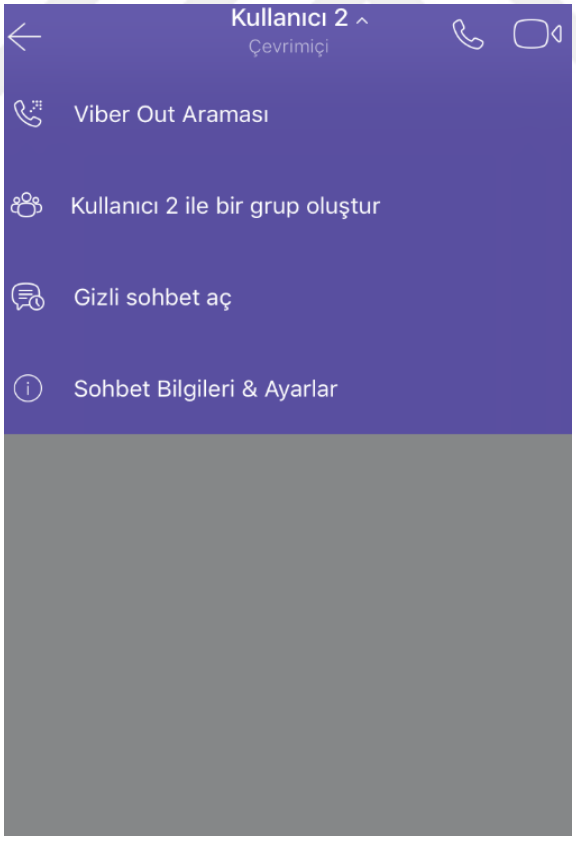
Viber, Telegram, Signal ve Google Allo uygulamaları uçtan uca şifreleme için farklı protokoller kullanmalarına rağmen kullanıdıkları Signal ve MTProto protokolleri anahtar üretmek için Diffie Hellman protokolünü kullanmaktadırlar.

2.2. Popüler Anlık Mesajlaşma Uygulamaları

2.2.1. Viber

Viber 800 milyondan fazla kullanıcısı olduğunu söyleyen güvenli anlık mesajlaşma uygulamasıdır. Viber şifreli mesaj yollama özelliğini 2016 Nisan ayında aktif hale getirmiştir.

Viber kendi internet sitesinde [31] kullanıcıya sağladığı güvenlik önlemleri için şunları yazmaktadır: "Kullanıcı gizliliği ve güvenliği konusundaki taahhüdümüzün bir parçası olarak, Viber'deki sohbetler uçtan uca şifreleme ile güvenceye alınmaktadır. Uçtan uca şifreleme, bir cihazdan gönderildiği andan itibaren alıcıya ulaşana kadar verilerin (her tür ileti, fotoğraf, video, sesli ve görüntülü çağrı) şifrelendiği anlamına gelir. Bu veriler başkaları tarafından ortada toplanamaz." Viber uygulamasında şifreli mesaj gönderilmek istendiği zaman sohbet ekranı açıldıktan sonra kullanıcı ismi üzerine basılır. Buradan "Gizli sohbet aç" seçeneği seçilir. Gizli sohbet açma ekran görüntüsü Şekil 2. 9'da gösterilmektedir.

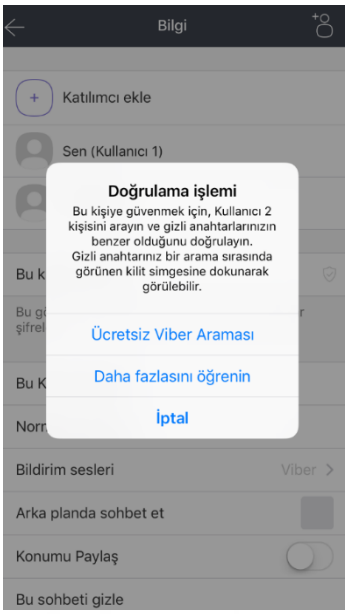


Şekil 2.9: Viber uygulaması gizli sohbet başlatma ekran görüntüsü.

Eğer kullanıcılar karşılıklı olarak şifreleme anahtarlarını doğrulamadılar ise; Şekil 2. 9'da de görülen "Sohbet Bilgileri & Ayarlar" seçeneğine girildiği zaman "Bu kişiye güvenin" seçeneğinin sağ yanında bulunan logo gri renk gözükmektedir. Anahtarın doğrulanmadığını gösteren bu ekran görüntüsü Şekil 2. 10'da gösterilmiştir.

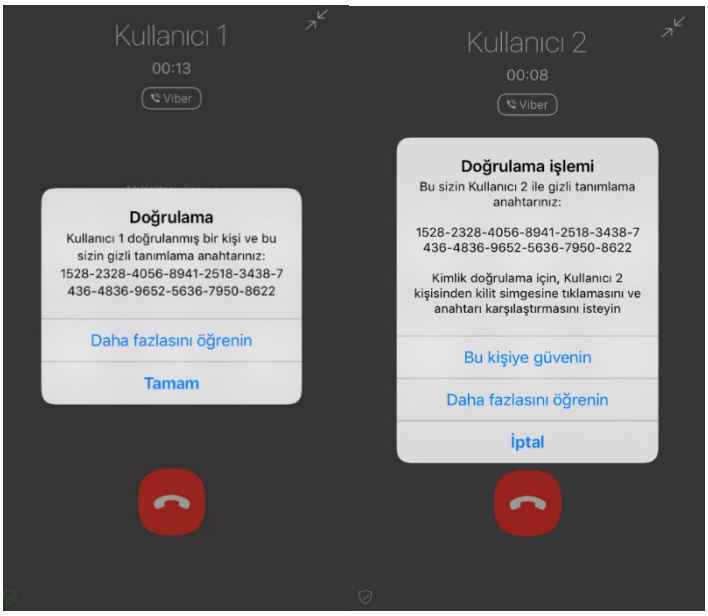
Şekil 2.10 : Viber uygulaması güvenilen kişi oluşturma ekran görüntüsü.

Şekil 2.10'daki bu kişiye güvenin seçeneği seçildiği zaman Viber uygulaması şifreleme anahtarının doğrulanması için Şekil 2. 11'de ki talimatları kullanıcıya gösterir. Viber uygulaması kullanıcıya arama yapması gerektiğini ve bu kişiye güvenin seçeneğinin yan tarafında bulunan logoya dokunularak doğrulama yapabileceği talimatlarını vermektedir. Yani Viber uygulamasında şifreleme anahtarının doğrulana bilmesi için Viber uygulaması üzerinden arama yapılması gerekmektedir.



Şekil 2.11 : Viber uygulaması şifreleme anahtarı doğrulama talimatları ekran görüntüsü.

Kullanıcılardan biri ücretsiz Viber araması başlatıp, karşısındaki kullanıcı da aramayı kabul ederse ekranlarda "Bu kişiye güvenin" seçeneğinin yanındaki logo çıkar. İki kullanıcı da bu logoya tıklayarak şifreleme anahtarlarını görebilirler. Kullanıcı 1 ve Kullanıcı 2 için Viber şifreleme anahtarları ekran görüntüleri Şekil 2.12 de gösterilmektedir.



Şekil 2.12 : Viber uygulaması Kullanıcı 1 ve Kullanıcı 2 şifreleme anahtarları ekran görüntüleri.

Kullanıcılar Şekil 2.12'deki şifreleme anahtarlarını karşılaştırıp aynı olduklarını anladıktan sonra "Bu kişiye güvenin" seçeneğini seçerek şifreleme anahtarı doğrulama işlemini manuel olarak tamamlamış olurlar. Önceden bu kişiye güvenin seçeneği "Güvenilen kişi" seçeneği olarak değişir. Sol taraftaki gri logo ise yeşil renk olur. Bu değişen ekran görüntüsü Şekil 2. 13'de gösterilmiştir.

Şekil 2.13 : Viber uygulaması şifreleme anahtarının doğrulandığını belirten ekran görüntüsü.

Viber uygulaması silinip tekrar yüklenildiğinde şifreleme anahtarı değişmektedir. Kullanıcı 1 uygulamayı silip tekrar yüklediği zaman Kullanıcı 2 Şekil 2. 13'deki güvenilen kişi seçeneğinin değiştiğini görür. Viber uygulaması şifreleme anahtarı değiştiği zaman kullanıcılara otomatik olarak bildirim yollamaz. Kullanıcıların anahtarın değişip değişmediğini sohbet ekranlarından girilen "Bilgi" sayfasından

kontrol etmeleri gerekmektedir. Şifreleme anahtarı değişmesi sonrasında oluşan ekran görüntüsü Şekil 2. 14'de gösterilmektedir.

Şekil 2.14 : Viber uygulamasında şifreleme anahtarının değişmesi sonrasındaki bildirim ekranı.

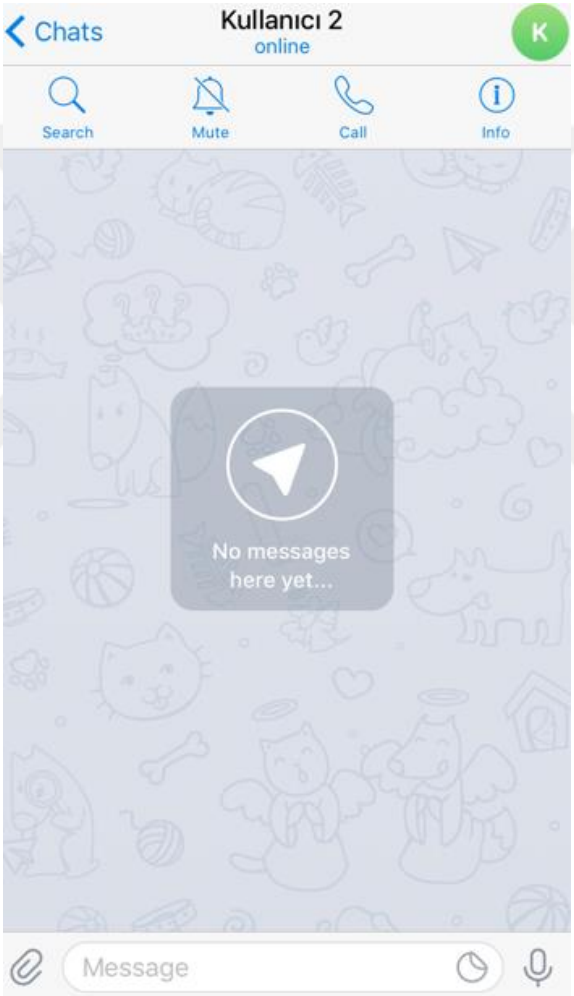
Önceden güvenilen kişi olarak işaretlenmiş olan Kullanıcı 1'in artık güvenilir kişi olmadığı bilgisine ulaşılmaktadır. Buradaki yeşil olan logo kırmızı rengine dönmüş ve bir uyarı bildirimi çıkmıştır. Kullanıcıların bu uyarıyı gördükten sonra şifreleme anahtarı doğrulama aşamalarını tekrar yapmaları beklenmektedir.

2.2.2. Telegram

Telegram, güvenlik ve hız odaklı, bulut tabanlı mobil ve masaüstü anlık mesajlaşma uygulamasıdır. Resmi kaynak kodunun bulunduğu internet sitesinde [32] Telegram "Telgraf, hız ve güvenlik odaklı bir mesajlaşma uygulamasıdır." şeklinde

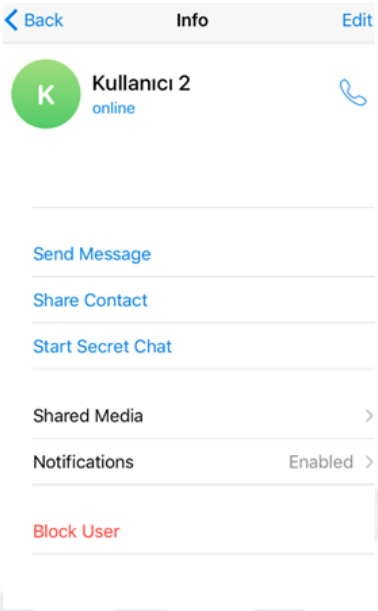
açıklanmaktadır. Telegram uygulaması Viber uygulamasından farklı olarak açık kaynak kodlu bir uygulamadır.

Kullanıcı Telegram uygulamasında hem şifreli hem de şifresiz mesaj gönderebilmektedir. Uygulama yüklendiği zaman varsayılan olarak şifresiz mesajlaşma başlatılır. Eğer kullanıcı şifreli mesajlaşma başlatmak istiyorsa gizli sohbet başlatmalıdır. Kullanıcı adı sekmesinden "Bilgi" seçeneği açılır. Bu açılan ekran görüntüsü Şekil 2. 15' de gösterilmektedir.



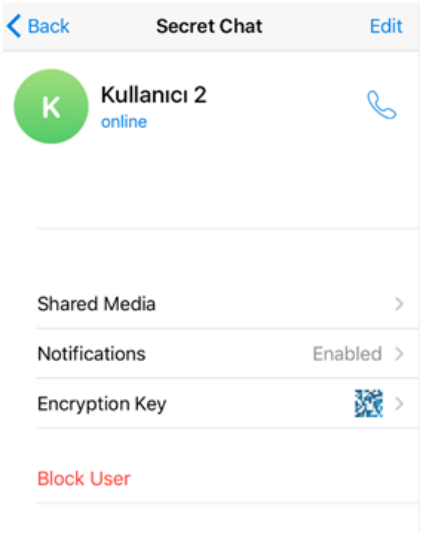
Şekil 2.15 : Telegram uygulaması şifreli mesajlaşma başlatmak için açılan bilgi sayfası ekran görüntüsü.

Bilgi alanına girildiği zaman gizli mesajlaşma sayfası açma ekranı görülmektedir. Gizli mesajlaşma ekranı başlatma ekran görüntüsü Şekil 2. 16' da gösterilmektedir.



Şekil 2.16 : Telegram uygulaması gizli sohbet başlatma ekran görüntüsü.

Gizli sohbet başlatıldıktan sonra Telegram uygulaması Kullanıcı 1 ve Kullanıcı 2'ye aynı olacak şekilde şifreleme anahtarı oluşturur. Bu şifreleme anahtarının kullanıcılar tarafından doğruluğu sadece gözle okunarak yapılabilmektedir. Kullanıcılar mesajlaşacağı kişinin kullanıcı ismine basarak şifreleme anahtarı görme ekranını bulabilirler. Şifreleme anahtarı görme ekranı Şekil 2. 17'de gösterilmektedir.

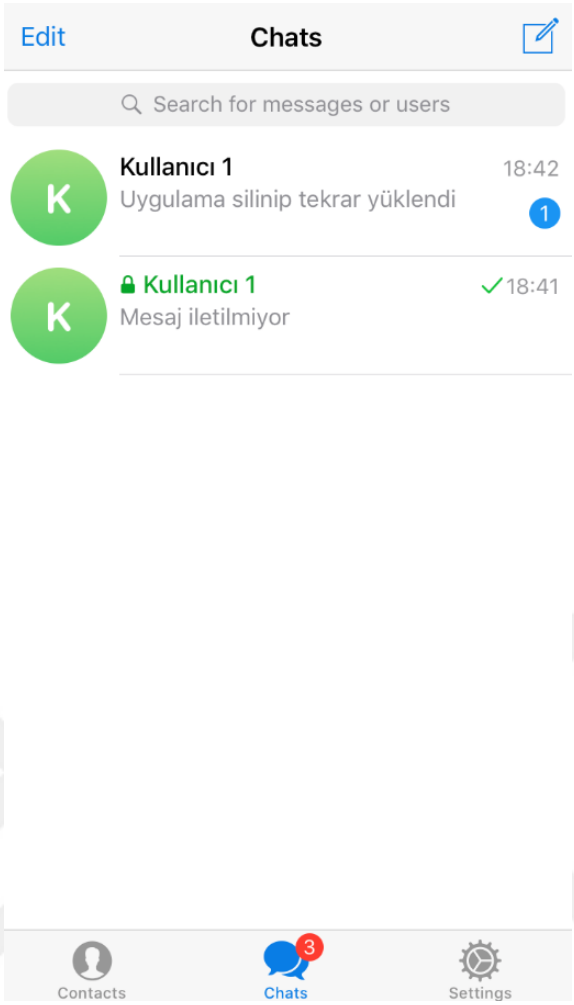


Şekil 2.17 : Telegram uygulaması anahtarı görme ekran görüntüsü.

Telegram uygulaması Kullanıcı 1'den silinip tekrar yüklendiği zaman mesaj şifreleme anahtarı değişir. Fakat Kullanıcı 2'ye bu bilgi bildirim olarak gitmez. Kullanıcı 2 eski güvenli sohbet kanalından mesaj göndermeye devam ederse bu mesajın Kullanıcı 1'e çevrim içi olmasına rağmen ulaşmadığı Şekil 2. 18'de gösterilmektedir.

Şekil 2.18 : Telegram uygulamasında şifreleme anahtarı değiştiği zaman eski sohbet sayfasından mesajın iletilmemesi.

Eğer Kullanıcı 1 güvenli sohbeti başlatmazsa Kullanıcı 2 ile şifresiz mesajlaştığı sohbet sayfasına yönlendirilir ve mesaj buradan iletilir. Bu işlem Şekil 2. 19' da gösterilmiştir. Yani Telegram uygulaması silinip tekrar yğklenirse şifreleme anahtarı değişir. Kullanıcılar önceden başlattıkları gizli sohbet sayfalarını kullanamaz olurlar. Eğer gizli sohbet başlatmazlarsa da yolladıkları mesajlar şifrelenmeyen sohbet sayfalarına iletilmeketedir.



Şekil 2.19 : Telegram uygulamasında Kullanıcı 1 uygulamayı silip tekrar yüklediği zaman yolladığı mesajların şifresiz sohbet ekranına gelmesi ekran görüntüsü.

Telegram uygulaması silinip tekrar yüklendikten sonra Kullanıcı 1 gizli sohbeti başlatırsa da üçüncü sohbet sayfası oluşturulur; mesajlar bu yeni sayfadan iletilir. Mesajlaşma anahtarın değiştiğini Kullanıcı 2 yeni bir sohbet sayfası açılması sayesinde anlayabilmektedir.

2.2.3. Signal

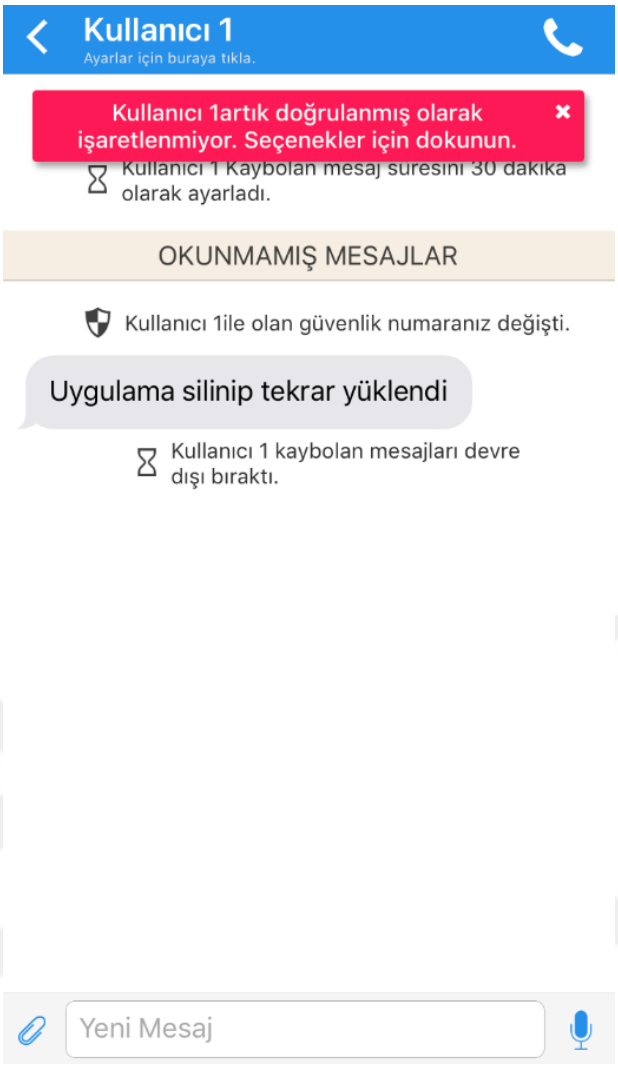
Open Whisper Systems tarafından açık kaynak olarak yayımlanan şifreli anlık mesajlaşma uygulaması 2013 yılında ortaya çıkmıştır. Signal TextSecure uygulamasının gelişmiş halidir. Güvenliğin zamanla önem kazanması sonucu Signal uygulamasının popülerliği de gün geçtikçe artmaktadır.

Signal kendi sitesinde [33] sağladığı güvenlik özellikleri için şunları söylemektedir: “Signal iletileri ve çağrıları her zaman uçtan uca şifrelenir ve iletişimi güvende tutmak için titizlikle tasarlanır. Mesajlarınızı okuyamıyoruz ya da görüşmelerinizi göremiyoruz, başka kimse de bunu yapamaz.”

Signal karşılıklı mesajlaşmak isteyen kullanıcılar için aynı olacak şekilde mesajlaşma anahtarı içerir. Ortak anahtarlar gözle manuel olarak veya Whatsapp uygulamasındaki gibi QR kod okutularak doğrulanabilir. Kullanıcı 1 ve Kullanıcı 2’nin mesajlaşma anahtarları Şekil 2. 20’ de gösterilmektedir.

Şekil 2.20 : Signal uygulaması Kullanıcı 1 ve Kullanıcı 2 şifreleme anahtarlarları ekran görüntüsü.

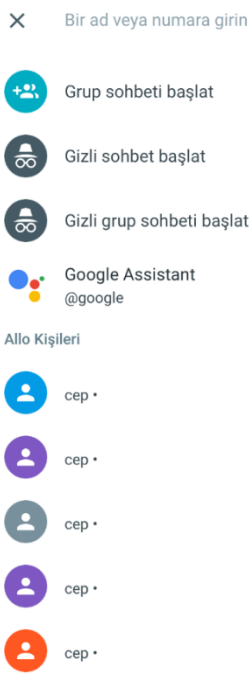
Kullanıcı 1 ve Kullanıcı 2 Şekil 2.20’ de gösterilen “Doğrulamış olarak işaretle” seçeneklerini seçerek birbirlerini doğrulamış olurlar. Signal uygulaması silinip tekrar yüklendiğinde zaman mesajlaşma anahtarı değişmiş olur. Viber ve Telegram uygulamalarından farklı olarak mesajlaşma anahtarı değiştiği zaman sohbet sayfasına Signal uygulaması bildirim göndermektedir. Bu şifreleme anahtarının değiştiğini gösteren bildirim Şekil 2. 21’ de gösterilmektedir.



Şekil 2.21 : Signal uyulaması şifreleme anahtarı değiştiği zaman sohbet ekranında gözüken bildirimin ekran görüntüsü.

2.2.4. Google Allo

Google tarafından güvenli mesajlaşma uygulaması Allo 2016 yılında resmi olarak duyurulmuştur. Diğer üç uygulamada olduğu gibi bu uygulamada da mesajlar uçtan uca şifrelenmektedir. Google Allo uygulamasında kullanıcı şifreli mesajlaşma başlatmak istiyorsa gizli sohbet başlatır. Gizli sohbet başlatma ekran görüntüsü Şekil 2. 22’ de gösterilmektedir.

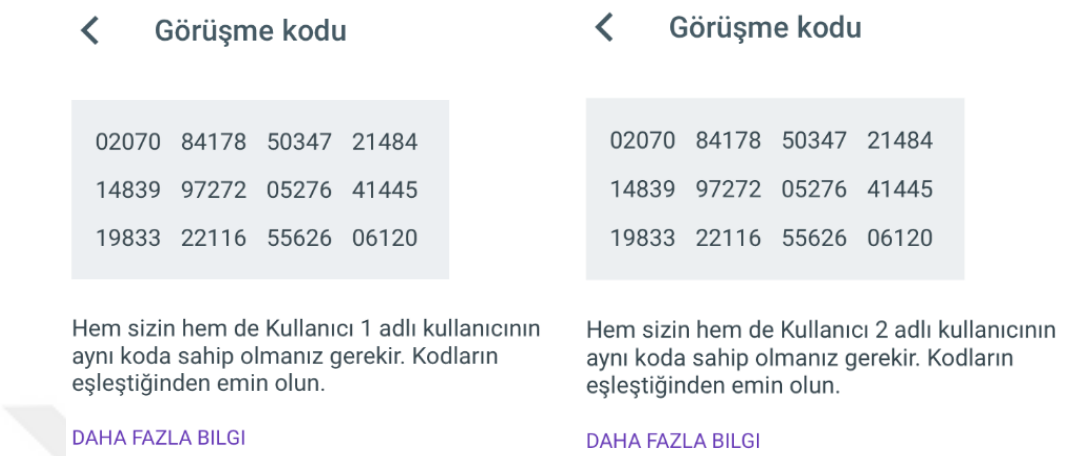


Şekil 2.22 : Google Allo uygulaması gizli sohbet başlatma ekran görüntüsü.

Gizli sohbet başlattıktan sonra oluşan sohbet anahtarlarını Kullanıcı 1 ve Kullanıcı 2 karşılıklı olarak doğrulamalıdırlar. Kullanıcıların şifreleme anahtarını görmek için sohbet ekranında isimleri üzerine basılır. Şekil 2. 23'de açılan sayfadan "Görüşme kodu" seçeneği seçilir.

Şekil 2.23 : Google Allo uygulaması görüşme kodu görme ekran görüntüsü.

Google Allo uygulaması mesajlaşma anahtarı açma ekran görüntüsü Kullanıcı 1 ve Kullanıcı 2 için oluşturulmuş görüşme kodları Şekil 2. 24'te gösterilmiştir.



Şekil 2.24 : Google Allo uygulaması Kullanıcı 1 ve Kullanıcı 2 görüşme kodları ekran görüntüsü.

Eğer kullanıcılardan birisi uygulamayı silip tekrar yüklerse şifreleme anahtarı değişir. Kullanıcılar bu mesajlaşma anahtarını değiştiği haberini almak istiyorlarsa Google Allo ayarlardan bu alanı aktif hale getirmesi gerekmektedir. Fakat bu özellik yalnızca Android işletim sistemine sahip telefonlarda bulunmaktadır. Allo uygulamasında alınan uyarı Şekil 2. 17' de gösterilmektedir. Android işletim sistemi dışındaki telefonlarda bu uygulama bu bildiri görememektedir.

Şekil 2.25 : Google Allo uygulaması şifreleme anahtarının değiştiği bilgisinin ekran görüntüsü.

3. ARAŞTIRMA ÇALIŞMASI

Popüler anlık mesajlaşma uygulamalarında şifreleme anahtarının değişmesi ile kullanıcı etkileşimi çalışması iki ayrı grup ile gerçekleştirilmiştir. Birinci grupta bulunan katılımcılar bilişim sektöründe çalışan fakat bilgi güvenliği üzerine bilgisi olmayan 18 katılımcıdan oluşmaktadır. İkinci gruptaki katılımcılar ise bilgi güvenliği dersini alan 48 üniversite öğrencisinden oluşmaktadır.

3.1. Kişisel Sorular Araştırması

Kişisel sorular araştırma çalışmasında hem bilişim sektöründe çalışan katılımcılara hem de bilgi güvenliği dersi öğrencilerine aşağıdaki uygulamalardan hangilerini duydukları sorulmuştur:

- Whatsapp
- Line
- Chatsecure
- Signal
- Telegram
- Threema
- Allo
- iMessage
- Skype
- Viber
- Wickr
- Silent

Tüm katılımcıların verdikleri cevaplar kayıt edilmiştir.

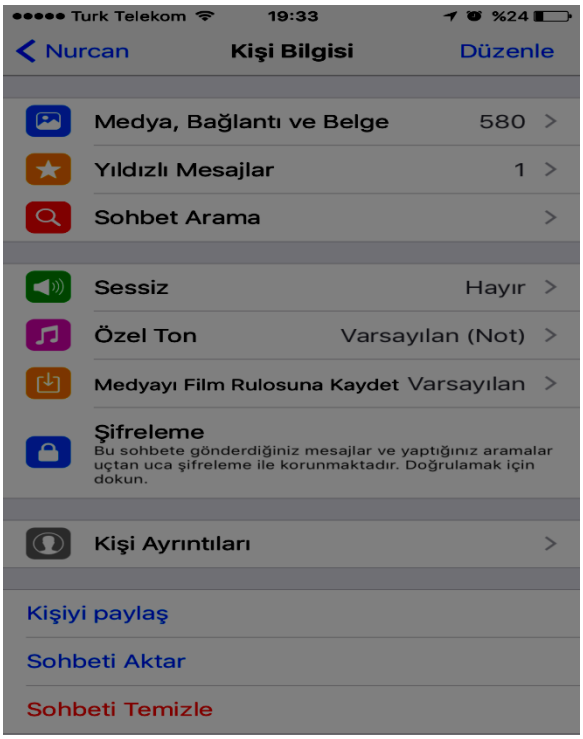
3.2. Uygulama Soruları Araştırması

Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılara uygulama çalışmasına başlamadan önce tüm katılımcıların da kullandığı en popüler mesajlaşma uygulaması olan Whatsapp'da [36] şifreleme anahtarı ve kimlik doğrulama etkinliğinin nasıl gerçekleştiği ve şifreleme anahtarının nasıl değiştirildiği bilgisi tüm katılımcılara aktarılmıştır. Bilgi güvenliği dersi öğrencilerine ise bu bilgi verilmemiştir. Whatsapp uygulamasında kimlik doğrulama etkinliği aşağıdaki aşamalardan oluşmaktadır:

1- Whatsapp uygulaması açılır ve sohbet edecek kişiler karşılıklı olarak birbirlerinin sohbet sayfalarını açarlar.

2- Sohbet sayfası üzerinde bulunan kullanıcı ismi sekmesine basılır. Yeni açılan sayfada şifreleme yazısı bulunur. Şifreleme yazısı çıkan ekran görüntüsü Şekil 3. 1'de gösterilmektedir.

3- Şifreleme sayfasına basılarak şifreleme anahtarı görülebilmektedir. Şekil 3.2'de görülen şifre anahtarı ekranları karşılıklı olarak doğrulanır.



Şekil 3.1 : Whatsapp uygulaması şifreleme anahtarı gösterme ekran görüntüsü.

Şekil 3.2 : Whatsapp uygulaması şifreleme anahtarı ekran görüntüsü.

Eğer karşılıklı olarak mesajlaşan kullanıcılardan bir tanesi uygulamayı telefonundan silip tekrar yüklerse şifreleme anahtarı değişmektedir.

Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılara Whatsapp uygulamasında şifreleme anahtarının doğrulanması ve nasıl değiştiğinin bilgisi verilmesinden sonra; bilgi güvenliği dersi öğrencilerine ise bu bilgi verilmeden tüm katılımcılardan; Viber, Telegram, Signal ve Allo uygulamalarında sohbet anahtarını doğrulamaları beklenmiştir. Katılımcılar kendi gruplarından arkadaşları ile ikişerli grup oluşturmuşlardır. Gruplar ilk olarak her uygulamada şifreleme anahtarlarını karşılıklı olarak doğrulamaya çalışmışlardır. Daha sonra çiftlerden bir tanesi uygulamayı silip tekrar yüklemiştir. Bu sayede şifreleme anahtarı dört uygulamada da değişmiştir. Şifreleme anahtarları değiştiği zaman grupların bunu nasıl anladıklarını not almaları istenmiştir.

Anahtar doğrulama işlemleri tamamlandıktan sonra ise tüm katılımcılara bu dört uygulamadan hangi uygulamanın favori uygulamaları olduğu ve anahtar doğrulama işlemlerinde kullanıcıyı en iyi yönlendiren uygulamanın hangi uygulama olduğu sorulmuştur.

3.3. Sistem Kullanılabilirlik Ölçeği Araştırması

En son aşama olarak hem bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılara hem de; bilgi güvenliği dersi öğrencilerine sistemlerin kullanışlılığını ölçen sistem kullanılabilirlik ölçeği (SUS) soruları Viber, Telegram, Signal ve Google Allo uygulamaları için doldurtulmuştur.

4. ARAŞTIRMA ÇALIŞMASI SONUÇLARI

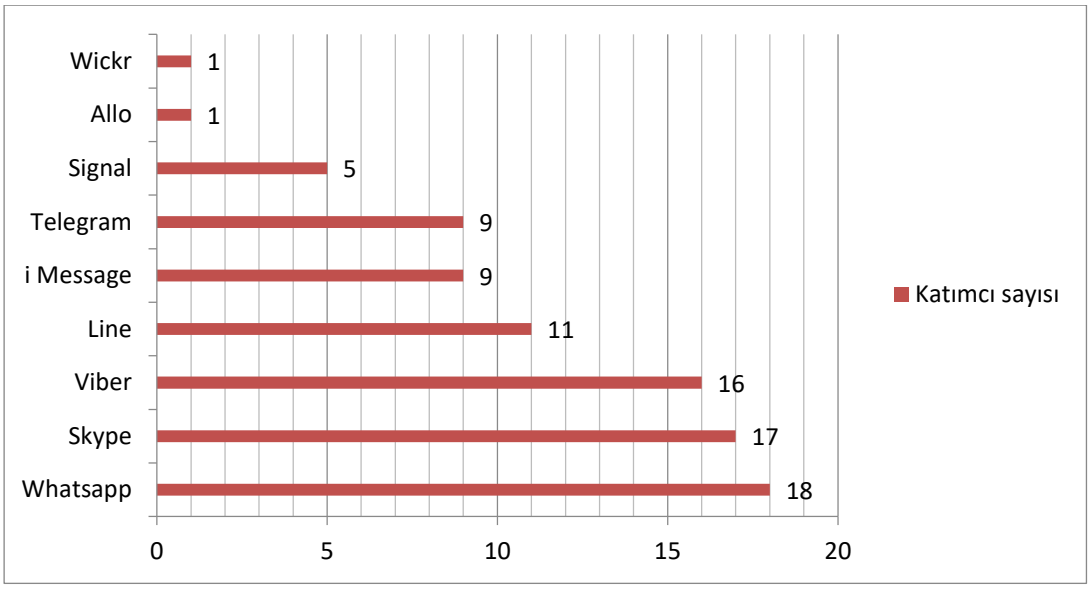
Popüler anlık mesajlaşma uygulamalarında şifreleme anahtarının değişmesi ile kullanıcı etkileşimi çalışması iki ayrı grup ile gerçekleştirilmiştir. Birinci grupta bulunan katılımcılar bilişim sektöründe çalışan fakat bilgi güvenliği üzerine bilgisi olmayan 18 katılımcıdan oluşmaktadır. İkinci gruptaki katılımcılar ise bilgi güvenliği dersi alan 48 üniversite öğrencisinden oluşmaktadır.

4.1. Kişisel Sorular Araştırması Sonuçları

Viber, Telegram, Signal ve Google Allo uygulamaları kullanılarak şifreli mesajlaşmada doğru kişiyle mesajlaştığını anlamak için 66 kişiye araştırma çalışması yapılmıştır. Bu çalışmanın başlangıç aşaması olarak kişisel sorular araştırma çalışması yapılmıştır. Hem bilişim sektöründe çalışan katılımcılara hem de bilgi güvenliği dersi öğrencilerine Whatsapp, Line, Chatsecure, Signal, Telegram, Threema, Allo, iMessage, Skype, Viber, Wickr, Silent uygulamalardan hangilerini duydukları sorulmuştur.

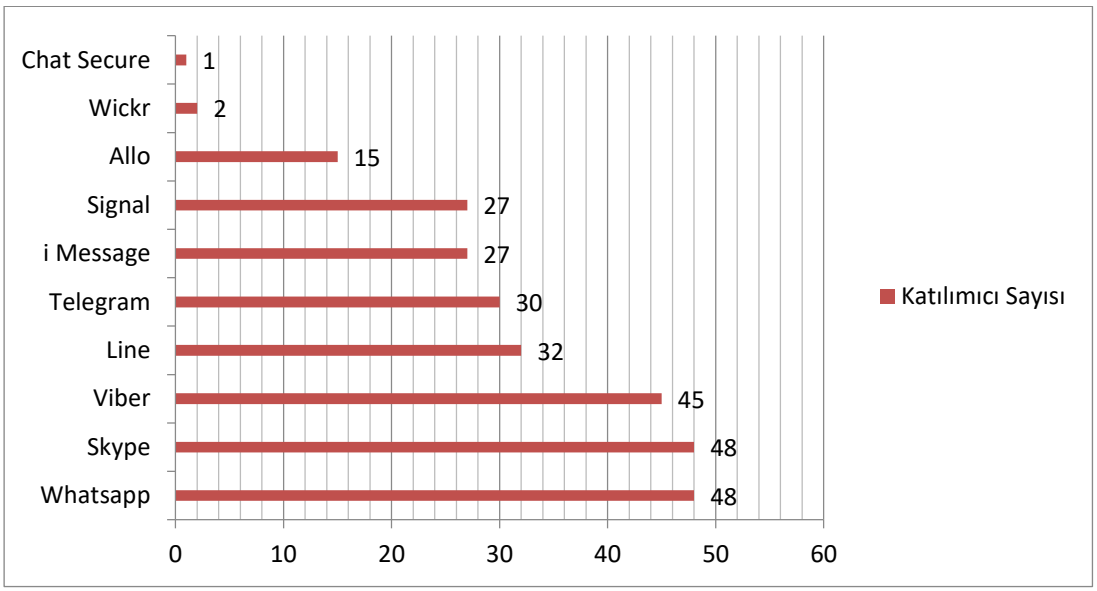
Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan 18 katılımcının tamamı Whatsapp uygulamasını bilmektedir. Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan 17 katılımcı Skype, 16 katılımcı Viber, 11 katılımcı Line, 9 katılımcı iMessage, 9 katılımcı Telegram, 5 katılımcı Signal, 1 katılımcı Allo ve 1 katılımcı Wickr uygulamalarını duyduklarını söylemişlerdir. Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan 18 katılımcının duydukları anlık mesajlaşma uygulamaları Şekil 4. 1'de gösterilmektedir.

Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan 18 katılımcının tamamının Whatsapp uygulamasını duyduklarını ve kullandıklarını belirtmeleri üzerine Whatsap uygulamasında şifreleme anahtarı doğrulama etkinliğinin nasıl gerçekleştiği ve şifreleme anahtarının nasıl değiştiği bilgisi katılımcılara aktarılmıştır. Viber, Telegram, Signal ve Goggle Allo uygulamalarında bu işlemleri kendileri yapmaları beklenmiştir.



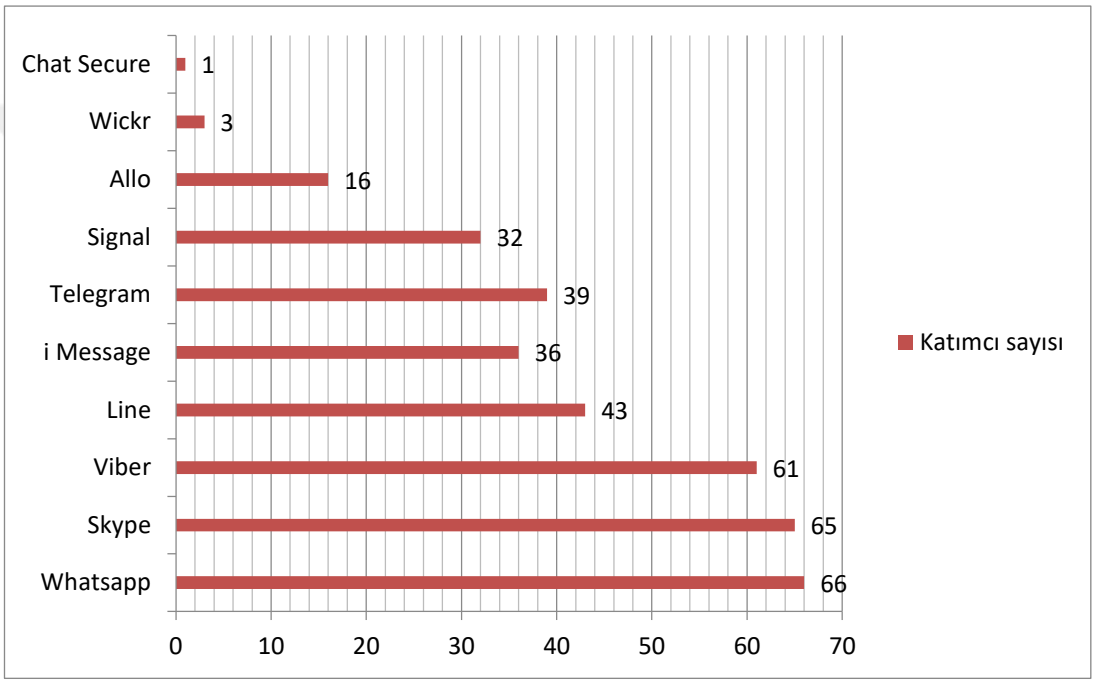
Şekil 4.1 : Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcıların duydukları anlık mesajlaşma uygulamaları.

Bilgi güvenliği dersini almakta olan üniversite öğrencilerden 48 katılımcının tamamı Whatsapp uygulamasını bilmektedir. Bilgi güvenliği dersi öğrencilerinden 48 katılımcı Skype, 45 katılımcı Viber, 32 katılımcı Line, 27 katılımcı iMessage, 30 katılımcı Telegram, 27 katılımcı Signal, 15 katılımcı Google Allo, 2 katılımcı Wickr ve 1 katılımcı ise Chatsecure uygulamalarını duyduklarını söylemişlerdir. Bilgi güvenliği dersini almakta olan üniversite öğrencilerden 48 katılımcının duydukları anlık mesajlaşma uygulamaları Şekil 4.2'de gösterilmektedir.



Şekil 4.2 : Bilgi güvenliği dersini almakta olan üniversite öğrencileri katılımcıların duydukları anlık mesajlaşma uygulamaları.

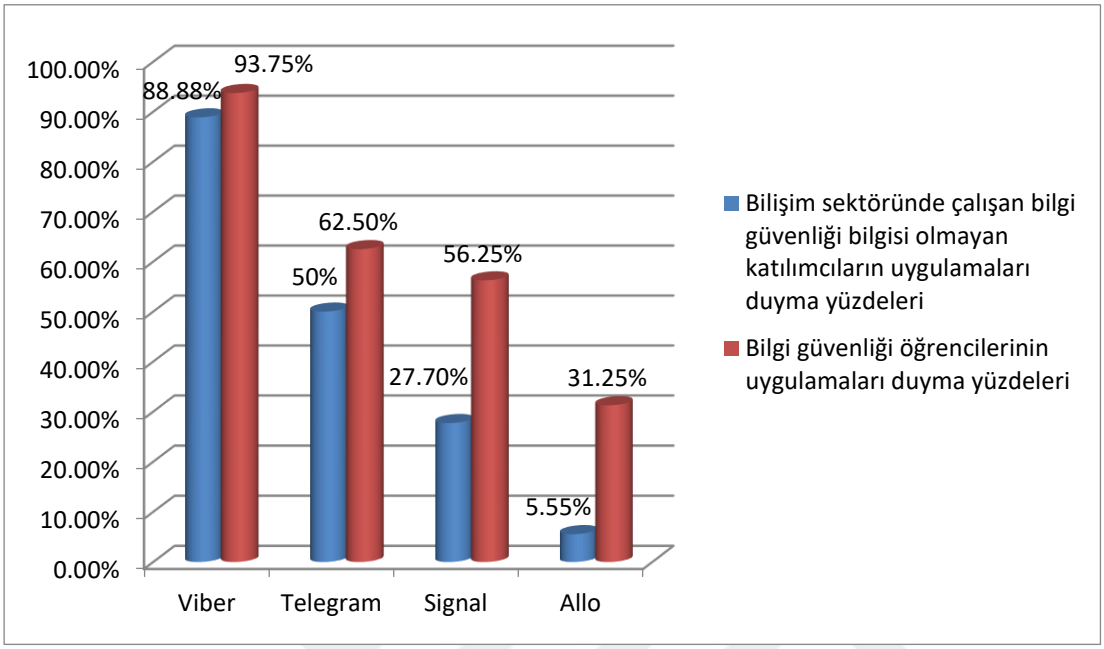
Viber, Telegram, Signal ve Allo uygulamaları kullanılarak şifreli mesajlaşmada doğru kişiyle mesajlaştığını anlamak için 66 kişiyle yürütülen araştırma çalışmasında tüm katılımcılar Whatsapp uygulamasını duyduklarını belirtmişlerdir. Tüm katılımcılardan 65 katılımcı Skype, 61 katılımcı Viber, 43 katılımcı Line, 36 katılımcı iMessage, 39 katılımcı Telegram, 32 katılımcı Signal, 16 katılımcı Allo, 3 katılımcı Wickr ve 1 katılımcı Chat Secure uygulamalarını duyduklarını belirtmişlerdir. 66 katılımcının duydukları anlık mesajlaşma uygulamaları Şekil 4. 3'te gösterilmektedir.



Şekil 4.3 : Tüm katılımcıların duydukları anlık mesajlaşma uygulamaları.

Bilişim sektörü çalışanlarının %88,88'i Viber uygulamasını, %50'si Telegram uygulamasını, %27,70'i Signal uygulamasını ve %5,55'i Google Allo uygulamasını önceden duymuştur. Bilgi güvenliği dersi öğrencilerinin %93,75'i Viber uygulamasını, %62,50'si Telegram uygulamasını, %56,25'i Signal uygulamasını ve %31,25'i Allo uygulamasını önceden duymuştur. Viber uygulaması hem bilişim sektörü çalışanları hem de bilgi güvenliği dersi öğrencileri tarafından en fazla duyulan mesajlaşma uygulamasıdır. Fakat bilgi güvenliği dersini almakta olan öğrencilerin Viber, Telegram, Signal ve Google Allo uygulamalarının duyulma yüzdeleri; bilişim sektöründe çalışan katılımcıların Viber, Telegram, Signal ve Google Allo uygulamalarının duyulma yüzdelerinden daha yüksek olduğu

görülmüştür. Viber, Telegram, Signal ve Allo uygulamalarının bilişim sektörü çalışanları ile bilgi güvenliği dersi öğrencilerinin duyma yüzdeleri Şekil 4. 4'te gösterilmiştir.



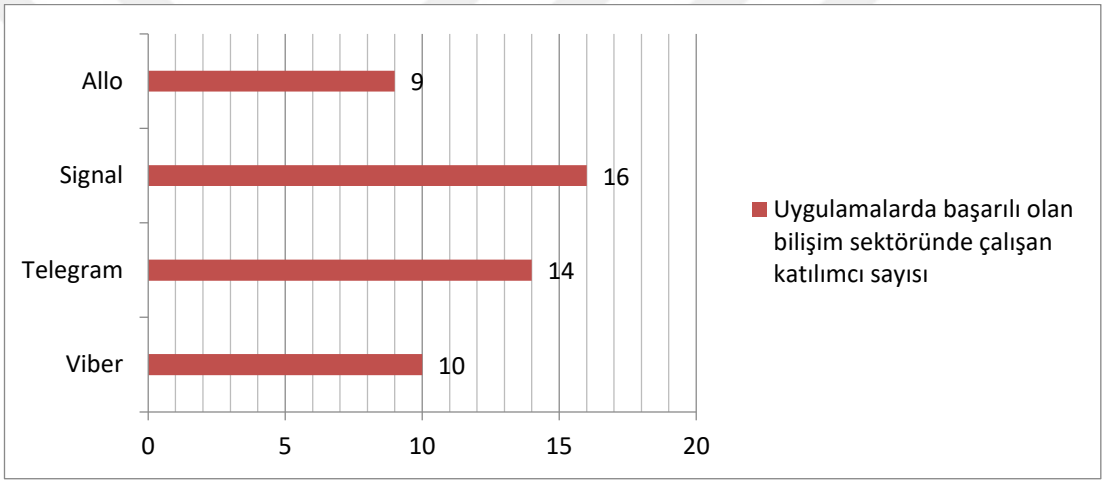
Şekil 4.4 : Tüm katılımcıların duydukları anlık mesajlaşma uygulamaları duyma yüzdeleri.

4.2. Uygulama Soruları Araştırması Sonuçları

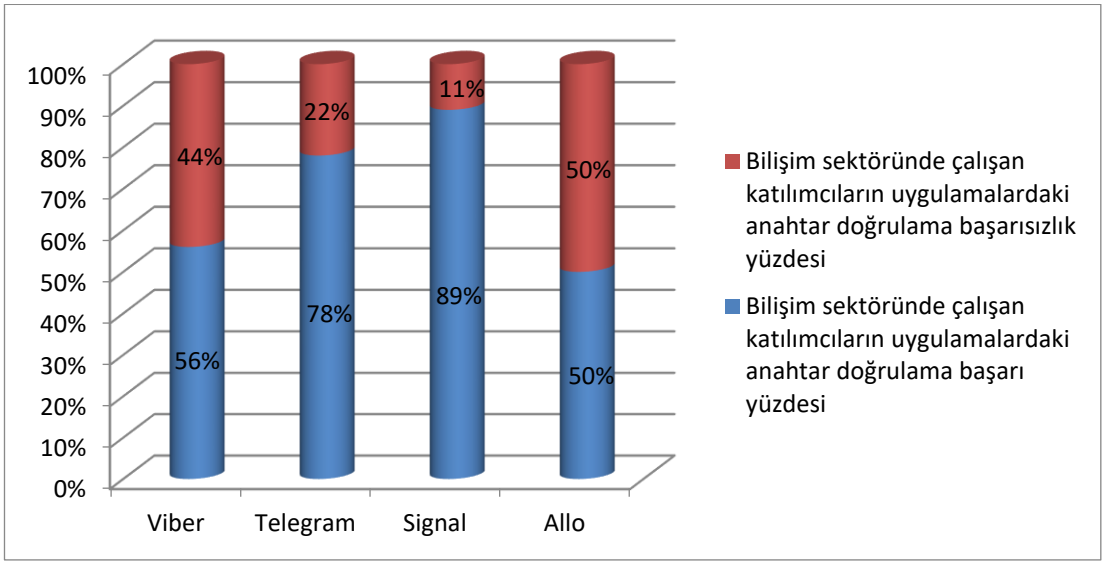
Bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılar ve bilgi güvenliği dersi öğrencilerinden sırasıyla Viber, Telegram, Signal ve Allo uygulamalarında şifreleme anahtarının doğrulanması istenmiş daha sonrasında da ikişerli gruplardan bir tarafın uygulamaları silip tekrar yüklenmesi istenmiştir. Bunun sonucunda şifreleme anahtarının değiştiğini nasıl anladıklarını not almaları beklenmiştir.

Bilişim sektöründe çalışan 9 grup katılımcılardan Viber uygulamasında sohbet sayfası dışında şifreleme anahtarının uyarısı verildiğini 5 grup bulabilmiştir. 4 grup ise anahtarın değiştiği uyarısını görememişlerdir. Bilişim sektöründe çalışan katılımcılardan 7 grup Telegram uygulamasında yeni sohbet sayfası açıldığı zaman şifreleme anahtarının değiştiğini düşünmüştür. Ayrıca Telegram uygulamasında şifreli mesajlaşma yaparken kapalı kilit simgesi görülmektedir. Eğer şifreli mesajlaşma başlatılmaz ise açık anahtar simgesi kullanılmaktadır. Katılımcılar bu

özellik sayesinde şifreli mesajlaştıklarına ikna olmuşlardır. Signal uygulamasında şifreleme anahtarı değiştiği zaman sohbet ekranına anahtarın değiştiği bilgisi gelmektedir. Bilişim sektöründe çalışan katılımcılardan yalnızca 1 grup bu uyarı bildirisini görememiştir; 8 grup ise görebilmiştir. Google'un Allo uygulaması yalnızca Android işletim sisteminde eğer şifreleme anahtarı değişirse sohbet sayfasında anahtarın değiştiği bildirimi gösterilmektedir. Diğer işletim sistemlerinde herhangi bir bildirim gösterilmemektedir. Bu bilgi ışığında bilişim sektöründe çalışan 9 kişi sohbet ekranında şifreleme anahtarının değiştiği bilgisini görmüştür; 9 kişi ise görememiştir. Bilişim sektöründe çalışan katılımcıların Viber, Telegram, Signal ve Allo uygulamalarında şifreleme anahtarının değiştiğini anlayabilen başarılı katılımcı sayıları Şekil 4. 5'de başarı yüzdeleri ise Şekil 4. 6'da gösterilmektedir.

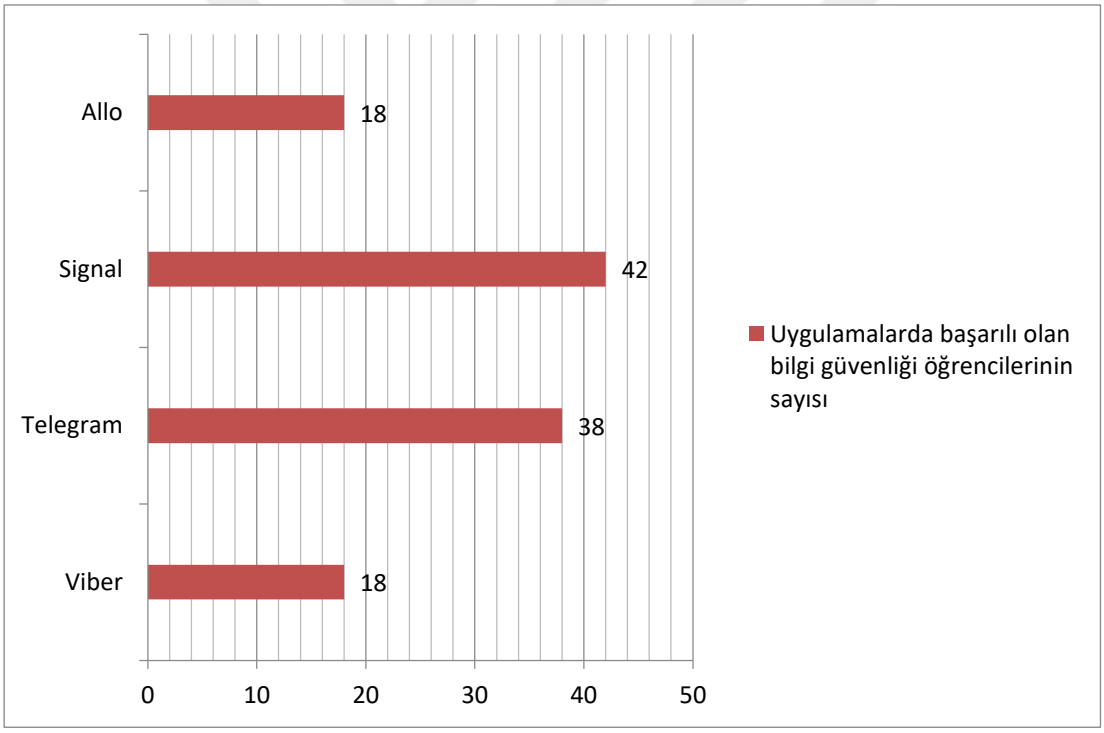


Şekil 4.5 : Bilişim sektöründe çalışan katılımcıların uygulamalardaki anahtar doğrulama başarı sonuçları.

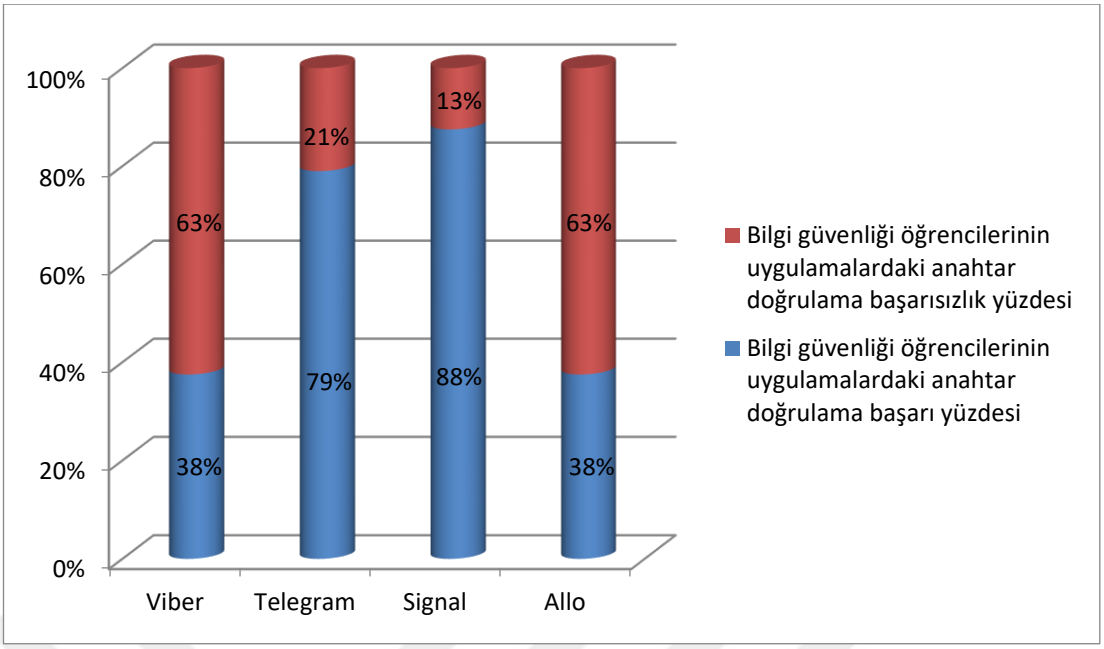


Şekil 4.6 : Bilişim sektöründe çalışan katılımcıların uygulamalardaki anahtar doğrulama başarı yüzdeleri.

Bilgi güvenliği dersi öğrencisi 48 (24 grup) katılımcıdan Viber uygulamasında sohbet sayfası dışında şifreleme anahtarının uyarısı verildiğini 9 grup bulabilmiştir. 15 grup ise anahtarın değiştiği uyarısını görememişlerdir. Bilgi güvenliği dersi öğrencilerinden 19 grup Telegram uygulamasında yeni sohbet sayfası açıldığı zaman şifreleme anahtarının değiştiğini düşünmüştür. Geriye kalan 5 grup ise yeni sohbet sayfası açıldığı zaman şifreleme anahtarının değiştiğini anlayamamıştır. Bilgi güvenliği dersi öğrencilerinden 21 grup Signal uygulamasında şifreleme anahtarı değiştiğinin uyarısını görmüştür; 3 grup ise bu uyarıyı görememiştir. Bilgi güvenliği dersi öğrencilerinden 9 grup sohbet ekranında şifreleme anahtarının değiştiği bilgisini görmüştür; 14 grup ise görememiştir. Bilgi güvenliği dersi öğrencilerinden Viber, Telegram, Signal ve Google Allo uygulamalarında şifreleme anahtarı değiştiği zaman bunu anlayabilen başarılı katılımcı sayıları Şekil 4. 7'de başarı yüzdeleri de Şekil 4. 8'de gösterilmektedir.

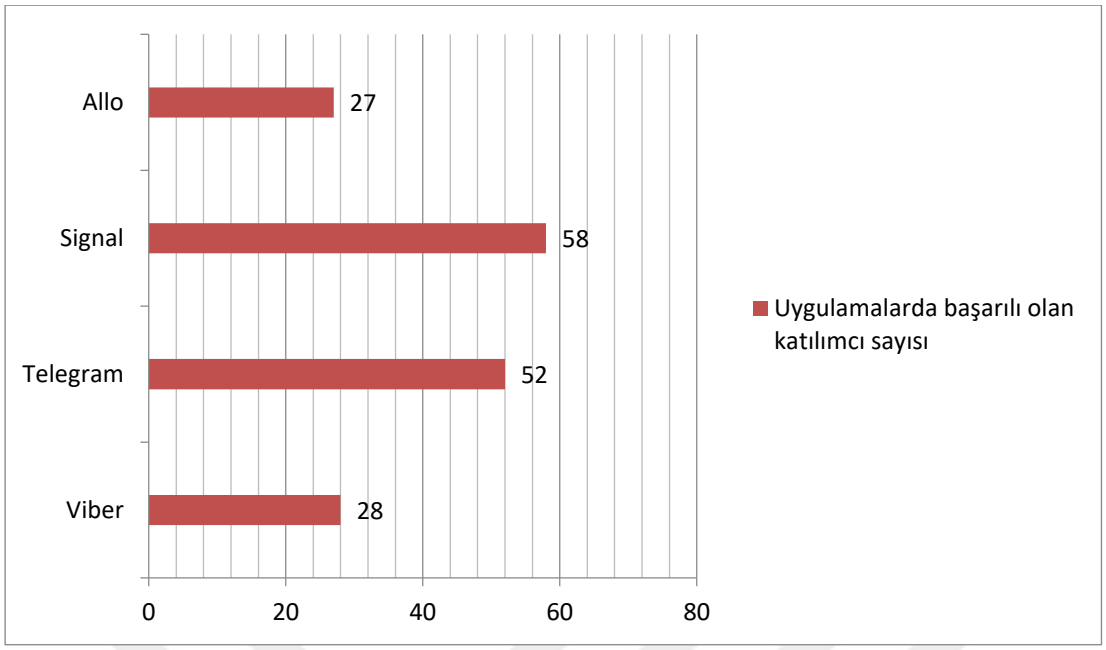


Şekil 4.7 : Bilgi güvenliği dersi öğrencilerinin uygulamalardaki anahtar doğrulama başarı sonuçları.

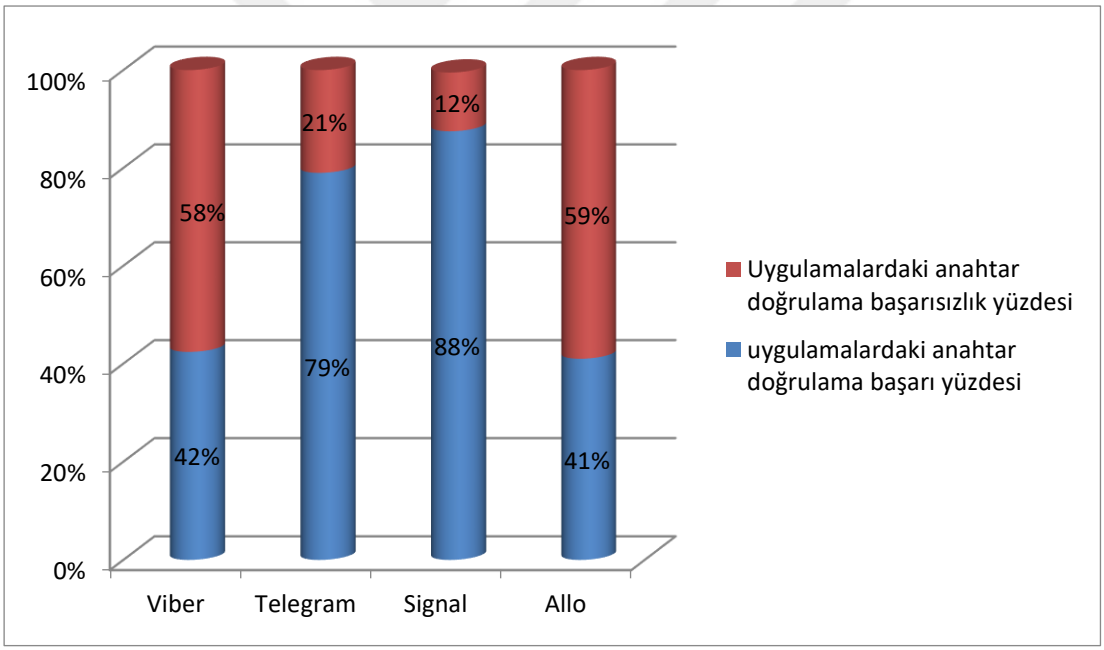


Şekil 4.8 : Bilgi güvenliği dersi öğrencilerinin uygulamalardaki anahtar doğrulama başarı yüzdeleri.

Tüm katılımcılardan (66 katılımcı) Viber uygulamasında sohbet sayfası dışında şifreleme anahtarının uyarısı verildiğini 14 grup bulabilmiştir. 19 grup ise anahtarın değiştiği uyarısını görememişlerdir. Tüm katılımcılardan 26 grup Telegram uygulamasında yeni sohbet sayfası açıldığı zaman şifreleme anahtarının değiştiğini düşünmüştür. Ayrıca Telegram uygulamasında şifreli mesajlaşma yaparken kapalı kilit simgesi bulunması katılımcıların şifreli mesajlaştıklarına ikna olmalarına neden olmaktadır. 7 grup ise Telegram'dan yeni sohbet sayfası açıldığı zaman şifreleme anahtarının değiştiğini anlayamamıştır. Tüm katılımcılardan 4 grup Signal uygulamasında şifreleme anahtarı değiştiği uyarı bildirimini sohbet ekranında görememiştir; 29 grup ise görebilmiştir. Tüm katılımcılardan Google Allo uygulamasında 27 katılımcı sohbet ekranında şifreleme anahtarının değiştiği bildirimini görmüştür; 39 katılımcı ise görememiştir. 66 katılımcının Viber, Telegram, Signal ve Allo uygulamalarında şifreleme anahtarı değiştiği zaman bunu anlayabilen başarılı katılımcı sayıları Şekil 4. 9'da başarı yüzdeleri de Şekil 4. 10'da gösterilmektedir.



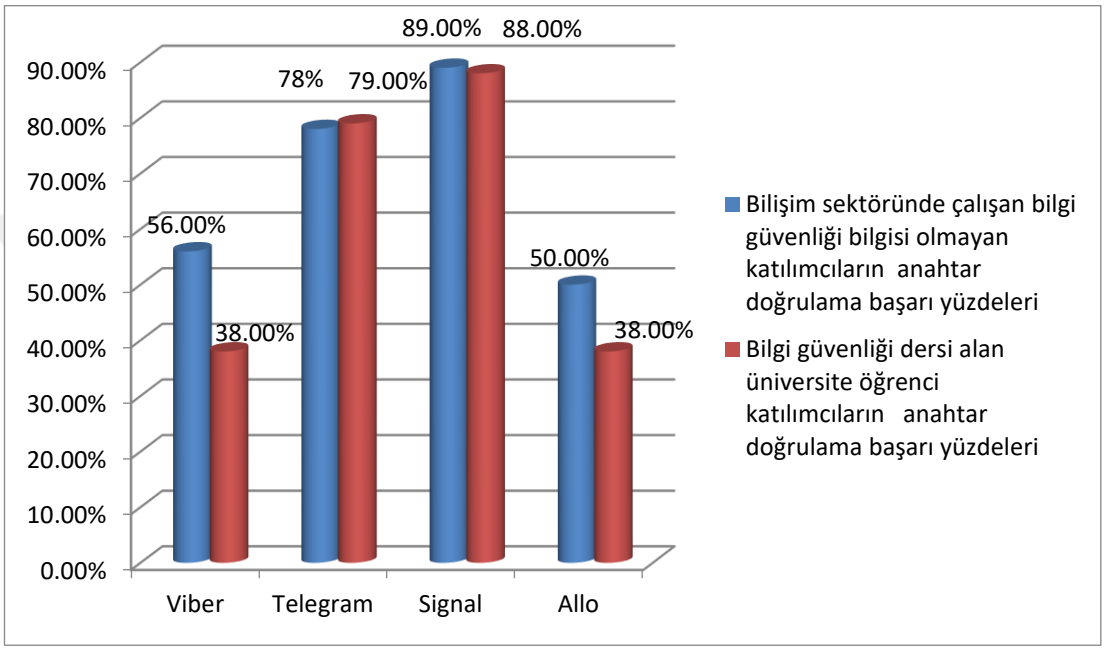
Şekil 4.9 : Tüm katılımcıların uygulamalardaki anahtar doğrulama başarı sonuçları.



Şekil 4.10 : Tüm katılımcıların uygulamalardaki anahtar doğrulama başarı yüzdeleri.

Bilişim sektöründe çalışan bilgi güvenliği bilgisi olmayan katılımcıların başarı yüzdeleri ile bilgi güvenliği dersi öğrencilerinin başarı yüzdeleri yan yana konulup değerlendirildiği zaman Signal ve Telegram uygulamalarında şifreleme anahtarının değiştiği bilgisinin daha kolay gözlemlenebildiği görülmektedir. Çizelge 4. 11'de uygulamalardaki başarı yüzdelerine bakıldığı zaman Telegram ve Signal uygulamalarında başarı oranları kullanıcıların bilişim sektöründe çalışıp bilgi

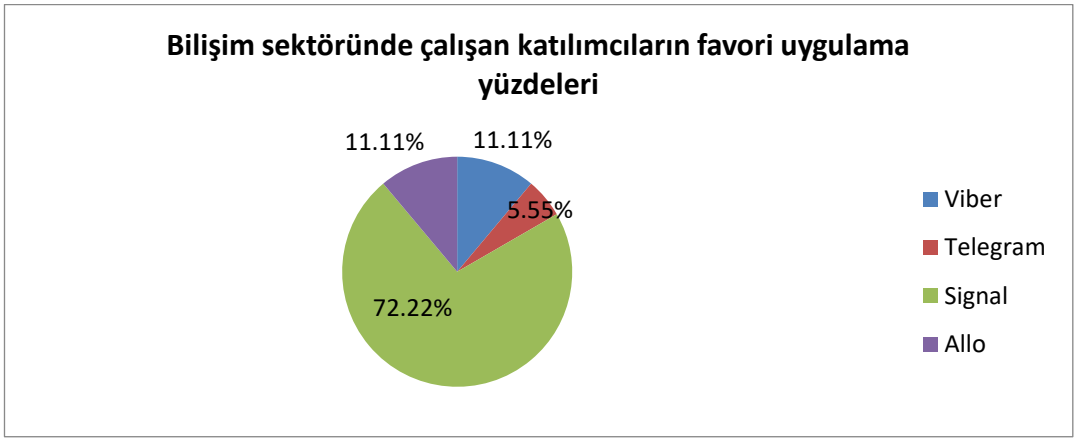
güvenliği dersi almayan ve bilgi güvenliği dersi öğrencileri arasında belirgin bir fark olmadığı gözlemlenmektedir. Viber uygulamasında başarı yüzdesi bilişim sektörü çalışanlarında; bilgi güvenliği dersini alan üniversite öğrencilerine göre daha yüksektir. Viber uygulamasındaki farkın oluşmasının her iki gruplardaki katılımcı sayısının farklı olduğundan kaynaklandığı düşünülmektedir. Allo uygulamasında çıkan farkın ise Android işletim sistemi kullanan ve kullanmayan katılımcı sayısından kaynaklandığı düşünülmektedir.



Şekil 4.11 : Bilişim sektöründe çalışan katılımcılar ile bilgi güvenliği dersi öğrencilerin anlık mesajlaşma uygulamaları anahtar doğrulama başarı yüzdeleri.

4.2.1 Katılımcıların favori uygulamaları

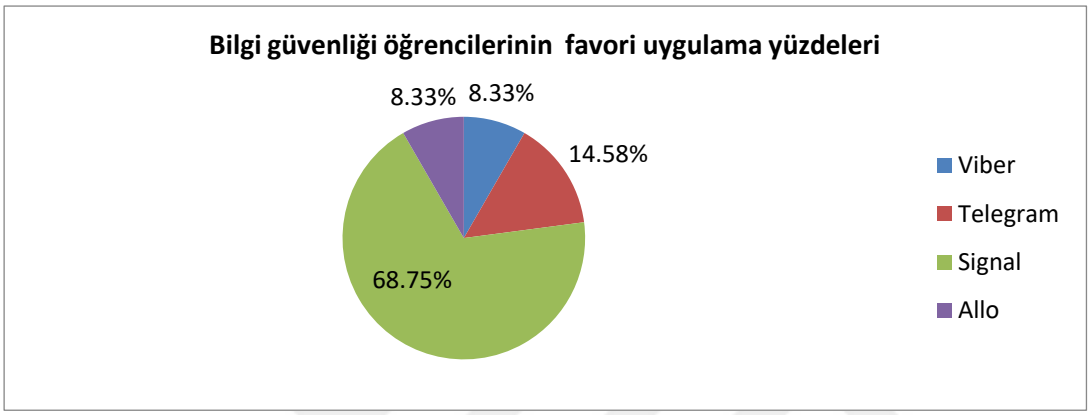
Bilişim sektöründe çalışan katılımcıların favori yüzdeleri Şekil 4. 12'de gösterilmiştir.



Şekil 4.12 : Bilişim sektöründe çalışan katılımcıların favori uygulama yüzdeleri.

Bilişim sektöründe çalışan katılımcılardan 13 tanesi Signal uygulamasını, 2 katılımcı Google Allo uygulamasını, 2 katılımcı Viber uygulamasını ve 1 katılımcı da Telegram uygulamasını favori uygulama seçmiştir.

Bilgi güvenliği dersi öğrencisi katılımcıların favori yüzdeleri Şekil 4. 13'de gösterilmiştir.

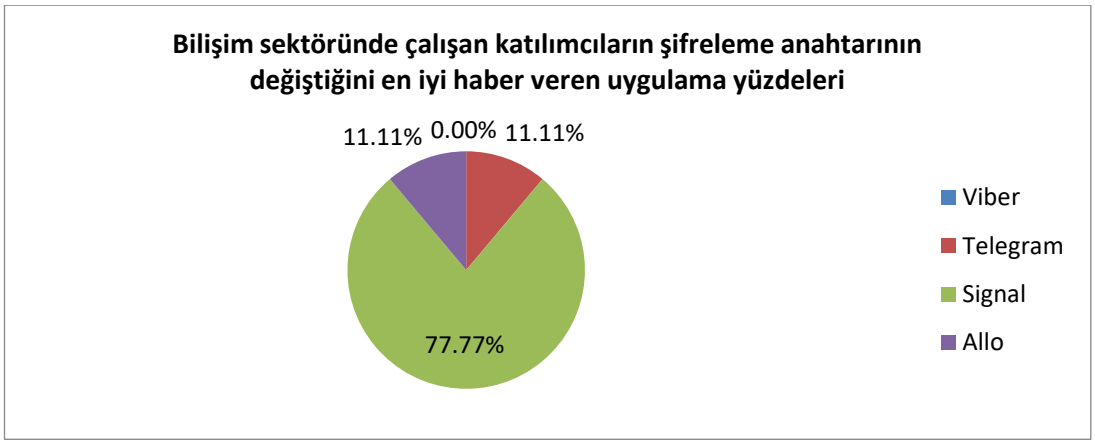


Şekil 4.13 : Bilgi güvenliği dersi öğrencilerinin favori uygulama yüzdeleri.

Bilgi güvenliği dersi öğrencilerinden 33 tanesi Signal uygulamasını, 4 tanesi Google Allo uygulamasını, 4 tanesi Viber uygulamasını ve 7 tanesi de da Telegram uygulamasını favori uygulama seçmiştir.

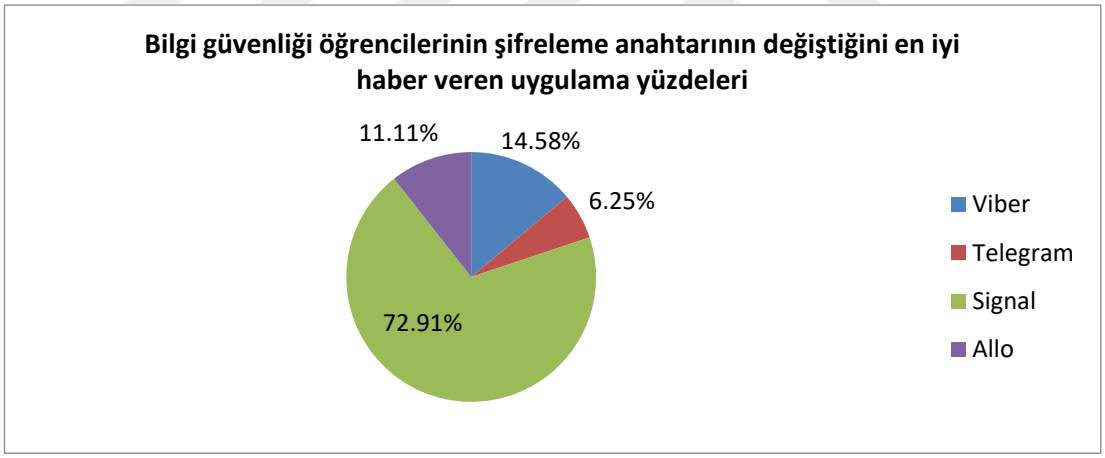
4.2.2. Şifreleme anahtarının değiştiğini en iyi haber veren uygulama

Bilişim sektöründe çalışan katılımcılardan 14 tanesi Signal uygulamasını, 2 katılımcı Google Allo uygulamasını, ve 2 katılımcı da Telegram uygulamasını şifreleme anahtarının değiştiğini en iyi haber veren uygulama seçmiştir. Viber uygulaması hiçbir katılımcı tarafından şifreleme anahtarının değiştiğini en iyi haber veren uygulama olarak seçilmemiştir. Bilişim sektöründe çalışan katılımcıların şifreleme anahtarının değiştiğini en iyi haber veren uygulama yüzdeleri Şekil 4. 14'da gösterilmiştir.



Şekil 4.14 : Bilişim sektöründe çalışan katılımcıların şifreleme anahtarının değiştiğini en iyi haber veren uygulama yüzdeleri.

Bilgi güvenliği dersi öğrencilerinden 35 tanesi Signal uygulamasını, 7 tanesi Viber uygulamasını, 3 tanesi Google Allo uygulamasını, ve 3 tanesi de Telegram uygulamasını şifreleme anahtarının değiştiğini en iyi haber veren uygulama seçmiştir. Bilgi güvenliği dersi öğrencisi katılımcıların şifreleme anahtarının değiştiğini en iyi haber veren uygulama yüzdeleri Şekil 4. 15'de gösterilmiştir.

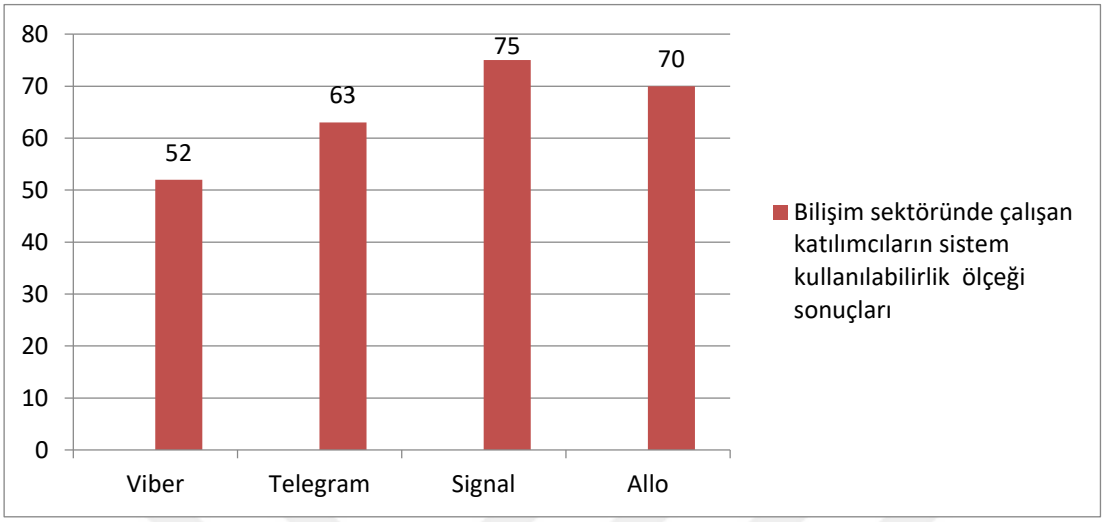


Şekil 4.15 : Bilgi güvenliği öğrencilerinin şifreleme anahtarının değiştiğini en iyi haber veren uygulama yüzdeleri.

4.3. Sistem Kullanılabilirlik Ölçeği Araştırması Sonuçları

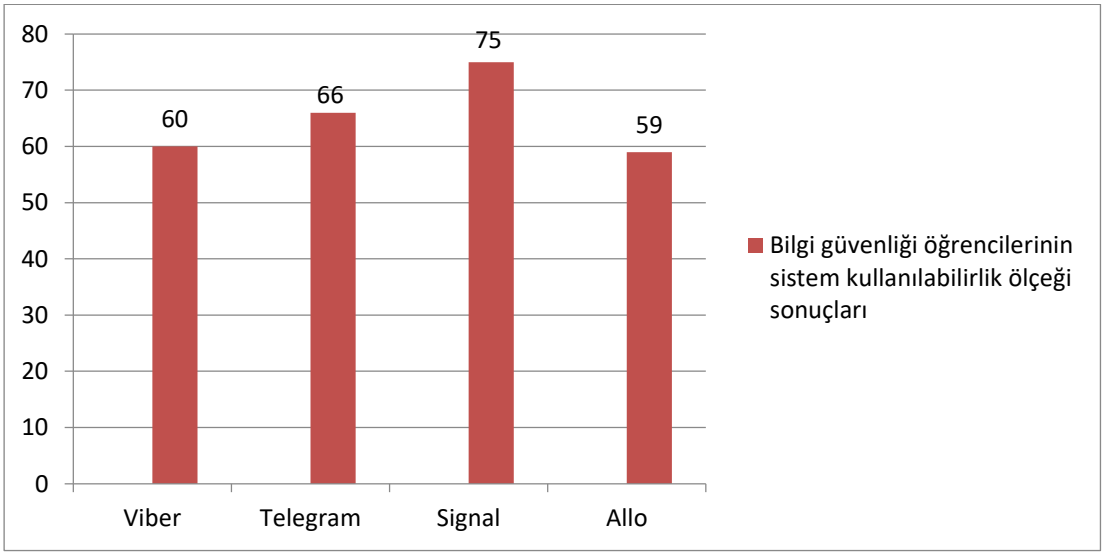
Bilişim sektöründe çalışan bilgi güvenliği bilgisi olmayan katılımcılara sistem kullanılabilirlik ölçeği (SUS) soruları cevaplandırılmıştır. Bilişim sektöründe çalışan

kullanıcıları sistem kullanılabilirlik ölçeği puanları Viber için 52, Telegram için 63, Signal için 75 ve Google Allo için 70'tir. Bu sonuçlar Şekil 4.16'da gösterilmiştir.



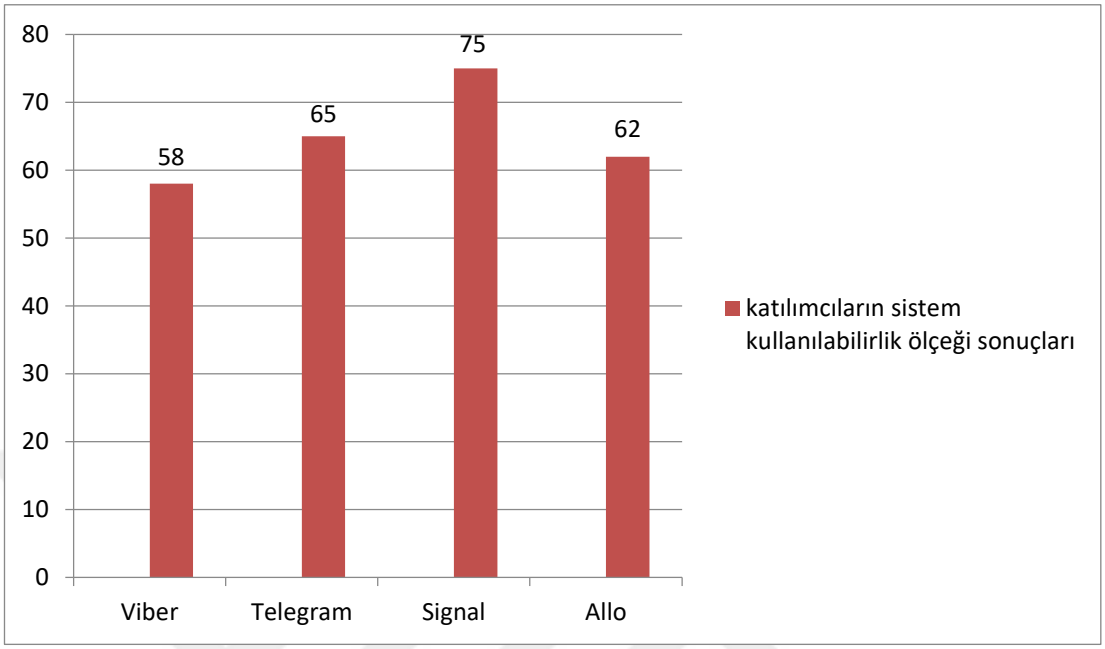
Şekil 4.16 : Bilişim sektöründe çalışan katılımcıların sistem kullanılabilirlik ölçeği sonuçları.

Bilgi güvenliği dersi öğrencileri sistem kullanılabilirlik ölçeği (SUS) sorularını cevaplamışlardır. Bilgi güvenliği öğrencisi katılımcıların sistem kullanılabilirlik ölçeği puanları Viber için 60, Telegram için 66, Signal için 75 ve Google Allo için ise 59'tir. Bu sonuçlar Şekil 4.17'de gösterilmiştir.



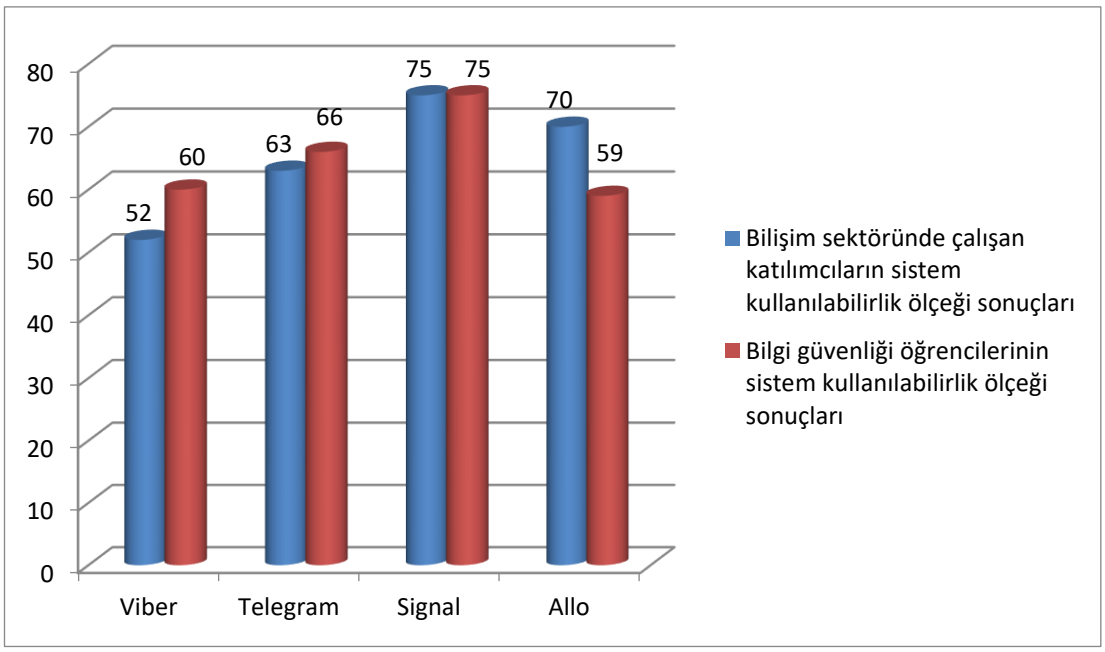
Şekil 4.17 : Bilgi güvenliği dersi öğrencilerinin sistem kullanılabilirlik ölçeği sonuçları.

Tüm katılımcıların sistem kullanılabilirlik ölçeği puanları Viber için 58, Telegram için 65, Signal için 75 ve Google Allo için ise 62'dir. Bu sonuçlar Şekil 4.18'de gösterilmiştir.



Şekil 4.18 : Tüm katılımcıların sistem kullanılabilirlik ölçeği sonuçları

Bilişim sektöründe çalışan katılımcılar ile bilgi güvenliği dersi öğrencilerinin sistem kullanılabilirlik ölçeği sonuçları yan yana değerlendirildiği zaman Şekil 4. 19 ortaya çıkmaktadır.



Şekil 4.19 : Bilişim sektöründe çalışan katılımcılar ile bilgi güvenliği öğrencilerin sistem kullanılabilirlik ölçeği sonuçları

Sistem kullanılabilirlik ölçeğine göre bilişim sektöründe çalışıp bilgi güvenliği bilgisi olmayan katılımcılar ile bilgi güvenliği öğrencileri en yüksek puanı Signal uygulamasına vermişlerdir. Her iki grup kullanıcı için Signal uygulaması 75 puan almıştır. Tullis ve arkadaşlarının kullandığı diğer ölçeklerle de değerlendirildiği zaman Signal uygulaması C üniversite notunu alarak iki grup içinde en kullanışlı güvenli mesajlaşma uygulaması seçilmiştir. En kullanışlı ikinci uygulama bilişim sektörü çalışanları ile üniversite öğrencileri arasında farklılık göstermektedir. Bu farklılığın sebebinin bilişim sektörü çalışanlarının daha fazla Android işletim sistemine sahip telefon kullanmalarından kaynaklandığı düşünülmektedir. Bilişim sektörü çalışanları Allo uygulamasına 70 puan vererek uygulamanın C geçer notu almasını sağlamışlardır. Viber uygulaması bilişim sektörü çalışanları tarafından 52 puan alarak en kullanışsız uygulama seçilmiştir. Google Allo uygulaması ise üniversite öğrencileri tarafından 59 puan alarak en kullanışsız uygulama olarak seçilmiştir.

5. SONUÇLAR

Bu tez çalışmasında popüler güvenli mesajlaşma uygulaması olan Viber, Telegram, Signal ve Google Allo uygulamalarında kimlik doğrulama ve şifreleme anahtarının değişmesi ile kullanıcı etkileşimi çalışması yapılmıştır. Bilişim sektöründe çalışan bilgi güvenliği ile ilgili bilgisi olmayan katılımcılar ve bilgi güvenliği dersi öğrencileriyle güvenli mesajlaşma uygulamalarında kimlik doğrulama işlemini bulmalarını incelemek ve mesajlaşma anahtarı değiştiği zaman katılımcıların bunu nasıl anladığını araştırmak için iki aşamalı bir araştırma çalışması yapılmıştır. Katılımcılardan ilk aşamada karşılıklı olarak mesajlaştığı kişinin doğru kişi olduğunu şifreleme anahtarını karşılaştırarak bulmaları beklenmiştir. Bunu doğrulamak için çiftler anahtarı QR kod ile tarama, göz ile doğrulama, arama ile doğrulama yöntemlerini kullanmışlardır. Kullanıcılar şifreleme anahtarlarını karşılaştırırken Signal uygulamasının kullandığı QR kod okutma yönteminin en pratik yöntem olduğunu belirtmişlerdir. Viber uygulamasının kullandığı uygulamada arama ile anahtar doğrulama işlemini ise pratik bulmamışlardır. Çalışmanın İkinci aşamasında çiftlerden bir tanesi dört uygulamayı silip ardından tekrar yüklemiştir. Bunun sonucunda her uygulamanın mesajlaşma anahtarı değişmiştir. Bu anahtarın değiştiğinin haberini kullanıcıya hangi şekilde haber verdiği araştırılmıştır. Signal uygulaması anahtar değiştiği bilgisini sohbet sayfasına yazarak bildirir. Signal uygulaması bu özelliğinden dolayı hem bilgi güvenliği dersi öğrencileri hem de bilişim sektöründe çalışan katılımcılar tarafından en kullanışlı uygulama, favori uygulama ve kullanıcıya anahtarın değiştiğini en açık ifade eden uygulama seçilmiştir. Bilişim sektöründe çalışan kullanıcıların büyük kısmının Android işletim sistemli telefon kullanmalarından kaynaklı olarak Allo uygulaması da bilişim sektörü çalışanları tarafından 2. en yüksek sistem kullanılabilirlik puanını almıştır. İki gruptan oluşan katılımcılardan bir grubun bilgi güvenliği dersini alıyor olmalarına rağmen şifreleme anahtarını doğrulama işlemlerinde tamamen başarılı olamamışlardır. Anahtar doğrulamanın manuel olarak gerçekleştirilmesi tüm katılımcılar tarafından zor olarak karşılanmıştır. Katılımcılar bilişim sektöründe

çalışmalarına veya bilgi güvenliği dersi almalarına rağmen manuel anahtar doğrulamada başarılı olamayabilmektedirler. Bu yüzden gelecekte CONIKS [27] tarzı çalışmaların pratiğe uygulanmasıyla kullanıcı memnuniyetinin artacağı beklenmektedir.

KAYNAKLAR

[1] https://towcenter.gitbooks.io/guide-to-chatapps/content/introductionthe_dawn_of/a_brief_history.html alındığı tarih:27.03.2018.

[2] Frosch T., Mainka C. "How Secure is TextSecure?" IEEE European Symposium on Security and Privacy, 2016.

[3] Blake S., Menezes W. "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol" International Workshop on Public Key Cryptography, 1999.

[4] Gordon K., Cremers C."A Formal Security Analysis of the Signal Messaging Protocol" IEEE European Symposium on Security and Privacy, 2017.

[5] Job J., Naresh V. "A modified secure version of the Telegram protocol (MTProto)" IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2015.

[6] Lee J., Choi R. "Security Analysis of End-to-End Encryption in Telegram" IEEE Symposium on Cryptography and Information Security Naha, 2017.

[7] Brooke J. "SUS — A Quick and Dirty Usability Scale. In Usability Evaluation in Industry." CRC Press,1996.

[8] Brooke J. "SUS: a retrospective" Usability Professionals' Association Bloomingdale, 2013.

[9] Tullis, T. S. & Stetson, J. N. "A Comparison of Questionnaires for Assessing Website Usability" Usability Professionals Association (UPA) Conference, 2004

[10] Chin J. P., Diehl V. A. "Development of an instrument measuring user satisfaction of the human-computer interface, Proceedings of ACM"

CHI '88 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1988

[11] Lewis J. "IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use" International Journal of Human-Computer Interaction,1995

[12] Whitten A., J. D. Tygar, J. N. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" In Proceedings of the 8th USENIX Security Symposium, 1999

[13] Ruoti S., Andersen J. "We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users" CHI Conference on Human Factors in Computing Systems, 2016

[14] Fahl S., Harbach M. "Helping Johnny 2.0 to Encrypt His Facebook Conversations" Symposium on Usable Privacy and Security, 2012

[15] Ruoti S., Roberts B. "Authentication Melee: A Usability Analysis of Seven Web Authentication Systems" International World Wide Web Conference, 2015

[16] https://developers.google.com/identity/protocols/OAuth2 alındığı tarih:27.03.2018.

[17] https://developer.mozilla.org/tr/docs/Mozilla/Persona alındığı tarih:27.03.2018.

[18] C. Robison, S. Ruoti "Private facebook chat " In International Conference on Privacy, Security, Risk and Trust and International Confernece on Social Computing, 2012.

[19] T. W. Horst and K. E. Seamons "Simple authentication for the web" In International Conference on Security and Privacy in Communications Networks and the Workshops, 2007.

[20] E. Hayashi, B. Pendleton "WebTicket: Account management using printable tokens" In SIGCHI Conference on Human Factors in Computing Systems, 2012.

[21] B. Dodson, D. Sengupta "Secure, consumer-friendly web authentication and payments with a phone" In International Conference on Mobile Computing, Applications, and Services, 2012.

[22] Sutikno T. , Handayani L. "WhatsApp, Viber and Telegram: which is the Best for Instant Messaging?" International Journal of Electrical and Computer Engineering, 2016.

[23] Tan J., Bauer L. "Can Unicorns Help Users Compare Crypto Key Fingerprints?" CHI Conference, 2017.

[24] Schroder S., Huber M. "When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging" 1st European Workshop on Usable Securit, 2016.

[25] Vaziripour E., Wu J. "Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications" Symposium on Usable Privacy and Security, 2017.

[26] Rosler P., Mainka C. "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema" 3rd IEEE European Symposium on Security and Privacy, 2018.

[27] Melara M. S., Blankstein A. "CONIKS: Bringing Key Transparency to End Users" 24th USENIX Security Symposium, 2015

[28] Laurie B., Kasper E. "Certificate Transparency" IETF RFC 6962, 2013

[29] https://security.googleblog.com/2017/01/security-through-transparency.html

[30] Bangor A., Kortum P "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale" Journal Of Usability Studies, 2009

[31] https://www.viber.com/ alındığı tarih:27.03.2018.

[32] https://github.com/DrKLO/Telegram alındığı tarih:27.03.2018.

[33] https://signal.org/ alındığı tarih:27.03.2018.

[34] https://allo.google.com/ alındığı tarih:27.03.2018.

[35] Diffie W., Hellman M. "New directions in cryptography" IEEE Transactions on Information Theory, 1976

[36] https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ alındığı tarih:27.03.2018.

[37] https://signal.org/docs/specifications/doubleratchet/ alındığı tarih:22.04.2018.

[38] https://signal.org/docs/specifications/x3dh/ alındığı tarih:22.04.2018.

[39] https://core.telegram.org/api/end-to-end alındığı tarih:22.04.2018.

[40] https://core.telegram.org/mtproto/security_guidelines alındığı tarih:22.04.2018.

EKLER:

EK 1: Kişisel Araştırma Soruları
EK 2: Uygulama Soruları
EK 3: Sistem Kullanılabilirlik Soruları

EK 1: Kişisel Sorular

1-Yaş aralığınız nedir?

☐16-17
☐18-24
☐25-34
☐35-45
☐46-64

2-Aşağıdaki anlık mesajlaşma uygulamalardan hangisi veya hangilerini duydunuz?

☐Whatsapp
☐Line
☐Chatsecure
☐Signal
☐Telegram
☐Threema
☐Allo
☐iMessage
☐Skype
☐Viber
☐Wickr
☐Silent
Başka anlık mesajlaşma uygulamaları duyduysanız lütfen buraya yazınız: ...

EK 2: Uygulama Soruları

BİLGİ: Telegram, Signal, Viber ve Allo anlık mesajlaşma uygulamaları güvenlik anahtarlarına sahip 4 farklı uygulamadır. Güvenlik anahtarları uygulamayı silip tekrar yüklendiği zaman değişmektedir. Biz anlık mesajlaşma uygulamalarında anahtar değişirse kullanıcıya nasıl haber verildiğini araştırmak istiyoruz. Bunun için telefonunuza üç uygulamayı yüklemek için yeterli alana sahip olduğundan emin olunuz ve ikili gruplar aşağıdaki adımları takip ediniz:

A-Viber uygulamasında karşılıklı kimlik doğrulaması yapılması.

1- Viber uygulamasında kimlik doğrulamasını hangi yöntemle yaptınız?

☐QR kod okutma
☐ Gözle karşılaştırma
☐Arama ile karşılaştırma
☐Diğer(Açıklama Giriniz)…

Viber uygulamasıyla sürekli güvenli mesajlaştığınıza emin olduktan sonra çiftlerden bir tanesi Viber uygulamasını silmeli ve tekrar yüklemeli.

2- Viber uygulaması size mesajlaşma anahtarının değiştiğinin haberini verdi mi?

☐ Evet
☐ Hayır

3- Viber uygulaması silinip tekrar yüklendiği zaman güvenli haberleştiğinizi nasıl anladınız?

☐ Güvenlik anahtarını gözle kontrol ettim
☐ Güvenlik anahtarını QR kod ile karşılaştırdım
☐ Güvenlik anahtarını arama ile karşılaştırdım
☐ Diğer(Açıklama Giriniz)…

4- Viber uygulamasının mesajlaşma anahtarı doğrulama için sizi yönlendirmesi yeterli mi?

☐ Evet
☐ Hayır

Sistem uygulanabilirlik ölçeğinizin ilgili alanlarını doldurunuz.

B- Telegram uygulamasında karşılıklı kimlik doğrulaması yapılması.

1- Telegram uygulamasında kimlik doğrulamasını hangi yöntemle yaptınız?

☐QR kod okutma
☐ Gözle karşılaştırma
☐Arama ile karşılaştırma
☐Diğer(Açıklama Giriniz)…

Telegram uygulamasıyla sürekli güvenli mesajlaştığınıza emin olduktan sonra çiftlerden bir tanesi Telegram uygulamasını silmeli ve tekrar yüklemeli.

2- Telegram uygulaması size mesajlaşma anahtarının değiştiğinin haberini verdi mi?

☐ Evet
☐ Hayır

3- Telegram uygulaması silinip tekrar yüklendiği zaman güvenli haberleştiğinizi nasıl anladınız?

☐ Güvenlik anahtarını gözle kontrol ettim
☐ Güvenlik anahtarını QR kod ile karşılaştırdım
☐ Güvenlik anahtarını arama ile karşılaştırdım
☐ Diğer(Açıklama Giriniz)…

4- Telegram uygulamasının mesajlaşma anahtarı doğrulama için sizi yönlendirmesi yeterli mi?

☐ Evet
☐ Hayır

Sistem uygulanabilirlik ölçeğinin ilgili alanlarını doldurunuz.

C- Signal uygulamasında karşılıklı kimlik doğrulaması yapılması.

1- Signal uygulamasında kimlik doğrulamasını hangi yöntemle yaptınız?

☐QR kod okutma
☐ Gözle karşılaştırma
☐Arama ile karşılaştırma
☐Diğer(Açıklama Giriniz)…

Signal uygulamasıyla sürekli güvenli mesajlaştığınıza emin olduktan sonra çiftlerden bir tanesi Signal uygulamasını silmeli ve tekrar yüklemeli.

2- Signal uygulaması size mesajlaşma anahtarının değiştiğinin haberini verdi mi?

☐ Evet
☐ Hayır

3- Signal uygulaması silinip tekrar yüklendiği zaman güvenli haberleştiğinizi nasıl anladınız?

☐ Güvenlik anahtarını gözle kontrol ettim
☐ Güvenlik anahtarını QR kod ile karşılaştırdım
☐ Güvenlik anahtarını arama ile karşılaştırdım
☐ Diğer(Açıklama Giriniz) …

4- Signal uygulamasının mesajlaşma anahtarı doğrulama için sizi yönlendirmesi yeterli mi?

☐ Evet
☐ Hayır

Sistem uygulanabilirlik ölçeğinin ilgili alanlarını doldurunuz.

D- Allo uygulamasında karşılıklı kimlik doğrulaması yapılması.

1- Allo uygulamasında kimlik doğrulamasını hangi yöntemle yaptınız?

☐QR kod okutma
☐ Gözle karşılaştırma
☐Arama ile karşılaştırma
☐Diğer(Açıklama Giriniz) …

Allo uygulamasıyla sürekli güvenli mesajlaştığınıza emin olduktan sonra çiftlerden bir tanesi Signal uygulamasını silmeli ve tekrar yüklemeli.

2- Allo uygulaması size mesajlaşma anahtarının değiştiğinin haberini verdi mi?

☐ Evet
☐ Hayır

3- Allo uygulaması silinip tekrar yüklendiği zaman güvenli haberleştiğinizi nasıl anladınız?

☐ Güvenlik anahtarını gözle kontrol ettim
☐ Güvenlik anahtarını QR kod ile karşılaştırdım
☐ Güvenlik anahtarını arama ile karşılaştırdım
☐ Diğer(Açıklama Giriniz) …

4- Allo uygulamasının mesajlaşma anahtarı doğrulama için sizi yönlendirmesi yeterli mi?

☐ Evet
☐ Hayır

Sistem uygulanabilirlik ölçeğinin ilgili alanlarını doldurunuz.

E- Kullandığınız dört uygulamadan hangisi mesajlaşma anahtarının doğrulamasında en açık şekilde sizi yönlendirdi?

☐Viber
☐Telegram
☐Signal
☐Allo

F- Şifreli mesajlaşma yapmanız gerektiği zaman kullanım kolaylığı açısından kullandığınız bu dört uygulamadan hangisini seçersiniz?

☐Viber
☐Telegram
☐Signal
☐Allo

EK 3: Sistem Kullanılabilirlik Ölçeği Soruları

BİLGİ: Sistem kullanılabilirlik ölçeği 10 sorudan oluşmaktadır. Sorulara 1 ve 5 arasında puan verilmesi beklenmektedir. Eğer soruya verebileceğiniz bir cevap yok ise 3 verilmesi beklenmektedir. Puan anlamlandırılması aşağıda açıklanmıştır.

1 -> Kesinlikle Katılmıyorum
2 -> Katılmıyorum
3 -> Kararsızım
4 -> Katılıyorum
5 -> Kesinlikle Katılıyorum

Telegram için;

1. Bu sistemi sık sık kullanmak isterim.

2. Sistemi gereksiz derecede karmaşık buldum.

3. Sistemin kullanımının kolay olduğunu düşündüm.

4. Bu sistemi kullanabilmek için teknik bir kişinin desteğine ihtiyacım olacağını düşünüyorum.

5. Bu sistemdeki çeşitli işlevlerin iyi entegre olduğunu keşfettim.

6. Bu sistemde tutrsızlığın çok fazla olduğunu düşündüm.

7. Çoğu kişinin bu sistemi çok hızlı bir şekilde kullanmayı öğreneceğini düşünüyorum.

8. Sistemi çok hantal buldum.

9. Sistemi kullanarak kendimi çok güvende hissettim.

10. Bu sisteme başlamadan önce çok şey öğrenmeliydim.

Signal için;

1. Bu sistemi sık sık kullanmak isterim.

2. Sistemi gereksiz derecede karmaşık buldum.

3. Sistemin kullanımının kolay olduğunu düşündüm.

4. Bu sistemi kullanabilmek için teknik bir kişinin desteğine ihtiyacım olacağını düşünüyorum.

5. Bu sistemdeki çeşitli işlevlerin iyi entegre olduğunu keşfettim.

6. Bu sistemde tutrsızlığın çok fazla olduğunu düşündüm.

7. Çoğu kişinin bu sistemi çok hızlı bir şekilde kullanmayı öğreneceğini düşünüyorum.

8. Sistemi çok hantal buldum.

9. Sistemi kullanarak kendimi çok güvende hissettim.

10. Bu sisteme başlamadan önce çok şey öğrenmeliydim.

Viber için;

1. Bu sistemi sık sık kullanmak isterim.

2. Sistemi gereksiz derecede karmaşık buldum.

3. Sistemin kullanımının kolay olduğunu düşündüm.

4. Bu sistemi kullanabilmek için teknik bir kişinin desteğine ihtiyacım olacağını düşünüyorum.

5. Bu sistemdeki çeşitli işlevlerin iyi entegre olduğunu keşfettim.

6. Bu sistemde tutrsızlığın çok fazla olduğunu düşündüm.

7. Çoğu kişinin bu sistemi çok hızlı bir şekilde kullanmayı öğreneceğini düşünüyorum.

8. Sistemi çok hantal buldum.

9. Sistemi kullanarak kendimi çok güvende hissettim.

10. Bu sisteme başlamadan önce çok şey öğrenmeliydim.

Google Allo için;

1. Bu sistemi sık sık kullanmak isterim.

2. Sistemi gereksiz derecede karmaşık buldum.

3. Sistemin kullanımının kolay olduğunu düşündüm.

4. Bu sistemi kullanabilmek için teknik bir kişinin desteğine ihtiyacım olacağını düşünüyorum.

5. Bu sistemdeki çeşitli işlevlerin iyi entegre olduğunu keşfettim.

6. Bu sistemde tutrsızlığın çok fazla olduğunu düşündüm.

7. Çoğu kişinin bu sistemi çok hızlı bir şekilde kullanmayı öğreneceğini düşünüyorum.

8. Sistemi çok hantal buldum.

9. Sistemi kullanarak kendimi çok güvende hissettim.

10. Bu sisteme başlamadan önce çok şey öğrenmeliydim.

ÖZGEÇMİŞ

Ad-Soyad : Gamze AKMAN

Uyruğu : T.C.

Doğum Tarihi ve Yeri : 1991, ANKARA

E-posta : gakman@etu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans** : 2014, Hacettepe Üniversitesi, Bilgisayar Mühendisliği
- **Yüksek Lisans** : 2018, TOBB ETÜ, Bilgisayar Mühendisliği

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	Yer	Görev
2015	Aselsan	Yazılım Tasarım Mühendisi

YABANCI DİL: İngilizce

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Akman G., Selcuk A. A.** Güvenli Mesajlaşma Uygulamalarında Kimlik Doğrulama ve Kullanılabilirlik, SIU 2018

DİĞER YAYINLAR, SUNUMLAR VE PATENTLER:

• **I. Karabey, G. Akman** A cryptographic approach for secure client - server chat application using public key infrastructure (PKI) 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).