KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

METİN TABANLI GÜVENLİK KODLARIN MOBİL ARA YÜZLERDE KULLANILABİLİRLİK VE GÜVENLİK KARŞILAŞTIRMASI

NUR MERDANOĞLU

KOCAELİ 2020

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

METİN TABANLI GÜVENLİK KODLARIN MOBİL ARA YÜZLERDE KULLANILABİLİRLİK VE GÜVENLİK KARŞILAŞTIRMASI

NUR MERDANOĞLU

Dr. Öğr. Üyesi Pınar ONAY DURDU
Danışman, Kocaeli Üniversitesi .....

Doç. Dr. Ahmet SAYAR
Jüri Üyesi, Kocaeli Üniversitesi .....

Dr. Öğr. Üyesi Yasemin KARAGÜL
Jüri Üyesi, Doğuş Üniversitesi .....

Tezin Savunulduğu Tarih: 03.01.2020

ÖNSÖZ VE TEŞEKKÜR

Gelişen teknoloji ile birlikte sistem geliştiricileri ve tasarımcıları kullanıcılar için hem kullanılabilir olan hem de güvenlik düzeyi yüksek sistemler oluşturma gayretindedir. Günümüzde özellikle mobil cihaz kullanımının hızla artması ile birlikte mobil cihazlarda kullanılan ara yüzlerin kullanılabilirlik ve güvenlik düzeyinin sağlanması ve dengelenmesi zorunlu hale gelmiştir.

Tez çalışması kapsamında mobil cihazlarda kullanılmak üzere metin tabanlı güvenlik kod türlerinin etkililik, verimlilik ve memnuniyet faktörlerine göre karşılaştırılmasına yönelik olarak deneysel bir kullanıcı testi çalışması yapılmıştır. Kullanıcı çalışmasından elde edilen bulgular aynı zamanda güvenlik kodların sağlamlığı ve kullanılabilirliği ile ilgili gerçekleştirilmiş önceki çalışmalarda da raporlanan çeşitli tavsiyeler ile birleştirilerek mobil ara yüz geliştiricilere yol gösterecek tavsiyeler oluşturulmuştur.

Çalışma kapsamında gerçekleştirilen kullanıcı çalışması deneyine katılan gönüllü katılımcılara teşekkürlerimi sunarım.

Çalışmam boyunca benden yardımını esirgemeyen ve sabırla bana destek olan ailem ve değerli danışman hocam Dr.Öğr Üyesi Sayın Pınar ONAY DURDU' ya ve tez savunmamda yer alan jüri üyeleri, Doç. Dr. Ahmet SAYAR ve Dr. Öğr. Üyesi Yasemin KARAGÜL'e teşekkürlerimi bir borç bilirim.

Ocak – 2020 Nur MERDANOĞLU

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

Sn : Saniye

Kısaltmalar

CAPTCHA	: Completely Automated Public Turing test to tell Computers and Humans Apart(İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi)
HIP	: Human Interaction Proof(İnsan Etkileşim Kanıtı)
İBE	: İnsan Bilgisayar Etkileşimi
OCR	: Optical Character Recognition(Optik Karakter Tanıma)
NASA-TLX	: NASA Task Load Index (NASA Zihinsel İş Yükü)
T-CSUQ	: Turkish version of Computer System Usability Questionnaire (Bilgisayar Sistemi Kullanılabilirlik Anketi Türkçe Sürümü)

METİN TABANLI GÜVENLİK KODLARIN MOBİL ARA YÜZLERDE KULLANILABİLİRLİK VE GÜVENLİK KARŞILAŞTIRMASI

ÖZET

Kullanıcılar açısından mobil ara yüzlerde hem güvenlik hem de kullanılabilirlik ihtiyaçlarını dengeli bir şekilde karşılayacak güvenlik kod mekanizmalarının kullanılması oldukça önemlidir.

Tez çalışması kapsamında mobil cihazlarda kullanılmak üzere farklı güvenlik özelliklerindeki metin tabanlı güvenlik kod türlerinin hem güvenlik açısından sağlamlığı test edilmiş hem de kullanılabilirlik açısından deneyler için geliştirilen mobil uygulama, T-CSUQ, NASA-TLX ve kullanıcı tercih sıralaması anketinden elde edilen verilerle etkililik, verimlilik ve memnuniyet faktörlerine göre karşılaştırılması deneysel bir kullanıcı testi ile gerçekleştirilmiştir. Kullanıcı testi için bozulma uygulanmış, bozulma uygulanmamış, sözlük kelime, rastgele kelime, renk ayrımı az ve renk ayrımı çok güvenlik kodlar olacak şekilde altı farklı güvenlik kod belirlenmiştir. Belirlenen güvenlik kodların güvenlik açısından sağlamlığını değerlendirmeye yönelik olarak çalışmanın birinci aşamasında güvenlik testleri uygulanmıştır. Güvenlik testleri sonrasında altı farklı güvenlik kod türü ile farklı yaş, cinsiyet ve deneyime sahip 30 katılımcı ile kullanıcı testleri gerçekleştirilmiştir. Güvenlik testlerine göre sağlamlığı yüksek olan güvenlik kodlar sırasıyla bozulma uygulanmış, rastgele kelime ve renk ayrımı az güvenlik kod türleri olmuştur. Kullanıcı testleri sonrasında ise güvenlik testlerine göre sağlamlığı yüksek olan güvenlik kodlar arasından en kullanılabilir olan tür rastgele kelime güvenlik kod türü olmuştur. Böylece, mobil uygulama geliştiricileri ara yüzleri tasarlarken rastgele kelime güvenlik kodu kullanmayı tercih ettiklerinde, dengeli bir güvenlik ve kullanılabilirlik seviyesinin sağlanabileceği tespit edilmiştir. Kullanıcı çalışmasından elde edilen bulgular ile alan yazında ilgili çalışmalarda raporlanan konular birleştirilerek, mobil ara yüz geliştiricilere yol gösterecek tavsiyeler oluşturulmuştur.

Anahtar Kelimeler: Güvenlik, Güvenlik Kod, İnsan Etkileşim Kanıtı, Kullanılabilirlik, Kullanılabilirlik Analizi.

SECURITY AND USABILITY COMPARISON OF TEXT BASED CAPTCHA ON MOBILE INTERFACE

ABSTRACT

It is very essential to use CAPTCHA designs that will meet both security and usability needs of users in a balanced way in mobile interfaces.

In the scope of the thesis, first the robustness of the text-based CAPTCHA types to be used in mobile devices was tested in terms of security, and then their efficiency, effectiveness and satisfaction were compared in terms of usability by an experimental user study in which efficiency and effectiveness data was gathered by a mobile application developed and satisfaction data was gathered by T-CSUQ, NASA-TLX and user preference ranking surveys. Six different text-based CAPTCHA types, which were distortion-based, non-distortion-based, dictionary based, random based, little contrast and full contrast, were compared. In the first phase, security tests were applied. Afterwards, user tests were conducted with 30 participants of different age, gender and experience. According to security test results, distortion, little contrast and random based CAPTCHA types were determined to be more robust respectively. The most usable CAPTCHA type among the secure CAPTCHA types was determined as random based CAPTCHA based on the user test results. Thus, it has been found that a balanced level of security and usability can be achieved when mobile application developers choose to use random word CAPTCHA when designing interfaces. Recommendations to guide mobile interface developers were provided based on the findings obtained both from the user study and previous relevant literature.

Keywords: Security, CAPTCHA, Human Interaction Proof**,** Usability, Usability Analysis.

GİRİŞ

Günümüzde bilgi ve iletişim teknolojilerinin de gelişmesiyle pek çok kullanıcı Internet ve web tabanlı uygulamaları günlük pek çok işi için yaygın bir şekilde kullanmaktadır. Özellikle çevrim içi bankacılık, e-ticaret ya da sosyal medya gibi uygulamaların kullanımları sırasında kişilerin ve kişilere ait bilgilerin çeşitli çevrim içi saldırılara maruz kalmamasının sağlanması, yani güvenlik önemli bir konu haline gelmiştir. Özellikle web sitelerine güvenli erişim sağlamak amaçlı olarak kimlik doğrulama ve yetkilendirme yöntemleri uygulanmaktadır. Bunların yanında insan ve bilgisayarlar arasında ayrım yapabilmeyi sağlamak da gerekmektedir. Çünkü, bot adı verilen, tıpkı insan gibi davranış gösteren çeşitli zararlı otomatik yazılımlar bulunmaktadır. Bot'lar web sitelerinde kullanıcının isteği dışında çeşitli tıklamalarda bulunarak uygulamalar çalıştırılabilmekte ya da otomatik tıklamalar ile web sitesinde istenmeyen noktalara yönlendirme yapabilmektedir. Spam ya da virüs göndererek servis kesintilerine (DoS - Denial of Service) yol açma da botlar tarafından gerçekleştirilen çeşitli saldırılardan bazılarıdır.

Özellikle bu tip bot saldırılarından korunmak için web sitelerinde insan etkileşim kanıtı (HIP – Human Interaction Proof) mekanizmaları kullanılmaktadır. Bu mekanizmaların başında Güvenlik kod (CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart - İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) (vonAhn vd.,2004) gelmektedir. Güvenlik kod karşısındakinin insan ya da bilgisayar olup olmadığını otomatik tespit etmeye yönelik olarak en yaygın kullanılan insan etkileşim kanıtıdır. Web siteleri ve çevrim içi servisleri çeşitli ataklardan özellikle de otomatik zararlı bilgisayar programlarından (bot) korumak için geliştirilmiştir (vonAhn vd., 2004). Güvenlik kod mekanizmaları, gerçek kullanıcıların bu sınama-yanıt doğrulama testinden rahatlıkla geçerken bilgisayar programlarının zorlanarak geçemeyeceği varsayımına dayanmaktadır (vonAhn vd., 2004).Kullanıcılar açısından hem güvenlik hem de kullanılabilirlik

ihtiyaçlarını dengeli bir şekilde karşılayacak güvenlik kod mekanizmalarının oluşturulması gerekmektedir (Belk vd., 2015). Çünkü güvenlik kod testlerinin zorluğunu artırmak uygulamaların güvenlik mekanizmasını arttırırken kullanılabilirliğini azalmaktadır (Bursztein vd., 2011, 2014; Golle, 2008). Alan yazında güvenlik kod mekanizmalarını kullanılabilirlik ve güvenlik boyutları ile inceleyen çeşitli çalışmalar vardır ancak bunların da genellikle boyutlardan birine daha fazla önem verdiği görülmektedir. Güvenlik kodun güvenlik düzeyi, otomatik ataklara karşı olan sağlamlığına bağlı olarak ölçülürken, kullanılabilirliği ise kullanıcının güvenlik kodunu kolaylıkla çözebilmesi ile ilişkili olarak ölçülmektedir (Chow vd., 2017).

Kullanılabilirlik kavramı, ISO (1998) tarafından "bir ürünün, belirli bir kullanıcı grubu tarafından belirli bir kullanım bağlamında etkili, verimli ve memnuniyet verici şekilde kullanım amaçlarına ulaşmayı ne ölçüde sağladığı" olarak tanımlanmaktadır. Ayrıca Nielsen (1994) kullanılabilirliği anlaşılabilirlik, verimlilik, hatırlanabilirlik, hatasızlık ve memnuniyet gibi beş temel bileşen ile açıklamaktadır. Diğer taraftan güvenlik ile ilgili tanımlar ise daha çok saldırganlar ile ilişkilendirilmekte (Kainda vd., 2010; Braz ve Robert, 2006) ve gizlilik, bütünlük ve erişilebilirlik kavramları ile açıklanmaktadır (Bishop, 2003). Güvenlik beklenmeyen davranışların olmasını engellemek için kullanıcıya esneklik sunmada zorlayıcı olurken, kullanılabilirlik istenen davranışı kullanıcıya sunmak için kolaylıklar tanır (Flechais, 2005). Kullanılabilir bir sistem beklenmeyen hataların olmasını minimize ederken, güvenli bir sistem beklenmeyen davranışların engellenmesi ve yok edilmesi amacını taşır (Kainda vd., 2010). Bu bakış açısı ile kullanılabilirlik ve güvenlik konularının birbirini destekleyecek şekilde sağlanması önemlidir.

Güvenlik amaçlı kullanılan güvenlik kod mekanizmaları için günümüzde pek çok şema tanımlanmıştır. Bunun nedeni güvenlik artırıcı tanımlanan her şema kısa bir süre sonra çözümlenebilir hale gelmektedir. Geliştiriciler her zaman daha sağlam bir şema üretme yoluna gitmektedir. Şemaların çeşitli ataklara dayanıklı olmasının yanında aynı zamanda kullanıcılar tarafından da kolay anlaşılır olmasının sağlanması kullanılabilirlik açısından gereklidir (Chow ve Susilo, 2017). Günümüzde en yaygın kullanımı bulunan güvenlik kod şemaları metin tabanlı (text-based) ve görüntü-tabanlı

(image-based) güvenlik kodlardır (Wismer, vd., 2012). Metin-tabanlı güvenlik kodlar yaygın kullanımlarının yanında metin bölümleme kullanarak kolayca saldırıya uğrayabilmektedirler (Chellapilla, Larson, Simard, ve Czerwinski, 2005). Görüntü-tabanlı güvenlik kodlar ise kullanıcı ve bilgisayar arasındaki etkileşimi kısaltırken daha fazla ekran alanı, daha fazla sunucu işlemi ve geniş kapsamlı bir görüntü veri tabanı gerektirmektedir (Chow, vd., 2008).

Güvenlik kod mekanizmalarında kullanılabilirlik önemli olduğu kadar güvenliğin de sağlanması gerekmektedir. Her sistemde olduğu gibi güvenlik kod sistemleri de çeşitli ataklara maruz kalabilmektedir. Atakları önlemek ve güvenlik düzeyini artırmak adına önerilen çeşitli yöntemler vardır. Örneğin metin-tabanlı güvenlik kodlarda renk kullanımında arka fon ile öndeki metnin birbirine yakın kullanılması ile zararlı programların ayrım yapmasını ve harfleri tanımasını zorlaştırılarak örüntü tanıma atağı oranının azaltılabileceği önerilmektedir (Beheshti ve Liahsis, 2015). Kullanılan karakter setlerinin geniş tutulması ve metinlerin uzunluğunun artırılması yöntemleri ile kelimelerin tahmin edilmesi zorlaştırılarak kaba kuvvet saldırısının başarılı olma (Random guessing attack) oranı azaltılabilmektedir (Yan ve El Ahmad, 2008). Ayrıca sözlük kelimelerine bozunma uygulanması (distortion), harflerin arasına çeşitli karakter ya da çizgi eklenmesi ile de sözlük atağının azaltılabilmesi sağlanabilir (Kaur ve Behal, 2014).

Güvenlik kod mekanizmalarının kullanılabilirlik veya güvenlik boyutlarının değerlendirilmesine yönelik çeşitli çalışmalar mevcuttur (Behesti ve Liatsis, 2015; Kaur ve Behal, 2014; Reynaga, Chiasson ve Oorschot, 2015; Chow, Susilo ve Thorncharoensri, 2019). Çalışmaların pek çoğu geleneksel masaüstü uygulamalardaki ara yüzlerdeki değerlendirmeleri içermekte mobil ara yüzler üzerinde değerlendirme yapan çalışma sayısı kısıtlı kalmaktadır. Bu nedenle bu çalışma kapsamında mobil ara yüzlerde kullanılan farklı türlerdeki metin-tabanlı güvenlik kodların kullanılabilirlik açısından kullanıcı testleri ile karşılaştırılması sağlanmıştır. Yaygın kullanımı bulunması ve mobil ara yüzler için ekran alanını daha az kaplayan bir tür olması nedeniyle çalışma 6 farklı türdeki metin-tabanlı güvenlik kod ile gerçekleştirilmiştir. Ayrıca güvenlik kodların kullanılabilirliği ve sağlamlığına yönelik olarak gerçekleştirilen araştırmalara yönelik olarak gerçekleştirilen alan yazın araştırmasının

sonuçlarından derlenen önerilerin kullanıcı çalışması sonuçları ile birleştirilmesi sağlanarak mobil ara yüzlerde kullanılabilecek sağlamlık ve kullanılabilirlik konularını dengeleyen tür konusunda uygulama geliştiricilere öneriler sağlanmıştır.

1. GENEL BİLGİLER

1.1. Tez Çalışmasının Amacı

Günlük hayatta bankacılıktan veri paylaşımına ya da sosyalleşmeye kadar kullanılan çeşitli web tabanlı uygulamalara erişim sırasında kullanıcılardan yetkilendirme bilgilerine ek olarak sahtekârlık ve istenmeyen mesajların önüne geçmek için insan etkileşim kanıtı olarak güvenlik kod girişi de yapmaları istenmektedir. Uygulama geliştiriciler açısından kullanılacak güvenlik kodlarının seçiminde sağlamlık ve kullanılabilirliğin beraber sağlanması bir zorluk oluşturmaktadır. Çünkü güvenliğin artırılması genellikle kullanılabilirliğin azalması sonucunu doğurmaktadır (Bursztein vd., 2011, 2014; Golle, 2008). Bu nedenle güvenlik kod araştırmalarında sağlamlık ile ilgili konular kadar son kullanıcılar açısından kullanılabilirliğin de beraber değerlendirilmesi önem kazanmaktadır. Ayrıca web tabanlı uygulamalara erişim için günümüzde mobil cihazların kullanımı da oldukça yaygındır ve bu cihazlarda geleneksel ara yüzlere göre ekran alanının daha kısıtlı olması ve klavye yerine el ile dokunularak veri girişi şeklinde farklı bir yaklaşım kullanılıyor olması nedeniyle kullanıcı etkileşimleri hataya daha açıktır (Brewster, 2002).

Bu tez çalışması kapsamında günlük hayatta pek çok çevrim içi hizmet kullanımı sırasında son kullanıcıların karşılaştıkları güvenlik kod türlerinden hem sağlamlığı daha yüksek hem de kullanıcılar açısından kullanılabilir olanın belirlenmesi hedeflenmiştir. Bu nedenle mobil uygulamalar için de kullanımı hem ekran alanını daha az kaplaması hem de gerektirdiği bellek ve ağ iletim kapasitesinin de az olması nedeniyle daha uygun olan metin temelli 6 farklı şemada güvenlik kodunun bir kullanıcı çalışması kapsamında değerlendirilmesi yapılarak değerlendirilen güvenlik kod şemalarının kullanıcılar açısından etkililik, verimlilik ve memnuniyet dereceleri kıyaslanmıştır. Kullanıcı çalışmasından elde edilen bulgular aynı zamanda güvenlik kodların sağlamlığı ve kullanılabilirliği ile ilgili gerçekleştirilmiş önceki çalışmalarda da raporlanan çeşitli tavsiyeler ile de birleştirilerek mobil ara yüz geliştiricilere yol gösterecek tavsiyeler oluşturulmuştur.

1.2. Tez Çalışmasının Katkıları

Güvenlik kod çalışmalarının pek çoğu geleneksel masaüstü uygulama ara yüzlerindeki değerlendirmeleri içermekte mobil ara yüzler üzerinde değerlendirme yapan çalışma sayısı kısıtlı kalmaktadır. Yapılan çalışmalarda güvenlik kod kullanılabilirliği ya da güvenlik kod güvenliği ele alınırken hem güvenlik hem kullanılabilirlik kavramının beraber ele alındığı çalışma yetersizdir. Bu çalışma kapsamında mobil ara yüzlerde kullanılabilecek güvenlik kodlar için hem güvenlik hem de kullanılabilirlik kavramı beraber ele alınmış, farklı güvenlik özellikleri içeren güvenlik kod türlerinin kullanılabilirlik değerlendirilmesi yapılmıştır. Böylece metin tabanlık güvenlik kodlar için hem güvenlik hem de kullanılabilirlik konularını dengeleyen türün belirlenmesi sağlanmıştır.

Çalışma kapsamında gerçekleştirilen alan yazın araştırması kapsamında incelenen güvenlik kodların sağlamlık ve kullanılabilirliğini değerlendiren önceki çalışmalardan da tavsiyeler çıkarılmıştır. Bu tavsiyeler ile kullanıcı çalışmasının bulguları birleştirilerek uygulamalarında kullanacakları güvenlik kod türüne karar verecek mobil uygulama geliştiricilere yol gösterecek tavsiyeler oluşturulmuştur.

1.3. Tezin Yapısı

Bu tez çalışması beş ana bölümden oluşmaktadır. Birinci bölümde tezin amacı ve özgün değerinden bahsedilerek tez çalışmasının katkılarından bahsedilmektedir. İkinci bölümde ilgili alan yazın kapsamında, konu ile ilgili genel tanımlamalar ve güvenlik kod tasarımında güvenlik ve kullanılabilirlik adına uygulanan yöntemler ile ilgili çalışmalara değinilerek mobil cihazlarda metin tabanlı oluşturulan güvenlik kod örneklerine yer verilmektedir. Tezin üçüncü bölümünde bu çalışmada izlenen yöntemin detayları anlatılmaktadır. Yapılan araştırmanın tasarımından bahsedilmiş, katılımcılara ait bilgiler, çalışma sırasında veri toplamak için kullanılan anketler, donanım ve yazılım bileşenleri ayrıntılı şekilde açıklanmaktadır. Dördüncü bölümde tez kapsamında gerçekleştirilen deneyin bulguları raporlanmaktadır. Tezin beşinci ve son bölümünde ise çalışmanın ana sonuçları, güçlü ve eksik yönleri ile gelecekte yapılacak çalışmalar tartışılmakta ve çalışma kapsamında elde edilen bulgulara dayanarak güvenlik kod türlerinden hem kullanılabilir hem güvenlik düzeyi yüksek olan tür belirlenerek güvenlik kod kullanımına karar verecek geliştiricilerin

uygulamalarına hangi şemayı dahil etmelerine karar vermelerinde yardımcı olacak öneriler alan yazın bulguları ile birleştirilerek sunulmaktadır.

2. ALAN YAZIN ARAŞTIRMASI

Alan yazın araştırması kapsamında öncelikle çalışmanın temelini oluşturan kullanılabilirlik ve güvenlik kavramları ile tez kapsamında değerlendirilmek üzere seçilen güvenlik amaçlı kullanılan güvenlik kod türü açıklanmaktadır. Daha sonra güvenlik kodlar ile gerçekleştirilen çeşitli kullanılabilirlik ve sağlamlığı değerlendirmeye yönelik çalışmalardan bahsedilmektedir.

2.1. Kullanılabilirlik

Kullanılabilirlik bir uygulamanın son kullanıcıları tarafından kullanımının kabul edilmesi açısından sağlanması gereken sistem kalite gereksinimlerinden biridir (Pressman, 2005). Bu kavram gerçekleştirilen tez çalışmasının da temelini oluşturduğundan bu bölümde tanımlanması önemlidir.

Kullanılabilirlik, bir uygulamanın kolay ve etkili şekilde, belirli grup kullanıcı ile belirli görevlerin yapılması ve senaryolar içinde kullanılma kapasitesi şeklinde tanımlamıştır (Shackel vd., 1991). Bu tanım daha çok kullanıcı hedefleri ve hedefleri gerçekleştirme gibi kullanılabilirlik bileşenlerine odaklanmıştır. Ancak alan yazında kullanılabilirliği başka bileşenler ile de açıklayan çeşitli tanımlar da mevcuttur. Örneğin Nielsen (1993) kullanılabilirliği öğrenilebilirlik, verimlilik, hatırlanabilirlik, hatalar ve kullanıcı memnuniyeti olarak listelen 5 temel bileşen ile açıklamıştır.

Kullanılabilirliğin herkes tarafından kabul görebilecek ölçülebilir bir tanımının oluşturulması ISO 9241-11 (1998) tarafından yapılmıştır. ISO tanımına göre kullanılabilirlik, “bir ürünün, belirli bir kullanım bağlamında etkinlik, verimlilik ve memnuniyetle belirlenen hedeflere ulaşmak için belirli kullanıcılar tarafından ne ölçüde kullanılabileceği” şeklinde tanımlanmıştır. Tez kapsamında da kullanılabilirliğin tanımı için kabul edilen ISO tanımında yer verilen etkinlik, verimlilik ve memnuniyet bileşenlerinin açıklamaları aşağıda detaylandırılmaktadır;

- Etkinlik; tasarımı kullanırken kullanıcıların beklenen görevi yapıp yapamaması ya da başarı oranı olarak tanımlanmaktadır. Örneğin bir uygulamada kullanıcının verilen görevi yapması, yapamaması ya da kısmi olarak yapması etkinlik oranını belirler
- Verimlilik; tasarımı kullanırken kullanıcıların beklenen görevi tamamlama süresi ile tanımlanmaktadır. Örneğin, bir uygulamada kullanıcının verilen görevi etkili biçimde gerçekleştirirken ilgili görevi hızlı ya da az maliyetle gerçekleştirmiş olması verimlilik oranını belirler
- Memnuniyet; tasarımı kullanırken kullanıcıların hissettiği memnuniyeti, beğenisi olarak tanımlanmaktadır. Örneğin kullanıcı bir uygulamayı kullanırken hissettiği olumlu duygular, beğeniler ne kadar fazla ise memnuniyet oranı o oranda fazla olmaktadır

(ISO, 1998)

2.2. Güvenlik

Günümüzde kullanılan pek çok yazılım sistemi kullanıcılara ait hassas bilgiler içermektedir. Bu nedenle uygulamaların güvenliğinin sağlanması yine yazılım kalite gereksinimleri içerisinde önemli bir yere sahiptir (Pressman, 2005).

Güvenlik kavramı kullanıcıların bir tasarımı kullanırken verilerinin korunması ve verilerin yetkisiz kullanıcıların eline geçmediğinden emin olunmasıdır. Yazılımın güvenli olması demek tüm bilgi güvenliği saldırılarına karşı dirençli ve hatasız çalışması anlamı taşımaktadır.

Yazılımda güvenliğin amaçları sırayla belirtilmiştir;

- Zararlı yazılımlardan (virüs, spyware, spam, bots vb.) korunmak
- Kimlik hırsızlığını önlemek
- Değerli bilginin-verinin korunmasını sağlamak
- Kullanıcılara sistemin güvenli olduğunu hissettirerek, yazılımı kullanan kullanıcıyı memnun etmektir.

(Siber Güvenlik Enstitüsü, 2018)

Güvenlik tanımında yer alan belli bileşenler bulunmaktadır. Bu bileşenler; gizlilik, mahremiyet, bütünlüktür (Alshamari 2016). Bileşenlerinin güvenlik alanındaki karşılıkları aşağıda detaylandırılmaktadır;

- Gizlilik; değerli verinin yetkisiz kullanıcılardan korunması, sadece yetkili kişilere erişim sağlanmasıdır (ISO 17799,2005).
- Mahremiyet; kullanıcı özel verilerinin yetkisiz kişilerin eline geçmesini engellemektir (Fischer-Hübner 2001).
- Bütünlük; değerli verinin yetkisiz kullanıcılar tarafından değiştirilmediğinin garantilenmesi yani bütünlüğünün korunmasıdır (ISO 17799, 2005).

Birçok yazılım sistemi çeşitli saldırılara maruz kalmaktadır, bu saldırılarından korunmak için öncelikle yazılımların, güvenlik ilkelerine uygun olarak tasarlanması ve geliştirilmesi gerekmekte ve yazılımın güvenliğini sağlayan yöntem ve araçların kullanılması gerekmektedir. Güvenli olan yazılımlar güvenlik düzeyinin bozulmaması için sürekli güncellenmesi gereken sistemlerdir. Güvenli yazılım sistemlerinin güvenliğini daim ettirebilmesi için aynı zamanda kullanıcılar tarafından kolay anlaşılabilir ve kolay kullanılabilir olmalıdır. Aksi halde kullanıcılar yanlış işlemler ve kullanımlarla sistemi açık hale getirebilir (Tognazzini 2014). Sistemin güvenliğinin devamı için, kullanıcıların sistemi kullanırken yapmış olduğu hatalarda geri dönüş sağlanmalı, sistemi kullanıcılar en az yardım ve çabayla kullanabilmeli, ayrıca sistemin amacı açık ve net olmalıdır. (Beautement, Sasse, ve Wonham 2008; Sasse ve Flechais 2005). Böylelikle güvenli olan sistem, güvenli olarak kalmaya devam edecektir.

Her bilgi sisteminin farklı güvenlik ihtiyaçları bulunmaktadır. Örneğin zararlı yazılımlardan bilgisayarları korumak için anti virüs programlarına, ağ portlarını virüs ve saldırganlardan korumak için güvenlik duvarına, web sitelerinin güvenliği için HTTPS protokollerine ihtiyaç duyulurken, kimlik doğrulama sırasında otomatik yetkilendirme yazılımlardan korunmak için de güvenlik kodu kullanımına ihtiyaç duyulmaktadır. Güvenlik kodu ile zararlı otomatik yazılımların yetkisizce veri gönderimi, web sitelerinde sahte olarak kayıt olma, kaydı yönetme ve hesap oluşturma işlemleri engellenmektir (von Ahn, Blum, ve Langford, 2004).

2.3. Güvenlik Kod (CAPTCHA)

Güvenlik kod (CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart - İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) (vonAhn vd.,2004) karşısındakinin insan olup olmadığını belirleyen araçtır. Bot adı verilen, tıpkı insan gibi davranış gösteren çeşitli zararlı otomatik yazılımlar web sitelerinde kullanıcının isteği dışında çeşitli tıklamalarda bulunarak uygulamalar çalıştırılabilmekte ya da otomatik tıklamalar ile web sitesinde istenmeyen noktalara yönlendirme yapabilmektedir.

Güvenlik koda olan ihtiyaç yaşanan birçok problem ile ortaya çıkmıştır. Bu olaylardan en bilineni 1999 yılında sosyal haber sitesinde bilgisayar bilimi alanında en iyi olan üniversitenin seçimi için çevrimiçi oylama ile ilgilidir. Bazı üniversitelerden öğrenciler kendi okullarını sıralamada üste çıkarmak için botlar (otomatik tıklamam yazılımı) yazmışlar ve kendi okullarının daha fazla puan almasını sağlamışlardır. Bahsi geçen okullar milyonlarca oy alırken diğer okullar yalnızca binlerde kalmıştır (Panda Security 2019). Bir diğer örnekte ise Yahoo ve Mail gibi programlarda spam hesapların çoğaldığı ve insan olmayan botların insan gibi davranarak başka hesaplara kandırıcı mailler attığı ortaya çıkmıştır (Panda Security 2019). Böylelikle yapılan işlemin gerçek bir kullanıcı tarafından mı robot bir yazılım tarafından mı gerçekleştirildiğini anlamayı sağlayacak önlemlere ihtiyaç duyulmuştur.

Güvenlik kod (Captcha) ilk olarak 2000 yılında Carnegie Mellon Üniversitesi tarafından Luis von Ahn, önderliğinde araştırmacılar tarafından geliştirilmiştir. Araştırmacılar Turing testini baz alarak sadece insanın geçebileceği güvenlik kod adını verdikleri test ile kullanıcı ve bilgisayarın ayrımını yapabilmişlerdir. Güvenlik kodlar gerçek kullanıcılar tarafından anlaşılırken bilgisayarlar tarafından anlaşılamaması sağlanan tasarımlardır. Çünkü otomatik yazılımların bozulmuş bir resimden kelimeyi anlaması, bozulmuş seslerden dinlediği kelimeyi anlayarak cevabı vermesi, çeşitli hareketli objelerden oluşan videodan gerekli objeleri ayırt etmesi insanın bu işlemleri yapmasına göre daha zordur.

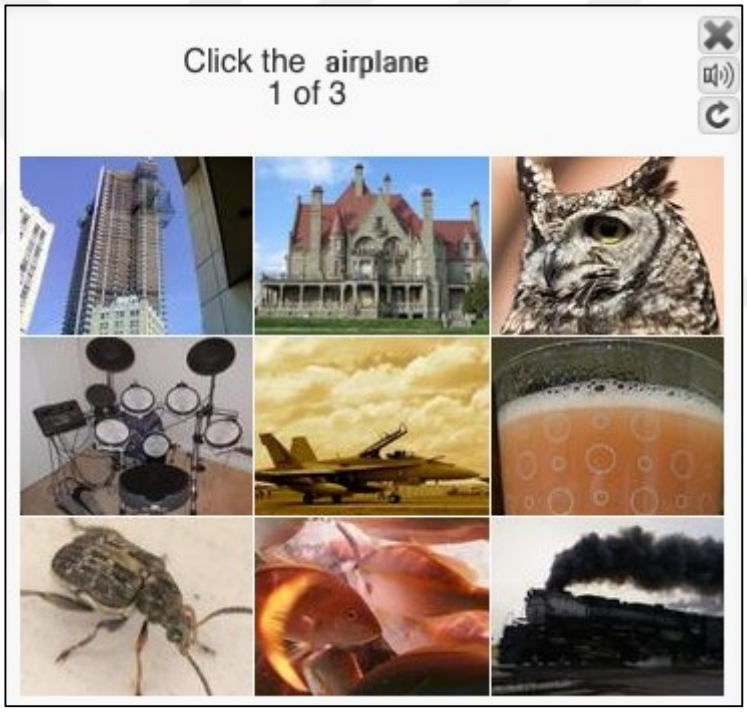
2.3.1. Güvenlik kod türleri

Güvenlik kodlar ihtiyaca göre çeşitli şemalara ayrılmaktadır. Metin-tabanlı (text-based), resim-tabanlı (image-based), ses-tabanlı (audio-based), kavramsal-tabanlı (cognitive-based), animasyon-tabanlı (animation-based), etkileşim gerektiren oyun tabanlı (game-based) gibi çokça farklı güvenlik kod şeması vardır. Her bir türün kendine has güvenlik sorunları olması nedeniyle geliştiriciler her zaman daha dayanıklı bir şema üretme yoluna gitmiştir. Şemaların çeşitli ataklara dayanıklı olmasının yanında aynı zamanda kullanıcılar tarafından da kolay anlaşılır olmasının sağlanması da önemlidir (Chow ve Susilo 2017).

En yaygın kullanılan güvenlik kod şeması metin-tabanlı güvenlik koddur. Bunun nedenleri kolay geliştirilmesi, maliyetinin ucuz olması ve hem mobil hem de masaüstü uygulamalarında kolaylıkla kullanılabilmesi olarak sayılabilir (Beheshti ve Liatsis 2015; El Ahmad, Yan, ve Ng 2012; Yan ve El Ahmad 2008b). Metin tabanlı şemalarda metin HTML kodlarının içinde bulunmaktadır. Metnin bu şekilde HTML kodları içeresinde yer alması güvenlik ataklarında başarı sağlanmasına açık kapı bırakabilmektedir (Baykara, Alnıak, ve Çınar 2018; Kulkarni ve Fadewar 2017; Zhang vd. 2017; Althamary ve El-Alfy 2017). Bu tez çalışmasında metin-tabanlı güvenlik kod şeması olarak, metni HTML kodları içerisinde değil de güvenlik ataklarının başarısını azaltacak şekilde bir resmin içerisine gömülmesi ile elde edilen metin-tabanlı şema kullanılmıştır. Resim içine metin gömülerek oluşturulan metin-tabanlı şemaların en bilindik örneği birçok web sitenin ve Google'nin kullandığı ReCAPTCHA'dir. Şekil 2.1'de görüldüğü üzere şemaya eğrilik, farklı hizalama, çizgi ekleme gibi bozulma işlemleri uygulanmış, alfa numerik karakterler kullanıcıya gösterilmekte ve kullanıcının onu tanıması beklenmektedir.

Şekil 2.1. Metin-tabanlı güvenlik kod örnekleri

Bir başka şema olan resim-tabanlı güvenlik kodlarda Şekil 2.2'de görüldüğü üzere kullanıcıya belli resimler arasından istenilen özellikteki resim ya da resimleri seçmesi istenmektedir. Tanımlanan özellikler ne kadar zor ve detaylı olursa otomatik yazılımların sistemi çözmesi o oranda zorlaşmaktadır (Brodić vd. 2016). Resim-tabanlı güvenlik kodlar yüksek maliyetlidir. Daha güvenli olabilmeleri için resimlerin karışık ve çeşitli şekilde kullanıcıya sunulması gerekmekte bu da fazla oranda resim ihtiyacına ve yüksek miktarda veri depolayabilen veri tabanlarına ihtiyaç yol açmaktadır. Bunun yanı sıra resim-tabanlı güvenlik kodların görüntülerinin yeteri kadar büyük olabilmesi gerektiği için masaüstünde yaygın kullanılırken mobil cihazlarda kullanımı ekran boyutu ve işlemci kapasitesi gibi sebeplerle tercih edilmemektedir (Reynaga ve Chiasson 2013).



Şekil 2.2. Resim-tabanlı güvenlik kod örneği

Ses-tabanlı güvenlik kodlar Şekil 2.3'de görüldüğü üzere sesli şekilde metinin gösterilmesi değil de seslendirilmesidir. Ses tabanlı güvenlik kodları çeşitli bozulma uygulanmış seslerden kelimeyi anlama işlemine dayanır.(Kulkarni ve Fadewar 2017). Bozulma uygulanmış sesten anlamlı kelimeyi bulmak otomatik yazılımlar için zor olurken insanlar için daha kolay olacağı düşünülerek tasarlanmıştır. Fakat sesteki telaffuz şekli ve her dilde seslendirilmesi problemi nedeniyle popülerlik kazanmamıştır (Choudhary 2013).

Şekil 2.3. Ses-tabanlı güvenlik kod örneği

Video-tabanlı güvenlik kodlar kullanıcıya ses içermeyen bir video izletilmesi veya videonun konusunun ya da video ile ilgili bir sorunun yanıtının kullanıcı tarafından yanıtlanmasını içermektedir. Video-tabanlı güvenlik kodlar dil bağımsız olması sebebiyle farklı dillerdeki kullanıcılar için avantajlı olarak görülürken, görme engelli kullanıcılar tarafından kullanılamamaktadırlar. Büyük boyutlu video içeriklerden oluşmaları nedeniyle çalıştırılma ve yüklenme zorlukları nedeniyle tasarımcılar tarafından maliyetli bulunurken kullanıcılar tarafından da cevaplanmaları her zaman kolay olmadığından yaygın olarak kullanılmamaktadır (Nadaph vd. 2007).

2.3.2. Güvenlik kodlar ve kullanılabilirlik

Güvenlik kodların son kullanıcılar tarafından kolaylıkla ayırt edilmesi ancak otomatik yazılımlar tarafından ayırt edilmesinin zor olması gerekmektedir. Güvenlik kodlar ile ilişkili değerlendirilebilecek kullanılabilirlik bileşenleri etkililik (doğruluk), verimlilik (veri giriş hızı) ve memnuniyet ile ilgili konulardır. Örneğin metin-tabanlı şemalarda güvenliği arttırma amaçlı kullanılan bozulma (distortion), içerik (content) ve sunum (presentation) olarak belirlenen faktörler güvenlik kodların kullanılabilirliğini olumsuz yönde etkileyebilmektedir (Behesti ve Liatsis, 2015), (Yan ve El Ahmad 2008b).

Bu faktörlerden bozulma (distortion) metne çeşitli çizgi ya da karakter ekleme, soluklaştırma, döndürme, şeklini değiştirme gibi işlemler uygulanarak bozma işlemi uygulanmasıdır (Yan ve El Ahmad 2008b). Bunun yanı sıra seçilen dilin kullanıcının ana dili olup olmaması da bozulma faktöründe yer alan kullanılabilirliği etkileyen konulardandır (Behesti ve Liatsis, 2015). Örneğin, von Ahn vd. (2008) yaptığı çalışmada, reCAPTCHA güvenlik kod kullanımında, anadilleri İngilizce olanların olmayanlara göre başarılı olma oranının daha fazla olduğunu belirtmiştir.

İçerik (content); güvenlik kodun metin içeriğinin uzunluğu ile içeriğin rastsal kelime ya da sözlük kelime olup olmaması ile ilgili kullanılabilirliğini etkileyen bir faktördür. Rastsal kelimeler kullanıldığında; metin ne kadar uzun ise kullanıcının harfleri tek tek anlaması o kadar zorlaşıp güvenlik kodun kullanılabilirliği azalırken (Behesti ve

Liatsis, 2015) bozulmaya uğramış uzun sözlük kelimeleri kullanıldığında kullanıcının kelimeyi anlayabilmesi kolaylaşmaktadır (von Ahn vd., 2008) .

Sunum (presentation) ise güvenlik kod içeriğinde kullanılan metinin yazı tipi ve büyüklüğü, arka fonda ve metinde renk kullanımı ile ilgili kullanılabilirliği etkileyen bir faktördür. Harflerin büyüklüğü ve kullanılan yazı tipi okunabilirliği ve tanınabilirliği etkilemektedir (Chew ve Baird, 2003; Coates, Baird, ve Faternan, 2001). Bunun yanı sıra güvenlik kodda çok fazla renk kullanımı kullanılabilirliği olumsuz etkilediği kadar güvenliği de etkilemektedir (El Ahmad, Yan, ve Ng, 2012).

Geliştiriciler ve tasarımcılar, kullanıcılar için en ideal, en kolay kullanılabilen, etkili bir güvenlik kodu tasarlama hedefindedir. Bu amaca yönelik alan yazında güvenlik kod mekanizmalarında kullanılabilirlik boyutunun incelendiği çeşitli çalışmalar bulunmaktadır.

Reynaga ve Chiasson (2013) çalışmalarında birden fazla metin, resim ve video tabanlı güvenlik kod şemalarını akıllı telefonlarda performans ve kullanılabilirlik testlerine tabi tutmuşlar ve elde ettikleri sonuçları geliştirici ve tasarımcılara yön verebilmek adına tasarım rehberi şeklinde sunmuşlardır. Bu çalışmada akıllı telefonlar için sesli güvenlik kodların hiç uygun olmadığı yapılan test ve memnuniyet anketleri sonuçlarından anlaşılmaktadır. Bunun yanı sıra kullanıcılar kendilerine yöneltilen metin tabanlı güvenlik kodlarından bozma oranı az olan ve büyük puntolarda yazılmış metin tabanlı güvenlik kod türünü daha fazla tercih etmişler ve daha başarılı olmuşlardır.

Behesti ve Liatsis (2015) masaüstünde kullanılan metin-tabanlı güvenlik kod şemalarında görüntü bozma (distortion) ve görüntüyü netleştirme, karakter sayısını artırma ve azaltma işlemleri uygulayarak kullanılabilirlik testi gerçekleştirmişlerdir. Kullanıcılar karakter sayısının az olduğu ve görüntünün daha net olduğu güvenlik kodlarda daha başarılı olmuşlardır.

Reynaga, Chiasson ve Oorschot (2015) , 2013 yılında Reynaga ve Chiasson tarafından yapılan çalışmanın devamı niteliğinde tasarım rehberine yeni tavsiyeler eklemek için akıllı telefonlarda kullanılan metin, resim ve video-tabanlı gibi farklı türde güvenlik kodlar için kullanılabilirlik testi gerçekleştirmişler ve elde ettikleri sonuçları geliştirici

ve tasarımcılara yön verebilmek adına tasarım rehberi şeklinde sunmuşlardır. Video tabanlı güvenlik kodlarını akıllı telefonlar için performans bakımından uygun görmezlerken resim ve metin-tabanlı güvenlik kod şemaları için mümkün olduğunca minimalist tasarımların tercih edilmesi, resim kullanılıyorsa cihazın ekranına uygun yerleştirilmesi, renk kullanımlarının dengelenmesi gibi görsel tasarımlar ile ilgili tavsiyelerde bulunmuşlardır.

Tangmanee (2018) masaüstü uygulamalarda kullanılan İngiliz alfabesindeki küçük harflerden rastgele oluşturulmuş metin-tabanlı güvenlik kodları, kullanıcıların hangi hızda ve doğrulukta cevapladığı verisine göre hangi küçük harflerden oluşan güvenlik kodların daha kullanılabilir olduğunu kullanılabilirlik testi ile analiz etmiştir. Çalışma sonucunda metinin içinde yer alan harflerin alfabe sırasında olup olmamasının performansa ve doğruluk oranına etkisi gözlemlenmemiştir.

Darko Brodić ve Amelio (2019) mobil uygulamalarda kullanılan çalışmalarında sadece rakam ve sadece harflerden oluşan metin-tabanlı güvenlik kod türlerinin cinsiyet, tecrübe, yaş gibi faktörlere göre başarı yüzdelerini öğrenmek için kullanılabilirlik testi gerçekleştirmişlerdir. Sonuçlar incelendiğinde ise katılımcıların, sadece rakamlardan oluşan güvenlik kodları ile sadece harflerden oluşan güvenlik kodlara göre daha başarılı olduğunu gözlemlemişlerdir.

2.3.4. Güvenlik kodlar ve güvenlik

Güvenlik kodlar uygulamalarda güvenliği arttırıcı amaçla kullanılmaktadır ancak bunlar da çeşitli ataklara maruz kalabilmektedir. Güvenlik kodlarda gözetilmesi gereken en önemli güvenlik bileşeni sağlamlıktır. Özellikle metin-tabanlı güvenlik kodlara yapılan en bilinen ataklar optik karakter tanıma atağı, piksel sayma atağı, bölütleme (segmentasyon) atağı, kaba kuvvet saldırısı ve sözlük atağıdır. Bu ataklara maruz kalmamak ve güvenlik kodun sağlamlığını arttırabilecek çeşitli önlemler uygulanabilmektedir.

Bu ataklardan optik karakter tanıma atağı (Chew ve Baird 2003); (Yan ve Ahmad 2009) resim üzerindeki harfleri tek tek seçererek onlardan kelime oluşturan saldırı yöntemidir. Optik karakter tanıma atağından korunmak için güvenlik kod için kullanılan metinlerde bilinen kelimler yerine rastgele oluşturulan metinlerin seçilmesi,

kelimelerin arasına özel karakter eklenmesi (Bentley ve Mallows 2006) farklı yazı tipi ile yazılmış el yazması kelimeler kullanılması (Yan ve Ahmad 2009), webde olmayan gazete ya da kitaplardan alınmış kelimelerin seçilmesi (Yamamoto, Tygar, ve Nishigaki 2010), kelimelere bozulma uygulanması (Rusu, Thomas, ve Govindaraju 2010); Yan ve El Ahmad, 2008b) gibi yöntemler kullanılmaktadır.

Bilgisayar sistemlerinde her bir harf farklı piksel numaralarına karşılık gelmektedir. Bu harfler güvenlik kodda birbirinden segmente edilebilirse, piksel numarası bilinip, o piksele karşılık gelen harf belirlenerek piksel sayma atağı gerçekleştirilmiş olunur. (Roshanbin ve Miller, 2013). Arka alan ve metin renginin birbirine yakın seçilmesi ile karakterlerin arka plandan kolayca ayrılmasına engel olarak bu atak türünden korunulabilmektedir. Bunun yanı sıra karakterlerin farklı hizalarda yerleşimi de aynı şekilde piksel sayma atağına karşı alınan önlemlerdendir (Baird, Moll, ve Sui-Yu Wang 2005).

Bölütleme atağı her bir harfi arka plandan ayırarak harflerin tek tek ortaya çıkarılması ve sonunda metinin ele geçirilmesi şeklinde uygulanır. Bölütleme atağından korunmak için karakterler arasına çizgi, karışık ya da anlamsız karakterler eklenmekte böylelikle metinde karakterlerin kolayca birbirinden ayrılması engellenmektedir (Ahmad, Yan, ve Marshall 2010).

Kaba kuvvet saldırısı güvenlik koda rastgele cevaplar verilerek tek tek deneme yöntemine dayanan bir atak çeşididir. Kaba kuvvet saldırısından korunmak için, içinde farklı ve özel karakterlerin yer aldığı büyük karakter setlerinin oluşturulması sağlanmalıdır. Bunun yanı sıra güvenlik kodu tahmin etmek için sınırlı sayıda tahmin hakkı tanınarak, atağın deneme oranı azaltılır (Ahmad, Yan, ve Marshall 2010).

Eğer kısıtlı bir karakter kümesi kullanılıyorsa bu kelimeler tek tek denenerek gerçekleştirilen atak çeşidi sözlük atağıdır. Bu ataktan korunmak için sözlük kelimelerinden çok, rastsal metinler kullanılır ve böylelikle saldırı tarafından kelimeyi tahmin etme durumu engellenir (Roshanbin ve Miller 2013).

Güvenlik kodların uygulamalarda kullanımı tercih edilirken mümkün olduğunca güvenliği artırmak amacıyla sağlamlığının değerlendirilmesi önemlidir. Alan yazında bu doğrultuda güvenlik kod mekanizmalarının sağlamlığını değerlendiren ve

artırmaya yönelik mekanizmaları geliştirmeye çalışan çeşitli çalışmalar bulunmaktadır.

Yan ve El Ahmad (2008), çalışmalarında masaüstünde metin tabanlı güvenlik kodlarına sözlük atak testi uygulamışlardır. Harf setlerinin artırılması, kelimeler içinde özel karakterlerin, çizgilerin kullanılmasının kelimeyi anlamayı zorlaştıracağı için sözlük ataklarının başarı yüzdesinin bu şekilde azaltılacağını belirtmişlerdir.

Roshanbin ve Miller (2013), çalışmalarında masaüstünde metin tabanlı güvenlik kodlarına bölütleme ve tanıma testi uygulamıştır. Metin karakterlerine özel karakterler eklemiş ve metin ile arka fonda renk kullanmıştır. Bu işlemlerin yanı sıra karakterler belli sayıda ve bilindik olduğu için fiziksel klavye yerine özel karakterler içeren sanal klavye kullanarak atakların başarı yüzdesinin azaltılacağını belirtmişlerdir.

Kaur ve Behal (2014) çalışmalarında masaüstünde metin tabanlı güvenlik kodlarına tanıma atağı testi uygulamış, rastsal harf ve rakamlardan oluşan ve her bir karakterin yazı tipinin ve karakterlerin hizalanmasının farklı olduğu, sözlük kelimelerinin kullanılmadığı güvenli olduğu düşünülen güvenlik kodu şeması tasarlamışlardır.

Alsuhibany (2016) yaptığı çalışmada masaüstünde metin tabanlı güvenlik koduna bölütleme testi uygulamış, metin tabanlı güvenlik kodlarının bölütleme atağına karşı güçlü olabilmesi için harflerin arasında olan boşlukların azaltılması hatta mümkünse birleştirilmesi, harfler arasına anlamsız birbiriyle karışan harflerin konulması gerektiğinden bahsetmiştir ve bunun da kullanılabilirliği düşüreceğini belirterek çizgi, yay içeren harflerden oluşmuş metin tabanlı güvenlik kodunu kullanıcının anlayacağı formata dönüştüren güvenlik kodu optimize aracı tasarlamıştır.

Baykara, Alnıak, ve Çınar (2018) çalışmalarında masaüstünde metin tabanlı güvenlik koduna optik karakter tanıma testi uygulamış, metin, resim ve video tabanlı güvenlik kodları karşılaştırmış ve mevcut güvenlik kod şemalarına alternatif olarak metin ve arka renklerin birbirine yakın olduğu ve metinin karakterlerini bozulduğu yeni bir güvenlik kodu şeması tasarlamışlardır.

2.3.4. Güvenlik kod ile kullanılabilirlik ve güvenlik konularının birlikte değerlendirildiği çalışmalar

Güvenlik kod mekanizmalarının hem kullanılabilirlik hem de güvenlik boyutlarının beraber değerlendirilmesine yönelik çalışmalar da mevcuttur. Ancak her iki özelliğin bir arada değerlendirildiği çalışmalar çoğunlukla masaüstü uygulamalar için gerçekleştirilmiştir.

El Ahmad, Yan, ve Ng (2012) masaüstü ortamları için, çalışmalarında metin tabanlı güvenlik kodunda renk faktörünün kullanılabilirlik ve güvenliğe etkisini araştırmışlar, Güvenliğe yönelik bölütleme atağı testi ve kullanılabilirliğe yönelik de sezgisel değerlendirme uygulamışlar ve elde ettikleri sonuçları geliştirici ve tasarımcılara yön verebilmek adına tasarım rehberi şeklinde sunmuşlardır. Araştırma sonucunda arka renk ile metin renginin siyah beyaz gibi birbirinden tamamıyla ayrılması ile kullanılabilirlik oranında artış sağlanırken, bölütleme atağının daha kolay başarıya ulaşacağını belirtmişlerdir. Bunun dışında güvenliği artırmak adına kullanıcıların yeteri düzeyde anlayacağı fazla zıt renklerin kullanılmadığı güvenlik kodun hem güvenilir hem de kullanılabilir olacağı sonucuna varmışlardır.

Kaur ve Behal (2014), masaüstü ortamları için, çalışmalarında metin tabanlı güvenlik koda tanıma testi uygulamışlar ve metin karakterlerini soluklaştırma, yazı tipini küçültme ve ek çizgiler ekleyerek kelimelerin anlaşılmasını zorlaştırılması ile hangi atak türlerini azaltılabileceğini ve bu işlemler sonucunda kullanılabilirliğin ne yönde değiştiğini değerlendirmişlerdir. Çalışmada elde ettikleri sonuçları geliştirici ve tasarımcılara yön verebilmek adına tasarım rehberi şeklinde sunmuşlardır. Karakterlerin soluklaştırıldığı ve yazı tipinin küçüldüğü bozulma işlemlerinin uygulandığı türlerde kullanılabilirlik düşük olurken güvenliğin yüksek olduğunu ve tanıma atağının başarı yüzdesinin azaldığını belirtmişlerdir.

Alsuhibany (2016), masaüstü ortamlarında kullanılan farklı oranlarda bozma işlemleri uygulanmış dört adet metin tabanlı güvenlik kod şemasına ilk olarak tanıma atağı uygulamış ve dört şemada tanıma atağından büyük oranda başarı ile geçmiştir ardından kullanıcı testi uygulayarak hangi türün daha kullanılabilir olduğunu ölçmeye çalışmıştır. Sans Serif yazı türünü içeren metin tabanlı güvenlik kodunun hem güvenilir hem de daha kullanılabilir olduğunu belirtmiştir. Kullanıcılar tarafından en

çok memnun olunan tür, harf sayısının 5 ile 7 arasında olduğu, harfler arasında eğim oranının eşit olduğu güvenlik kodu olurken, en az memnun kalınan tür bozma oranı artırılmış güvenlik kod türleri olmuştur.

Chow, Susilo ve Thorncharoensri (2019), metin ve resim tabanlı güvenlik kod şemalarını karşılaştırarak tasarım rehberi geliştirmişlerdir. Çalışmalarında, özellikle yoğun renklerin kullanımının hem güvenliği hem de kullanılabilirliği olumsuz yönde etkilediğini, "0 (sıfır)" ve "o (harf)" gibi bazı karakterlerin beraber kullanılmasının kullanıcı tarafında karmaşaya yol açtığını ve resim-tabanlı güvenlik kodların kullanım kolaylığı olmasına karşın özellikle görme engelliler açısından ekran okuyucular tarafından tanınamayacağı için zorluk oluşturduğunu belirtmektedirler. Ayrıca resim-tabanlı güvenlik kodların mobil cihazlarda ekran alanı ve bellek kullanımı açısından kullanımının uygun olmadığını vurgulamaktadırlar.

Aljarbou (2019) metin, resim ve ses tabanlı güvenlik kod şemalarının avantaj ve dezavantajlarını açıklayan tasarım rehberi oluşturmuştur. Metin-tabanlı güvenlik kodların mevcut sistemlerde en fazla kullanılan tür olduğu ve az maliyetli oluşu bunun yanı sıra görme engeli olan kişiler için uygun olmadığı bu nedenle sesli güvenlik kodların da kullanılması gerektiğini belirtmiştir.

Güvenlik kodlar ile ilgili güvenlik ve kullanılabilirlik özelliklerinin birlikte ya da ayrı ayrı ele alındığı çalışmalar Tablo 2.1 de özetlenmektedir. Tabloda her çalışmaya ait araştırma çalışmasının hangi ortamda (masaüstü (Ma), mobil (Mo)) gerçekleştirildiği; çalışmanın hedefi (tasarım rehberi önerisi (TRÖ), yeni güvenlik kod önerisi (YGKÖ); çalışmanın odağı (kullanılabilirlik (K), güvenlik (G) ya da kullanılabilirlik ve güvenlik (K&G)), çalışmada incelenen güvenlik kod türü (metin-tabanlı (M), video-tabanlı (V), resim-tabanlı (R)); değerlendirilen kullanılabilirlik ya da güvenlik nitelikleri (memnuniyet (M), okunabilirlik (O), anlaşılabilirlik (A), basitlik (B), hatırlanabilirlik (H), doğruluk (D), ve sağlamlık (S) ve değerlendirme için kullanılan yöntemler (sezgisel değerlendirme (SD), kullanıcı testi (KT), kullanılabilirlik değerlendirmesi (KD),güvenlik testi(GT)).

Tablo 2.1. Güvenlik kodu güvenilirlik ve kullanılabilirlik adına yapılan çalışmalar

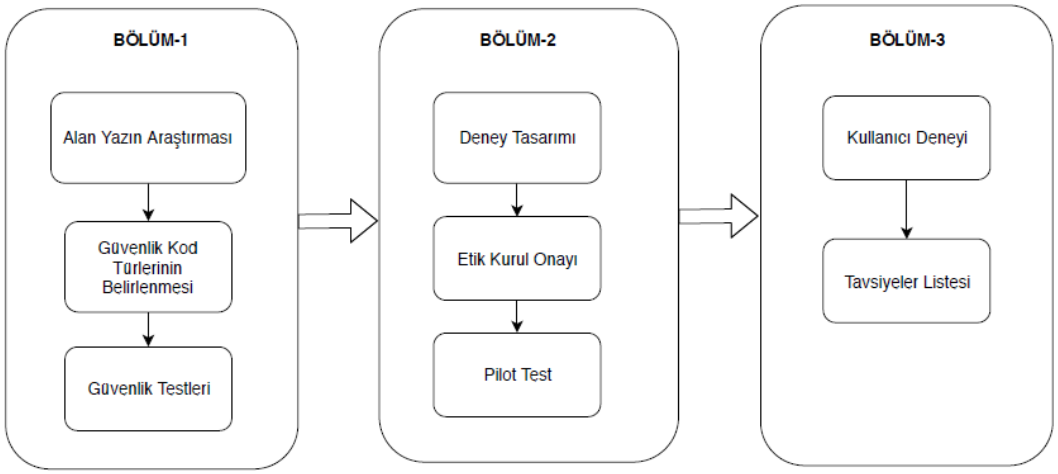
Çalışma	**Ortam**	**Hedef**	**Odak**	**Güvenlik kod**	**Nitelik**	**Yöntem**
(Reynaga ve Chiasson 2013)	*Mo*	*TRÖ*	K	V-R-M	M,O	SD,KT
Reynaga, Chiasson ve Oorschot, (2015)	*Mo*	*TRÖ*	K	V-R-M	A,B,H,D	KT,KD
(Beheshti ve Liatsis 2015)	*Ma*	*YGKÖ*	K	M	A,O	KT,KD
(Tangmanee, 2018)	*Ma*	YGKÖ	K	M	A,M	KT
(Darko Brodić ve Amelio 2019)	*Mo*	YGKÖ	K	M	A	KT
(El Ahmad ,Yan 2008)	*Ma*	YGKÖ	G	M	S	GT
(Roshanbin ve Miller 2014)	*Ma*	YGKÖ	G	M	S	GT
(Kaur ve Behal 2015)	*Ma*	YGKÖ	G	M	S	GT
Alsuhibany 2016)	*Ma*	YGKÖ	G	M	S	GT
(Baykara, Alnıak, ve Çınar 2018)	*Ma*	YGKÖ	G	M	S	GT
(El Ahmad, Yan, ve Ng 2012)	*Ma*	*TRÖ*	K&G	M	A,S	GT, SD
(Kaur ve Behal 2014)	*Ma*	*TRÖ*	K&G	V-R-M-S	A,M,S	SD
Alsuhibany 2016)	*Ma*	YGKÖ	K&G	M	A,S	GT, KD
(Tharad vd. 2018)	*Ma*	*TRÖ*	K&G	M-R-S	S,O	SD
(Y.-W. Chow, Susilo, ve Thorncharoensri 2019)	*Ma*	*TRÖ*	K&G	M-R-S	S,A	SD

3. YÖNTEM

Tez çalışması kapsamında mobil ara yüzlerde kullanılan farklı özelliklerdeki metin-tabanlı güvenlik kodların kullanılabilirlik açısından karşılaştırılması ve hangisinin daha verimli, daha az hataya yol açan ve daha memnuniyet verici olduğunun belirlenmesine yönelik olarak deneysel bir kullanıcı çalışması gerçekleştirilmiştir. Bu bölümde, çalışma kapsamında uygulanan araştırma tasarımı, katılımcılar, kullanılan veri toplama araçları, deney prosedürü ve elde edilen verilerin analizinde kullanılan yöntemler ile ilgili bilgiler paylaşılmaktadır.

3.1. Araştırma Tasarımı

Farklı özelliklerdeki metin-tabanlı güvenlik kod türlerinin değerlendirilmesini içeren bu tez çalışması üç ana aşamada gerçekleştirilmiştir. Çalışmada kullanılan araştırma tasarımı Şekil 3.1' de görülmektedir.



Şekil 3.1. Tez çalışması için kullanılan araştırma tasarımı

Çalışmanın ilk aşamasında tüm yazılım sistemleri için kullanılabilirlik ve güvenlik, teze konu olan güvenlik kod sistemlerinde kullanılabilirlik ve güvenlik konuları ile ilgili detaylı alan yazın araştırmaları gerçekleştirilmiş ve bunun sonucunda değerlendirilecek güvenlik kod türünün ne olacağı belirlenmiştir. Bu aşamanın

sonunda belirlenen güvenlik kodların, gerçekleştirilecek kullanıcı deneyleri öncesinde güvenlik açısından sağlamlığını değerlendirmeye yönelik olarak testler uygulanmıştır.

Çalışmanın ikinci aşamasında, belirlenip sağlamlık değerlendirmesi tamamlanan güvenlik kodlarının kullanılabilirlik açısından da değerlendirilmesini sağlayacak kullanıcı deneylerinin tasarlanması, deney için etik kurul onayının alınması ve pilot testlerin yapılarak deney tasarımının iyileştirilmesi sağlanmıştır. Kullanıcı testleri öncesi etik kurul onay belgesi Kocaeli Üniversitesi Fen ve Mühendislik Bilimleri Etik Kurulu'ndan alınarak ve Ek-1'de sunulmaktadır. Yine testler öncesinde 5 kullanıcı ile test adımları ve test amacıyla geliştirilmiş uygulamanın doğruluğunun sağlanması için pilot test gerçekleştirilmiştir. Pilot testten elde edilen verilerle test uygulamasında ve test adımlarında gerekli düzenlemeler yapılmıştır.

Çalışmanın son aşamasında tasarlanan kullanıcı deneyi ile 30 katılımcı ile testler gerçekleştirilmiştir. Bu aşamada yapılan kullanıcı deneyleri ile değerlendirilen güvenlik kodlarda hangisinin mobil ara yüzlerde daha etkili, verimli ve memnuniyet verici olduğunu tespit edilerek elde edilen bulgular ve ilk aşamadaki araştırmaların sonuçları birleştirilerek yazılım geliştiricilerde metin tabanlı güvenlik kod seçimleri için yol gösterici olacak tavsiyelerin oluşturulması sağlanmıştır.

3.2. Güvenlik Testleri

Çalışmanın ilk aşamasındaki araştırmalar sonucunda mobil uygulamalarda kullanımının daha uygun görüldüğü ve sıklıkla karşılaşılan metin-tabanlı güvenlik kodlar için alan yazında da önerilen çeşitli güvenlik arttırıcı özellikler ile üretilen güvenlik kodlar oluşturulmuştur. Bu kodların özellikleri detaylı olarak bölüm 3.3.1 de açıklanmaktadır.

Oluşturulan güvenlik kodlar, çeşitli güvenli ataklarına karşın alan yazında da önerilen (Vithlani ve Kumbharana, 2015; Sakila, Vijayarani 2015) beş farklı güvenlik aracı ile test edilerek her birinin sağlamlık oranları belirlenmiştir. Bu araçlar Google Docs, İ2OCR, Convert image to text.net, OCR Convert ve SimpleOCR'dir. Güvenlik araçları OCR kütüphaneleri kullanılarak oluşturulmuş resim içine gömülmüş olan metin ya da karakterleri ayırt eden ve tanıyan araçlardır. Tanınma oranı artıkça güvenlik kod

türünün güvenlik düzeyi düşmektedir. Böylelikle daha az tanınan, çözülme oranının az olduğu güvenlik kodu daha güvenli olmaktadır.

3.3. Kullanıcı Deneyi Tasarımı

Deney Tasarımı İBE alanında, bir ara yüz ya da uygulamanın değerlendirilmesi için incelenecek değişkenler, çalışmaya dahil edilecek katılımcılar, katılımcılara verilecek görevler ve uygulanacak prosedürlerin belirlenmesi ile ilgili karar verme sürecini kapsar (MacKenzie, 2013). Tez çalışması kapsamında ilk olarak bağımsız ve bağımlı değişkenlere karar verilmiştir.

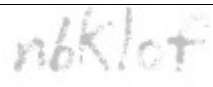
3.3.1. Bağımsız değişken

Çalışma kapsamında incelemeye tabi tutulan ve araştırmacının üzerinde kontrolü olan koşul ya da durumlar bağımsız değişken olarak nitelendirilir (MacKenzie, 2013). Bağımsız değişkenler katılımcı davranışından bağımsız olan ve bağımlı değişken üzerinde etkisi araştırılan etmenlerdir.

Bu tez çalışması kapsamında mobil uygulamalarda kullanımı yaygın olan farklı özelliklerdeki metin-tabanlı güvenlik kod türlerinin etkililik (doğruluk), verimlilik (veri giriş hızı) ve kullanıcı memnuniyeti açısından karşılaştırılması gerçekleştirilmektedir. Bu amaçla metin-tabanlı güvenlik kod türlerinde Yan ve el Ahmad (2008)'in çalışmalarında kullandığı güvenliği arttırma amaçlı uygulanan bozulma (distortion), içerik (content) ve sunum (presentation) olarak belirlenen faktörlerin farklı seviyelerde uygulandığı 6 güvenlik kod belirlenmiştir. Bunlar bozulma uygulanmış (distortion) ve uygulanmamış (non distortion), sözlük-tabanlı (dictionary-based) ve rastgele (random) ile renk ayrımı az (little Contrast) ve çok (full Contrast) güvenlik kod türleridir.

Çalışmada kullanılacak güvenlik kodlar için bozulma faktörünü içeren güvenlik kod oluşturmak için, güvenlik kod için kullanılacak metne farklı seviyelerde bulanık hale getirme (blurring) işlemi uygulanmıştır. İçerik faktörüne karşılık gelecek güvenlik kodlar için, karışık harflerden oluşan kelimeler ya da sözlük-tabanlı kelimeler kullanılmıştır. Sunum faktörü için ise arka fon ve ön fonda yer alan metnin renklerinin farklı ayrımları kullanılmıştır. Bu farklı yöntemlerin ve kullanılan güvenlik kod türlerinin her birine ait örnekler Tablo 3.1'de sunulmaktadır.

Tablo 3.1. Bağımsız değişken olan güvenlik kodu şemalarına ait örnekler

Yöntemler	**Güvenlik kodu kategorisi**	**Örnek**
Bozulma	Bozulma uygulanmış	
	Bozulma Uygulanmamış	
Sunum	Renk ayrımı çok	
	Renk ayrımı az	
İçerik	Rastgele kelime	
	Sözlük kelime	

3.3.2. Bağımlı değişken

Çalışma kapsamında araştırmacının ilgilendiği katılımcı davranışına dayalı olan sonuçlar ya da etkiler bağımlı değişken olarak tanımlanmaktadır (MacKenzie, 2013). Tez kapsamında ölçülmek istenen bağımlı değişkenler güvenlik kodlar için veri giriş hızı (verimlilik), doğruluk oranı (etkililik) ve kullanıcı memnuniyetini içeren kullanıcı tercihlerinden oluşmaktadır.

Bağımlı değişkenlere ait ölçümleri gerçekleştirebilmek için geliştirilen mobil uygulama ara yüzü ile kullanıcıların her bir güvenlik kod için ne kadar süre harcadıkları ve ne kadar hata yaptıkları kayıt altına alınmıştır. Kullanıcı testi sırasında uygulanan sesli düşünme protokolü ve sonrasında kullanılan memnuniyet ve zihinsel iş yükü anketleri aracılığıyla da katılımcılardan geribildirim alınmıştır. Böylece incelemeye alınan güvenlik kod türlerinin doğruluk, hız ve memnuniyet faktörlerine göre karşılaştırılması yapılmıştır.

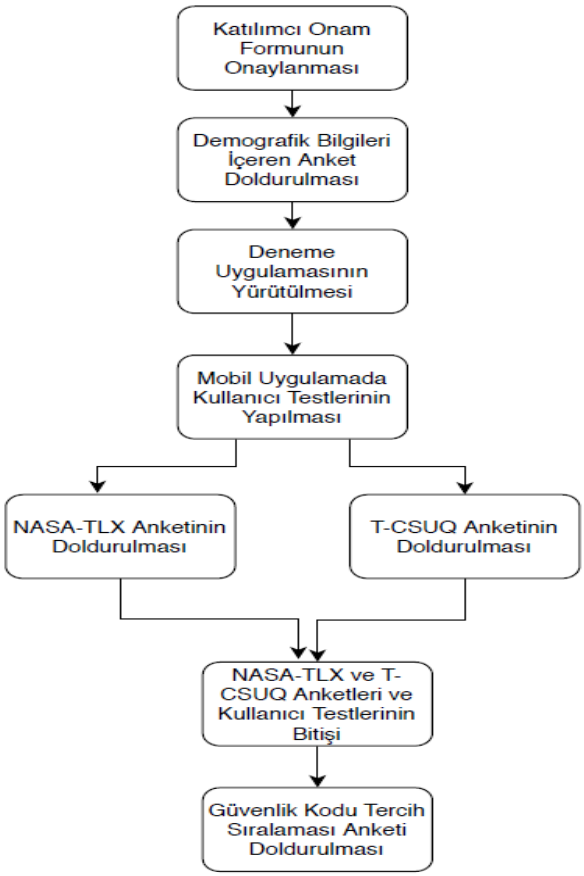
3.3.3. Deney prosedürü

Çalışma kapsamında gerçekleştirilen kullanıcı çalışması için Şekil 3.2'de izlenen bir deney prosedürü belirlenmiştir. Belirlenen prosedür gereği her bir kullanıcıya çalışmanın amacı ve çalışma kapsamındaki deneyi kısaca anlatan bir bilgilendirme yapılmış ve katılımcılardan deney için onay alınmış, kendilerine mobil uygulama ile yapacakları görevler verilmiş, deney süresince sesli düşünmeleri istenmiş, deney sonrasında da kendilerine sunulan anketleri doldurmaları istenmiştir. Yapılan işlemler için takip edilen adımlar aşağıda 7 madde ile açıklanmaktadır.

1. Deneyin başında, çalışmanın amacı ve içeriği ile ilgili katılımcılara kısa bir açıklama yapılarak bilgilendirilmiş onam formunu okumalarını ve çalışmaya katılmayı kabul ettiklerine dair formu (Ek-B) imzalamaları istenmiştir. Deney süresince katılımcılara bir deney gözlemcisi yol göstermiştir.
2. Katılımcılardan deneyin başında demografik bilgilerine yönelik olarak içeriği Ek-C'de sunulan "Kullanıcı Demografik Bilgi Anketi'ni" doldurmaları istenmiştir.
3. Katılımcıların çalışma kapsamında ele alınan farklı güvenlik kod türlerinin kullanımlarını anlamalarına yönelik olarak bir deneme uygulamasını kendilerine sağlanan mobil uygulama cihazı ile gerçekleştirmeleri istenmiştir.
4. Bu deneme kullanımı sonrasında katılımcılar yine deney için geliştirilen uygulama içerisinden "Yeni CAPTCHA (güvenlik kod)" düğmesine basarak girişlerini gerçekleştirecekleri güvenlik kod türlerine erişmiş ve her bir veri girişini bitirdikten sonra "cevapla" ya da "pas" butonuna basarak veri girişini sağlamışlardır.
   4.1. Veri girişleri sırasında katılımcılara silme ya da geri dönme hakkı verilmemiş.
   4.2. Katılımcıların yanlış veri girişleri ve pas geçme istekleri hata olarak sayılmıştır.
5. Her güvenlik kod türü ile etkileşimleri sonunda katılımcılardan o tür ile ilgili Ek-D'de sunulan NASA TLX (NASA Task Load Index – NASA zihinsel iş yükü) ve Ek-E'de sunulan T-CSUQ (Turkish version of Computer System Usability Questionnaire - Bilgisayar sistemi kullanılabilirlik anketi Türkçe sürümü) anketlerini doldurmaları istenmiştir.
   5.1. Katılımcılara görev senaryoları arasında dinlenebilme imkanı sağlanmıştır.

6. Tüm veri girişlerinin tamamlanmasından sonra katılımcılar “bitir” düğmesi ile görevi sonlandırmışlardır.
7. Tüm senaryolar sonlandığında katılımcılardan kullandıkları tüm güvenlik kod türleri arasında tercih sıralaması yapmaları istenmiştir. (Ek-F)

Katılımcıların deney sırasında mobil uygulama ile gerçekleştirdikleri tüm işlemler uygulama tarafından kayıt altına alınmıştır. Ayrıca katılımcılardan test ve memnuniyet anketlerinin doldurulması süresince sesli düşünme protokolünü (Van Someren vd., 1992) uygulamaları istenmiştir. Bu sayede katılımcıların güvenlik kodlarda yaşadıkları problemlerin ya da beğenilerinin belirlenmesinin yanı sıra memnun kalınmayan türler için neden beğenilmediğine dair yorumların alınması ve varsa sisteme yönelik kullanıcı önerilerinin alınması amaçlanmıştır.



Şekil 3.2. Deney prosedürü akış diyagramı

3.4. Katılımcılar

Çalışmaya farklı yaş grupları ve deneyime sahip, mümkün olduğunca eşit cinsiyet dağılımına sahip katılımcılar dahil edilerek çeşitlilik sağlanmaya çalışılmıştır. Kullanıcı deneyi yaklaşık 30 gönüllü katılımcı ile gerçekleştirilmiştir.

Deney sırasında kullanılan mobil test cihazının IOS işletim sistemine sahip olması nedeniyle bu tür cihazlar ile ilgili kullanım deneyimi olmamış kullanıcıların bulgularını etkileyebileceği düşünülmüştür. Deneyden etkili sonuç alabilmek için IOS kullanım deneyimi olan kullanıcılara daha fazla yer verilmeye çalışılmıştır. IOS kullanımı 2 yıldan daha uzun olan kullanıcılar deneyimli kullanıcı olarak belirlenmiştir. IOS deneyimi kategorisi içerisinde kullanıcılar yaş dağılımına göre orta yaşlı ya da genç olacak şekilde ayrılmış ve her bir yaştaki kullanıcılar da cinsiyete göre bir alt kategoriye ayrılmıştır. Test katılımcılarına ait bilgilerin detayları Tablo 3.2' de yer almaktadır.

Tablo 3.2. Test kullanıcıları dağılımı

Mobil İşletim Sistemi Deneyimi	Yaş	Cinsiyet	Kullanıcı Sayısı	Katılımcı Kodu
IOS Deneyimli	Genç	Kadın	7	K1,K7,K11,K21,K23,K29,K30
		Erkek	7	K6, K9, K13, K15, K17, K18, K29
	Orta Yaşlı	Kadın	4	K3, K4, K26, K27
		Erkek	3	K10, K0, K22
IOS Deneyimsiz	Genç	Kadın	2	K16, K28
		Erkek	2	K12, K14
	Orta Yaşlı	Kadın	2	K19, K4
		Erkek	3	K2, K5, K8

Katılımcılar, K1' den K30 'a kadar ilerleyecek şekilde kodlanmıştır ve elde edilen bulguların raporlanmasında bu isimlendirme kullanılmıştır. Katılımcıların yaşları 21 ile 60 yaşları asında değişmekte olup, ortalama yaş 31,03 tür. Katılımcı yaş sınıflandırması 30 yaşından küçük katılımcılar genç, büyük katılımcılar ise yaşlı olarak sınıflandırılmış, deney katılımcılarının yaklaşık üçte ikisi genç, üçte biri yaşlı sınıfında

yer almıştır. IOS deneyimi göz önünde bulundurulduğunda ise üçte iki oranında kullanıcı IOS deneyimli, üçte bir oranında kullanıcı ise hiç IOS işletim sistemli mobil cihaz kullanmamış Android işletim sistemli cihaz kullanan katılımcılardan oluşmaktadır. Katılımcılara ait bu özellikler Tablo 3.3'de sunulmaktadır.

Tablo 3.3. Katılımcı dağılım yüzdeleri

Cinsiyet		**Yaş**		**İşletim Sistemi Deneyimi**	
Kadın	**Erkek**	**Genç**	**Orta Yaşlı**	**IOS**	**Android**
15 (%50)	15 (%50)	20 (%67)	10 (%33)	20 (%67)	10 (%33)
		Yaş			
Minimum		21			
Maksimum		60			
Ortalama		31.03			

3.5. Veri Toplama Araçları

3.5.1. Anketler

Kullanıcı çalışması kapsamında gerçekleştirilen deney prosedürü içerisinde deney öncesinde katılımcılar hakkında detaylı bilgi almak ve deney tamamlandıktan sonra da katılımcıların veri girişi yaptıkları güvenlik kodlar ile ilgili olarak kullanıcı memnuniyetini değerlendirmek üzere anketler uygulanmıştır. Bu anketler ile katılımcıların deney sırasında kullandıkları güvenlik kodun kullanılabilirliği ile ilgili geribildirimlerini, her bir güvenlik kodun kullanıcı üzerinde oluşturduğu bilişsel yükün miktarını ve katılımcıların güvenlik kod tercihlerini belirlemek hedeflenmiştir.

Katılımcılardan deney başlangıcında kullanıcı testine katılım onayı almak için Ek-B'de yer alan "Katılımcı Onam Formunu" doldurmalarını ve demografik bilgilerini almak amacıyla da Ek-C'de yer alan "Kullanıcı Demografik Bilgi Anketi" ni doldurmaları istenmiştir. Kullanıcı demografik bilgi anketi ile cinsiyet, yaş, eğitim durumu gibi bilgilerin elde edilmesinin yanı sıra, akıllı telefon deneyimine ait bilgileri de elde edilmiştir.

Deney sırasında her bir güvenlik kod kategorisi ile ilgili veri girişleri tamamlandıktan sonra katılımcılardan önce Ek-D'de yer alan NASA-TLX (NASA Task Load Index –

NASA zihinsel iş yükü) (Hart ve Sateveland, 1998) anketini yanıtlamaları istenmiştir. Bu anket ile katılımcılarda oluşan genel iş yükü ölçülmektedir. Anket 6 faktörün değerlendirildiği bir ölçektir. Bu faktörler: zihinsel talep (MD: Mental Demand), fiziksel talep (PD: Physical Demand), zamansal talep (TD: Temporal Demand), performans (P: Performance), çaba (E: Effort) ve bıkkınlık seviyesi (F:Frustration) dir. Kullanıcılar bir sistemi bu 6 faktöre göre değerlendirmektedir. Her bir faktöre 1 den 20 ye kadar puan verilmektedir. 1 en az iş yükünü, 20 ise en fazla iş yükünü ifade etmektedir. Böylelikle kullanıcıların verdiği puanların ortalaması ile oluşan genel iş yükü belirlenmektedir.

Yine her bir güvenlik kod ile ilgili veri girişini tamamladıktan sonra katılımcılardan Ek-E'de yer alan T-CSUQ anketini (Turkish version of Computer System Usability Questionnaire - Bilgisayar sistemi kullanılabilirlik anketi – Türkçe sürümü) (Erdinç , 2015) doldurmaları istenmiştir. Bu anket sistem kullanışlılığı (system usefulness), bilgi kalitesi (information quality), ara yüz kalitesi (interface quality) ve genel (overall) değerlendirme boyutlarından oluşan 13 maddelik, 1 den 7'ye kadar çok katılımdan az katılıma doğru ölçeklenmiş memnuniyet belirlemede kullanılan bir ölçektir (Erdinç, 2015). Bu 13 maddelik anketten tez çalışması kapsamında değerlendirmesi yapılan güvenlik kod türleri için hata mesajlarının kalitesini ölçen bilgi kalitesi başlığı altındaki maddeler dışındaki sistem yararlılığı, ara yüz kalitesi ve genel memnuniyet başlıklarını içeren 10 madde kullanılmıştır.
T-CSUQ anketinde yer alan 10 soruda 1.sorudan 6.soruya kadar olan sorular güvenlik kodu kullanışlılığı başlığı altında,7.sorudan 9. soruya kadar olan sorular güvenlik kodu ara yüz kalitesi başlığı altında ve 10.soru ise güvenlik kod türündeki memnuniyet başlığı altında incelenmektedir (Lewis,1993).

Ek-F de yer alan katılımcıların güvenlik kod türleri arasında tercih sıralamalarının istendiği güvenlik kod tercih anketi katılımcıların tüm güvenlik kodlar ile ilgili veri girişlerini tamamlandıktan sonra kullandıkları türleri tercih sıralamasına koydukları bir memnuniyet anketi olarak hazırlanmıştır.

3.5.2. Deneyler sırasında kullanılan donanım ve yazılım bileşenleri

Çalışma kapsamındaki kullanıcı deneylerini gerçekleştirebilmek için farklı güvenlik kod türleri ile kullanıcıların veri girişi yapmasını sağlayacak bir mobil uygulama ara

yüzü geliştirilmiştir. Bu uygulamanın geliştirilmesi için MacBook Air, uygulamanın çalıştırılması için de iPhone 6 model bir iOS cihaz kullanılmıştır. Uygulamayı geliştirmede yazılım bileşeni olarak; geliştirme ortamı olarak XCode kullanılırken uygulama Objective C dili ile geliştirilmiştir. Çalışma kapsamında kullanılan tüm yazılım ve donanım bileşenlerine ait bilgiler Tablo 3.4' de yer almaktadır.

Tablo 3.4. Tez çalışması kapsamında kullanılan donanım ve yazılımlar

Donanım	Akıllı telefon	Iphone 6
	Geliştirme Bilgisayarı	MacBook Air
Yazılım	Geliştirme Ortamı	XCode 11
	Geliştirme Uygulaması	CAPTCHA Uygulaması

3.5.3. Deney için geliştirilen mobil uygulama

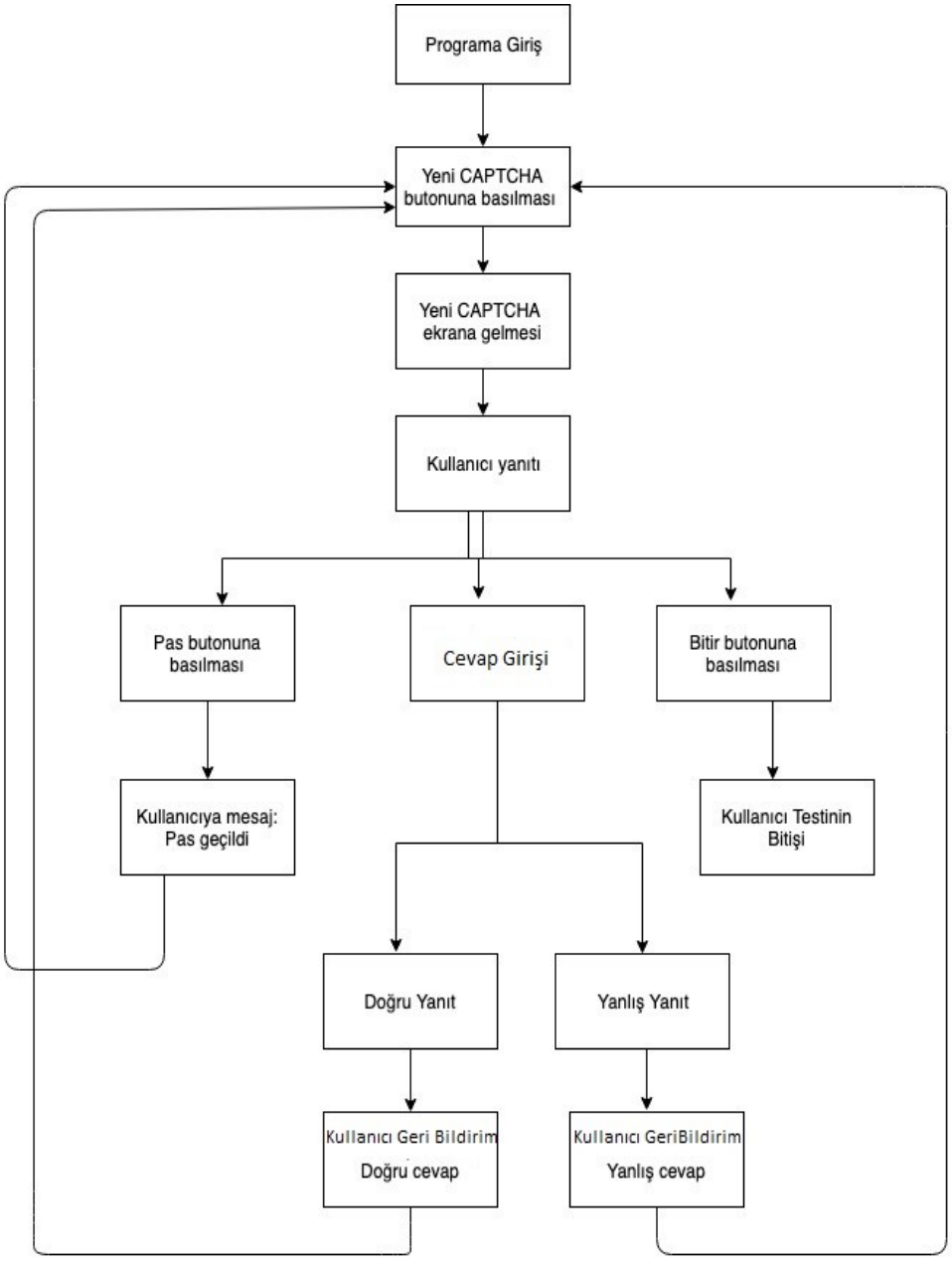
Çalışma kapsamındaki kullanıcı deneyleri dokunmatik özelliğe sahip IOS işletim sistemli akıllı telefon üzerinden gerçekleştirilmiştir. Akıllı telefonda çalışacak uygulama Objective C dilinde geliştirilmiştir. Geliştirilen bu uygulama aracılığıyla katılımcıların hata ve süre verilerinin otomatik olarak kayıt altına alınması sağlanmıştır. Uygulama her bir güvenlik kod türü için toplam hata, doğru cevap sayısı ve harcanan zamanı kaydetmektedir.

Kullanıcı uygulamayı açtığında karşısına gelen güvenlik kodları ara yüzdeki metin alanına sırasıyla girer. Katılımcılara altı farklı güvenlik kod türü için 4'er adet farklı güvenlik kod gösterilmesi her kullanıcı için sıralama rastgele olacak şekilde sağlanmaktadır. Böylece katılımcılar toplamda 24 adet güvenlik kod girişi gerçekleştirmişlerdir. Her güvenlik kod türü ile ilgili veri girişi tamamlandıktan sonra kullanıcıya grup testinin bittiği ve o kategori ile ilgili anketlere geçebileceğine dair mesaj verilir ve ilgili anketleri doldurmaları beklenir. Güvenlik kod türleri ve her tür içerisindeki güvenlik kodlar her bir katılımcıya rastgele sıra ile sunulmaktadır.

Güvenlik kod uygulaması açıldığında kullanıcının karşısına bir kullanıcı giriş ekranı çıkmaktadır. Kullanıcının teste başlaması için ilk olarak "Yeni CAPTCHA" düğmesine tıklaması ile ilk güvenlik kod türü karşısına çıkar. Şekil 3.3'de bir örneği görüldüğü üzere kullanıcı kendisi için ayrılan veri giriş kutusuna ekranda gördüğü güvenlik kodu yazar ve ardından "Cevapla" düğmesine basar. Eğer güvenlik kodu anlamakta zorluk çekiyor ya da cevaplamak istemiyor ise "Pas" butonuna basabilir bu işlem güvenlik kodu cevaplamadan bir sonrakine geçebilmesini sağlar. Kullanıcının

güvenlik kod ile gerçekleştirdiği işlemin durumuna göre kullanıcıya yapılan işlemin doğru, yanlış ya da pas olup olmadığı konusunda geribildirim sunulur. Test kapsamındaki 24 adet güvenlik kodun kullanıcı tarafından girişi tamamlandıktan sonra testin bittiğine dair kullanıcıya uyarı mesajı gösterilir. Geliştirilen uygulamaya ait sistem akışı Şekil 3.4'de görülmektedir.

Şekil 3.3. Uygulama ekranı



Şekil 3.4. Mobil uygulama akışı

Deney uygulamasında kullanıcı kendisine gösterilen güvenlik kodları cevaplarken arka planda kullanıcının harcadığı süre kayıt altına alınır. Her bir güvenlik kod türünde harcanan zamanın tutulması işlemi, kullanıcının "hazır" butonuna basması ile başlar ve "cevaplama" ya da "pas" butonuna basması ile sonlandırılır. Her bir güvenlik kod türü için harcanan süre ayrı ayrı tutulmaktadır. Uygulama süre bilgisinin yanı sıra kullanıcıların verdikleri yanıtların doğruluğunu da ayrıca kayıt altına almaktadır.

3.6. Veri Analizleri

Tez çalısması içerisinde deney esnasında kullanıcıların görev tamamlama süresi (verimlilik), hata sayısı (etkililik), kullanıcı memnuniyet anketleri ve sesli düşünme verileri kayıt altına alınmıştır. Tüm veriler tanımlayıcı istatistiksel yöntemlerle analiz edilmiştir. Her bir güvenlik kod türü için kullanıcıların cevaplama süresi ortalamaları hesaplanmış, hatalı cevapları belirlenmiş ve sonuçlar diğer güvenlik kod türlerinden elde edilen sonuçlar ile kıyaslanmıştır. Güvenlik kod türlerinin süre ve hata farklarının anlamlılığına dair tek yönlü varyans analizi uygulanmıştır. Farklılığın hangi türler arasında olduğunu incelemek adına post-hoc analizi yapılmıştır. Kullanıcıların yaş, deneyim ve cinsiyet faktörlerinin elde edilen değerlerdeki etkisi de incelenmiştir.

Nasa TLX bilişsel yük matrisinin uygulanması ve analiz edilmesi için NASA'nın kendi yapmış olduğu NASA Task Load Index (TLX @ NASA Ames - NASA TLX App t.y.) adlı mobil uygulama kullanılmıştır. Bu uygulama her bir kullanıcıya ait olan verileri analiz edip iş yükü matris sonucunu raporlamaktadır. Uygulama tarafından en fazla skora sahip olan eleman en fazla iş yüküne sahip, en az skora sahip olan eleman ise en az iş yüküne sahiptir şeklinde sonuçlandırılıp analiz edilmektedir.

TCSU-Q memnuniyet anketi ile elde edilen sonuçların analizi her bir maddenin ortalaması alınarak analiz edilmiştir (Erdinç, 2015). TCSU-Q da kullanıcılar anketteki her bir soruya karşılık 1 den 7 ye kadar puan vermektedir ve tüm soruların bitmesi ardından soruların ortalaması alınarak o kullanıcının memnuniyet puanı ortaya çıkmaktadır. Aynı zamanda verilen puanlarda 1 yüzde yüz memnuniyeti ifade ederken 7 yüzde sıfır memnuniyeti ifade etmektedir. Böylelikle birden fazla katılımcının yer aldığı ankette her bir kullanıcının puanı ya da puana karşılık gelen memnuniyet yüzdesi hesaplanarak, genel memnuniyet derecesi ortaya çıkmaktadır. (Lewis ve R 1993). TCSU-Q anketinde sorulan 13 sorunun içinde sistemin hata mesajlarının anlaşılır olup olmaması, problemlerin nasıl giderileceğine dair bilgi kalitesinin ölçüldüğü 3 madde yapılan çalışma ile ilgili olmadığı için dahil edilmemiştir. Tüm analizler sistem yararlılığı, ara yüz kalitesi ve genel memnuniyetin ölçüldüğü 10 madde için yapılmıştır.

Kullanıcı tercih sıralamasının sonuçları ise en fazla oranda kullanıcıların tercih ettikleri güvenlik kod türünün ilk sırayı alması ve en az tercih ettiklerinin en son sırayı alacak şekilde sıralanması ile analiz edilmiştir.

Son olarak da deney sırasında elde edilen sesli düşünme protokolüne ait notlar da ayrıca nitel olarak değerlendirilmiştir.

4. BULGULAR

Tez çalışması kapsamında deneyler kapsamında elde edilen bulgular dört ana bölümde sunulmuştur. İlk bölümde değerlendirilen güvenlik kodlara uygulanan güvenlik test sonuçları raporlanmaktadır. İkinci bölümde kullanıcı deneyi kapsamında katılımcıların farklı güvenlik kod türleri ile gerçekleştirdikleri performansın analizlerini içermektedir. Üçüncü bölüm katılımcıların farklı güvenlik kod türleri ile yaptıkları hataların analizlerini içermektedir. Dördüncü ve son bölüm ise dört alt bölümden oluşmaktadır. Katılımcıların memnuniyetine yönelik olarak NASA-TLX, T-CSUQ anketi, katılımcıların tüm deney bittikten sonra doldurdukları tercih sıralaması anketi ve nitel olarak incelenen katılımcılara ait sesli düşünme verilerinin sonuçlarını içermektedir.

4.1. Güvenlik Kodların Sağlamlık Değerlendirmeleri

Tez çalışması kapsamında değerlendirmeye tabi tutulan farklı özelliklerde 6 güvenlik kod türüne çeşitli güvenlik ataklarına karşın alan yazında da önerilen (Vithlani ve Kumbharana, 2015; Sakila, Vijayarani 2015) beş farklı güvenlik aracı ile test edilmiştir. Bahsedilen beş güvenlik testi araçları Google Docs, İ2OCR, Convert image to text.net, OCR Convert ve SimpleOCR'dir. Bu araçlar OCR kütüphaneleri kullanılarak oluşturulmuş resim içine gömülmüş olan metin ya da karakterleri ayırt eden ve tanıyan araçlardır. Her bir aracın tüm güvenlik kod türlerindeki çözülme yüzdesi Tablo 4.1 de görülmektedir. Çözülme oranı arttıkça güvenlik kodunun tanınma oranı artarak, güvenlik düzeyi düşmektedir.

Güvenlik testler sonucu incelendiğinde bozulma uygulanmış ve renk ayrımı az olan güvenlik kodlarında 5 güvenlik aracında da çözülme oranı %0 olmuş, hiçbir güvenlik aracı tarafından tanınmamıştır. Böylelikle güvenli güvenlik kod olduğu doğrulanmıştır.

Rastgele kelime, güvenlik testi sonucu incelendiğinde ise 4 ayrı rastgele kelime güvenlik kodlarından birinin Google Docs ve İ2OCR araçları tarafından çözülmüştür.

%25'lik çözülme oranıyla rastgele kelime güvenlik kodu güvenli olduğu fakat bozulma uygulanmış ve renk ayrımı az olan güvenlik kodlarına göre daha az güvenli olduğu görülmektedir.

Bozulma uygulanmamış, sözlük kelime ve renk ayrımı çok olan güvenlik kodları incelendiğinde ise 5 güvenlik aracı tarafından %100 oranında çözülmüş ve böylelikle tanınma oranına göre güvenli güvenlik kodları olmadığı doğrulanmıştır.

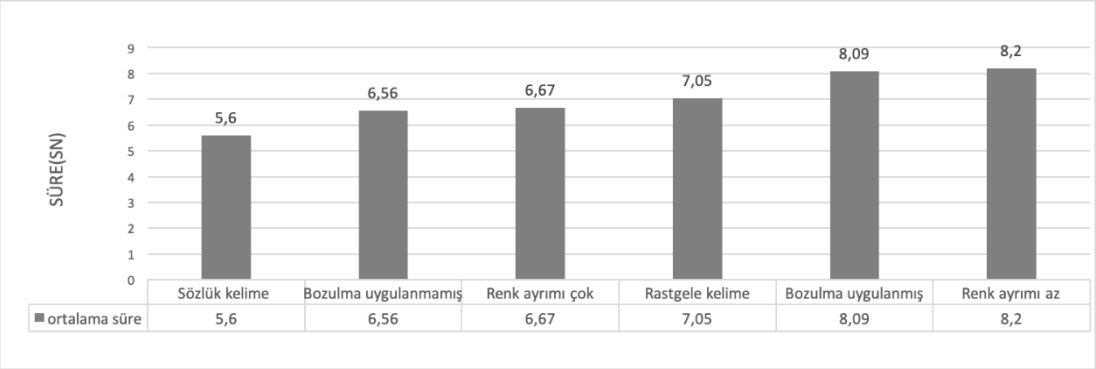
Tablo 4.1. Güvenlik kodlarının 5 ayrı güvenlik testi araçlarındaki sağlamlık oranı

OCR Araçları	İ2OCR Çözümü Başarı Yüzdesi	Convert image to text.net Çözümü Başarı Yüzdesi	Google Docs Çözümü Başarı Yüzdesi	OCR Convert Çözümü Başarı Yüzdesi	SimpleOCR Çözümü Başarı Yüzdesi	Güvenlilik Düzeyi
Rastgele kelime	%25	%0	%25	%0	%0	Güvenli
Bozulma uygulanmış	%0	%0	%0	%0	%0	Güvenli
Renk Ayrımı Az	%0	%0	%0	%0	%0	Güvenli
Sözlük Kelime	%100	%100	%100	%100	%100	Güvenli Değil
Bozulma uygulanmamış	%100	%100	%100	%100	%100	Güvenli Değil
Renk Ayrımı Çok	%100	%100	%100	%100	%100	Güvenli Değil

4.2. Veri Giriş Hızı (Verimlilik)

4.2.1. Farklı güvenlik kod türlerinin katılımcıların cevaplama sürelerine etkisi

Tez çalışması kapsamında değerlendirmeye tabi tutulan farklı özelliklerde 6 güvenlik kod türünde 30 katılımcının her bir güvenlik kod türünü cevaplama süresi Şekil 4.1'de görülmektedir. Ortalama görev cevaplama sürelerine göre sözlük kelime güvenlik kodu 5,6 sn ile en hızlı cevaplanırken, 8,2 sn ile renk ayrımı az güvenlik kodu katılımcılar tarafından en yavaş cevaplanmaktadır.



Şekil 4.1. Katılımcıların güvenlik kod türlerindeki ortalama cevaplama süreleri

Güvenlik kod türünün görev tamamlama süresine etkisi Tablo 4.2 de görüldüğü üzere istatistiksel olarak anlamlıdır (F(2.839, 82.319) =10.742, p=0,000). Bonferroni post-hoc analizi ile anlamlı farkın bulunduğu türler Tablo 4.3'de verilmiştir. Tabloda verilen ikililer (bozulma uygulanmış - bozulma uygulanmamış), (bozulma uygulanmış - sözlük kelime), (bozulma uygulanmış - renk ayrımı çok), (rastgele kelime - sözlük kelime) ve (renk ayrımı az - sözlük kelime) dışında kalan türler arasında anlamlı bir fark bulunmamıştır.

Tablo 4.2. Veri giriş hızı ANOVA analizi

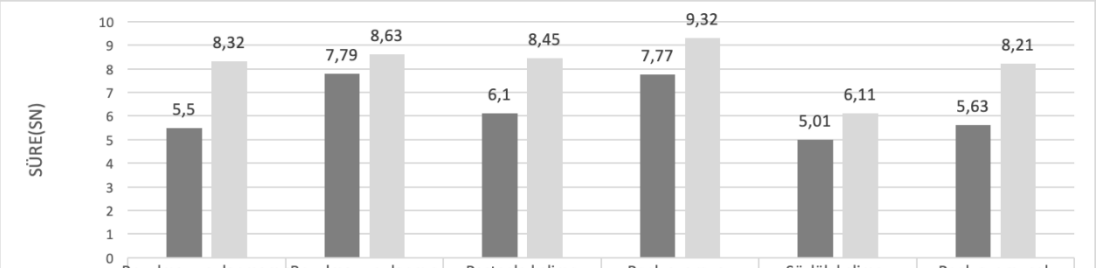
Kaynak	Kareler Toplamı	df	Ortalama Kare	F	p
Gruplar arası	146,724	2,839	51,689	10,742	0,000
Gruplar içi	396,115	82,319	4,812		
Toplam	542,839	85,158			

Tablo 4.3. Post Hoc analizi sonucuna göre ortalama cevaplama sürelerinde anlamlı farkın olduğu güvenlik kodlar

Güvenlik kodu(i)	Güvenlik kodu(j)	Ortalama farkı(i-j)	Standart sapma	p
Bozulma uygulanmış	Bozulma uygulanmamış	-1,527	0,440	0,025
Bozulma uygulanmış	Sözlük kelime	2,491	0,424	0,00
Bozulma uygulanmış	Renk ayrımı çok	1,419	0,436	0,043
Rastgele kelime	Sözlük kelime	1,448	0,333	0,002
Renk ayrımı az	Sözlük kelime	-2,602	0,595	0,002

Katılımcıların yaş faktörüne göre güvenlik kod türlerine ait ortalama süre bilgileri Şekil 4.2'de verilmiştir. Genç katılımcıların orta yaşlı katılımcılara göre tüm türlerde daha hızlı oldukları belirlenmiştir. Genç katılımcılar tarafından en hızlı cevaplanan tür 5,01 sn ile sözlük kelime, en yavaş cevaplanan tür 7,79 sn ile bozulma uygulanmış güvenlik kod olurken, orta yaşlı katılımcılar tarafından ise en hızlı cevaplanan tür 6,11

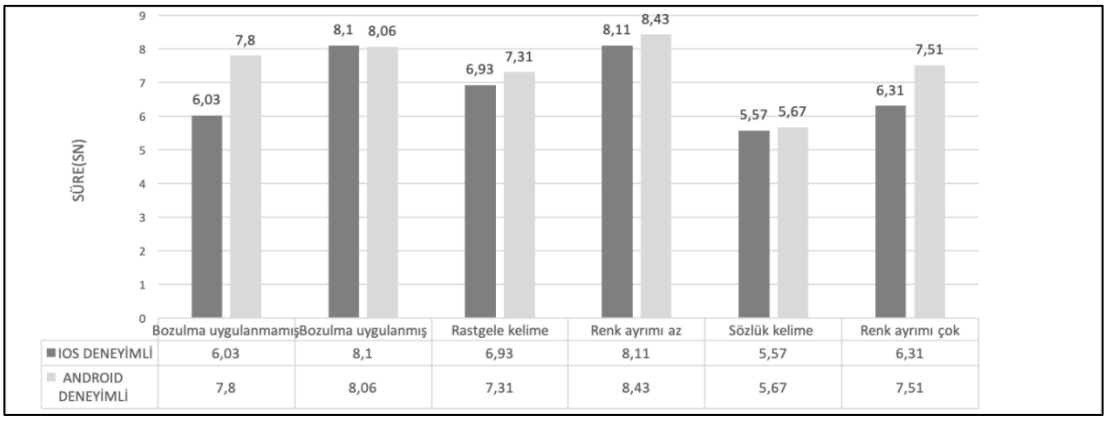
sn ile sözlük kelime, en yavaş cevaplanan tür ise 9,32 sn ile renk ayrımı az güvenlik kod olmuştur. Böylelikle hem genç hem de orta yaşlı katılımcıların en hızlı cevapladıkları tür sözlük kelime olmuştur. Genç ve orta yaşlılarda bozulma uygulanmamış türde en fazla fark yaşanırken, bozulma uygulanmış türde en az fark yaşanmıştır. Genç katılımcılar her bir türde orta yaşlı katılımcılardan daha hızlı veri girişi yapmıştır. İstatistiksel açıdan bozulma uygulanmamış, rastgele kelime ve renk ayrımı çok olan güvenlik kodu türlerinde fark genç katılımcılar yönünde anlamlıdır ($p< ,05$). Bunun dışında kalan bozulma uygulanmış, renk ayrımı az ve sözlük kelime türlerinde ise anlamlı fark bulunmamaktadır.



	Bozulma uygulanmamış	Bozulma uygulanmış	Rastgele kelime	Renk ayrımı az	Sözlük kelime	Renk ayrımı çok
Genç	5,5	7,79	6,1	7,77	5,01	5,63
Orta yaşlı	8,32	8,63	8,45	9,32	6,11	8,21

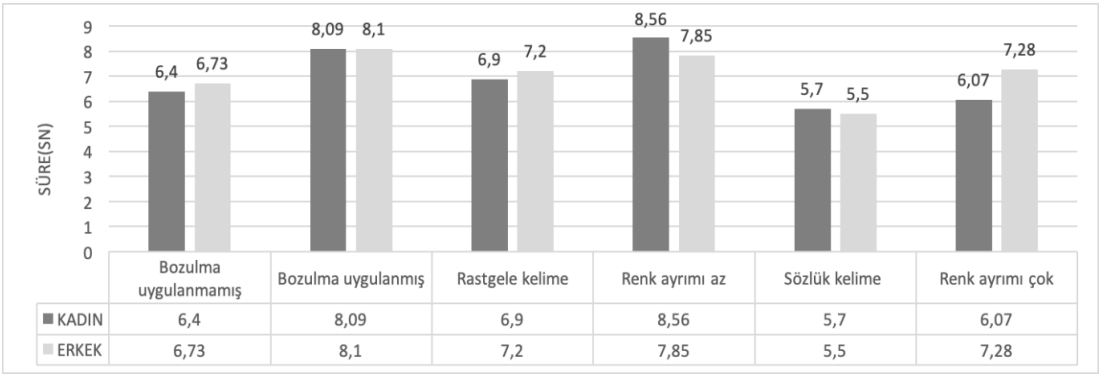
Şekil 4.2. Yaş faktörüne göre her bir güvenlik kod türünde ortalama görev tamamlama süresi

Deney katılımcılarının ortalama görev tamamlama süresi IOS işletim sistemli mobil cihaz kullanım tecrübesine göre değerlendirildiğinde Şekil 4.3'de görüldüğü gibi deneyimli katılımcıların deneyimsiz katılımcılara göre daha hızlı oldukları belirlenmiştir. Deneyimsiz kategorisindeki Android kullanıcıların en hızlı cevapladıkları tür 5,67 sn ile sözlük kelime olurken, en yavaş cevapladıkları tür ise 8,43 sn ile renk ayrımı az güvenlik kodu olmuştur. Deneyimli IOS kullanıcıların sonuçları incelendiğinde ise en hızlı cevapladıkları tür 5,57 sn ile yine sözlük kelime olurken, en yavaş cevapladıkları tür ise 8,11 sn ile renk ayrımı az güvenlik kodu olmuştur. Deneyim faktörüne göre hiçbir güvenlik kod türlerinde istatistiksel olarak anlamlı bir fark bulunmamıştır ($p> ,05$).



Şekil 4.3. Deneyim faktörüne göre her bir güvenlik kod türünde ortalama görev tamamlama süresi

Deney katılımcılarının ortalama görev tamamlama süresi cinsiyet faktörüne göre değerlendirildiğinde Şekil 4.4'de görüldüğü üzere kadın katılımcıların erkeklere göre daha hızlı oldukları belirlenmiştir. Kadın katılımcılarının en hızlı cevapladıkları tür 5,7 sn ile sözlük kelime olurken, en yavaş cevapladıkları tür ise 8,56 sn ile renk ayrımı az güvenlik kodu olmuştur. Erkek katılımcılarının en hızlı cevapladıkları tür 5,5 sn ile sözlük kelime olurken, en yavaş cevapladıkları tür ise 8,1 sn ile bozulma uygulanmış güvenlik kodu olmuştur. Cinsiyet faktörüne göre hiçbir güvenlik kod türlerinde istatistiksel olarak anlamlı bir fark bulunamamıştır (p> ,05).

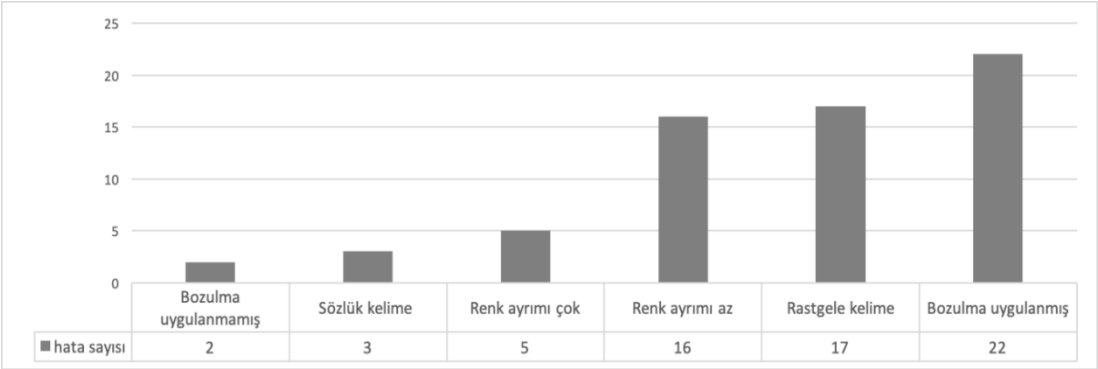


Şekil 4.4. Cinsiyet faktörüne göre her bir güvenlik kod türünde ortalama görev tamamlama süresi

4.3. Hata

Tez çalışması kapsamında değerlendirmeye tabi tutulan farklı özelliklerdeki 6 güvenlik kod türünde 30 katılımcının yapmış oldukları hata sayıları Şekil 4.5'de görüldüğü gibidir. Tüm katılımcıların veri girişleri incelendiğinde en fazla hata yapılan güvenlik kod türünün toplamda 22 hata ile bozulma uygulanmış güvenlik kod olduğu

ve en başarılı olarak yanıtlanan türün toplamda 2 hata ile bozulma uygulanmamış güvenlik kod olduğu görülmüştür.



Şekil 4.5. Katılımcıların güvenlik kod türlerindeki hata sayıları

Güvenlik kod türünün hata sayısına etkisi Tablo 4.4 de görüldüğü üzere istatiksel olarak anlamlıdır (F(3,005, 88,587) = 6,005, p=.001). Bonferroni post-hoc analizi ile anlamlı farkın bulunduğu türler Tablo 4.5 de verildiği üzere bozulma uygulanmış güvenlik kodu ile bozulma uygulanmamış (p=,035) ve sözlük kelime güvenlik kodu (p=,043) arasında anlamlı fark bulunmuştur. Benzer şekilde rastgele kelime ile bozulma uygulanmamış güvenlik kod (p=,035) arasında da anlamlı fark bulunmuştur. Verilen ikililer dışında kalan türler arasında anlamlı bir fark bulunmamıştır.

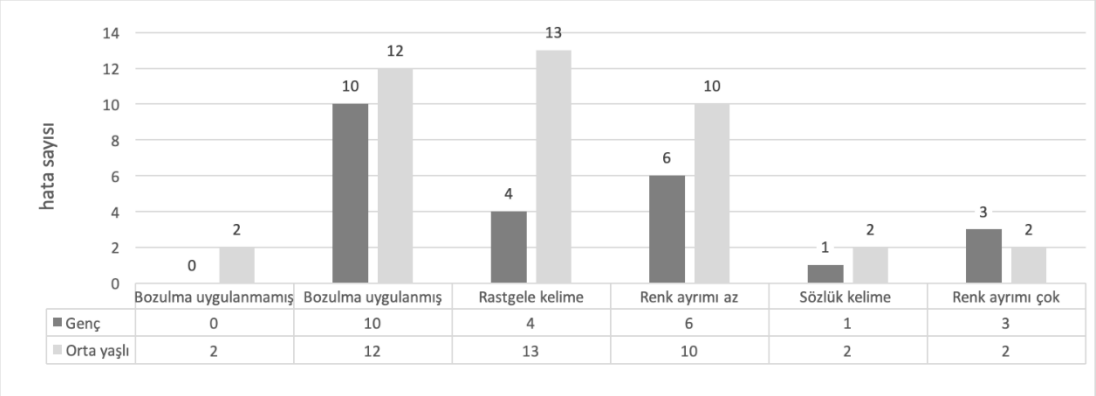
Tablo 4.4. Etkililik düzeyi ANOVA analizi

Kaynak	Kareler Toplamı	df	Ortalama Kare	F	p
Gruplar arası	12,094	3,055	3,959	6,005	0,001
Gruplar içi	58,406	88,587	0,659		
Toplam	869,3	91,642			

Tablo 4.5. Post Hoc analizi sonucu etkililikte anlamlı farkın olduğu güvenlik kodları

Güvenlik kodu(i)	Güvenlik kodu(j)	Ortalama farkı(i-j)	Standart sapma	p
Bozulma uygulanmış	Bozulma uygulanmamış	-0,667	0,200	0,035
Bozulma uygulanmış	Sözlük kelime	0,633	0,195	0,043
Rastgele kelime	Bozulma uygulanmamış	0,500	0,150	0,035

Deney katılımcılarının her bir güvenlik kod türünde yapmış olduğu hatalar yaş faktörüne göre değerlendirildiğinde genç katılımcıların orta yaşlılara göre daha az hata yaptığı belirlenmiştir. Genç katılımcıların en başarılı oldukları tüm yanıtları doğru cevapladıkları güvenlik kod türü bozulma uygulanmamış güvenlik kod türü olurken en başarısız oldukları güvenlik kod türü ise toplamda 10 hata ile bozulma uygulanmış güvenlik kod türü olmuştur. Orta yaşlı katılımcıların en başarılı oldukları türler incelendiğinde eşit sayıda 2'şer hata ile sözlük kelime ve renk ayrımı çok güvenlik kod türleri olurken, en fazla hata yaptıkları güvenlik kod türü ise toplamda 13 hata ile rastgele kelime olmuştur. İstatistiksel açıdan rastgele kelime güvenlik kod türünde fark genç katılımcılar yönünde anlamlıdır ($p < ,05$). Bunun dışında kalan bozulma uygulanmış, bozulma uygulanmamış, renk ayrımı çok, renk ayrımı az ve sözlük kelime türlerinde ise anlamlı fark bulunmamaktadır. Katılımcıların yaş faktörüne göre güvenlik kod türlerinde yapmış oldukları hata sayılarına ait bilgiler Şekil 4.6' de verilmiştir.

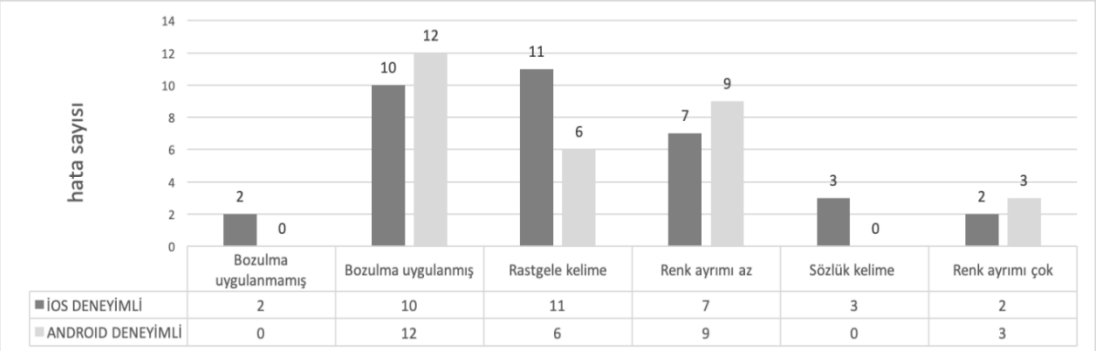


	Bozulma uygulanmamış	Bozulma uygulanmış	Rastgele kelime	Renk ayrımı az	Sözlük kelime	Renk ayrımı çok
Genç	0	10	4	6	1	3
Orta yaşlı	2	12	13	10	2	2

Şekil 4.6. Yaş faktörüne göre her bir güvenlik kod türünde yapılan hata sayısı

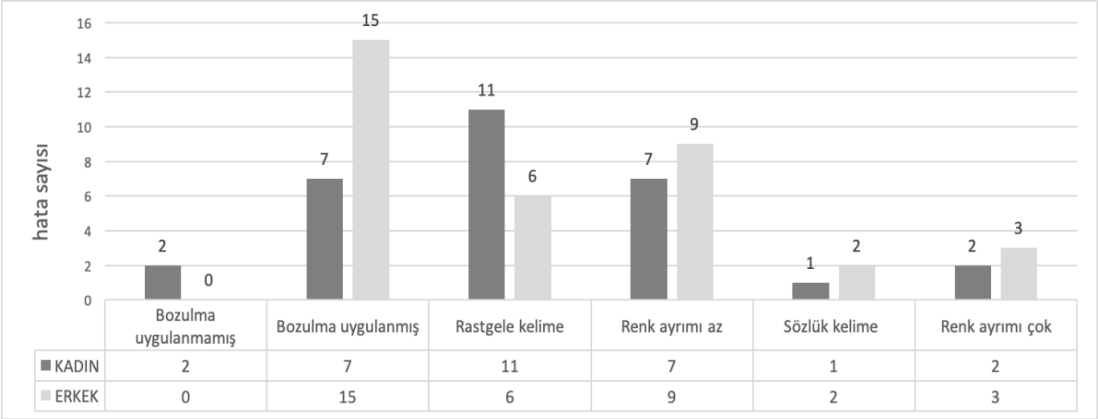
Deney katılımcılarının her bir güvenlik kod türünde yapmış olduğu hatalı cevap sayıları deneyime göre değerlendirildiğinde deneyimsiz katılımcıların IOS deneyimi olan katılımcılara göre bozulma uygulanmış, renk ayrımı az ve renk ayrımı çok güvenlik kodları dışındaki tüm türlerde daha az hata yaptığı ve daha fazla başarılı olduğu görülmüştür. IOS deneyimli katılımcıların en başarılı oldukları güvenlik kod türü 2 hata ile bozulma uygulanmamış ve renk ayrımı çok güvenlik kodu türleri olurken en başarısız oldukları güvenlik kod türü ise toplamda 11 hatalı yanıt ile rastgele kelime güvenlik kod türü olmuştur. Deneyimsiz katılımcıların en başarılı oldukları tüm yanıtları doğru cevapladıkları güvenlik kod türleri bozulma

uygulanmamış ve sözlük kelime güvenlik kodu olurken, en başarısız oldukları güvenlik kod türleri ise toplamda 12 hatalı yanıt ile bozulma uygulanmış güvenlik kod türü olmuştur. Deneyim faktörüne göre hiçbir güvenlik kod türlerinde istatistiksel olarak anlamlı bir fark bulunamamıştır (p>,05). Katılımcılarının tecrübe faktörüne göre güvenlik kod türlerinde yapmış oldukları hata sayılarına ait bilgiler Şekil 4.7' de verilmiştir.



Şekil 4.7. Deneyim faktörüne göre her bir güvenlik kod türünde yapılan hata sayısı

Deney katılımcıların her bir güvenlik kod türünde yapmış olduğu hatalı cevap sayıları cinsiyet faktörüne göre değerlendirildiğinde kadın katılımcıların bozulma uygulanmamış ve rastgele kelime güvenlik kodu dışındaki tüm türlerde daha az hata yaptığı ve erkek katılımcılara göre daha hızlı olduğu görülmüştür. Kadın katılımcıların en başarılı olarak cevap verdikleri güvenlik kod türü 1 hatalı cevap ile sözlük kelime olurken, en başarısız oldukları güvenlik kod türü ise 11 hatalı yanıt ile rastgele kelime olmuştur. Erkek katılımcılar incelendiğinde en başarılı oldukları tüm yanıtları doğru cevapladıkları bozulma uygulanmamış güvenlik kod türü olurken, en başarısız oldukları ise 15 hatalı yanıt ile bozulma uygulanmış güvenlik kod türü olmuştur. Cinsiyet faktörüne göre güvenlik kod türlerinin hiçbiri arasında istatistiksel olarak anlamlı bir fark bulunamamıştır (p>,05). Katılımcılarının cinsiyet faktörüne göre güvenlik kod türlerinde yapmış oldukları hata sayılarına ait bilgiler Şekil 4.8' de verilmiştir.



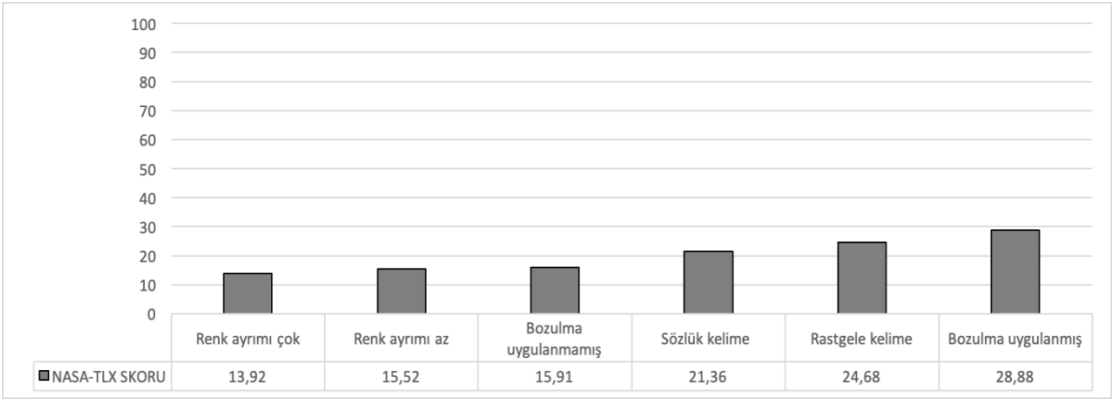
Şekil 4.8. Cinsiyet faktörüne göre her bir güvenlik kod türünde yapılan hata sayısı

4.4. Memnuniyet

Tez çalışması kapsamında gerçekleştirilen deneylerden elde edilen görev tamamlama süresi verilerine ek olarak katılımcıların her bir güvenlik kod türündeki memnuniyetlerini ölçmek için NASA-TLX, T-CSUQ anketi ve kullanıcı tercih sıralaması anketlerini doldurmaları istenmiştir. Ayrıca katılımcılardan deney sırasında sesli düşünmeleri istenmiştir. Bu verilere ait bulgular bu bölümde sunulmaktadır.

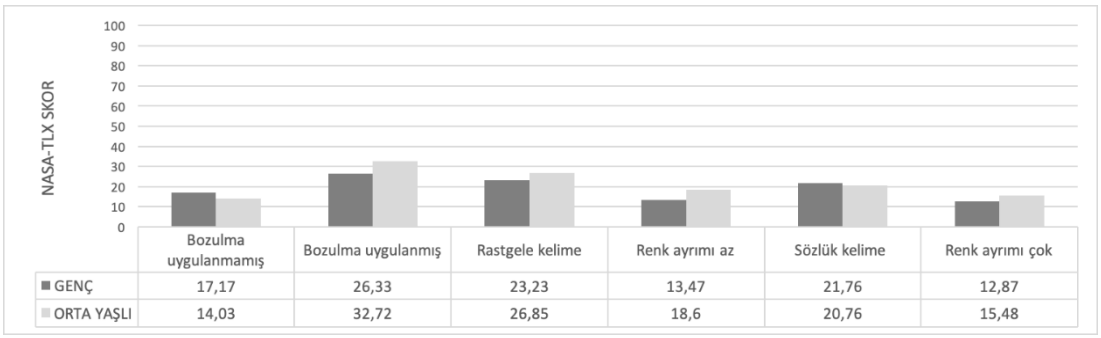
4.4.1. NASA-TLX bilişsel yük anketi

Katılımcılara ait NASA-TLX bilişsel yük matrisi verileri incelendiğinde 100 skorluk matriste en fazla iş yüküne sahip olan güvenlik kod türü 28,88 puanla bozulma uygulanmış güvenlik kodu olurken, en az iş yüküne sahip olan güvenlik kod türü ise 13,92 puanla renk ayrımı çok güvenlik kod türü olmuştur. Katılımcıların her bir güvenlik kod türü için bilişsel yük matrisinde vermiş oldukları puanlara ait bilgiler Şekil 4.9' da verilmiştir. Bu skor dağılımına göre çalışma kapsamında incelenen güvenlik kod türlerinin katılımcılar üzerinde fazla iş yükü oluşturmadığı ortaya çıkmıştır.



Şekil 4.9. Her bir güvenlik kod türünde ortalama NASA TLX skorları

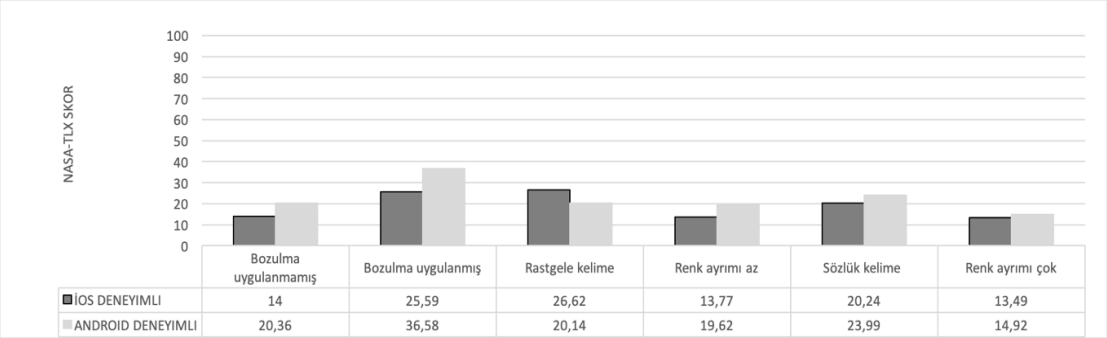
Deney katılımcılarının her bir güvenlik kod türünde NASA –TLX verileri yaş faktörüne göre değerlendirildiğinde, orta yaşlı katılımcıların genç katılımcılara göre daha fazla iş yükü yaşadıkları ortaya çıkmaktadır. Genç katılımcıların en fazla iş yükü yaşadığı güvenlik kod 26,33 puanla bozulma uygulanmış güvenlik kodu olurken, en az iş yükü yaşadıkları ise 12,87 puanla renk ayrımı çok güvenlik kod olmuştur. Orta yaşlı katılımcıların da en fazla iş yükü yaşadıkları güvenlik kod türü 32,72 puanla genç katılımcılar gibi bozulma uygulanmış güvenlik koddur. Diğer taraftan en az iş yükü yaşadıkları tür ise 14,03 puanla bozulma uygulanmamış güvenlik kod türü olmuştur. Katılımcılarının yaş faktörüne göre bilişsel yük matrisinde vermiş oldukları puanlara ait bilgiler Şekil 4.10'da verilmiştir.



Şekil 4.10. Yaş faktörüne göre her bir güvenlik kod türünde ortalama NASA TLX skorları

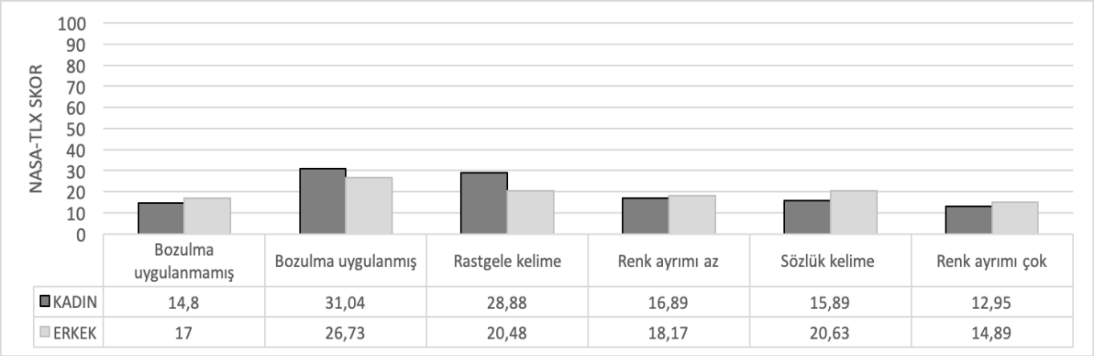
Deney katılımcılarının her bir güvenlik kod türünde NASA–TLX verileri deneyim faktörüne göre değerlendirildiğinde, rastgele kelime güvenlik kodu dışında kalan tüm türlerde deneyimli katılımcılar deneyimsiz katılımcılara göre daha az iş yükü yaşadıkları görülmektedir. IOS deneyimli katılımcıların en fazla iş yükü yaşadığı güvenlik kod türü 26,62 puanla rastgele kelime güvenlik kodu olurken, en az iş yükü

yaşadıkları güvenlik kod türü 13,49 puanla renk ayrımı çok güvenlik kod türü olmuştur. IOS tecrübesi olmayan, Android tecrübesi olan katılımcıların en fazla iş yükü yaşadıkları güvenlik kod türü 36,58 puanla bozulma uygulanmış güvenlik kod türü olurken, en az iş yükü yaşadıkları güvenlik kod türü tıpkı tecrübeli katılımcılar gibi 14,92 puanla bozulma uygulanmış güvenlik kod türü olmuştur. Katılımcılarının deneyim faktörüne göre bilişsel yük matrisinde vermiş oldukları puanlara ait bilgiler Şekil 4.11' de verilmiştir.



Şekil 4.11. Deneyim faktörüne göre her bir güvenlik kod türünde ortalama NASA TLX skorları

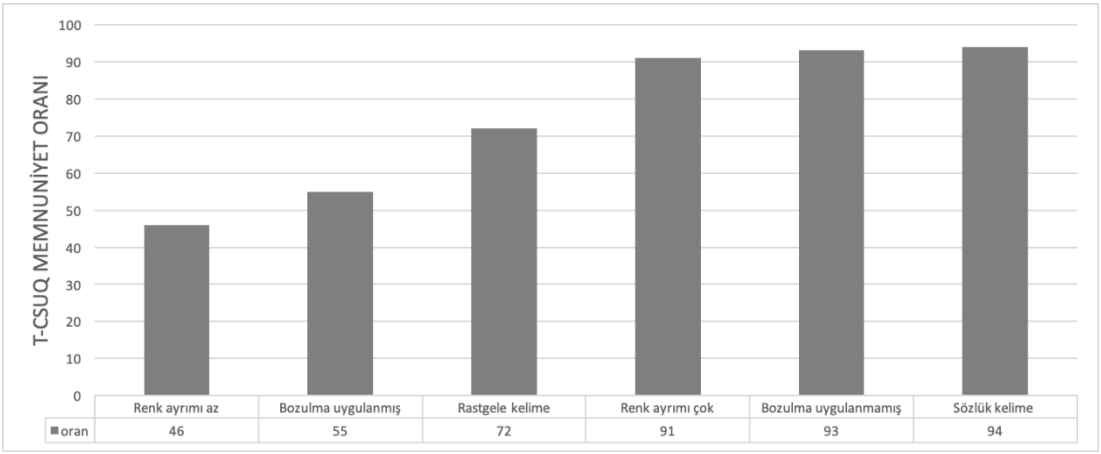
Deney katılımcılarının her bir güvenlik kod türünde NASA–TLX verileri cinsiyet faktörüne göre değerlendirildiğinde, bozulma uygulanmış ve rastgele kelime güvenlik kod türlerinde erkek katılımcılar kadın katılımcılara göre daha az iş yükü yaşarken bunların dışında kalan tüm türlerde kadın katılımcılar erkek katılımcılara göre daha az iş yükü yaşamışlardır. Kadın katılımcıların iş yükünü en fazla değerlendirdikleri güvenlik kod türü 31,04 puanla bozulma uygulanmış güvenlik kod türü olurken en az iş yükü gördükleri güvenlik kod türü ise 12,95 puanla renk ayrımı çok güvenlik kod türü olmuştur. Erkek katılımcılar incelendiğinde ise tıpkı kadın katılımcılar gibi en fazla iş yükünü 26,73 puanla bozulma uygulanmış güvenlik kod ile yaşarken, en az iş yükünü ise 14,89 puanla renk ayrımı çok olan güvenlik kod türünde yaşamışlardır. Katılımcılarının cinsiyet faktörüne göre bilişsel yük matrisinde vermiş oldukları puanlara ait bilgiler Şekil 4.12' de verilmiştir.



Şekil 4.12. Cinsiyet faktörüne göre her bir güvenlik kod türünde ortalama NASA TLX skorları

4.4.2. T-CSUQ memnuniyet anketi

T-CSUQ anketinde sistem yararlılığı, ara yüz kalitesi ve genel memnuniyet başlıkları altında yer alan toplamda 10 soruluk ankette her bir güvenlik kod türünde katılımcıların memnuniyetleri belirlenmiştir. Katılımcılar tarafından en fazla memnun olunan tür %94 oranındaki memnuniyet ile sözlük kelime güvenlik kodu olurken, en az memnun olunan tür ise %46 oranındaki memnuniyet ile renk ayrımı az olan güvenlik kod olarak belirlenmiştir. T-CSUQ anketinde her bir güvenlik kod türünde yaşanan memnuniyet dereceleri Şekil 4.13'de verilmiştir.



Şekil 4.13. T-CSUQ anketinde her bir güvenlik kod türünde yaşanan memnuniyet dereceleri

T-CSUQ anketine katılımcılar tarafından verilen yanıtlar kullanışlılık, ara yüz kalitesi ve genel memnuniyet boyutlarına göre incelendiğinde tüm güvelik kod türleri için memnuniyet yüzdeleri Tablo 4.6'da verilmektedir. Tablo incelendiğinde tüm maddelerde bozulma uygulanmamış güvenlik kodu uygulanmış güvenlik koduna göre,

renk ayrımı çok renk ayrımı az olana ve sözlük kelime rastgele kelimeye göre daha fazla memnun kalınan güvenlik kodu olmuştur.

Tablo 4.6. Katılımcıların güvenlik kod türlerindeki farklı T-CSUQ boyutlarındaki memnuniyet dereceleri

Memnuniyet faktörleri	**Bozulma Uygulanmamış**	**Bozulma Uygulanmış**	**Renk ayrımı çok**	**Renk ayrımı az**	**Sözlük kelime**	**Rastgele kelime**
Kullanışlılık	%85	%58	%90	%52	%94	%73
Ara yüz kalitesi	%91	%49	%88	%40	%95	%68
Genel memnuniyet	%93	%48	%91	%41	%96	%65

T- CSUQ anketi bulguları yaş, deneyim ve cinsiyet farklılıklarına göre de incelenmiştir. Yaş faktörüne göre memnuniyet dereceleri incelendiğinde hem genç hem de orta yaşlı katılımcıların en memnun oldukları türler bozulma uygulanmamış güvenlik kod olurken, en az memnuniyet yaşanılan tür yine her iki yaş grubu için renk ayrımı az güvenlik kod olmuştur. Deneyimli katılımcıların en memnun oldukları tür sözlük kelime olurken, en az memnuniyet yaşadıkları tür renk ayrımı az güvenlik kodu olmuştur. Deneyimsiz katılımcıların en memnun oldukları tür bozulma uygulanmamış güvenlik kodu iken, en az memnun oldukları tür deneyimli katılımcılarda da olduğu gibi renk ayrımı az güvenlik kod olmuştur. Cinsiyet faktörüne göre güvenlik kod türünde memnuniyet incelendiğinde erkek katılımcıların en memnun oldukları tür sözlük kelime olurken, en az memnuniyet yaşadıkları tür renk ayrımı az güvenlik kod olmuştur. Kadın katılımcıların en memnun oldukları tür ise bozulma uygulanmamış güvenlik kod türü olurken, en az memnun oldukları tür erkek katılımcılarda da olduğu gibi renk ayrımı az güvenlik kodu olmuştur. Kullanıcılara ait yaş, deneyim ve cinsiyet faktörlerine göre T-CSUQ anket sonuçları Tablo 4.7 de verilmiştir.

Tablo 4.7. Kullanıcılara ait yaş, deneyim ve cinsiyet faktörlerine göre T-CSUQ anket sonuçları

GÜVENLİK KOD MEMNUNİYETİ	YAŞ		DENEYİM		CİNSİYET	
	Genç	Orta yaşlı	Deneyimli	Deneyimsiz	Kadın	Erkek
En çok memnun kalınan	bozulma uygulanmamış	bozulma uygulanmamış	sözlük kelime	bozulma uygulanmamış	bozulma uygulanmamış	sözlük kelime
En az memnun kalınan	renk ayrımı az	renk ayrımı az	renk ayrımı az	renk ayrımı az	renk ayrımı az	renk ayrımı az

4.4.3. Tüm katılımcıların her bir güvenlik kod türündeki tercih sıralamaları

Katılımcıların en çok tercih etmiş olduğu güvenlik kod türlerini belirlemek için deney kapsamında kullandıkları güvenlik kod türlerini 1 den 6 ya kadar çok beğenilenden az beğenilene doğru sıraya koymaları istenmiştir. Tercih sıralaması anketi incelendiğinde ise ilk sırayı 18 katılımcının oyu ile bozulma uygulanmamış güvenlik kodu, 2. sırayı 9 katılımcının oyu ile sözlük kelime, 3.sırayı 15 katılımcının oyu ile renk ayrımı çok güvenlik kodu,4.sırayı 22 katılımcının oyu ile rastgele kelime güvenlik kodu, 5.sırayı 20 katılımcının oyu ile bozulma uygulanmış güvenlik kodu ve son sırayı ise 24 katılımcının oyu ile renk ayrımı az olan güvenlik kodu almıştır.

Tercihler incelendiğinde katılımcılar büyük çoğunlukta güvenlik kodlarında daha kullanılabilir olanları tercih etmişler ve güvenlik düzeyleri daha yüksek olan rastgele kelime, bozulma uygulanmış ve renk ayrımı az olan güvenlik kodlarını ise daha az tercih etmişlerdir.

4.4.4. Sesli düşünme

Kullanıcı deneyleri esnasında, katılımcılardan güvenlik kod türleri ile ilgili düşündüklerini ve yorumlarını ve her bir türü özellikle ara yüz, işlevsellik ve anlama kolaylığı açısından beğenip beğenmediklerini sesli olarak ifade etmeleri istenmiştir. Her bir katılımcının sesli olarak güvenlik kod türü ile ilgili ara yüz memnuniyeti, anama kolaylığı ve işlevselliğini değerlendirmeleri istenmiştir. Belirtilen yorumlar kayıt altına alınmıştır. Her bir güvenlik kodu için katılımcıların genel görüşü sırayla verilmiştir.

Katılımcılar çalışmada incelenen tüm güvenlik kod türlerinden özellikle bozulma uygulanmamış, sözlük kelime ve renk ayrımı çok olan güvenlik kodları; beğendiklerini ifade etmişlerdir. Bu türler için ara yüzlerinin tatmin edici olduğunu ve işlevsel açıdan yeterli olduklarını belirtmişlerdir. Ayrıca sistemi anlama kolaylığı açısından da olumlu değerlendirmişler ve verimli olduğu yönünde görüş bildirmişlerdir. Özellikle sözlük kelime güvenlik kodu için K3 "harfleri tek tek bakmak yerine bütün olarak kelimeye bakabildiğim için hızlı ve kolay cevaplıyorum" yorumunda bulunmuştur.

Katılımcılar renk ayrımı az olan güvenlik kodun tatmin edici olmadığını, işlevsel açıdan ve anlama kolaylığı açısından yeterli olmadığını belirtmiş ve ara yüzü konusunda olumsuz değerlendirme yapmışlardır. Özellikle K2, K10, K19 kodlu katılımcılar metin ve arka planın yakın renklerde olmasının kendilerini rahatsız ettiğini ve gözlerinin yorulduğunu, kelimeleri anlamak için oldukça zahmet çekildiğini ifade etmişlerdir.

Bozulma uygulanmış güvenlik kodu için katılımcılar ara yüzü, işlevselliği ve anlama kolaylığı açısından olumsuz değerlendirme yapmışlardır. Özellikle K6 ve K10 kodlu katılımcılar bozulma uygulanmış güvenlik kodunda bozulmuş bir kelimeye bakmanın gözlerini yorduğunu, doğru giriş yapılabilse bile bunun katılımcıları olumsuz anlamda etkileyeceğini belirtmişlerdir.

Rastgele kelime güvenlik kodu için katılımcılar belirtilen türün anlaşılabilir olduğunu ve işlevsel açıdan yeterli olduğunu belirtmektedirler. Ara yüzü konusunda net olarak olumlu ya da olumsuz değerlendirme yapamamışlardır. Özellikle K3 harfler arasındaki mesafenin kısaltılması cevap süresini azaltacağına dair öneride bulunmuştur bunun yanı sıra birden fazla sesli ya da sessiz harflerin yan yana gelmesi belirtilen türde harflerin tek tek değil de bir sözcük gibi kodlanmasını zorlaştıracağı için cevaplama süresini azaltabileceğini belirtmiştir.

Katılımcıların her bir güvenlik kod türü için yaptıkları yorumlarına dayalı olarak, ara yüz, işlevsellik ve anlama kolaylığı açısından genel değerlendirme sonuçları Tablo 4.8'de verilmiştir. Bozulma uygulanmamış, sözlük kelime ve renk ayrımı çok olan güvenlik kod katılımcılar tarafından ara yüz, anlama kolaylığı ve işlevsellik açısından beğenilirken; bozulma uygulanmış ve renk ayrımı az olan güvenlik kod ara yüz, anlama kolaylığı ve işlevsellik yönüyle beğenilmemiştir. Rastgele kelime güvenlik

kodunu ise katılımcılar anlama kolaylığı ve işlevsellik açılarından yeterli bulurken, ara yüz açısından beğenilmemiştir.

Tablo 4.8. Sesli düşünme her bir türdeki değerlendirme sonuçları

Güvenlik kod türü	Destekleyen Katılımcılar	Ara yüz memnuniyeti	Anlama kolaylığı	İşlevsellik
Bozulma uygulanmamış	K1-30	X	X	X
Sözlük kelime	K1-30	X	X	X
Renk ayrımı çok	K1-30	X	X	X
Bozulma uygulanmış	K1-30	-	-	-
Rastgele kelime	K1-30	-	X	X
Renk ayrımı az	K1-30	-	-	-

5. SONUÇLAR VE ÖNERİLER

Sonuç bölümü üç ana bölümden oluşmaktadır. Birinci bölüm çalışmanın özetini, ikinci bölüm alan yazın araştırmasından elde edilen bilgiler ve test bulgularının birleştirilmesi ile metin-bazlı güvenlik kod türünde yazılım geliştiricilere yönelik oluşturulan tavsiyeleri son bölüm ise çalışmaya ait kısıt ve gelecek çalışma önerilerini içermektedir.

5.1. Çalışmanın Özeti

Bu tez çalışması kapsamında mobil ara yüzlerde kullanılan farklı türlerdeki metin-tabanlı güvenlik kodlarının etkililik, verimlilik ve memnuniyet faktörleri açısından kullanıcı testleri ile karşılaştırılması sağlanmıştır. Alan yazında incelenen güvenlik kodlar ile ilgili birçok çalışmada güvenlik ve kullanılabilirlik ayrı ayrı incelenirken hem güvenlik hem de kullanılabilirlik faktörlerinin beraber değerlendirildiği çalışmalar kısıtlıdır. İncelenen bu çalışmaların sonucunda bazı tasarım prensipleri ya kullanılabilirliği geliştirmeye yönelik ya da güvenlik düzeyini artırmaya yönelik olarak önerilmektedir. Uygulama geliştiriciler açısından uygulamaya dahil edilecek güvenlik kodun belirlenmesi sırasında hem kullanılabilirlik düzeyi yüksek olan hem de saldırılara karşı sağlam olan bir türün tercih edilmesi oldukça önemlidir. Bu çalışma ile güvenlik kodlar için kullanılabilirlik ve güvenlik, beraber değerlendirilerek mobil ara yüzlerde kullanılabilecek sağlamlık ve kullanılabilirlik konularını dengeleyen bir türün belirlenmesi konusunda uygulama geliştiricilere yönelik öneriler oluşturularak alan yazına katkı sağlamak hedeflenmiştir.

Çalışma kapsamında mobil uygulamalarda kullanılmak üzere bozulma uygulanmış, bozulma uygulanmamış, sözlük kelime, rastgele kelime, renk ayrımı az ve renk ayrımı çok olacak şekilde metin temelli altı farklı türde güvenlik kod belirlenmiştir. Çalışmanın birinci aşamasında bu güvenlik kodlarının sağlamlığını ölçmek için çeşitli güvenlik ataklarına karşın alan yazında da önerilen (Vithlani ve Kumbharana, 2015; Sakila, Vijayarani 2015) beş farklı güvenlik aracı ile sağlamlık testleri uygulanmıştır. Bu araçlar Google Docs, İ2OCR, Convert image to text.net, OCR Convert ve SimpleOCR'dir. Testler sonucunda güvenlik testlerinden sözlük kelime, renk ayrımı

çok ve bozulma uygulanmamış güvenlik kod türleri %100 tanınma oranı ile güvenli bulunmazken, rastgele kelime yüzde %10, bozulma uygulanmış ve renk ayrımı az güvenlik kod türleri ise %0 tanınma oranı ile güvenli olduğu belirlenen güvenlik kod türleri olmuştur.

Çalışma kapsamında sağlamlık testleri yapılan güvenlik kod türlerinin kullanılabilirliğini ölçmek için kullanıcı testleri otuz gönüllü katılımcıyla gerçekleştirilmiştir. Kullanıcı testleri kapsamında gerçekleştirilen deney prosedürü içerisinde katılımcıların güvenlik kodlarını cevaplama süreleri, güvenlik kodlarındaki hata sayıları ölçülmüş, katılımcıların veri girişi yaptıkları güvenlik kodlar ile ilgili olarak kullanıcı memnuniyetini değerlendirmek üzere de anketler uygulanmıştır. Bu anketler ve uygulamadan elde edilen verilerle katılımcıların deney sırasında kullandıkları güvenlik kodun kullanılabilirliği, her bir güvenlik kodun kullanıcı üzerinde oluşturduğu bilişsel yükün miktarını ve katılımcıların güvenlik kod tercihlerini belirlemek hedeflenmiştir. Kullanıcı çalışmasından elde edilen bulgular aynı zamanda güvenlik kodların sağlamlığı ve kullanılabilirliği ile ilgili gerçekleştirilmiş önceki çalışmalarda da raporlanan çeşitli tavsiyeler ile birleştirilerek mobil ara yüz geliştiricilere yol gösterecek tavsiyeler listesi oluşturulmuştur.

Çalışma kapsamında altı farklı türde güvenlik kodları ile katılımcıların cevaplama süreleri, yapmış oldukları hata sayıları, NASA TLX, T-CSUQ ve tercih sıralaması anketi sonuçları incelendiğinde en kullanılabilir güvenlik kod türleri ortalama süre ve T-CSUQ sonuçlarına göre sözlük kelime, hata sayısı analizi ve kullanıcı tercih sıralamasına göre bozulma uygulanmamış, NASA TLX analiz sonuçlarına göre ise renk ayrımı çok olan güvenlik kod türleri olmuştur. Süre, T-CSUQ ve tercih sıralaması anketlerine göre renk ayrımı az güvenlik kod türü, NASA TLX anketi ve hata sayısına göre bozulma uygulanmış güvenlik kod türü en az kullanılabilirlik düzeyinde olan güvenlik kod türlerinden olmuştur. Bu sonuçlar, alan yazındaki çalışmalar ile de büyük oranda da tutarlılık göstermektedir (Bursztein vd. 2010; Banday ve Sheikh 2013; Tangmanee ve Sujarit-apirak 2012). Bozulma uygulanmamış güvenlik kodunda herhangi bir bozma işlemi ya da renk karmaşıklığı yer almadığı için; sözlük kelime güvenlik kodunda ise kullanıcılar tarafından bilinen sözlük kelimeleri olduğu için daha kolay tanınması başarı ve memnuniyet düzeyini artırmıştır. Renk ayrımı az olan ve bozulma uygulanmış güvenlik kodlarında harflerle arka tonun birbirine daha kolay

karışması, harflerin bozulma işlemlerinden dolayı tanınmasının zorlaşması ve zaman alması, katılımcılar tarafından daha az süre harcanması ve memnuniyetle karşılanmasına sebep olmuştur.

Araştırma sonucunda güvenlik testlerinden sözlük kelime, renk ayrımı çok ve bozulma uygulanmamış güvenlik kod türlerine göre daha başarıyla geçen rastgele kelime, bozulma uygulanmış ve renk ayrımı az güvenlik kod türlerinden ortalama süre, T-CSUQ ve tercih sıralaması anketi sonuçlarına göre en kullanılabilir olan tür rastgele kelime güvenlik kodu olmuştur. Rastgele kelime güvenlik kod türü bozulma uygulanmış ve renk ayrımı az güvenlik kod türüne göre sağlamlık testlerinde tanınma oranı daha fazla olmasına rağmen insan tarafından kolay anlaşılabilmesi, kullanılabilir olması gerektiği için dengeyi sağlamaya yönelik tercih edilen tür olmuştur. Rastgele kelimede, sözlük kelime kullanılmadığı için sözlük ataklarına ve tanıma atağına karşı sözlük kelimelerine göre daha güçlüdür (Yan ve El Ahmad 2008; Roshanbin ve Miller 2013). Bunun yanında bozulma uygulanmadığı ve katılımcıların zorlanacağı farklı renk işlemlerine maruz kalmadığı için katılımcılar harfler karışık şekilde yazılmış olsa da kolay anlayabilmekte ve daha yüksek memnuniyet seviyesiyle tercih etmektedirler. Bozulma uygulanmış güvenlik kodu alan yazında ve güvenlik testlerindeki sonuçlara göre de güvenli olan güvenlik kod türlerinden olmuştur (Yan ve El Ahmad 2008),(Vidya ve Shrinivasa), kullanılabilirlik olarak incelendiğinde ise rastgele kelimeden sonra en kullanılabilir olan güvenli güvenlik kod türü olmuştur. Renk ayrımı az olan güvenlik kodları hem alan yazın hem de yapılan güvenlik testleri ile güvenilir olduğu belirlenen güvenlik kod türüdür (Roshanbin ve Miller 2013), (Baykara, Alnıak, ve Çınar 2018). Fakat rastgele kelime ve bozulma uygulanmış güvenlik kod türlerine göre daha az kullanılabilir olduğu analiz sonuçlarına göre belirlenmiştir. Tablo 5.1 de çalışma bulgularına dayalı olarak güvenli güvenlik kod seçiminde aynı zamanda kullanılabilir olan türe yönelik öneriler sunulmuştur. İlk sırada hem sağlamlığı yüksek hem de kullanılabilirlik açısında önerilebilecek olan güvenlik kod türü rastgele kelime güvenlik kodu iken alternatif olarak ise bozulma uygulanmış güvenlik kod önerilmektedir.

Tablo 5.1. Sağlam ve kullanılabilir güvenlik kod seçimi için öneriler

Güvenlik kod Türü	Destekleyen Veri	Destekleyici Atıflar
Rastgele kelime	(Süre), (T-CSUQ), (Tercih Anketi)	(Yan ve El Ahmad 2009), (Roshanbin ve Miller 2013), (Bentley ve Mallows 2006)
Bozulma uygulanmış	(Süre), (T-CSUQ), (Tercih Anketi)	(Yan ve El Ahmad 2008), Kaur ve Behal (2014), (Rusu, Thomas, ve Govindaraju 2010)

5.2. Metin Tabanlı Güvenlik Kod Türlerinde Geliştiricilere Yönelik Tavsiyeler

Güvenlik kodlar birçok otomatik atağa maruz kalmaktadır. Uygulama geliştiriciler açısından uygulamaya dahil edilecek güvenlik kodun belirlenmesi sırasında hem güvenlik düzeyi hem de kullanılabilirliği yüksek olan bir türün tercih edilmesi oldukça önemlidir. Tez çalışması kapsamında yapılan test sonuçları ve alan yazından elde edilen bilgilere dayalı olarak mobil ara yüz tasarımcılarına uygulamaları için tercih edecekleri güvenlik kod türlerini belirlemede yol gösterici olacak tavsiyeler belirlenmiştir.

Mobil cihazlar için güvenlik kodlarda klavyede harflerden karakterlere geçerken kaydırma gerçekleşmesi kullanılabilirlik oranını azaltmaktadır. Bunu engellemek adına yalnızca harflerden ya da yalnızca rakamlardan oluşan güvenlik kod tasarımlarının daha kullanılabilir olduğu belirtilmektedir (Reynaga, Chiasson ve Oorschot, (2015). Bunun dışında, anadili dışında başka dilleri bilseler dahi kullanıcıların kendi anadilinde bulunan sözlük kelime güvenlik kodu türlerinde daha başarılı olacağı vurgulanmaktadır (Banday ve Sheikh 2013; Tangmanee ve Sujarit-apirak 2012; Bursztein vd. 2010; Fidas ve Voyiatzis 2013). Tez çalışmasında değerlendirme kapsamında alınan güvenlik kodlarda bu doğrultuda rakam ve harf beraber kullanılmamış sadece alfabede yer alan harflerden oluşmuş, birbiri ile karışabilecek kullanıcıların zorlanacağı karakterler (o harfi ve 0 rakamı gibi) yan yana kullanılmamış ve anadili Türkçe olan kullanıcılarla çalışılacağı için Türkçe alfabeden

harfler seçilen güvenlik kod örnekleri kullanılmıştır. Bu örneklere ait kullanılabilirlik bulguları alan yazınla tutarlı olarak katılımcılar tarafından daha olumlu değerlendirilmiştir.

Metin tabanlı güvenlik kodlarda cevaplama zamanı oldukça önem arz etmektedir ve önerilen değer ise 10 saniyeyi geçmemesidir (Bursztein vd. 2010). Bunun yanında kullanıcıların ilk denemede cevaplayabilecekleri zorlukta güvenlik kodu oluşturulması da kullanıcıların ilk denemede çözemediklerinde olumsuz etkilenmesine ve diğer denemelerde de başarı oranlarını düşürdüğüne yönelik çalışmalar mevcuttur (Fidas vd. 2011), (Yan ve Ahmad 2007). Tez çalışması kapsamında değerlendirilen tüm güvenlik kod türlerinde cevaplama süresi 10 saniyeyi geçmemiştir.

Diğer taraftan güvenlik arttırmaya yönelik olarak atakları önlemek için metin tabanlı güvenlik kodlarda harflere daha fazla çarpıklık, bozulma, eğrilme, hizalama, döndürme işlemlerinden geçirilmesi (Yan ve El Ahmad 2008) ve sözlük kelimeleri değil de karışık karakterlerin kullanılması (Yan ve El Ahmad 2009), (Roshanbin ve Miller 2013) önerilmektedir. Bu öneriler doğrultusunda belirlenen güvenlik kodların katılımcılar tarafından kullanılabilirliği diğerlerine göre daha düşük olarak değerlendirilmiştir.

Sonuç olarak özellikle güvenlik ve kullanılabilirliği dengeleyici şekilde mobil ara yüzlerde kullanılacak metin tabanlı güvenlik kodlarda alan yazın ve tez çalışması kapsamında elde edilen bulgular doğrultusunda mobil ara yüz geliştiricilere önerilecek tavsiyeler aşağıdaki şekilde listelenmektedir.

- Yalnız rakam veya yalnız harflerin kullanımı,
- Birbiri ile karışabilecek kullanıcıların zorlanacağı karakterlerin yan yana kullanılmaması,
- Mümkün olduğunca kullanıcıların anadiline yönelik alfabelerden harflerin seçilmesi
- Karakterlerin rastgele seçilmesi
- Karakterlere bozulma uygulanması

5.3 Kısıtlar ve Gelecek Çalışmalar

Tez çalışması ile ilgili bahsedilmesi gereken bazı kısıtlar vardır. Öncelikle güvenlik kodlar web site ve uygulamalarda kimlik denetimi sırasında kullanılmaktadır. Ancak çalışmada kullanılan ara yüz gerçek kullanım ortamında olmayan bir prototip olarak tasarlanmıştır. Gerçek bir kimlik denetimin yapıldığı otantik bir görev ortamında güvenlik kod türlerinin test edilmesi gelecek çalışma konuları arasında değerlendirilebilir.

Tez çalışmasında yer alan katılımcı sayısı sınırlıdır ve büyük çoğunluğu bilgi teknolojileriyle ilgilenen kullanıcılardır. Bu nedenle daha fazla sayıda ve farklı alanlarda deneyime sahip katılımcılarla çalışmanın örnekleminin genişletilerek çalışma yeniden gerçekleştirilebilir.

Tez sonucunda önerilen tavsiyelere göre mobil ortamda kullanılabilecek hem kullanılabilir hem de sağlam güvenlik kod tasarımlarının geliştirilmesi ve yine test edilerek değerlendirilmesi de gelecek çalışma konuları arasında değerlendirilebilir

KAYNAKLAR

Acar Y., Fahl S., Mazurek M. L., You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users, *2016 IEEE Cybersecurity Development (SecDev)*, 2016, 3-8.

Ahmad A., Yan J., Marshall L., The robustness of a new CAPTCHA, Proceedings of the 3rd European Workshop on System Security, EUROSEC'10, 2010, 36-41.

Ahmad A., Yan J.,Wai-Yin N., CAPTCHA design: Color, usability, and security. Internet Computing, 2012 IEEE. **16**(2), 44 - 51. DOI: 10.1109/MIC.2011.102.

Ahmad A., Yan J., Marshall L., The robustness of a new CAPTCHA. Proceedings of the 3rd European Workshop on System Security, 2010, EUROSEC'10. 36-41. DOI: 10.1145/1752046.1752052.

Ahn L., Blum M. , Hopper N. , Langford J. CAPTCHA: using hard AI problems for security. Advances in Cryptology, Eurocrypt, 2003, 2656. 294-311, DOI: 10.1007/3-540-39200-9_18.

Ahn L., Blum M., McMillen C., Abraham D. , Blum, M. reCAPTCHA: Human-based character recognition via Web security measures. Science (New York, N.Y.), 2008, DOI:321. 1465-8. 10.1126/science.1160379.

Ahn L., Blum M., Langford J., Telling Humans and Computers Apart Automatically, *Commun. ACM*, 2004, **47**(2), 56–60.

Aljarbou Y.S., Improving of Current CAPTCHA Systems, 2019 *2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, 1-6., DOI:10.1109/CAIS.2019.8769466

Alsuhibany S., Evaluating the Usability of Optimizing Text-based CAPTCHA Generation. International Journal of Advanced Computer Science and Applications, 2016, 164-169, DOI: 10.14569/IJACSA.2016.070823.

Alshamari M., A Review of Gaps between Usability and Security/Privacy, *International Journal of Communications, Network and System Sciences*, 2016, **9**, 413-429.

Althamary I.A., El-Alfy E.S.M, A more secure scheme for CAPTCHA-based authentication in cloud environment, *2017 8th International Conference on Information Technology (ICIT)*, 2017, 405-411.

Arachchilage N. A. G., Love S., A Game Design Framework for Avoiding Phishing Attacks, *Comput. Hum. Behav.*,2013, **29**(3), 706–714

Banday M.T., Sheikh S.A., Design of CAPTCHA Script for Indian Regional Websites. In: Thampi S.M., Atrey P.K., Fan CI., Perez G.M. (eds) Security in Computing and Communications. SSCC 2013. Communications in Computer and Information Science, vol 377. Springer, Berlin, Heidelberg

Basin D., Radomirovic S., Schmid L., Modeling Human Errors in Security Protocols, *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, 2016, 325-340.

Baird H.S., Moll M.A., Wang S.Y., ScatterType: a legible but hard-to-segment CAPTCHA, *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)*, 2005, 2, 935-939.

Baykara M., Alnıak F., Çınar K., Review and comparison of captcha approaches and a new captcha model, *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, 2018, pp. 1-6. DOI:10.1109/ISDFS.2018.8355316

Beautement A., Sasse A., Wonham M., The compliance budget: managing security behaviour in organisations, *Proceedings of the 2008 workshop on New security paradigms - NSPW '08*, Lake Tahoe, California, USA, 2008, 47.

Belk M., Fidas C., Germanakos P., Samaras G., Do Human Cognitive Differences in Information Processing Affect Preference and Performance of CAPTCHA?. International Journal of Human-Computer Studies, 2015, DOI:84. 10.1016/j.ijhcs.2015.07.002.

Bentley J., Mallows C., CAPTCHA challenge strings: Problems and improvements, c. 6067, Oca. 2006.

Berbecaru D., Lioy A., Efficient Attribute Management in a Federated Identity Management Infrastructure, *2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*, 2016, 590-595.

Beheshti S. M., Liatsis P., CAPTCHA Usability and Performance, How to Measure the Usability Level of Human Interactive Applications Quantitatively and Qualitatively?, *2015 International Conference on Developments of E-Systems Engineering (DeSE)*, 2015, 131-136.

Bishop M., *Computer security art and science*. Boston, MA: Addison-Wesley, 2003.

Braz C., Robert J.M., Security and Usability: The Case of the User Authentication Methods, içinde *Proceedings of the 18th Conference on L'Interaction Homme-Machine*, New York, NY, USA, 2006, 199–203.

Brewster S., Overcoming the Lack of Screen Space on Mobile Computers. Personal and Ubiquitous Computing, 2002, DOI: 6.10.1007/s007790200019.

Brodić D., Amelio A., Exploring the usability of the text-based CAPTCHA on tablet computers, Connection Science, 2019, 31:4, 430444,
DOI: 10.1080/09540091.2019.1609417

Brodić D., Petrovska S., Jevtić, M., Milivojević Z. N., The influence of the CAPTCHA types to its solving times, *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016, 1274-1277.

Bursztein E., Martin M., Mitchell J. Text-based CAPTCHA strengths and weaknesses, 2011, 125-138, DOI: 10.1145/2046707.2046724.

Bursztein E., Moscicki A., Fabry C., Bethard S., Mitchell J., Jurafsky D. Easy does it: more usable CAPTCHAs, 2014, Conference on Human Factors in Computing Systems - Proceedings. DOI: 10.1145/2556288.2557322.

Bursztein E., Bethard S., Fabry C., Mitchell J., Jurafsky D., How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation, 2010 IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, 2010, 399-413, DOI:10.1109/SP.2010.31

Caputo D. D., Pfleeger S. L., Sasse M. A., Ammann P., Offutt J., Deng L., Barriers to Usable Security? Three Organizational Case Studies, *IEEE Secur. Privacy*,2016, **14**(5), 22-32

Chellapilla K., Larson K., Simard P.Y., Czerwinski M., Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs), *Human Interactive Proofs*, 2005, 1-26.

Chew M., Baird H. S., BaffleText: a Human Interactive Proof, Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, 2003, **50**(10), 305-316.

Choudhary S., Understanding Captcha: Text and Audio Based Captcha with its Applications, *International Journal of Advanced Research in Computer Science and Software Engineering*, c. 3, Haz. 2013.

Coates L., Baird H.S., Faternan R.J., Pessimal print: a reverse Turing test, içinde *Proceedings of Sixth International Conference on Document Analysis and Recognition*, 2001, 1154-1158.

Chow Y.W., Susilo W., Text-based CAPTCHAs over the years, *IOP Conference Series: Materials Science and Engineering*, c. 273, s. 012001, Kas. 2017.

Chow Y.W., Susilo W., Thorncharoensri P., CAPTCHA Design and Security Issues, 2019, 69-92.

Chow R., Golle P., Jakobsson M., Wang L., Wang X, Making CAPTCHAs clickable, 2008, 91-94, DOI:10.1145/1411759.1411783.

Cranor L.F., Garfinkel S., *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc., 2005.

Çağıltay K., *İnsan bilgisayar etkileşimi ve kullanılabilirlik mühendisliği: Teoriden pratiğe*, ODTÜ Yayıncılık, Ankara, 2011.

Erdinc O., Kullanılabilirlik Çalışmaları için Türkçe Computer System Usability Questionnaire (CSUQ) Anketi, 2015.

Fidas C., Voyiatzis A., On Users' Preference on Localized vs. Latin-Based CAPTCHA Challenges, 2013, 358-365.DOI: 10.1007/978-3-642-40498-6_28.

Fidas C., Voyiatzis V., Nikolaos M. Avouris M.,On the necessity of user-friendly CAPTCHA. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11),2011, Association for Computing Machinery, New York, NY, USA, 2623–2626. DOI: 10.1145/1978942.1979325

Fischer-Hübner S., *IT-Security and Privacy - Design and Use of Privacy-Enhancing Security Mechanisms*. 2001.

Flechais I., Sasse A. Usable Security: Why Do We Need It? How Do We Get It?, 2005.

Frøkjær E., Hertzum M., Hornbæk K., Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?, *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '00*, The Hague, The Netherlands, 2000, 345-352.

Golle P., Machine learning attacks against the asirra CAPTCHA. Proceedings of the ACM Conference on Computer and Communications Security,2008, 535-542. DOI:10.1145/1455770.1455838.

Green M., Smith M., Developers are Not the Enemy!: The Need for Usable Security APIs, *IEEE Security Privacy*,2016, **14**(5), 40-46

Hart S. G., Staveland L. E., *Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research*. 1988.

Hof H.J., Socher G., *Security Design Patterns With Good Usability*. 2016.

ISO 17799, Information technology — Security techniques — Code of practice for information security managementn, Switzerland, 2005.

ISO 9241-9, Ergonomic requirements for office work with visual display terminals (VDTs)-Part 9: Requirements for non-keyboard input devices (FDIS-Final Draft International Standard), *International Organization for Standardization*, Switzerland, 2000.

ISO 9241-11: Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11 Guidance on usability, The international organization for standardization, 1998

Jeffries R., Miller J. R., Wharton C., Uyeda K. M., User interface evaluation in the real world: A comparison of four techniques, *Proceedings of ACMCHI'91*, 1991, 119–124.

Kainda R., Usability and Security of Human-Interactive Security Protocols., 2011.

Kainda R., Flechais I., Roscoe A. W., Security and Usability: Analysis and Evaluation, *2010 International Conference on Availability, Reliability and Security*, 2010, 275-282.

Kaur K., Behal S., Captcha and Its Techniques: A Review, *International Journal of Computer Science and Information Technologies,* c. 5, Oca. 2014.

Kaur K., Behal S., Designing a Secure Text-based CAPTCHA. Procedia Computer Science, 2015, **57**, 122-125.

Kulkarni S., Fadewar H. S., Pedometric CAPTCHA for mobile Internet users, *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, 2017, 600-604.

Lewis J.R., *IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use*, c. 7. 1993.

Li K.C., Chen X., Susilo W., *Advances in Cyber Security: Principles, Techniques, and Applications*. Springer, 2018.

MacKenzie I. S., *Human-Computer Interaction: An Empirical Research Perspective*, 1st bs. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2013.

Martin R. ISO 14001 Guidance Manual, National Centre for environmental decision-making research:Technical report, 1998

Nadaph A., Shaikh J., Bodhe N., Pingale H., Video CAPTCHA – Design Based on Moving Object Recognition, International Journal of Innovative Research in Computer and Communication Engineering, 2007, **4**, 4-7.

Nielsen J., *Usability Engineering*, Academic Press, Boston,1993.

Pala M., Wang Y., On the Usability of User Interfaces for Secure Website Authentication in Browsers, 2009, 239-254.

Parkin S., Fielder A., Ashby A., Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes, 2016.

Pressman R. Software Engineering: A Practitioner's Approach. Palgrave Macmillan, London,2005.

Realpe-Muñoz P., Collazos C. A., Hurtado J., Granollers T., Velasco-Medina J., An Integration of Usable Security and User Authentication into the ISO 9241-210 and ISO/IEC 25010:2011, *Human Aspects of Information Security, Privacy, and Trust*, 2016, 65-76.

Reynaga, G., Chiasson S., Oorschot P. Exploring the Usability of CAPTCHAS on Smartphones: Comparisons and Recommendations, 2015, DOI:10.14722/usec.2015.23006.

Reynaga G., Chiasson S., The usability of CAPTCHAs on smartphones, *2013 International Conference on Security and Cryptography (SECRYPT)*, 2013,**4**, 1-8.

Roshanbin N., Miller J., A survey and analysis of current CAPTCHA approaches, *Journal of Web Engineering*, 2013, **12**, 1-40

Rubin J., *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*, 1st bs. New York, NY, USA: John Wiley & Sons, Inc., 1994.

Rusu A., Thomas A., Govindaraju V., Generation and use of handwritten CAPTCHAs, *IJDAR*, c. 13, sy 1, 49-64, Mar. 2010.

Shackel B., Human factors for informatics usability. Cambridge University Press, USA, 1991

Tangmanee C., Sujarit-apirak P., Attitudes towards CAPTCHA: A survey of thai internet users. Journal of Research and Practice in Information Technology, 2012, **44**(4), 441-458.

Tangmanee C., User Test on Text-Based CAPTCHA: A Letter Case Examination. Journal of Applied Security Research. 2018,13, 250-266. DOI:10.1080/19361610.2018.1422372.

Tharad A., Bhatt A., Srivastava S., Kumar P., Analysis & Impact of Current Captcha Approaches and its Significance, *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS),* Belgaum, India, 2018, pp. 487-493. DOI: 10.1109/CTEMS.2018.8769168

Tognazzini B., First Principles of Interaction Design (Revised & Expanded) 2014.

TÜBİTAK, SGEP: Güvenli Yazılım Geliştirme Kılavuzu,TÜBİTAK, Kocaeli, 2018

URL-1: https://www.webopedia.com/TERM/S/security.html, (Ziyaret tarihi: 21-Eki-2019).

URL-2:https://www.yumpu.com/en/document/view/16717715/strong-captcha-guidelines-v12-123seminarsonly , (Ziyaret tarihi: 28-Eki-2019).

URL-3: https://humansystems.arc.nasa.gov/groups/TLX/tlxapp.php, TLX @ NASA Ames - NASA TLX App,Kaliforniya, (Ziyaret tarihi: 30-Eki-2019).

URL-4: https://its.ucsc.edu/security/training/intro.html, (Ziyaret tarihi: 21-Eki-2019).

Van Someren M., The Think Aloud Method: A Practical Guide to Modelling Cognitive Processes, 1994.

Vijayarani S., Sakila A., Performance Comparison of OCR Tools. International Journal of UbiComp, 2015, **6**, 19-30.

Vithlani P., C.K.Kumbharana C., Comparative Study of Character Recognition Tools. International Journal of Computer Applications, 2015, **118**(9), 31-36.

Wilkins J. Strong CAPTCHA Guidelines v1.2, 2009.

Wismer A., Madathil R., Koikkara K., Juang J., Greenstein J., Chalil M.,Evaluating the usability of CAPTCHAs on a mobile device with voice and touch input. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2012, 56. DOI:10.1177/1071181312561217.

Yan J., Ahmad A., CAPTCHA security: A case study, *Security & Privacy, IEEE*, 2009, **7**(4), 22-28.

Yan J., Ahmad A.S.E., Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms, *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, 2007,4, 279-291.

Yan J., Ahmad A.S.E, Usability of CAPTCHAs or usability issues in CAPTCHA design, *Proceedings of the 4th symposium on Usable privacy and security - SOUPS '08*, Pittsburgh, Pennsylvania, 2008, s. 44.

Yan J., Ahmad A.S.E, Captcha Robustness: A Security Engineering Perspective. Computer, 2011, **44**(2), 54 - 60.

Yan J., Ahmad A. A low-cost attack on a microsoft CAPTCHA. Proceedings of the ACM Conference on Computer and Communications Security. 2008, 543-554, DOI:10.1145/1455770.1455839.

Yamamoto T., Tygar J. D., Nishigaki M., CAPTCHA Using Strangeness in Machine Translation, *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, 430-437.

Zhang L., Xie Y., Luan X., He J., Captcha automatic segmentation and recognition based on improved vertical projection, *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, 2017, 1167-1172.

EKLER

Ek-A Etik Kurul Onayı

Evrak Tarih ve Sayısı: 03/05/2019-E.34962

T.C.
KOCAELİ ÜNİVERSİTESİ
Fen ve Mühendislik Bilimleri Etik Kurulu

Sayı : 10017888-100/
Konu : Nur MERDANOĞLU Etik Kurul İstemi Hk.

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 22/04/2019 tarihli, 32085 sayılı ve "Nur MERDANOĞLU Etik Kurul İstemi Hk." konulu yazı

Fen ve Mühendislik Bilimleri Etik Kurulunun 30/04/2019 tarih ve 2019/07 no lu toplantısında alınan 1 sıra sayılı kararı aşağıda sunulmuştur.

Bilgilerinize rica ederim.

Prof.Dr. Alpaslan FIĞLALI
Kurul Başkanı

Karar No 1: Fen Bilimleri Enstitüsü Müdürlüğünün 22/04/2019 tarih ve 32085 sayılı yazısı görüşüldü. Bilgisayar Mühendisliği Anabilim Dalı programı yüksek lisans öğrencisi Nur MERDANOĞLU'nun, Dr.Öğr.Üyesi Pınar ONAY DURDU'nun danışmanlığında yürüttüğü "Mobil Ara Yüzlerde CAPTCHA Türlerinin karşılaştırılması" konulu yüksek lisans tez çalışması için kullanacağı çalışmanın uygulanmasında, **bilimsel araştırma ve yayın etiği açısından bir sakınca olmadığına oy birliği ile karar verildi.**

Mevcut Elektronik İmzalar

ALPASLAN FIĞLALI (Fen ve Mühendislik Bilimleri Etik Kurulu - Kurul Başkanı) 03/05/2019 12:38

Fen ve Mühendislik Bilimleri Etik Kurulu Kocaeli Üniversitesi Umuttepe Yerleşkesi 41380, Kocaeli
Tel:+90 (262) 303 10 01 Faks:+90 (262) 303 10 33
E-Posta :rekiletisim@kocaeli.edu.tr Elektronik Ağ :http://www.kocaeli.edu.tr

Ek-B Gönüllü Bilgilendirme Formu

Sayın Katılımcı,

Bir araştırma çalışmasına davet edilmektesiniz. Karar vermeden önce araştırmanın neden ve nasıl yapılacağını anlamanız çok önemlidir. Lütfen biraz zaman ayırın ve aşağıdaki bilgileri dikkatlice okuyun, isterseniz başkalarıyla tartışın. Açık olmayan bir bölüm varsa ya da daha ayrıntılı bilgiye ihtiyaç duyuyorsanız lütfen bizi arayın. Ancak araştırmaya katılmak isteyip istemediğinize karar vermek için lütfen biraz düşünün.

Bu araştırma çalışması Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda Dr. Öğr Üyesi Pınar Onay Durdu danışmanlığında yüksek lisans öğrencisi Nur Merdanoğlu tarafından yüksek lisans tezi kapsamında " Metin-tabanlı Güvenlik Kodların Mobil Ara yüzlerde Kullanılabilirliğinin Karşılaştırması" amacı ile gerçekleştirilmektedir.

Dr Öğr Üyesi Pınar Onay Durdu	Nur Merdanoğlu
Kocaeli Üniversitesi	Kocaeli Üniversitesi
Bilgisayar Mühendisliği Bölümü	Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği ABD
pinar.onaydurdu@kocaeli.edu.tr	
303 3570	nurmer93@gmail.com

Çalışma kapsamında değerlendirilmesi yapılan güvenlik kodlar (CAPTCHA- Completely Automated Public Turing test to tell Computers and Humans Apart - İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) karşısındakinin insan ya da bilgisayar olup olmadığını otomatik tespit etmeye yönelik olarak kullanılan insan etkileşim kanıtı, sınama-yanıt doğrulaması mekanizmalarıdır. Web siteleri ve çevrim içi servisleri çeşitli ataklardan özellikle de otomatikleşmiş bilgisayar programlarından (bots) korumak için geliştirilmiştir.

Çalışmanın amacı mobil ara yüzlerde uygulanan çeşitli güvenlik düzeylerindeki metin-temelli güvenlik kod türlerinin kullanılabilirliğini değerlendirmektir. Böylece günlük hayatta pek çok çevrim içi hizmette kullanıcıların karşılaştıkları güvenlik kod türlerinden kullanıcılar için daha fazla güvenlik sağlarken aynı zamanda daha az çaba gerektiren ve anlaşılır olanın belirlenmesi sağlanacaktır.

- Bu amaçla kullanıcı testleri uygulanarak güvenlik kod türlerinin kullanıcılar açısından etkililik, verimlilik ve memnuniyet dereceleri kıyaslanacaktır.

Çalışmaya 18 yaş üzeri gönüllüler katılabilmektedir. Çalışmaya katılmaya gönüllü olduğunuz için seçildiniz. Katılımınız tamamen gönüllülük esasına dayalıdır. Çalışmadan istediğiniz zaman neden göstermeden ayrılabilirsiniz.

Çalışma sırasında sizden öncelikli olarak demografik bilgilerinizi içerecek anket doldurmanız istenecektir. Sonrasında uygulamanın nasıl kullanılacağına dair kısa bir bilgilendirme aktarımı yapılacaktır. Uygulama esnasında size verilen mobil cihaz üzerinden erişebileceğiniz ara yüz ile her bir güvenlik kod türüne ait veri girişi yapmanız istenecek ve sonrasında ilgili güvenlik kod türü için iş yükü matrisini ve kullanılabilirlik değerlendirme anketini doldurmanız istenecektir. Veri giriş

görevlerini yaparken sesli düşünmeniz istenmektedir. Görevler sırasında takip ettiğiniz adımları ve yaşadığınız zorlukları sesli olarak dile getiriniz.

Çalışma kapsamında mobil ara yüzle etkileşimininiz sırasında sizin başarınız ölçülmemekte, kullanıcıların karşılaştıkları problemlerin ortaya çıkarılması hedeflenmektedir.

Gizlilik: Çalışmada kullanılacak anketler kapsamında kişisel bilgilerinize yönelik cevaplamanız gereken herhangi bir soru bulunmamaktadır.

Bilgilere giriş: Elde edilen bilgiler yalnızca çalışma kapsamındaki araştırmacılar tarafından analiz edilecek ve tüm katılımcılara ait bulgular derlenerek sunulacaktır

Çalışma ile ilgili detaylı bilgi almak isterseniz yukarıdaki iletişim bilgilerini kullanabilirsiniz

Araştırma çalışmamıza katılım davetimizi kabul ederek katkı sağlamayı kabul ettiğiniz için teşekkür ederiz.

Çalışmaya katılmayı kabul ediyorum _____

Ek-C Kullanıcı Demografik Bilgi Anketi

Kullanıcı Demografik anketi ile katılımcı profillerinin belirlenmesi sağlanacaktır.

Lütfen aşağıdaki sorulardan kendinize uygun olan cevabı seçerek yanıtlayınız.

1. Yaş : _____

2. Cinsiyet

   ◯ Kadın

   ◯ Erkek

3. Herhangi bir görme kusurunuz var mı?

   ◯ Hayır

   ◯ Renk Körlüğü

   ◯ Miyop

   ◯ Hipermetrop

   ◯ Diğer :_____

4. Günlük hayatta hangi elinizi kullanırsınız?

   ◯ Sağ

   ◯ Sol

   ◯ Her ikisi

5. Eğitim durumunuz nedir?

   ◯ Lise

   ◯ Lisans

   ◯ Yüksek Lisans

   ◯ Doktora

   ◯ Diğer :_____

6. Okuğunuz bölüm ya da varsa üniversite derecenizi aldığınız bölüm nedir?

   _____

Ankette yer alan soruların hepsi dokunmatik ekranlı cihazlar göz önüne alınarak hazırlanmıştır. Bu tür cihazlar ile hiç tecrübeniz bulunmuyor ise bundan sonraki soruları yanıtlamadan "Demografik Bilgi Anketini" test gözlemcisine teslim edebilirsiniz.

Eğer dokunmatik ekranlı cihazlar ile tecrübeniz var ise aşağıdaki sorular ile devam ediniz

Ne kadar zamandır akıllı telefon kullanıyorsunuz?

◯ 0-3 yıl

◯ 3-5 yıl

◯ 5-10 yıl

◯ Diğer: _____

7. Şu an kullandığınız akıllı telefonun işletim sistemi nedir?

◯ İOS

◯ Android

◯ Windows/Windows Phone

◯ Diğer: _____

8. Şu anda iOS kullanıcı iseniz Android işletim sistemli bir telefon deneyiminiz oldu mu?

◯ Evet

◯ Hayır

9. Şu anda Android kullanıcı iseniz iOS işletim sistemli bir telefon deneyiminiz oldu mu?

◯ Evet

◯ Hayır

10. 10 ya da 11. sorulardan birine yanıtınız "Evet" ise ne kadar süre kullandınız?

_____

11. Daha önce Iphone 6 modeli telefon kullandınız mı?

◯ Evet

◯ Hayır

12. Yanıtınız evet ise ne kadar süre?

_____

13. Akıllı telefonunuzu aşağıdaki amaçlar ile ne kadar sıklıkla kullanmaktasınız? Birden fazla işaretleyebilirsiniz.

	Uygulama	**Sıklık derecesi (Haftada ya da ayda)**
◯	Sosyal ağlara bağlanma	
◯	Çevrim-içi bankacılık	
◯	Alışveriş yapmak	
◯	Rezervasyon yapmak (otel, uçak, vb.)	
◯	Araştırma ve Öğrenme	

Ek-D NASA Zihinsel İş Yükü (NASA TLX)

Bu anket ile sistemin kullanımı sırasında kullanıcılarda oluşacak genel iş yükü, zihinsel talep, fiziksel talep, zamansal talep, performans, çaba ve başarısızlık seviyesi ne ait değerlendirmeler gerçekleştirilecektir .Aşağıda bu faktörlerin kısa tanımları verilmiştir.

Zihinsel Talep
Ne kadar zihinsel ve algılama aktivitesine ihtiyaç duyulduğu. (Düşünme, karar verme, hesaplama, hatırlatma, bakma, arama vb.) Görevin icrası hatasız ve kesin mi olmalı yoksa hata kabul edilebilir mi? Görev kolay mı zor mu? Sade mi karışık mı?

Fiziksel Talep
Ne kadar fiziksel aktiviteye ihtiyaç duyulduğu. (ittirme, çekme, çevirme, kontrol etme, çalıştırma vb.) Görev basit mi yorucu mu, yavaş mı hızlı mı, gelişi güzel yapılabiliyor mu özel bir özen mi istiyor?

Zamansal Talep
Belirli bir görevin bir aşamasını yerine getirirken ne kadar bir zaman baskısı, kısıtı üzerinizde hissetmektesiniz? Görevi yerine getirmek için atılan adımların hızlı ya da yavaş olması?

Efor
Görevinizi yerine getirmek için ne kadarlık ağır çalışma gereklidir? (zihinsel ve fiziksel)

Performans
Verilen görevin hedeflerine ulaşmada size göre veya denetçilere göre ne derece başarılı olduğunuzu düşünüyorsunuz? Görevi yerine getirirken ne derece tatmin oluyorsunuz?

Rahatsızlık Seviyesi
Görevinizi yerine getirirken kendinizi ne kadar güvensiz, gayri memnun, zarar görmüş, gerilmiş, sinirlenmiş, karışık, gevşek ya da karmaşık hissediyorsunuz?

Aşağıda verilen ifadelere katılımınızı az önce veri girişini tamamladığınız CAPTCHA türü için 0 Çok Düşük – 20 Çok Yüksek aralığında olacak şekilde işaretleyiniz.

ZİHİNSEL TALEP

FİZİKSEL TALEP

ZAMANSAL TALEP

EFOR

PERFORMANS

RAHATSIZLIK SEVİYESİ

Ek-E Türkçe Bilgisayar Sistemi Kullanılabilirlik Anket Soruları

Bu anket, bir bilgisayar sisteminin kullanılabilirliğini değerlendirmeye yönelik ifadelerden oluşmaktadır. Aşağıda verilen ifadelere katılımınızı az önce veri girişini tamamladığınız güvenlik kod türü için 1 Kesinlikle Katılıyorum – 7 Kesinlikle Katılmıyorum aralığında olacak şekilde işaretleyiniz!

		Kesinlikle Katılıyorum						Kesinlikle Katılmıyorum
#	İfade	1	2	3	4	5	6	7
1	Genel olarak, en son kullandığım güvenlik kod türünün kullanım kolaylığından memnunum	○	○	○	○	○	○	○
2	En son kullandığım güvenlik kod türü ile sistemi kullanma basittir	○	○	○	○	○	○	○
3	En son kullandığım güvenlik kod türü ile sistemi kullanarak işlerimi etkin bir şekilde yapabiliyorum	○	○	○	○	○	○	○
4	En son kullandığım güvenlik kod türü ile sistemi rahatlıkla kullanabiliyorum	○	○	○	○	○	○	○
5	En son kullandığım güvenlik kod türü ile Sistemi kullanmayı öğrenmem kolay oldu	○	○	○	○	○	○	○
6	En son kullandığım güvenlik kod türü ile sistemi kullanarak kısa zamanda üretken hale geldiğime inanıyorum	○	○	○	○	○	○	○
7	En son kullandığım güvenlik kod türünün ara yüzünü beğendim	○	○	○	○	○	○	○
8	En son kullandığım güvenlik kod türünün ara yüzünü kullanmak hoşuma gidiyor	○	○	○	○	○	○	○

9	En son kullandığım güvenlik kod türü ile oluşturulmuş Sistem, beklediğim bütün işlevlere sahiptir ve yeterlidir	◯	◯	◯	◯	◯	◯	◯
10	Genel olarak en son kullandığım güvenlik kod türü ile oluşturulan sistem tatmin edicidir	◯	◯	◯	◯	◯	◯	◯

Ek-F Güvenlik kod Tercih Sıralaması Anketi

Güvenlik kod tercih sıralaması anketi ile Tüm veri girişlerinin tamamlanmasından sonra hangi güvenlik kod türünün katılımcılar tarafından tercih edildiğini belirlemek istenmektedir.
Aşağıdaki tabloda da örnekleri verilen az önce veri girişlerini tamamladığınız güvenlik kod türleri için 1'den 6'ya kadar tercih sırlamanızı yanlarına belirtiniz.

Tercih Sıralaması	Güvenlik kod türü	Güvenlik kod türü resmi
_____	Bozulma uygulanmış	
_____	Bozulma Uygulanmamış	
_____	Renk ayrımı çok	
_____	Renk ayrımı az	
_____	Rastgele kelime	
_____	Sözlük kelime	

KİŞİSEL YAYIN VE ESERLER

Merdanoğlu N., Durdu P. O., A Systematic Mapping Study of Usability vs Security, *6th International Conference on Control Engineering Information Technology*, İstanbul, Türkiye, 2018

ÖZGEÇMİŞ

1993 yılında İstanbul' da doğdu. İlk, orta ve lise öğrenimini Kocaeli' de tamamladı. 2011 yılında girdiği Marmara Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nden 2016 yılında Bilgisayar Mühendisi olarak mezun oldu. 2016 yılından bu yana TÜBİTAK'da araştırmacı olarak çalışmaktadır.2017 yılında başladığı Kocaeli Üniversitesi Fen Bilimleri Bilgisayar Mühendisliği Anabilim Dalı'ndaki Yüksek Lisans eğitimine devam etmektedir.