Vücut Alan Ağlarındaki Medikal Cihazların ve Mobil Sağlık Uygulamaların Güvenlik Analizleri

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Abdulkerim DEMİR
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Yılmaz ÇANKAYA .....
(Tez Danışmanı)

Dr. Emin İslam TATLI .....
(Tez Eş-danışmanı)

Prof. Dr. Tahsin Erkan Türe .....

Dr. Mehmet KARA .....

Yrd. Doç. Dr. Selçuk BAKTIR .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

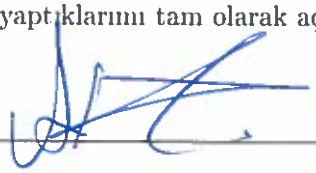
ONAY TARİHİ: 2 Haziran 2016

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Abdulkerim DEMİR, başlığı, 'Vücut Alan Ağlarındaki Medikal Cihazların ve Mobil Sağlık Uygulamaların Güvenlik Analizleri' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 

Tarih: 02.06.2016

Vücut Alan Ağlarındaki Medikal Cihazların ve Mobil Sağlık Uygulamaların Güvenlik Analizleri

Abdulkerim Demir

Öz

Sağlık alanındaki teknolojik gelişmelerle birlikte insan vücudu ile etkileşimde bulunan medikal cihazlardan oluşan Vücut Alan Ağları (BAN) geliştirildi. Bu sayede örneğin insan kan basıncını ya da insülin değerini otomatik ölçen ve hastane yönetim sistemlerine transfer edebilen cihazlar günlük hayatta kullanılmaya başlandı. Bu medikal cihazlar bir yandan sağlık yönetimini iyileştirirken diğer taraftan bunlara yapılacak izinsiz müdahale ile insan sağlığını riske atabilmekte hatta ölümlere neden olabilmektedirler. Bu çalışmada Kablosuz Vücut Alan Ağları (WBAN)' nda kullanılan medikal cihazların ve mobil sağlık uygulamalarının güvenlik açısından analizleri gerçekleştirildi. Öncelikle WBAN' ın tehdit modellemesi yapılarak WBAN' daki özellikle uzaktan erişilebilir medikal cihazların karşı karşıya kaldıkları bütün tehditler ve riskler belirlendi. Bunun yanında akıllı cihazlar üzerinde çalışan mobil sağlık uygulamaları için güvenlik analizleri gerçekleştirildi. Ayrıca, WBAN sistem tasarımı için güvenlik gereksinimleri belirlendi.

Anahtar Sözcükler: Hasta İzleme Sistemi, BAN, WBAN Mimari, Güvenlik Prensipleri, WBAN Güvenlik Analizi, Bluetooth

Saygıdeğer aileme ve sevgili eşime . . .

Teşekkür

Çalışmam süresince her türlü yardım ve fedakârlığı sağlayan, bilgi ve tecrübeleri ile çalışmama ışık tutan danışmanım Sayın Dr. Emin İslam TATLI' ya,

Bilgi ve tecrübelerini aktararak beni yönlendiren, gelişmeme katkıda bulunan, yardıma ihtiyaç duyduğum her konuda desteğini esirgemeyen danışmanım Sayın Yılmaz ÇANKAYA' ya,

Tezimin hazırlanması sırasında beni cesaretlendiren, ümit veren ve manevi destek sağlayan değerli eşim Gülizar Elif DEMİR' e,

Çalışmalarım esnasında manevi desteklerini her zaman hissettiğim değerli aileme teşekkürü bir borç bilirim.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

AES	**A**dvanced **E**ncryption **S**tandard - **G**elişmiş **Ş**ifreleme **S**tandardı
BAN	**B**ody **A**rea **N**etwork - **V**ücut **A**lan **A**ğı
BTLE	**B**lue**T**ooth **L**ow **E**nergy
CIA	**C**onfidentiality **I**ntegrity **A**vailability
EKG	**E**lektrokardiyogram
FFD	**F**ull **F**unction **D**evice - **T**am **F**onksiyonlu **C**ihaz
HAN	**H**ome **A**rea **N**etwork
ICD	**K**ardiyoverter **D**efibrilatör
IMDs	**I**mplantable **M**edical **D**evices - **V**ücuda **Y**erleştirilebilir **M**edikal **C**ihazlar
MAC	**M**edia **A**ccess **C**ontrol - **O**rtam **E**rişim **D**enetimi
MBU	**M**obile **B**ase **U**nit - **M**obil **T**abanlı **B**irim
MCPS	**M**edical **C**yber-**P**hysical **S**ystems - **M**edikal **S**iber-**F**iziksel **S**istemler
MEMS	**M**icro-**E**lectro-**M**echanical **S**ystems - **M**ikro-**E**lektro-**M**ekanik **S**istemler
MIC	**M**essage **I**ntegrity **C**heck
NFC	**N**ear **F**ield **C**ommunication
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
PCG	**F**onokardiyografi
PDA	**P**ersonal **D**igital **A**ssistant
PPG	**F**otopletismogram
RFD	**R**educed **F**unction **D**evice - **K**ısıtlanmış **F**onksiyonlu **C**ihaz
SMS	**S**hort **M**essage **S**ervice
SSP	**S**ecure **S**imple **P**airing
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol
TSE	**T**ürk **S**tandartları **E**nstitüsü
URL	**U**niform **R**esource **L**ocator

UWB	**U**ltra-**W**ide**B**and
WBAN	**W**ireless **B**ody **A**rea **N**etwork - **K**ablosuz **V**ücut **A**lan **A**ğı
WEP	**W**ired **E**quivalent **P**rivacy
WMAN	**W**ireless **M**etropolitan **A**rea **N**etwork
WPA	**W**i-Fi **P**rotected **A**ccess
WSN	**W**ireless **S**ensor **N**etwork - **K**ablosuz **A**lgılayıcı **A**ğ
WWAN	**W**ireless **W**ide **A**rea **N**etwork

Bölüm 1

Giriş

Kablosuz algılayıcı ağlar günlük hayatta çeşitli alanlarda uygulanabilen güncel önemi yüksek teknolojilerdendir. Bu teknolojinin tıbbi teknolojilerle birlikte kullanımıyla sağlık alanında birçok konuya çözüm sunulabilmektedir. Geleneksel hasta izleme sistemlerinde kablosuz algılayıcı ağların kullanımıyla birlikte sistemin uygulanmasında önemli değişiklikler olmuştur. Gelişen hasta izleme sistemleri genel olarak takibi yapılan hasta verilerinin hastane ve/veya doktoru kapsayan medikal sunucuya aktarılmasından oluşur. Hasta izleme sistemlerinde ilk katmanı oluşturan ve yaygın kullanılan teknolojilerden biri olan BAN uygulanabilirliği ve maliyet açısından dikkat çekmektedir. BAN genel olarak insan vücuduna veya doku içerisine yerleştirilen akıllı sensörlerden oluşmaktadır. Sensörlerden alınan verilerin analiz edilmesi veya saklanması için kablosuz bağlantı kullanarak bir sunucuya aktarılması durumunda ise bu teknoloji WBAN olarak adlandırılmaktadır. WBAN teknolojisinin hastanın tıbbi verilerinin zamansal ve mekânsal sınır olmaksızın izlenmesi gibi avantajları olsa da; teknolojinin güvenlik açıkları bu durumu dezavantaja dönüştürebilir. Bu anlamda kullanılan sistemlerin güvenliğini artırmak adına pek çok çalışma yapılmış ve çalışmalar sonucu yeni güvenlik önerileri sunulmuştur.

Çalışma içeriğinde, 2. bölümde konunun daha iyi anlaşılabilmesi amacıyla, çalışma kapsamında kullanılan kavramlar hakkında genel bilgi verilmiştir. 3. bölümde, bilgi güvenliğinin temelini oluşturan CIA prensipleri ve güvenlik gereksinimleri açıklanmıştır. Ayrıca bu bölümde WBAN sistemine yapılan detaylı tehdit analizi anlatılmıştır. 4. bölümde, bu konu ile ilgili daha önce yapılmış olan benzer çalışmalar incelenmiştir. 5. bölümde ise tez çalışması için edinilen medikal bir cihazın, cihazın kullandığı mobil uygulamaların

ve ayrıca uygulama marketlerden kolay şekilde edinilebilen mobil sağlık uygulamalarının güvenlik testlerinin sonuçları detaylı olarak açıklanmıştır. Bunlara ek olarak, güvenli mimari tasarım ve geliştirme gereksinimleri açıklanmıştır. Son bölüm olan 6. bölümde ise çalışmanın sonuçları yorumlanmış ve gelecekte yapılabilecek çalışmalara yönelik önerilerde bulunulmuştur.

Bölüm 2

Temel Bilgiler

2.1 Genel Olarak Sağlık Hizmetleri Sektöründe Kablosuz Algılayıcı Ağlar

Kablosuz iletişim, elektronik ve Mikroelektro Mekanik Sistemler (MEMS) alanlarındaki gelişmeler düşük maliyetli, düşük güç gerektiren, küçük boyutlu ve kısa mesafelerde iletişim kurabilen, akıllı ve çok fonksiyonlu sensörlerin gelişimini sağlamıştır. Bu sensörlerin sınırlı veri algılama, iletişim, ölçüm toplama ve veri olarak işleme kapasitelerinin olması, izlenecek alan üzerinde çok sayıda yerleştirilmiş sensör ağları kümesi olan Kablosuz Algılayıcı Ağ (WSN) fikrine yol açmıştır [1, 2]. WSN teknolojisi eğlence, seyahat, askeri, sanayi, sağlık gibi birçok alanda uygulanabilmektedir [3–6]. Yapılan araştırmalar WSN teknolojisinin tıbbi teknolojiler ile birlikte kullanımıyla evde bakım hizmetleri, uzaktan hasta takibi ve yeni nesil klinik uygulamalar gibi konularda yeni çözümler sunabileceğini göstermiştir. Son yıllarda dünyanın karşı karşıya kaldığı önemli sorunlardan biri; artan büyüme oranlarıyla ilerleyen yaşlı nüfus artışının, toplam nüfus artışından daha fazla olmasıdır.

Nüfus Danışma Bürosu (Population Reference Bureau)' nun verilerine göre [7] 2050 yılında dünya yaşlı nüfusunun toplam nüfusun yaklaşık olarak %20'sini oluşturması beklenmektedir. Ayrıca bu konuda yapılan çalışmalara göre; küresel sağlık ekonomisine en büyük maliyeti yaşlı ve yetişkin hastalarda daha yaygın olarak görülen kalp, şeker hastalığı gibi bulaşıcı olmayan kronik hastalıklar oluşturmaktadır. Bu nedenle sağlık bakım maliyetlerini azaltırken hızla büyüyen yaşlı nüfusun kaliteli sağlık bakımı

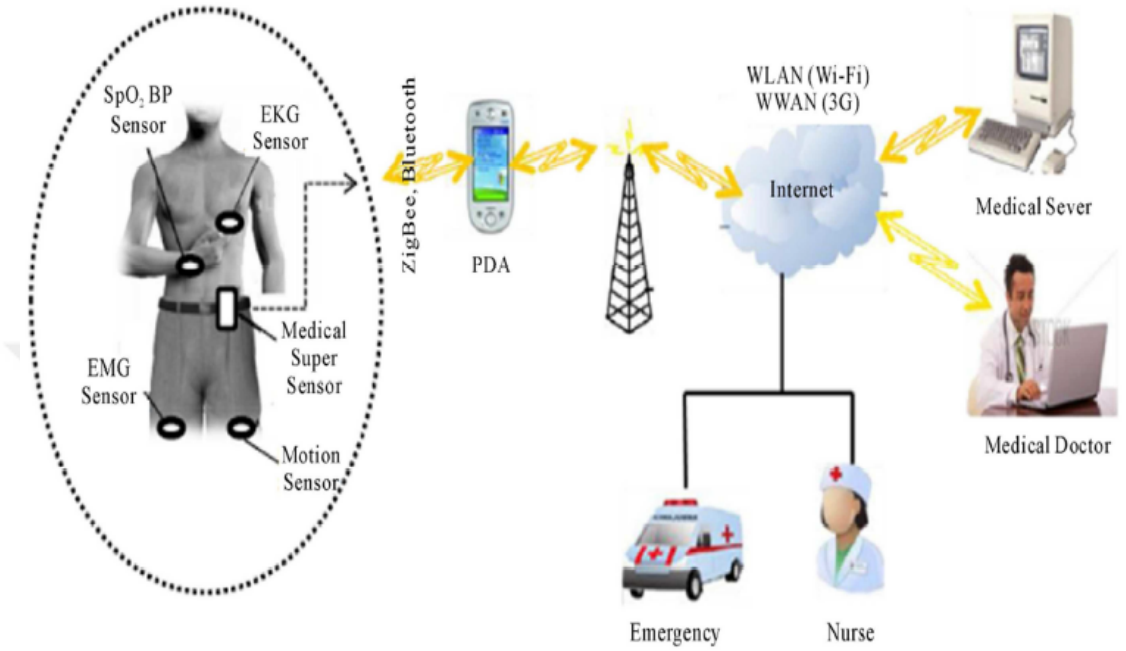
konusundaki ihtiyaçlarını karşılamak, üzerinde çalışılması gereken bir konudur [8, 9]. WSN teknolojilerinin tıbbi teknolojilerle birlikte kullanımı sonucu sağladığı avantajlar bu anlamda maliyetin azaltılabileceğini düşündürmektedir. Örneğin; evde bulunan yaygın ağlar aracılığıyla hastanın sürekli olarak medikal görüntülenmesi, taşınabilir cihazların kontrolü, tıbbi verilere erişim ve acil durum anında iletişim sağlanabilir [10, 11].

Sağlık hizmetlerinde WSN teknolojisinin bir diğer avantajı ise hastanın konforudur. Kablosuz olarak tıbbi algılayıcıların bağlanmasıyla sağlanan sürekli görüntüleme, yüksek riskli hastalar için acil durumların erken tespiti, acil durumlarda hızlı müdahale, çeşitli derecelerde zihinsel ve fiziksel olarak engelli kişilerin sağlık bakım hizmetlerini herhangi bir mekânsal kısıt olmaksızın gerçek zamanlı olarak hastanın izlenmesiyle büyük ölçüde sağlayabilmektedir. Ayrıca bu sistem yaşlı ve/veya kronik hastaların dışında, ebeveynleri çalışan bebekler ve küçük çocuklar için de kullanılabilmektedir [2, 12].

2.2 Hasta İzleme Sistemi

Hasta izleme sistemi hastaya ait önemli sinyallerin alınması ve işlenmesi ile hastalığının teşhisini ve izlenmesini içermektedir. Bu sistemin kullanıcıları genel olarak kronik hastalar, hastane hastaları ve yaşlı hastalardır. Örneğin kronik hastalıklardan biri olan yüksek tansiyon hastalığının tedavi sürecinde tansiyonun düzenli olarak izlenmesi gerekir. Hasta izleme sistemleri doktorlara, günlük yaşamlarında hastaların tansiyonlarını takip etme imkânını sağlamaktadır. Ayrıca doktorların hastalığı daha iyi anlamasını sağlayarak hangi tedaviye başlanması gerektiği ve hastanın uygulanan tedaviye tepkisi konusunda da yardımcı olmaktadır. Hasta izleme sistemine ihtiyaç duyulan alanlardan biri de hastane ortamlarıdır. Hastanelerde bulunan hastalar, hastalık durumuna göre çeşitli aralıklarla izlenmektedir. Örneğin yoğun bakım hastalarının sürekli olarak kalp hızı, solunum hızı, vücut sıcaklığı, tansiyon gibi verileri izlenmektedir. Yoğun iş gücü, manuel ölçüm ve raporlama gerektiren bu veri takibi insan hatasına oldukça yatkındır. Bu sürecin otomasyonuyla hastanenin herhangi bir yerinde bulunan hastanın veri takibi kolaylıkla sağlanır. Yaşlı hastalar ise tedavi edilebilir hastalıklarda bile erken teşhise ihtiyaç duyduklarından sürekli izleme gerektirirler. Hastanın durumundaki herhangi bir değişikliğin fark edilip gerekli müdahalenin zamanında yapılmasıyla ölüm oranları azaltılabilir.

Hasta izleme sistemlerinde genellikle; giyilebilir cihazlar ve sensörler yardımıyla hasta vücudundaki kan basıncı, vücut sıcaklığı, elektrokardiyogram (EKG) gibi sinyaller sensörler yardımıyla elde edilir. Elde edilen bu sinyaller hasta izleme merkezindeki sunucular ve sunucular üzerinden de medikal personele ulaştırılır [13–16].



Şekil 2.1: Hasta izleme sistemi prototipi [16]

Şekil 2.1.' de görülen hasta izleme sistemi prototipi genellikle 3 katmanlı mimariden oluşmaktadır. Hasta izleme sistemlerinin ilk katmanı, ham verinin üretildiği BAN veya giyilebilir bilgisayar katmanıdır. Bu katmanda, vücut yüzeyine yerleştirilen ya da doku içine yerleştirilmiş kablosuz algılayıcı sensörlerden gelen hasta vücudundaki önemli sinyaller bir ağ kontrolcüsü ile toplanır. Ağ kontrolcüsü olarak BAN sunucusuyla bağlantılı kişisel alan ağı teknolojilerinden Bluetooth, ZigBee, Ultra-Wideband (UWB) gibi teknolojiler kullanılabilir.

İkinci katman sensörlerden gelen verilerin toplandığı BAN sunucusu katmanıdır. Bu katman sensörlerden gelen verileri en son katman olan medikal sunucu katmanına iletmekle görevlidir. Ayrıca bazı veri türleri için bu katmanda değerlendirme yapılıp sonuç iletilebilir. BAN sunucusu olarak kişisel bilgisayar uygulaması (PDA-Personal Digital Assistant), kişisel bilgisayarlar veya cep telefonları kullanılabilir. BAN sunucusu ile medikal sunucu arasında en yaygın olarak kullanılan teknolojiler kablosuz geniş alan ağları diye adlandırılan Wimax, GSM/GPRS, EDGE, 3G ve LTE teknolojileridir.

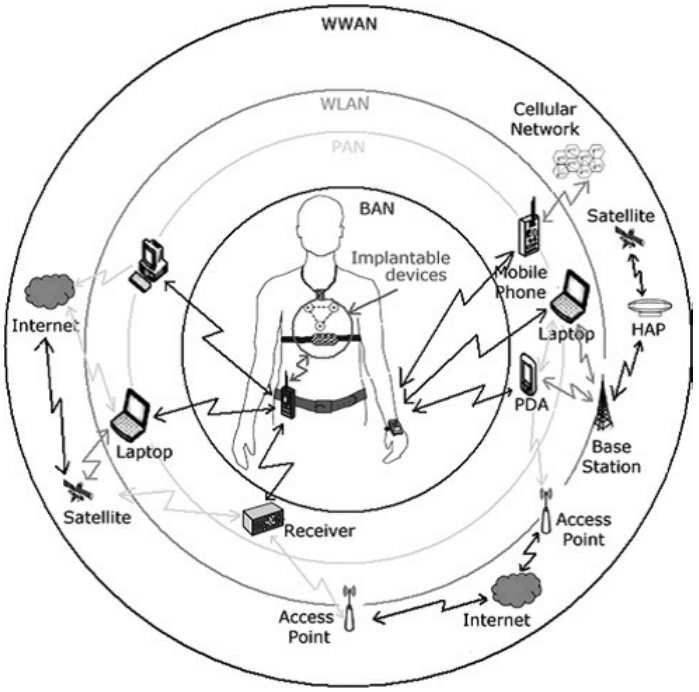
Üçüncü ve en son katman medikal sunucu katmanıdır. BAN sunucusunun gönderdiği veriler bu katmanda işlenir ve depolanır. Bu katman aynı zamanda hastane bilgi yönetim sistemine de bağlıdır. Böylece işlenen veri sonucu ilgili personellere (doktor, hemşire, ambulans vb.) alarm ya da rapor olarak iletilir [15].

2.3 WBAN Mimarisi

Hasta izleme sistemi prototipinde açıklanan iletişimin sağlanmasında iletişimin tipine ve uzaklığına bağlı olarak çeşitli teknolojiler kullanılmaktadır. Hasta izleme sistemi ağları heterojen ağların hiyerarşik olarak düzenlenmesiyle oluşturulmuştur [16, 17].

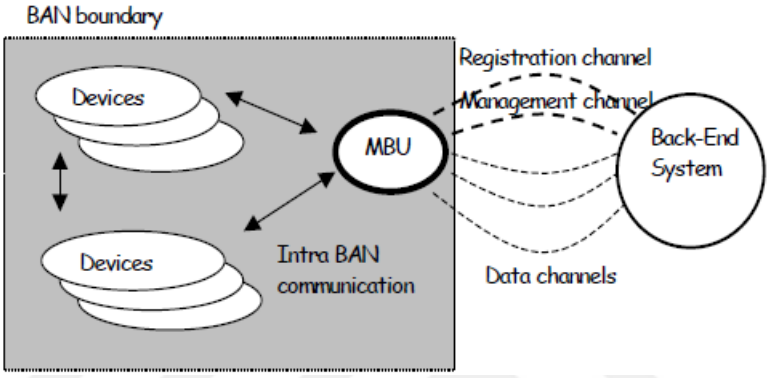
- Kısa menzilli kablosuz teknolojiler (WBAN)
- Orta menzilli kablosuz teknolojiler (HAN (Home Area Network), WLAN)
- Uzun menzilli kablosuz teknolojiler (WMAN (Wireless Metropolitan Area Network), WWAN (Wireless Wide Area Network))

Gruplandırılmış bu cihazların en çok kullanılan örnekleri ve insan vücudundan bağıl uzaklık haritası Şekil 2.2' de verilmiştir.



Şekil 2.2: Kablosuz cihaz teknolojisi haritası [17]

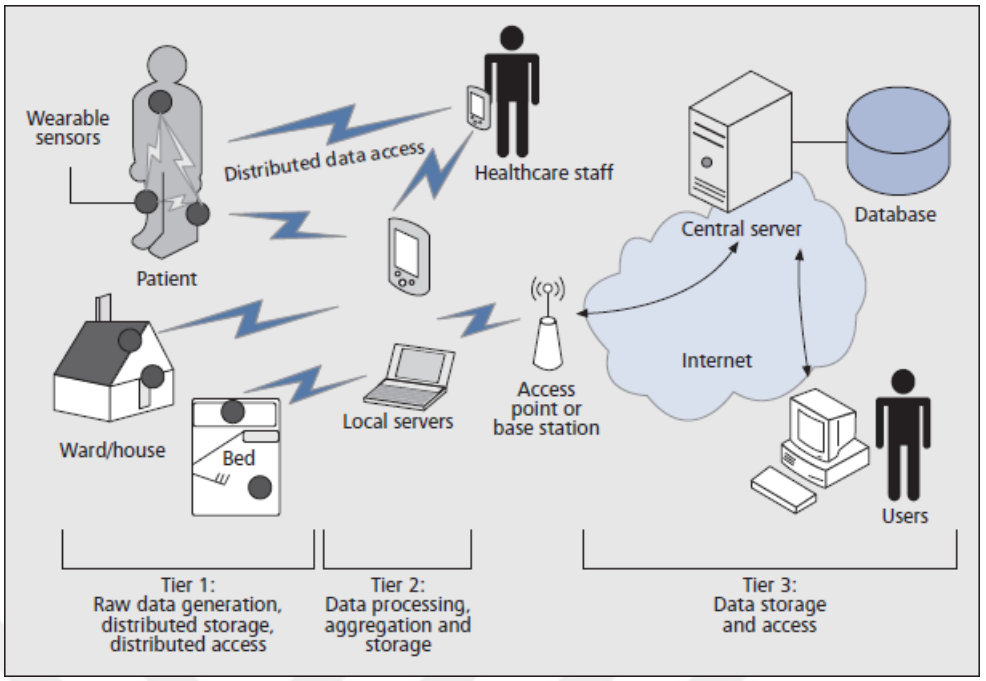
Hasta izleme sisteminde giyilebilir bilgisayarlar, kablosuz yerel alan ağları, kişisel alan ağları, BAN, GSM/GPRS, Wimax ve bilişsel radyo yaygın olarak kullanılan teknolojilerdendir. Bu teknolojilerden BAN, maliyet ve uygulanabilirlik açısından dikkat çekmektedir. Genel olarak BAN; sensör, mikroişlemci, çip, batarya gibi bileşenlerden oluşmaktadır. BAN bileşenleri arasındaki iletişim BAN içi, BAN ve uzaktan izlemeyi yapan medikal sunucusu arasındaki iletişim BAN dışı olarak tanımlanmaktadır. BAN dışı iletişimi kolaylaştıran ağ geçidi ise mobil tabanlı birim (MBU) olarak adlandırılmaktadır [18]. Şekil 2.3' de BAN mimarisi şekilsel olarak görülmektedir.



Şekil 2.3: BAN Mimarisi [18]

Sensörler ve aktüatörler ad-hoc ağ kurarak BAN dışı iletişim için MBU kullanmaktadır. Sensör veri toplama işinden sorumludur. Hastanın hareketi, kas aktivitesi veya kan akışı gibi fiziksel olgular ilk önce elektriksel bir sinyale dönüştürülür. Bu sinyal yükseltilir, kaydedilir, sayısallaştırılır ve BAN dışına iletilir. Sensörler kendi kendini desteklemeli veya ön ucu (front-end) desteklemelidir. Kendi kendini destekleyen sensörler ilerleme, konumlandırma, sayısallaştırma, iletişim için kullanabilecekleri güç kaynağına sahiptir. Ön uç destekleyen sensörlerin kullanıldığı durumda ise, çoklu sensörler, güç kaynağını ve veri toplama için kullanılan gücü paylaşırlar. Ön uç destekleyen sensörler tek bir zamanlayıcı kullanırlar. Bu sensörlerden elde edilen veriler veri bloğu şeklindedir ve bu durum sensörler arası senkronizasyon ihtiyacını ortadan kaldırır. Kendi kendini destekleyen sensörler BAN' nın bağımsız yapı taşlarıdır ve BAN' ın farklı şekillerde yapılandırılmasına olanak sağlar. Ancak her sensörün kendi zamanlayıcısı vardır ve farklı örnek sıklıklarına sahip olabilirler. Sonuç olarak kendi kendini destekleyen sensörler arasında senkronizasyona ihtiyaç duyulabilir [18].

WBAN mimarisi (Şekil 2.4) "Hasta İzleme Sistemi" başlığı altında anlatılan hasta izleme sistemi prototipindeki 3 katmanı içermektedir. İnsan vücudu çevresindeki sensörlerden



Şekil 2.4: WBAN Mimarisi [15]

oluşan WBAN kısa menzilli bir kablosuz iletişim teknolojisidir. WBAN teknolojisinde temel olarak vücudun içine veya üzerine yerleştirilen biyomedikal sensörlerden alınan verilerin analiz edilmesi veya saklanması için kablosuz bağlantı kullanarak bir sunucuya aktarılması söz konusudur. Yani diğer teknolojilerden ayırt edici yanı sensörlerden alınan sinyalin BAN sunucusuna aktarılmasında kısa menzilli kablosuz ağ teknolojisi kullanmasıdır. WBAN teknolojisi günümüzde IEEE 802.15.6 standardını temel almaktadır [19].

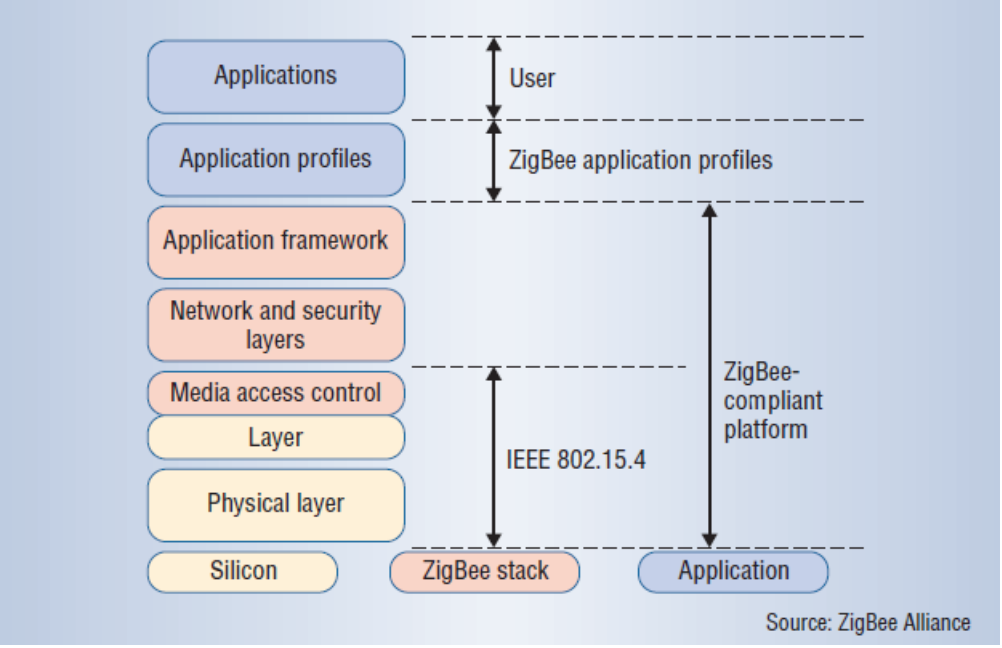
2.4 WBAN Mimarisinde Kullanılan Protokoller

WBAN teknolojisinde kullanılan sensörlerin yapısı gereği üzerlerinde bulunan güç kaynağı sınırlı miktarda güce sahiptir [20]. Bunun için alınan sinyalin BAN sunucularına aktarımında az güç harcayan Bluetooth ve ZigBee gibi kablosuz alan ağlarını kullanılır.

2.4.1 ZigBee

Bu teknoloji düşük güç tüketimi nedeniyle ilgi çeken kablosuz ağ teknolojileri için iletişim protokollerini tanımlayan bir standarttır. Temel olarak düşük veri yoğunluğu, uzun pil ömrü, düşük maliyet gerektiren uygulamalar ve pille çalışan cihazlar için geliştirilmiş

bir teknolojidir [21, 22]. Bu uygulamalarda cihaz çoğunlukla güç tasarruf modunda çalışır. ZigBee protokol yığını Şekil 2.5' de gösterilmiştir. ZigBee standardı, fiziksel katmanı ve Ortam Erişim Denetimi (MAC) protokolleri için IEEE 802.15.4 standardını kullanır. ZigBee standardı 802.15.4 ağ tabakasının orijinal standarda eklenmesiyle ad-hoc ağ tekniğini kullanabilir hale gelmiştir. Ayrıca 2.4 GHz band kullanımında 10 m iç ve 200 m dış iletişim aralığı kullanırken bu aralık diğer bandların kullanımında 30 m iç ve 1000 m dış olarak genişlemiştir. ZigBee veri iletim hızı Bluetooth teknolojisine göre düşüktür. Zamanlamanın önemli olduğu uygulamalar için yeterli bir seviye olan 2.4 GHz bandda saniyede 250 kbits veri iletebilmektedir. Genel kullanım için 2.4 GHz, Avrupa Birliği ülkeleri için 868 MHz ve Kuzey Amerika ve Avustralya için 902 MHz olmak üzere üç RF bandı tanımlanmıştır [22].



Şekil 2.5: ZigBee protokol yığını [22]

Tam Fonksiyonlu Cihaz (FFD) ve Kısıtlanmış Fonksiyonlu Cihaz (RFD) olmak üzere iki tip cihaz tanımlanmıştır. RFD kısıtlanmış protokol serisiyle çalışıp belirli topolojileri kullanıp bir ağ koordinatörü ile konuşabiliyorken, FFD herhangi bir topolojiye uyumlu bütün protokol serileriyle çalışıp diğer cihazlarla da konuşan ve PAN koordinasyonu yapabilen bir cihazdır. ZigBee cihazları kendi kendini düzenleyen, iyileştiren, çok sayıda sensörden oluşan dinamik ağlar oluşturabilir. Bu ağlar yönlendirici, koordinatör ve uç cihazından oluşur. ZigBee yönlendiricisi tam fonksiyonlu bir cihazdır ve ağdaki görevi rotaları bulmak ve bakımını yapmaktır. Ayrıca IEEE 802.15.4 PAN koordinatörü olarak

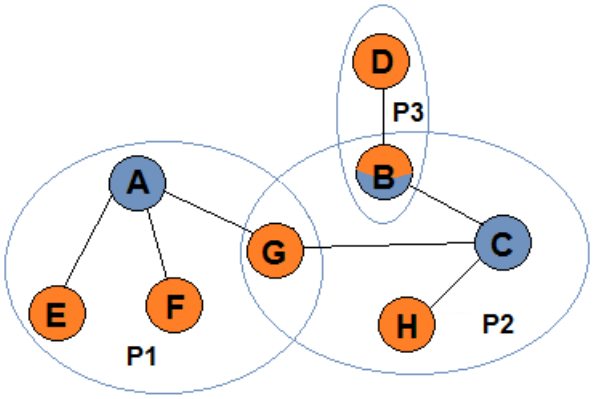
davranır. ZigBee koordinatörü tam fonksiyonlu bir cihazdır ve IEEE 802.15.4 PAN koordinatörü olarak davranır. ZigBee koordinatörünün ağ katmanında, yeni bir ağ kurulması, ağ topolojisinin seçilmesi ve cihazlara ağ adreslerinin atanması gerçekleştirilir. ZigBee uç cihazı kısıtlı fonksiyonlu bir cihazdır ve ağdaki en düşük hafızaya, işlem kapasitesine ve maliyete sahiptir. Bu cihaz koordinatör veya yönlendirici değildir [23].

Ağ katmanı ve uygulama katmanının düşük seviyelerinde ağın güvenliği gerçekleştirilir. IEEE 802.15.4 standardı veri gizliliği ve kimlik doğruluğundan emin olmak için Gelişmiş Şifreleme Standardını (AES) kullanmaktadır. Şifreleme algoritması iletilen mesajı şifreleme anahtarıyla değiştirip yeniden düzenleyerek sadece tanımlanmış alıcının mesajı doğru olarak alabilmesini sağlar.

2.4.2 Bluetooth - IEEE 802.15.1

Bluetooth kablosuz kişisel cihazların bağlanmasında kabloların yerine geçmeyi hedefleyen, yaygın olarak kullanılan bir kablosuz ağ teknolojisidir. Bluetooth genel olarak bir RF alıcı ve vericisinden, bir ana banttan ve bir protokol yığınından oluşmaktadır [16, 23, 24]. Haberleşme birimi olarak "piconet" kullanan Bluetooth, günümüzde mobil cihazların çoğunda kullanılmaktadır. Her Bluetooth kendi içerisinde bir zamanlayıcıya sahiptir. Diğer cihazlarla senkronizasyonun sağlanmasında karşılıklı senkronize olmuş geçici bir zamanlayıcı kullanılır. Bu senkronizasyona kaynaklık eden cihaz "master", senkron hale gelen diğer cihazlar ise "slave" olarak adlandırılır. Bluetooth teknolojisi "piconet" ve "scatternet" olmak üzere iki ağ topolojisi kullanmaktadır. Bağlantıyı oluşturan "master" konumundaki Bluetooth cihazı "piconet" topolojisi kullanarak en fazla yedi cihazı "slave" olarak konumlandırabilir. Çok sayıda "piconet"in bir araya gelmesiyle ise "scatternet" oluşur [24].

Dağınık ağ üyesi olan bir Bluetooth cihazı yalnızca tek bir ağ için "master" olarak konumlanırken, birden fazla "piconet" te "slave" olarak konumlanabilir. Şekil 2.6' da "master" olarak konumlanmış üç cihaz (A, B, C) tarafından yönetilen üç piko ağına (P1, P2, P3) sahip örnek bir Bluetooth topolojisi görülmektedir. Bu ağda B cihazı P2 ve P3 piko ağlarını bağlamaktadır. P2 piko ağında "slave" olarak konumlanmış B cihazı, P3 piko ağında "master" olarak konumlanmıştır.



Şekil 2.6: Bluetooth topoloji örneği

2.4.3 Ultra-Wideband (UWB)

UWB son derece düşük bir enerji yoğunluğu ile frekans spektrumunun çok geniş bir bandı üzerinde dijital verinin iletimini yapabilen kablosuz ağ teknolojisidir. Bu teknoloji kablosuz ağ uygulamalarında çok yüksek hızda veri aktarımı yapabilmektedir. Düşük güçlü cihaza, düşük maliyete, yüksek hıza, geniş band aralıklı radyo spektrumuna sahip olması ve kapı, duvar gibi engellerin dışına sinyal taşıyabilmesi, birçok uygulamayı destekliyor olması UWB teknolojisinin avantajlarındandır. Ayrıca UWB sinyalleri kilitleme riskine karşı güçlü olduğundan güvenilirliği yüksektir. Bu özelliğinden dolayı radyo tabanlı sistemlerde hastalarının sağlık verilerinin güvenli bir şekilde iletilmesi için kullanılabilir. Fiziksel katmanı ve MAC protokolleri için IEEE 802.15.3a standardını kullanmaktadır [16, 17].

2.5 Wi-Fi ve Bluetooth Güvenlik Özellikleri

WBAN teknolojisinde haberleşme için Wi-Fi ve Bluetooth yaygın olarak kullanılan kablosuz teknolojilerdir. WBAN teknolojisinin güvenlik özelliklerinin belirlenebilmesi için bu iki kablosuz teknolojinin güvenlik özelliklerinin de incelenmesi gerekir.

2.5.1 Wi-Fi Güvenlik Özellikleri

Gelişen kablosuz iletişim çözümleri, kablo kirliliğinin minimuma indirgenmesi ve taşınabilirliğe olanak sağlaması gibi avantajları kablosuz ağları, kablolu ağlardan daha sık ve daha fazla kullanılır duruma getirmiştir. Kablosuz ağların güvenliğini sağlamak amacıyla

doksanlı yılların sonlarında çalışmalar yapılmaya başlamıştır. Yapılan bu çalışmalar sonucunda kablosuz ağın yetkisiz kullanımını önlemek amacıyla, ağa erişmek isteyen her kablosuz cihazın aynı anahtarı girmesi gereken bir mekanizma üzerine inşa edilmiş çeşitli güvenlik standartları geliştirilmiştir. Bu standartlar yönlendirici veya erişim noktası olarak hizmet veren cihazların yapılandırılmasında kullanılmıştır. Günümüzde geçerli olan üç farklı kablosuz ağ güvenlik standardı vardır. WEP (Wired Equivalent Privacy) geliştirilen ilk standart olup, barındırdığı açıklık ve zafiyetlerden dolayı yerini daha güvenli olan WPA (Wi-Fi Protected Access)' ya bırakmıştır. WPA' nın desteklediği TKIP protokolünün RC4 şifreleme algoritmasını kullanıyor olması gelişen teknoloji karşısında çaresiz kalmış ve yapılan saldırılar ile anahtar kolay bir şekilde elde edilmiştir. WPA' nın da kırılmasıyla daha güvenli bir şifreleme algoritması kullanan WPA2' ye geçiş gerçekleşmiştir.

WEP kablosuz ağ bağlantılarında (Wi-Fi) veri bağı katmanında çalışır. 802.11 kablosuz ağ güvenlik standartlarına uygun olarak geliştirilmiştir. WEP' in bir kablosuz ağ güvenlik standardı olarak kabul edilmesi Eylül 1999'da gerçekleşmiştir. WEP' in erişim kontrolünü, mesaj gizliliğini ve bütünlüğünü sağladığı iddia edilmektedir. Gizlilik için Ron Rivest tarafından bulunan RC4 şifreleme algoritmasını, bütünlük için ise CRC-32 bütünlük kontrol değerini kullanır. Standart olan WEP şifrelemesi WEP-64 olarak bilinir ve 40 bitlik anahtar kullanır. Günümüzde ise daha çok WEP-128 olarak bilinen ve 104 bitlik anahtar kullanılan sürümüne rastlanılır. Geriye dönük uyumluluğu sağlayabilmek amacı ile WEP kullanımı devam etmektedir, ancak önerilmemektedir. Önerilmemesinin en büyük nedeni ise barındırdığı birçok güvenlik açığı ve zafiyettir.

WEP'in güvenlik açıklarını ve zafiyetlerini ortadan kaldırmak amacıyla yapılan tüm düzenlemeler ve güncellemeler gelişerek artan saldırılar karşısında yetersiz kalmıştır. Yeni bir standart belirlenmesi için başlatılan çalışmalar sonucunda daha güvenli bir yapıya sahip olan WPA, IEEE 802.11i standardını temel alarak geliştirilmiş ve geçici bir standart olarak yayınlanmıştır. 2003 yılında Wi-Fi Alliance var olan cihazların güncellemelerinin daha güvenli bir şekilde, çeşitli sistemlerin birlikte çalışmasına olanak sağlayan bu standarda göre yapılabileceğini duyurmuştur.

802.1x/EAP tabanlı karşılıklı kimlik doğrulama, daha güçlü bir şifreleme yöntemi olan TKIP kullanımı ve veri bütünlüğü için CRC-32 yerine MIC kullanılmasıyla WEP' de var

olan üç temel sorun çözülmüş, iddia ettiği üç ana hedefin (mesaj gizliliği, mesaj bütünlüğü, erişim kontrolü) gerçekleştirilmesi amaçlanmıştır. Gizlilik için 128 bit anahtar ve TKIP kullanarak her pakete özel anahtar üretimi gerçekleştirir. Bu sayede daha yüksek bir güvenlik sağlanmış olur. Anahtar yönetimi için 802.1x standardı uygulanmıştır. RADIUS altyapısının bulunduğu durumlarda EAP ve RADIUS kullanılarak, RADIUS altyapısının bulunmadığı durumlarda ise önceden paylaşımlı şifre yöntemi kullanılarak kimlik doğrulama işlemleri iki farklı yöntemle gerçekleştirilmektedir. Veri bütünlüğü için ise WEP' de kullanılan ve zafiyeti bulunan ICV(CRC-32) yerine daha güçlü olan MIC değeri kullanılmaktadır.

WPA geçici bir güvenlik standardı olarak yayınlanmasına rağmen yüksek güvenlik gerektirmeyen durumlarda yeterli ölçüde güvenliği sağlamıştır. Ancak RC4 şifreleme algoritması temelli olan TKIP protokolünün açıkları olduğu tespit edilmiş ve bu açıklar sömürülmeye başlanmıştır. 2006 yılında WEP' in tüm zayıflık ve açıklarını ortadan kaldırmak amacıyla çok daha güçlü ve güvenli olan WPA2 standardı resmi olarak duyurulmuştur. WPA2, WPA ile aynı yapı üzerine inşa edilmiştir. 802.11x standardı ile tam uyumlu olarak geliştirilerek geriye dönük uyumluluk korunmuştur. Bu uyumluluğun sağlanabilmesi amacıyla TKIP tamamen ortadan kaldırılmamıştır; ancak AES şifreleme algoritmasının CCMP modunda kullanılması zorunlu tutulmuştur [25–27].

2.5.2 Bluetooth Güvenlik Özellikleri

Bluetooth, birçok alanda karşılaştığımız kısa menzilli kablosuz ağ teknolojisidir. Bluetooth teknolojisi evde, ofiste, araçlarda, telefonlarda ve diğer alanlarda karşımıza çıkmaktadır. Günlük hayatta oldukça fazla kullanılmasının yanında birçok güvenlik açığını bünyesinde barındırır. Bu teknolojiyi kullanan kişilerin güvenlik açıklarını bilmemesi kullanılan sistemlerde yüksek risk oluşturmaktadır. Bu risk; kullanıcıların kişisel bilgilerini ve telefon verilerini, kişileri taklit ederek bir başka hedefe saldırmayı ya da kişileri manipüle edilmiş uygulamalara yönlendirerek verilerin sızdırılmasını kapsar. Güvenlik konusunda Bluetooth sistemleri tarafından sağlanan üç temel özellik vardır [24].

- **Gizlilik (Confidentiality):** İletim esnasında alınıp verilen verinin üçüncü kişiler tarafından dinlenmesinin engellenmesidir. Böylece kullanıcıların mahremiyetini korumayı hedefler.

- **Kimlik Doğrulama (Authentication):** Bluetooth sistemlerinin yapısında kullanıcı kimlik doğrulaması bulunmaz. İletişim kurulacak cihazın kimlik doğrulaması cihaz adresleri baz alınarak gerçekleştirilir.
- **Yetkilendirme (Authorization):** Sunulan servis/servislerin kullanılabilmesi için cihazın yetkilendirilmiş olmasıdır.

Bluetooth sistemler için dört farklı güvenlik modu tanımlanmıştır. Bunlar; Güvenlik Modu 1, Güvenlik Modu 2, Güvenlik Modu 3 ve Güvenlik Modu 4 şeklindedir [28].

Bluetooth versiyonlarının gelişimiyle birlikte dört farklı sistem tanıtılmıştır. Bu sistemlerden ilki olan Basic Rate, veri iletişim hızı olarak en yüksek 1 mbps'e kadar destek veren Bluetooth 1.1 ve 1.2 versiyonları olarak bilinir. Enhanced Data Rate Bluetooth versiyon 2.0 da tanıtılmıştır. Bu özellik ile en yüksek veri iletim hızı 3 mbps olarak belirtilmiştir. High Speed Bluetooth version 3.0 + üzerinde desteklenmektedir. En yüksek hız olarak 24 mbps'e kadar destek vermektedir. Low Energy ise Bluetooth 4.0 versiyon ile tanıtılmıştır. "Wibree" ve "Ultra Düşük Güç Bluetooth" olarak da bilinmektedir. Güç ihtiyacı fazla olan medikal cihazlar ve sensörler için tasarlanmıştır. Tasarlanan sistem bu cihaz ve sensörlerde kullanıldığında düşük güç tüketimi, düşük hafıza ihtiyacı, verimli keşif, kısa paket uzunlukları, basit protokol ve servis özelliklerini sisteme kazandırır. Bu sebeple LE eşleşmeleri ağ trafiğinin dinlenmesini koruyamamaktadır. Bu mod MITM koruması dahi sağlayamamaktadır [29, 30].

- **Güvenlik Modu 1:** Bluetooth' un ilk zamanlarında kullanılan moddur ve en güvensiz mod olarak kabul edilir. Kimlik doğrulama ve trafik şifrelemesi bulunmamaktadır. Dolayısıyla her türlü saldırıya açıktır. Bu moddaki cihazlar "fark gözetmeyen" cihazlar olarak tanımlanır yani; diğer cihazlardan gelecek her türlü bağlantıya açıktır. Bu modda çalışan cihaz, bağlantı kurulan cihazın eşleşme, kimlik doğrulama veya şifreleme isteğinde bulunması durumunda direkt olarak izin vermekte ve saldırılara açık hale gelmektedir. Bluetooth v2.0' a kadar tüm cihazlar bu modu desteklemektedir. Üst versiyonlar da geçmişe uyumluluk prensibi gereği bu modu desteklemektedir.
- **Güvenlik Modu 2:** Servis seviyesinde uygulanan güvenlik modudur. Güvenlik prosedürleri bağlantı kurulduktan sonra devreye girer. Lokal güvenlik yönetici birimi spesifik servislere erişimi kontrol etmektedir. Merkezi güvenlik yönetici birimi

ise erişim kontrolü ve diğer protokollerle iletişim için politikaları kontrol etmektedir. Bu mod ile birlikte "Yetkilendirme" kavramı da Bluetooth teknolojisinde kullanılmaya başlanmıştır. Bluetooth v2.0' a kadar tüm cihazlar ve geçmişe uyumluluk prensibi gereği üst versiyonlar da bu modu desteklemektedir.

- **Güvenlik Modu 3:** Bağlantı seviyesinde uygulanan güvenlik modudur. Tüm güvenlik prosedürleri fiziksel bağlantı kurulmadan önce yerine getirilir. Kimlik doğrulama ve trafik şifrelemesini tüm bağlantılar için zorunlu tutar. Kimlik denetleme, yetkilendirme ve şifreleme tamamlanmadan servis keşfine dahi izin vermez. Servis seviyesinde yetkilendirme cihazın kimlik doğrulamasının yapılmasıyla yapılmamaktadır. Fakat NIST (National Institute of Standards and Technology) kimlik doğrulama istismarının önüne geçilmesi açısından servis seviyesinde yetkilendirme kullanılmasını tavsiye etmektedir. Yani bağlantı kurulacak cihazın sahibinin bağlantı isteğinden haberdar olması gerektiğini vurgulamaktadır. Bu mod, güvenlik açısından en güçlü mod olarak kabul edilir.

- **Güvenlik Modu 4:** Bluetooth v2.1 + EDR ile kullanılmaya başlanmıştır. Güvenlik prosedürleri, bağlantı kurulduktan sonra devreye girmektedir. Bu güvenlik modu Secure Simple Pairing (SSP) kullanmasının yanında bağlantı kurulumu için Diffie – Hellman anahtar değişim protokolünü kullanılır. Bu mod tarafından korunan servisler; kimlik doğrulanmış bağlantı anahtarı gereksinimi, kimlik doğrulanmamış bağlantı anahtarı gereksinimi ve güvenliğin olmadığı durumlar olmak üzere bu üç kategoriden birinde olmak zorundadır. Geçmişe uyumluluk prensibi gereği Bluetooth v2.0 ve öncesi cihazlarla iletişim kurulması durumunda düşük güvenlik modlarını (Güvenlik Modu 1, 2 ve 3) destekler. Bluetooth v2.1 ve sonrası versiyonlarda tüm servisler için şifrelemeyi zorunlu kılar.

Bölüm 3

Güvenlik Analizi

Bilişim dünyasında yaşanan gelişmelerle birlikte kişi, kurum ve kuruluşlar açısından bilgi güvenliğinin önemi de giderek artmaktadır. Bilgi güvenliği bilgilerin izinsiz veya yetkisiz şekilde erişim, kullanım, açığa çıkarılması, yok edilmesi, değiştirilmesi veya hasar verilmesinden korunması işlemidir [31]. Bilgi güvenliğinin anlaşılmasında bilgi güvenliğini oluşturan alt unsurlarında tanımlanması gerekir. Bu temel unsurların başlıkları Şekil 3.1' de görülmektedir.

Şekil 3.1: Bilgi güvenliği unsurları [32]

3.1 CIA Prensipleri ve Güvenlik Gereksinimleri

Bilgi güvenliği yönetim sistemi bir kuruluşun gizli ve korunması gereken bilgilerinin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan sistematik bir yaklaşımdır. Uluslararası Standartlar Organizasyonu ile Uluslararası Elektroteknik Komisyonunun ortak çalışmasıyla bilgi güvenliği yönetim sistemini her yönüyle belirleyen ISO 27000 standartları hazırlanmıştır. Bu standartlar içerisinde ISO 27001 ve ISO 27002 öne çıkmaktadır. ISO 27002 Bilgi Güvenliği Yönetim Sistemi için uygulama prensiplerini içeren standarttır. Bilgi güvenliği ile ilgili riskleri karşılamak amacıyla kontrol hedeflerini ortaya koymaktadır. Bilgi Güvenliği Yönetim Sistemi' nin bir kuruluşta kurulumu, devamlılığı, sürekli iyileştirme için genel prensip ve yönlendirici bilgiler açıklanmıştır. ISO 27001 ise Bilgi Güvenliği Yönetim Sistemi temel standardıdır. Kuruluşta Bilgi Güvenliği Yönetim Sistemi' nin nasıl uygulanacağı ve denetleneceği bu standartta açıklanmıştır. Ülkemizde güncel olarak Türk Standartları Enstitüsü (TSE) tarafından yayınlanan TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı kullanılmaktadır. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gizlilik (Confidentiality), Veri Bütünlüğü (Data Integrity), Süreklilik (Availability) prensiplerini temel almaktadır. Ancak bilgi güvenliği konusunda bu prensiplere ek olarak İzlenebilirlik, Kimlik Sınaması, Güvenilirlik, İnkâr Edememe, Yetkilendirme başlıkları da değerlendirilmektedir [33–35].

- **Gizlilik:** Kuruluş bünyesinde korunması gereken bilginin yetkisiz kişilerin eline geçmesinin önlenmesi amaçlanmaktadır. Bu bilgi bilgisayar sistemlerinde, harici bellek, DVD, CD gibi depolama ortamlarında veya ağ üzerinde gönderici ve alıcı arasında taşınırken korunmalıdır. Saldırgan yapılandırma hatası, yazılım hatası veya sosyal mühendislik tekniklerini kullanarak yetkili kişilerin hatalarından faydalanarak bilgilere erişimi izinsiz olarak sağlayabilir. Yetkili kullanıcının farkında olmadan kullanıcı adı ve parola bilgilerinin alınması, sisteme giriş yapan kullanıcının saldırgan tarafından bilgisayarının kullanılması, ağ üzerindeki trafiğin izlenmesi, kaydedilmesi gibi durumlar Gizlilik prensibi kapsamında değerlendirilir.
- **Veri Bütünlüğü:** Bu prensibin amacı veriyi kaynağında olduğu şekliyle değiştirilmeden ve bozulmadan tutmak ve korumaktır. Bilgi kısmen de olsa değiştirilmiş veya bozulmuşsa bilginin bütünlüğünden bahsedilemez. Veri Bütünlüğü prensibini uygulamayı amaçlayan bir kuruluş bilginin bulunduğu noktaları sınıflandırmalı ve korunma yöntemine karar vermiş olmalıdır.

- **Süreklilik:** Bu prensip, bilginin ihtiyaç duyulduğu her an ulaşılabilir ve kullanılabilir olmasını amaçlar. Süreklilik hizmetiyle, kullanıcılar, erişim yetkileri olan verilere, zamanında ve güvenilir bir şekilde ulaşabilirler. Kullanıcı ve yazılım hataları, donanım kaynaklı sorunlar, yangın gibi beklenmedik ortam şartlarındaki değişiklikler de bu prensip kapsamındadır [15, 33–35].

- **İzlenebilirlik/Kayıt Tutma (Accountability):** Bu prensibin amacı kullanıcıların erişim saatleri ve işlemleri gibi sistemde gelişen her türlü olayın daha sonra incelenmesini sağlayacak şekilde kayıt altına alınmasıdır. Bir sorunla karşılaşıldığında sorunun anlaşılması ve çözülmesinde bu kayıtlardan yararlanılır.

- **Kimlik Sınaması (Authentication):** Kullanıcının sisteme bağlanabilmesi için kullanıcı adının ve kullanıcıya verilen parolanın doğrulanması işlemidir. Sisteme girişte ilk başta yapılan işlemdir. Cihaz kimliğinin doğrulanması işlemini de kapsar. Bilgisayar ağları ve bilgisayar sistemlerinin yanında fiziksel sistemlerde de oldukça önemlidir. Kimlik sınamasının sağlanması adına akıllı kartlar veya biyometrik teknolojiler kullanılmaktadır.

- **Güvenilirlik (Reliability – Consistency):** Sistem; güvenilir veri ölçümünü, iletişimini ve analizini sağlamalıdır. Sistemde gerçekleştirilen aynı işlemden her defasından aynı sonucun tutarlı bir şekilde alınmasıdır. Ayrıca öngörülen sonuç ile elde edilen sonuç arasında tutarlılık olması durumudur.

- **İnkâr Edememe (Non-repudiation):** Bu prensibin amacı verinin iletildiği gönderici ve alıcı arasındaki meydana gelebilecek iletişim sorunlarını en aza indirmektir. İki sistem arasında yapılan bilgi aktarımında gönderen veriyi gönderdiğini ve/veya alıcı veriyi aldığını inkâr edememelidir. Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanılmaktadır.

- **Yetkilendirme (Authorization):** Kullanıcı adı ve parola doğrulaması yapılan kullanıcıların sisteme, programa veya ağa belirlenen yetkilerle erişim hakkına sahip olmasıdır. Sisteme kayıtlı olan kullanıcılar gruplanarak bu grupların yetkileri belirlenir. Kullanıcı içerisinde bulunduğu grup veya grupların bütün yetkilerine sahiptir. Güvenliğin tam sağlanabilmesi için kullanıcılara gerekenden fazla yetki verilmemelidir [15, 35].

3.2 Detaylı Tehdit Analizi

WBAN mimarisinde kullanılan sistem prototipinin genellikle 3 katmanlı mimariye sahip olduğundan "WBAN Mimarisi" başlığı altında bahsedilmiş ve katmanlar ayrıntılı şekilde açıklanmıştır. Bu katmanlar sırasıyla; WBAN katmanı, WBAN sunucu katmanı ve medikal sunucu katmanıdır [15].

WBAN mimarisinde bulunan bu katmanların detaylı tehdit analizinin yapılabilmesi için dört katmandan oluşan "Güvenli Mimari Tehdit Kataloğu" oluşturulmuştur. Yapılan analizde kullanılan tehdit kataloğunun katmanları Şekil 3.2' de görülmektedir.

Şekil 3.2: Güvenli mimari tehdit kataloğu

Ayrıca analiz sırasında ortaya çıkan riskler Microsoft' un STRIDE Tehdit Modeline [36] göre değerlendirilmiştir. Bu tehdit modelinin içeriği şu şekildedir;

- **Yanıltıcı Kimlik (Spoofing Identity):** Sisteme yetkisiz erişim sağlayarak diğer kullanıcıların kullanıcı adı, parola gibi kimlik doğrulama bilgilerinin kullanılmasıdır.

- **Veriyle Oynama (Tampering with Data):** Verinin kötü yönde değiştirilmesidir.
- **İnkar Etme (Repudiation):** İşlemlerde yeterli denetim veya kayıt altına alma olmaması durumunda kullanıcıların yapılan işlemlere itiraz edebilmesidir.
- **Bilgi İfşası (Information Disclosure):** Paylaşılmak istenmeyen kişisel bilgilerin ifşa edilmesidir.
- **Servis Dışı Bırakma (Denial of Service):** Sistem özkaynaklarının kullanılamaz duruma düşmesidir. Bir sisteme yapılan saldırı niteliğindeki yoğun erişim isteklerinden dolayı o sistemin gerçek isteklere cevap veremez duruma gelmesidir.
- **Ayrıcalık Seviyesi (Elevation of Privilege):** Yetkisiz bir kullanıcının yüksek yetkili bir kullanıcı hakkına sahip olmasıdır.

WBAN mimarisinde bulanan katmanların detaylı tehdit analizleri sırası ile Tablo 3.1, Tablo 3.2 ve Tablo 3.3' de gösterilmektedir.

Tablo 3.1: WBAN katmanı güvenlik riskleri

Güvenlik Riskleri	S	T	R	I	D	E
WBAN katmanında kullanılan sensörlere zararlı yazılım bulaşması sonucu örneğin; sensörün kullanılamaz hale gelmesi veya vücut üzerinden aldığı veriyi WBAN sunucusuna gönderememesi	X	X	X	X	X	X
WBAN katmanında kullanılan sensörlere yapılacak olan bir servis dışı bırakma saldırısı sonucu örneğin; vücut üzerinden veri alınamaması veya WBAN sunucusuna verinin iletilememesi					X	
WBAN katmanında kullanılan sensörlerin verileri iletmeden önce kullandığı kriptografi yöntemi ve kullanımının doğru yapılmaması sonucu örneğin; güç kaynağının verimli kullanılamaması ve sürekli değiştirilme gereksinimi		X		X		

Tablo 3.1: WBAN katmanı güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
WBAN katmanında kullanılan akıllı sensörler üzerinde koşan yazılımda bulunan açıklıklar	X	X	X	X	X	X
WBAN katmanında kullanılan akıllı sensörlere erişimde kimlik doğrulama ve yetkilendirmede yapılan hatalar sonucu örneğin; yetkisiz erişimlerin sağlanması	X	X		X	X	X
WBAN katmanında kullanılan akıllı sensörlerin yapılandırılmalarında hatalar bulunması	X	X	X	X	X	
WBAN katmanında kullanılan akıllı sensörler ile WBAN sunucusu arasındaki iletişim için kullanılan ağın servis dışı kalması sonucu örneğin; gönderilmesi veya alınması gereken acil verilerin ulaşmaması					X	
WBAN katmanında kullanılan akıllı sensörler ile WBAN sunucusu arasındaki iletişim için kullanılan ağın dinlenmesi ya da manipüle edilmesi sonucu örneğin; eğer veriler açık metin olarak iletiliyorsa saldırganların eline geçmesi veya asıl hedef yerine başka bir yere gönderilmesi	X	X		X	X	
WBAN katmanında kullanılan akıllı sensörler ile WBAN sunucusu arasındaki iletişim için kullanılan ağın tasarımında yapılan hatalar sonucu örneğin; iletilen verinin açık metin olması	X	X		X	X	
WBAN katmanında kullanılan akıllı sensörler ile WBAN sunucusu arasındaki iletişim için kullanılan ağ üzerinden izinsiz erişime fırsat verilmesi sonucu örneğin; yetkisiz kişilerin sensörlere erişim sağlayabilmesi	X	X		X	X	

Tablo 3.1: WBAN katmanı güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
WBAN katmanında kullanılan akıllı sensörlere izinsiz fiziksel erişim sağlanması sonucu örneğin; WBAN sunucusu ile iletişimin kesilmesi veya sensörün bulunduğu yerden çıkartılması sonucu veri üretilememesi				X	X	
WBAN katmanında kullanılan akıllı sensörlerin fiziksel olarak (bozulma, kırılma vb.) servis dışı kalması sonucu örneğin; vücut üzerinden veri alınamaması					X	

Tablo 3.2: WBAN sunucu katmanı güvenlik riskleri

Güvenlik Riskleri	S	T	R	I	D	E
WBAN sunucusu olarak kullanılan cihaz (cep telefonu, kişisel bilgisayar veya PDA) ile yapılacak bilgi ve farkındalık eksikliğinden kaynaklanan işlemler sonucu örneğin; sunucudaki sağlık verilerinin saldırganlar tarafından ele geçirilmesi	X	X	X	X	X	X
WBAN sunucusu olarak kullanılan cihaza bir şekilde zararlı yazılım bulaşması sonucu örneğin; cihazın kullanılamaz hale gelmesi, verilerin yetkisiz kişilerle paylaşılması veya cihaz kontrolünün başkalarının eline geçmesi	X	X	X	X	X	X
WBAN sunucusu olarak kullanılan cihaza yapılacak olan bir servis dışı bırakma saldırısı sonucu örneğin; sağlık verilerine erişimin sağlanamaması					X	

Tablo 3.2: WBAN sunucu katmanı güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
WBAN sunucusunda tutulan veriler için kullanılan kriptografi yöntemi ve kullanımının doğru yapılmaması sonucu örneğin; verilerin şifreleme ve şifre çözme durumlarında problem yaşanması		X		X		
WBAN sunucusu olarak kullanılan cihaz üzerinde koşan yazılımda veya üzerindeki uygulamalarda açıklık bulunması	X	X	X	X	X	X
WBAN sunucusuna yapılan erişimlerde kimlik doğrulama ve yetkilendirmede yapılan hatalar sonucu örneğin; kimlik doğrulamanın atlatılması veya yetkisiz erişimlerin sağlanması	X	X	X	X	X	X
WBAN sunucusuna WBAN içinden veya WBAN dışından yapılan iletişim için kullanılan ağın servis dışı kalması sonucu örneğin; gönderilmesi veya alınması gereken acil verilerin yerine ulaşmaması					X	
WBAN sunucusuna WBAN içinden veya WBAN dışından yapılan iletişim için kullanılan ağın dinlenmesi veya manüpile edilmesi sonucu örneğin; eğer veriler açık metin olarak iletiliyorsa saldırganların eline geçmesi	X	X		X	X	
WBAN sunucusuna WBAN içinden veya WBAN dışından yapılan iletişim için kullanılan ağın tasarımında yapılan hatalar sonucu örneğin; iletilen verinin açık metin olması	X	X		X	X	
WBAN sunucusuna WBAN içinden veya WBAN dışından yapılan iletişim için kullanılan ağ üzerinden izinsiz erişime fırsat verilmesi sonucu örneğin; yetkisiz kişilerin verilere ve sisteme erişim sağlayabilmesi	X	X		X	X	

Tablo 3.2: WBAN sunucu katmanı güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
WBAN sunucusu olarak kullanılan cihazın çalınması veya kaybolması sonucu örneğin; üzerinde tutulan verinin üçüncü şahısların eline geçmesi veya silinmesi	X	X		X	X	
WBAN sunucusu olarak kullanılan cihaza yetkisiz kişiler tarafından fiziksel erişim sağlanması sonucu örneğin; WBAN katmanı veya medikal katman ile iletişimin kesilmesi veya sunucu üzerinde olan verilerin silinmesi		X		X	X	
WBAN sunucusu olarak kullanılan cihazın diskinde meydana gelen hatalar sonucunda örneğin; verilere erişimin sağlanamaması				X	X	
WBAN sunucusu olarak kullanılan cihazın fiziksel olarak (bozulma, kırılma vb.) servis dışı kalması sonucu örneğin; WBAN katmanından gelen kritik verilerin değerlendirilememesi ve aksiyon alınamaması					X	

Tablo 3.3: Medikal sunucu katmanı güvenlik riskleri

Güvenlik Riskleri	S	T	R	I	D	E
Medikal sunucu katmanın da bulunan, sağlık çalışanlarının memnuniyetsiz olmaları sonucu örneğin; acil koduyla gelen bir sinyalin vaktinde değerlendirilmemesi	X	X		X	X	

Tablo 3.3: Medikal sunucu güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
Medikal sunucu katmanında kullanılan cihazlar ile yapılacak bilgi ve farkındalık eksikliğinden kaynaklanan işlemler sonucu örneğin; sunucudaki sağlık verilerinin saldırganlar tarafından ele geçirilmesi veya hasta verilerinin karıştırılabilmesi	X	X		X	X	
Medikal sunucu katmanında oluşabilecek organizasyonel hatalar sonucu örneğin; sağlık personelinin yanlış yönlendirilmesi ve hastaya zamanında müdahale edilememesi		X		X	X	
Medikal sunucu katmanında kullanılan IT siteminin kullanımından dolayı oluşacak hatalar sonucunda örneğin; farklı hasta verilerinin karıştırılması		X		X	X	
Medikal sunucu katmanında kullanılan cihaza ya da cihazlara bir şekilde zararlı yazılım bulaşması sonucu örneğin; cihazların kullanılamaz hale gelmesi, verilerin yetkisiz kişilerle paylaşılması veya cihaz kontrollerinin başkalarının eline geçmesi	X	X	X	X	X	X
Medikal sunucu katmanına yapılacak olan bir servis dışı bırakma saldırısı sonucu örneğin; sağlık verilerine ve personeline erişimin sağlanamaması					X	
Medikal sunucu katmanında kullanılan kriptografi yöntemi ve kullanımının doğru yapılmaması sonucu örneğin; verilerin şifreleme ve şifre çözme durumlarında problem yaşanması		X		X		
Medikal sunucu katmanında kullanılan yazılımlarda veya uygulamalarda açıklık bulunması	X	X	X	X	X	X

Tablo 3.3: Medikal sunucu güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
Medikal sunucu katmanına, katman içerisinde bulunan uygulama ve cihazlara erişimlerde kimlik doğrulama ve yetkilendirmede yapılan hatalar sonucu örneğin; kimlik doğrulamanın atlatılması veya yetkisiz erişimlerin sağlanması	X	X	X	X	X	X
Medikal sunucu katmanındaki sistemlerde yapılandırma hataları bulunması	X	X	X	X	X	
Medikal sunucu katmanının WBAN sunucusuyla veya katman içerisindeki iletişim için kullanılan ağın servis dışı kalması sonucu örneğin; gönderilmesi veya alınması gereken acil verilerin yerine ulaşmaması					X	
Medikal sunucu katmanının WBAN sunucusuyla veya katman içerisindeki iletişim için kullanılan ağın dinlenmesi veya manüpile edilmesi sonucu örneğin; eğer veriler açık metin olarak iletiliyorsa saldırganların eline geçmesi	X	X		X	X	
Medikal sunucu katmanının WBAN sunucusuyla veya katman içerisindeki iletişim için kullanılan ağın tasarımında yapılan hatalar sonucu örneğin; hasta verilerinin tutulduğu sunucunun internete açılması	X	X		X	X	
Medikal sunucu katmanının WBAN sunucusuyla veya katman içerisindeki iletişim için kullanılan ağ üzerinden izinsiz erişime fırsat verilmesi sonucu örneğin; yetkisiz kişilerin verilere ve sistemlere erişim sağlayabilmesi	X	X		X	X	
Medikal sunucu katmanında kullanılan özellikle mobil cihazların çalınması veya kaybolması	X	X		X	X	

Tablo 3.3: Medikal sunucu güvenlik riskleri - Devam

Güvenlik Riskleri	S	T	R	I	D	E
Medikal sunucu katmanında kullanılan cihazlara yetkisiz kişiler tarafından fiziksel erişim sağlanması sonucu örneğin; WBAN sunucu katmanı ile iletişimin kesilmesi veya sunucu üzerinde olan verilerin silinmesi		X		X	X	
Medikal sunucu katmanında kullanılan cihazların diskinde meydana gelen hatalar sonucunda örneğin; verilere erişimin sağlanamaması				X	X	
Medikal sunucu katmanında kullanılan cihazların fiziksel olarak (bozulma, kırılma vb.) servis dışı kalması sonucu örneğin; WBAN sunucu katmanından gelen kritik verilerin değerlendirilememesi ve aksiyon alınamaması					X	

3.3 Tez Çalışmasının Kapsamı

WBAN teknolojisinin her katmanında karşılaşılabilecek güvenlik riskleri detaylı şekilde incelenmiştir. Bu inceleme de gösteriyor ki WBAN sitem tasarımları yapılırken güvenlik konusunun üzerinde daha fazla durulmalıdır. "İlgili Çalışmalar" başlığı altında örneklendirildiği gibi WBAN siteminin güvenliğinin geliştirilmesi konusunda çeşitli sistem önerileri bulunmaktadır.

WBAN teknolojisinin güvenlik riskleri ve bu konu ile ilgili yayınlanmış çalışmalar değerlendirilerek, tez kapsamında vücut alan ağlarında kullanılan medikal cihazların ve mobil sağlık uygulamalarının güvenlik açısından analizleri gerçekleştirildi. Çalışma kapsamında öncelikle vücut alan ağlarındaki uzaktan erişilebilir medikal cihazların karşı karşıya kaldıkları tehditler ve riskler belirlendi. Bununla birlikte uygulama marketlerden kolay şekilde edinilebilen, akıllı cihazlar üzerinde çalışan mobil sağlık uygulamaları için güvenlik testleri gerçekleştirildi. Ayrıca bu sağlık uygulamalarının bulut ortamları ile yapmış olduğu kişisel sağlık verilerinin paylaşımı irdelenip mahremiyetin gözetilip gözetilmediği değerlendirildi.

WBAN teknolojisinin Hastane Yönetim Sistemi ile olan ilişkisi tez çalışması dışında tutulmuştur.

Bölüm 4

İlgili Çalışmalar

4.1 WBAN Teknolojisi

BAN teknolojisinin sağlık sektöründeki avantajları araştırmacıları bu alanda pek çok çalışma yapmaya yönlendirmiştir. BAN teknolojisinin içerisinde ise WBAN uygulamaları düşük güç gereksinimi ve uygulanabilirliğiyle ilgi çekmektedir. Araştırmacılar ve sistem tasarımcıları tarafından olabildiğince geniş kapsamda uygulanabilen birçok sistem tasarlanmıştır. Tasarımcılar ve araştırmacılar için geniş alanda uygulanabilen sistemlerin tasarlanması, sistemin verimliliğini ve değerini artıracağından önemlidir.

Örneğin 2011 yılında yapılan bir çalışmada Zhang ve arkadaşları [37] kalp hastalarında EKG'nin gerçek zamanlı izlenmesini sağlayan kablosuz bir EKG plasteri tasarlamıştır. Tasarlanan plaster 25 gramlık düşük ağırlığıyla, giyilebilir olması ve çalışır durumdayken 26 saatlik pil ömrüyle dikkat çekmektedir. Ayrıca plaster, hastaların EKG sinyalini kablosuz olarak cep telefonlarına veya ZigBee kullanan bilgisayarlarına aktarabilmektedir. Araştırmacılar prototipin doğrulamasını klinik çalışmalarla da sağlamıştır.

Volmer ve Orglmeister [38] ise profilaksi ve kalp-damar hastalıkları rehabilitasyonu uygulamaları için bir sistem tasarlamıştır. Minyatür algılayıcı modüllerden oluşan sistem EKG, fotopletismogram (PPG) ve fonokardiyografi (PCG) ölçümlerini yapabilmektedir. Sistemde her algılayıcı modülü, hastanın duruş ve aktivite ölçümleri için üç-eksenli bir ivmeölçer ile birleştirilmiştir. Sistemde farklı biyosensörlerden gelen verilerle sağlık durumu hakkında ayrıntılı bilgi elde etmek mümkün olduğundan, IEEE 802.15.4' ü temel

alan kablosuz ağ, sensörlerin senkron örnekleme yapmasını sağlayan bir senkronizasyon mekanizmasıyla geliştirilmiştir.

2008 yılında Flack ve arkadaşları [39] BASUMA projesini sundular. Proje kapsamında evde bakım ortamında kronik hastaların sağlık durumunun takibini, WBAN için etkin enerji kullanımı ve dayanıklı çip-üzeri-sistem platformunu sundular. BASUMA' nın ilk uygulama alanları kronik obtrüktif akciğer hastalarının tedavilerinin ve meme kanseri hastası kadınların ayakta kemoterapi tedavilerinin geliştirilmesidir.

4.2 WBAN Teknoloji Güvenliği

BAN teknolojisinin yapısında bulunan tüm sensörlerden alınan veriler kişisel veri kapsamındadır. Bu verilerin BAN içi ve BAN dışı aktarımı, verinin saklanması ve ihtiyaç durumunda erişim sağlanabilmesi durumlarındaki güvenlik gereksinimleri araştırmacıların bu konuya olan ilgisini arttırmıştır. Kablosuz teknolojileri kullanmasından dolayı WBAN teknolojilerinin güvenlik zafiyetlerini barındırma olasılığı daha fazladır. Bu yüzden araştırmacılar ve sistem tasarımcıları tarafından birçok çalışma yayınlanmıştır.

Örneğin; Jank ve çalışma grubu [40] kablosuz vücut alan ağlarındaki bilginin korunması için yeni bir güvenlik modeli ve güvenlik anaçatısı (framework) önermişlerdir. Bu çalışmanın WBAN içerisindeki kablosuz iletişimin uygun güvenlik ve gizliliğinin sağlanmasında rehber niteliğinde olması amaçlanmıştır.

Garcia-Morchon ve arkadaşları [41] hasta yaşam alanı ve medikal sensör ağları kavramlarına dayanan, yaygın hasta bakım hizmetinde kullanılan kablosuz sensör ağlar için bir dağıtım modeli geliştirmiştir. Hasta alan ağındaki operasyon ve güvenlik gereksinimleri, medikal sensör ağı ve arka-uç (back-end) seviyelerine yönelik üç seviyeden oluşan tam ve etkili güvenli bir yapı önermişlerdir. Ayrıca, bu üç seviyenin birbirleri arasındaki ve medikal sensör ağlarını temel alan güvenli yaygın hasta bakım sistemlerinin pratik uygulamaları için gerekli olan güvenlik ve gizlilik mekanizmalarıyla etkileşimini açıklamışlardır.

Glikoz takibi ve insülin pompası sistemleri diyabetli hastalar arasında giderek yaygın hale gelmektedir. Bu cihazlar sık sık güvenlik saldırılarına maruz kalan kablosuz iletişim ağlarını kullanmaktadır. Li ve arkadaşları 2011 yılında yaptığı bir çalışmada [42] piyasada

bulunan, glikoz kontrolü de yapan bir insülin pompasını laboratuar ortamında uygulamışlar ve çeşitli saldırılara karşı savunma yöntemleri önermişlerdir. Çalışma kapsamında; kablosuz iletişimin dinlenmesi gibi pasif atakların ve hedeflenen tedavide değişiklik yapmak için medikal cihazın kontrolünün saldırganın eline geçmesi gibi aktif atakların, herkese açık bilgilerin ve yaygın olarak kullanılan off-the-shelf donanımının kullanılmasıyla gerçekleştirilebileceği gösterilmiştir. Bahsedilen ataklar hastaların gizlilik ve güvenliğini tehlikeye atabilmektedir. Bu tür saldırılara karşı araştırmacılar rolling-code kriptografik protokollere ve body-coupled iletişime dayanan iki tür savunma önermiştir. Bu savunma yöntemlerinin kişisel sağlık sistemlerindeki güvenlik risklerini azaltmada etkili olduğu gösterilmiştir.

Vücuda yerleştirilebilir medikal cihazların (IMDs) kullanımı hastaların tıbbi ihtiyaçlarıyla birlikte artmaktadır. IMDs tasarımcıları güvenlik, güvenilirlik, kullanım kolaylığı, güç tüketimi ve maliyet konularında çalışmalar yapmaktadır. Ancak son yıllarda yapılan çalışmalar, araştırmacıların özellikle diğer sistemlerle iletişimde kablosuz iletişim veya internet kullanan medikal teknolojilerde hastaları saldırılardan korumak için güvenlik ve veri gizliliği konularında da araştırma yapılması gereğini göstermiştir. Burleson ve çalışma grubu [43] güvenli, vücuda yerleştirilebilir medikal cihazlarla ilgili yayınlanmış çalışmaları inceleyerek tasarım zorluklarını değerlendirmişlerdir. Güvenlik prensiplerinin uygulanması ve yaygın güvenlik risklerinden kaçınılması konularını tartışmışlardır.

Vücuda yerleştirilebilir bir cihaz olan kardiyoverter defibrilatör (ICD) cihazının güvenlik ve gizlilik özellikleri Halperin ve çalışma grubu [44] tarafından incelenmiştir. Çalışma grubunun incelediği kalp pili teknolojisi içeren bu cihaz, kablosuz iletişim kullanmaktadır ve piyasada bulunmaktadır. Araştırmacılar hasta güvenliği ve gizliliğini tehlikeye atacak çeşitli yazılımlara radyo tabanlı saldırılar uygulamışlardır. Hasta güvenliğini sağlama isteği ve sınırlı kaynağa sahip cihazlardaki güç tüketimi ve güvenlik arasındaki ilişkiyi dikkate alarak, RF güç toplayıcı tabanlı üç yeni sıfır-güç (zero-power) savunma yöntemini tanıtmışlardır.

Silva ve çalışma grubu [45] Medikal Siber-Fiziksel Sistemlerle (MCPS) ilgili temel bir hasta modeli geliştirmişlerdir. Çalışmalarının amacı hasta güvenliğinin sağlanması ve MCPS' nin doğrulamasıdır. Bu amaçla hastanın sağlığını tehlikeye atmadan sağlık bakım hizmeti sistemlerinin doğrulamasında kullanılabilecek bir hasta modeli sunmuşlardır. Sundukları model kalp hızı, solunum hızı, nabız ve vücut sıcaklığı sinyallerini kullanarak

temel hasta durumunu belirlemektedir. Sinyaller için klinik veri tabanının istatistiksel analizine dayalı regresyon modeli kullanarak temel hasta modelinin modellemesini ve değerlendirmesini göstermişlerdir.

2013 yılında Ramlı ve arkadaşları [46] WBAN' daki güvenli veri iletişiminde biyometrik karakteristiklerin kullanımı ve güç verimliliğinin yanı sıra hesaplama karmaşıklığını da azaltma konusunda çalışmışlardır. Hibrid kimlik doğrulama modelini sistem için kavramsal ana çatı (framework) olarak kullanmışlardır. Diğer teknikler yazılım ve donanım kullanırken, önerilen sistem kimlik doğrulaması için insan vücudunun benzersiz bir özelliğini kullanmaktadır. Ayrıca bu çalışmayı örnekler nitelikte Ramlı ve arkadaşları aynı yıl güvenli WBAN teknolojisinde kullanılmak üzere EKG sinyallerini biyometrik veri olarak kullandıkları bir çalışma yayınlamıştır [47].

Bölüm 5

WBAN Güvenlik Analizi

Bu bölümde, giyilebilir medikal cihaz kategorisine giren MI BAND edinilerek haberleşmede kullandığı Bluetooth teknolojisi güvenlik açısından analiz edildi. MI BAND cihazının WBAN sistemi mobil uygulamalarının güvenlik testleri gerçekleştirildi. Ayrıca cihazın mobil uygulamalarından farklı olarak, uygulama marketlerden kolay şekilde edinilebilen mobil sağlık uygulamalarının güvenlik testleri de gerçekleştirildi.

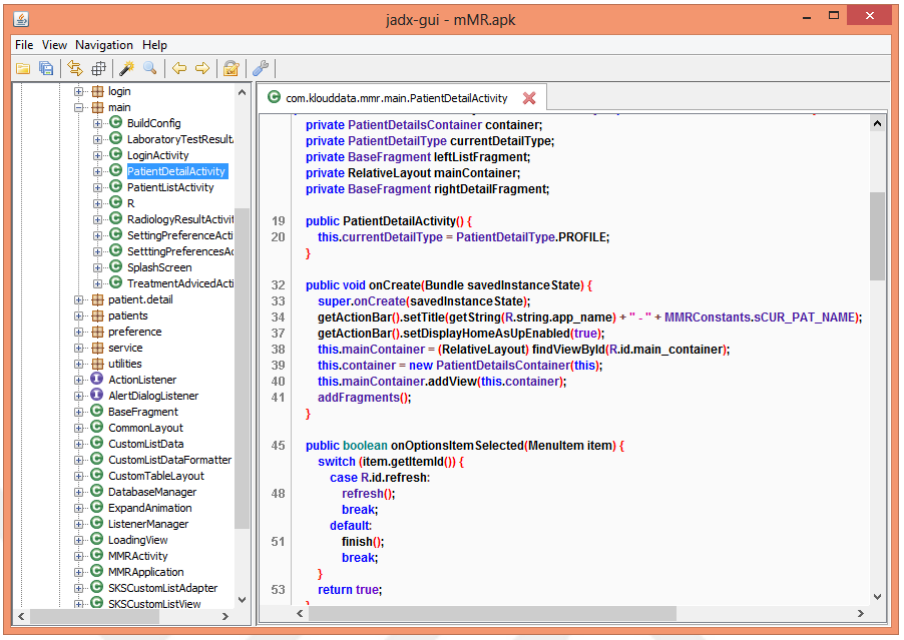
Gerçekleştirilen bu güvenlik testleri 3 ana başlık altında yapıldı. Bu başlıklar Tersine Mühendislik, Depolama Analizi ve Ağ Trafiği Analizidir.

- Tersine Mühendislik adımında, uygulamaların izinleri ve uygulama kodlarının karmaşıklaştırma işlemine tabi tutulup tutulmadığı incelendi.
- Depolama Analizi adımında, uygulamaların yerel depolama alanlarında tuttukları veriler, veritabanlarına erişim, hassas verilerin loglanması ve cache durumları incelendi.
- Ağ Trafiği Analizi adımında, veri iletimi, SSL sertifika kontrolü ve istemci taraflı enjeksiyon olup olmadığı incelendi.

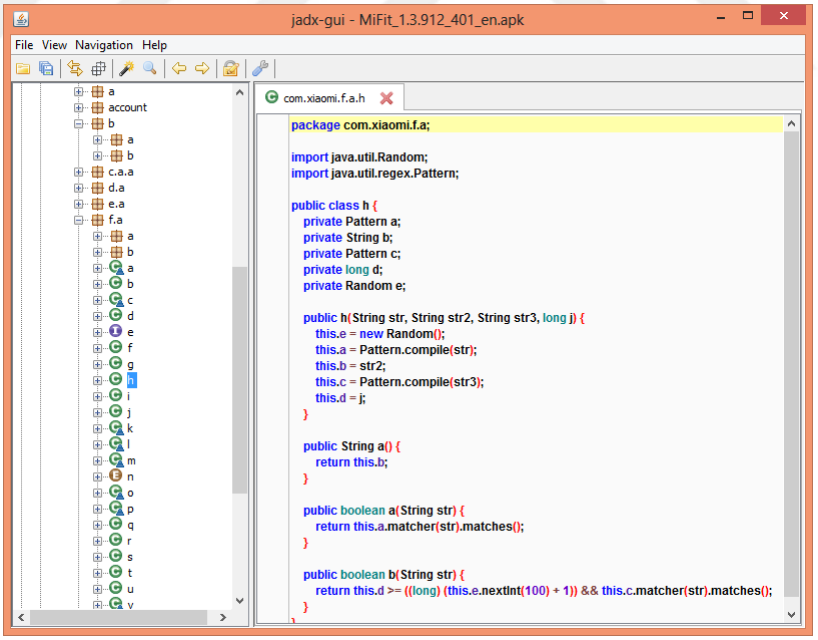
Yapılan güvenlik testlerinde Android SDK [48], Genymotion Emülatör [49], Burp Suite [50], Wireshark [51], Nexus 5 Android Phone, Mi Band 1s [52] araçları ve Vezir2_0 linux dağıtımı [53] kullanılmıştır.

Tersine Mühendislik adımında incelenen kod karmaşıklaştırma işlemi gerçek kodun ele geçirilememesi için yapılan bulanıklaştırma işlemidir. Bu işlem sonucunda kodda bulunan

obje, değer ve metodların ismi değişerek anlaşılmayacak hale gelir [54]. Kod karmaşıklaştırma işlemi yapılmamış bir kod örneğinin ekran görüntüsü 5.1' de, kod karmaşıklaştırma işlemi yapılmış bir kod örneğinin ekran görüntüsü ise 5.2' de gösterilmiştir.



Şekil 5.1: Karmaşıklaştırılmamış kod örneği



Şekil 5.2: Karmaşıklaştırılmış kod örneği

Tersine Mühendislik adımı altında incelenen uygulama izinleri, kendi veya diğer uygulamaların belirli bileşenlerine veya özelliklerine erişimi sınırlandırmak için kullanılan bir güvenlik mekanizmasıdır. Bu izinler koruma seviyesi (protection level) olarak adlandırılan 4 farklı özellikte bulunurlar. Bu özelliklerden ilki olan Normal, herhangi bir

uygulamanın talebi ile ulaşılmasına izin verilmesidir. Tehlikeli (Dangerous), sadece kullanıcı onayı ile izin verilmesidir. İmza (Signature) ise, aynı imza ile imzalanmış uygulamaların erişimine izin verilmesidir. İmza veya Sistem (Signature or system), imza izni gibi çalışır, ek olarak android sistem imajı kontrolü ile de erişim sağlanmasıdır [55].

Ağ trafiği analizi adımında incelenen SSL sertifika kontrolü, uygulama ile uygulamanın iletişim kurduğu sunucu arasındaki trafiğe üçüncü kişiler tarafından girilip girilemediğinin testidir. Ayrıca dinlenen tarfikte akan verilerin açık metin olarak taşınıp taşınmadığı da bir diğer test adımıdır.

Google I/O 2012' de yapılan bir sunumda güvenlik ve mahremiyetin sömürülmesinde etkili olan on tehlikeli izin sıralanmıştır [56]. Yapılan analizlerde bu kategorideki izinler "*" ile işaretlenerek belirtildi.

GCM fonksiyonu uygulama geliştiricilerin farklı platformlar arasında ileti göndermelerine olanak sağlar. Senkronizasyon işlemi başlatılmasında bu fonksiyon kulanılabilir. Ayrıca; mesajın içinde gönderilecek bir link ile video anında oynatmaya başlanabilir. İstenilen bir programı (telefon görüşmesi, SMS gönderme dahil) başlatabilir, telefondaki herhangi bir ayarı değiştirebilir ve lokasyon servisine erişim sağlanabilir [57]. Yapılan analizlerde bu kategorideki izinler "**" ile işaretlenerek belirtildi.

Yapılan analizler sonucu WBAN sistemi mobil uygulamaları ve mobil sağlık uygulamalarında en çok kullanıldığı tespit edilen uygulama izinleri kısaca aşağıda açıklanmıştır [58].

BLUETOOTH: Eşleşmiş Bluetooth cihazlarına uygulamalara erişim için izin verir.

BLUETOOTH_ADMIN: Bluetooth cihazlarına keşif ve eşleme için uygulamalara izin verir.

ACCESS_NETWORK_STATE: Ağlarıyla ilgili bilgi erişimi için uygulamalara izin verir.

INTERNET: Ağ bağlantısı açmak için uygulamalara izin verir.

WAKE_LOCK: Cihazın uyku moduna geçmesi veya ekran kararmasına karşı Power Manager Wake Locks kullanmasına izin verir.

WRITE_EXTERNAL_STORAGE: Harici depolama yapmak için uygulamaya izin verir.

SEND_SMS: Uygulamaya SMS göndermek için izin verir.

RECEIVE_SMS: Uygulamanın SMS alması için izin verir.

SYSTEM_ALERT_WINDOW: TYPE_SYSTEM_ALERT kullanarak uygulamanın diğer tüm uygulamalar üzerinde görünen pencereler açmasına izin verir. Bu izni çok az uygulama kullanabilir.

TYPE_SYSTEM_ALERT: Düşük güç uyarısı gibi sistem penceresidir. Bu pencereler her zaman uygulama ekranlarının en üstündedir.

READ_HISTORY_BOOKMARKS: Browser' in ziyaret ettiği bütün URL geçmişlerinin okunması için uygulamaya izin verir. Bu izin üçüncü parti uygulamalar veya WEB taraması yapabilen diğer uygulamalar tarafından uygulanmayabilir.

WRITE_HISTORY_BOOKMARKS: Uygulamaya telefonunuza depolanmış Browser geçmişi veya yer işaretlerini değiştirmek için izin verir. Bu izin uygulamanın Browser verilerini değiştirmek veya silmek için de izin verir. Bu izin üçüncü parti uygulamalar veya WEB taraması yapabilen diğer uygulamalar tarafından uygulanmayabilir.

READ_CONTACTS: Uygulamaya kullanıcının iletişim bilgilerini okuması için izin verir.

WRITE_CONTACTS: Uygulamaya kullanıcının iletişim bilgilerini yazması için izin verir.

READ_CALENDAR: Uygulamaya kullanıcının takvim bilgilerini okuması için izin verir.

WRITE_CALENDAR: Uygulamaya kullanıcının takvim bilgilerini yazması için izin verir.

CALL_PHONE: Uygulamaya bir telefon araması başlatması için izin verir.

READ_LOGS: Uygulamaya düşük seviyeli sistem log dosyalarını okuması için izin verir.

ACCESS_FINE_LOCATION: Uygulamaya hassas bir şekilde konum erişimi sağlayabilmesi için izin verir.

GET_TASKS: Uygulamanın çalışmakta olan veya en son çalışmış görevlerle ilgili bilgi almasına izin verir. Bu izin hangi uygulamanın cihazda kullanıldığıyla ilgili bilgi almasına da izin verebilir.

CHANGE_WIFI_STATE: Uygulamaya Wi-Fi bağlantı durumunu değiştirmek için izin verir.

RECEIVE_BOOT_COMPLETED: Uygulamaya sistem ön yüklemesi tamamlandıktan sonra yayınlanan ACTION_BOOT_COMPLETED iznini almak için izin verir.

ACTION_BOOT_COMPLETED: Sistem ön yüklemesi tamamlandıktan sonra yapılan broadcast yayınıdır. Uygulamaya özel başlatma gerçekleştirmek için kullanılabilir.

5.1 Güvenlik İncelemesi

Tez çalışması kapsamında medikal cihaz kategorisinde uzaktan yönetim için mobil uygulamaya sahip, Bluetooth teknolojisi ile haberleşen insülin pompası alınması hedeflendi. Ancak tedarikçi firmaların şirket politikaları gereği cihaz elde edilemedi. Bu yüzden uzaktan yönetim için mobil uygulamaya sahip, haberleşme için de Bluetooth teknolojisini kullanan MI BAND 1S cihazı ile çalışmalar gerçekleştirildi.

MI BAND 1S (Şekil 5.3) ile günlük olarak ne kadar yüründüğünü/koşulduğunu, ne kadar kalori yakıldığını, gece ne kadar uyunduğunu, uykunun ne kadarının derin uykuda ne kadarının hafif uykuda geçtiği takip edilebilir. Ayrıca; Bluetooth özelliği olan mobil cihazın kilidini açar, gelen çağrı ve bildirimlerde titreşimli uyarı verir, bağımsız alarmlar kurulabilir ve bu alarm saatlerinde titreşimli ve ışıklı şekilde uyarı verebilir. Bunların yanında ip atlama, şınav, barfiks gibi fitness aktivitelerini takip etmek veya koşu yardımcısı gibi özellikler ile spor güzergâhını kontrol etmek gibi pek çok ek özelliğe de sahiptir. Yönetimi mobil cihaz üzerindeki uygulamadan yapılmakta olup, içerisinde bulunan çeşitli sensörler ile bilgi toplayarak Bluetooth v4.0 sayesinde mobil cihazla iletişim kurar.

Şekil 5.3: MI BAND 1S cihazı [52]

MI BAND cihazının kullandığı resmi uygulama marketinden indirilen Mi Fit 2 ve Mi Band Notify & Fitness uygulamaları için güvenlik testleri yapıldı. Ayrıca Mi Fit uygulamasının üçüncü parti olarak MI BAND kullanıcıları tarafından geliştirilen bir versiyonu (Tweaked) ve cihazın üretici firmasının internet sitesinden dağıtılan versiyonu (Mi Fit 1) da incelendi.

Yapılan analizler sonucunda dört uygulamanın da veritabanlarına parolasız erişim gerçekleştirildi. Bu veritabanlarında bulunan verilerin çekilebildiği; ayrıca uygulamaların kritik verileri kayıt altına (loglama) aldığı görüldü. Uygulamalarda kod karmaşıklaştırma işlemi yapıldığı ve yerel depolama alanlarının kullanım öncesi temiz olduğu görüldü.

Mi Fit uygulamasının üç farklı versiyonu kendi arasında değerlendirildiğinde; ortak uygulama izinlerini bulundurmalarının yanı sıra farklı uygulama izinleri de bulundurmaktadırlar. Üç uygulamada da ortak olarak Mi hesabı ile oturum açılmakta, sertifika kontrolü yapılmakta ve Mi sunucularına yapılan veri iletimi şifreli olarak sağlanmaktadır.

Mi Band Notify & Fitness uygulaması ise kritik on izinden ikisini barındırmaktadır. Uygulamayı kullanabilmek için herhangi bir kullanıcı hesabı istememektedir. Fakat MAC adresi üzerinden MI BAND ile eşleşmesi gerekmektedir. Bu eşleşme işlemi manuel olarak da yapılabilmektedir. Ayrıca sertifika kontrolü de yapılmamaktadır.

Uygulamaların detaylı analizi aşağıda verilmektedir. Ayrıca Tablo 5.1 ile Tablo 5.4 arasında her uygulamanın izinleri listelenmiştir.

MI BAND 1S cihazı Bluetooth Version 4.0 BTLE teknolojisini kullanarak haberleşmeyi sağlamaktadır. Bluetooth teknolojisini kullanan medikal cihazlarda özelliklerinden dolayı Bluetooth Low Energy (BTLE, Bluetooth Smart) teknolojisi tercih edilir. BTLE teknolojisi güç tüketimi, basit protokol ve servis özellikleri gibi konularda avantajlar sağlamasının yanında güvenlik ile ilgili bir çok gereksinimi göz ardı etmiştir. Örneğin bu teknolojide dinleme ve araya girme saldırılarına karşı bir önlem geliştirilmemiştir. Ayrıca "Wi-Fi ve Bluetooth Güvenlik Özellikleri" başlığı altında detaylı anlatılan Bluetooth Versiyon 4.0, bütün güvenlik modlarını desteklemesine rağmen BTLE modunun kullanılması durumunda en güvensiz mod olan Güvenlik Modu 1 seviyesine inebilmektedir. Bu durum tavsiye edilmemektedir. Bluetooth BTLE teknolojisi ile haberleşen cihazların trafiği dinlenildiğinde açık olarak giden BD_ADDR, RAND, SRES gibi değerler elde edilerek haberleşmede kullanılan PIN değeri kırılabilir. Elde edilen bu PIN değeri sayesinde

üretilen bir paket trafiğe enjekte edilip cihaza gönderilebilir. Bunlara ek olarak bir çalışmada [59] BTLE' nin şifreleme için kullandığı anahtar değişim protokolüne yapılan saldırı sonucunda anahtarın elde edilebildiği ve şifreli trafiğin çözülebildiği gösterilmiştir.

5.1.1 Mi Fit 1

Mi App Mağazasından edinilmiş bir uygulama olan Mi Fit ile zamandan bağımsız olarak sağlık ve fitness verileri ayarlanabilir, görüntülenebilir ve takip edilebilir. Ayrıca uyku kalitesi de görüntülenebilir ve takip edilebilir [60].

Tersine Mühendislik

Tablo 5.1: Mi Fit 1 uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
BLUETOOTH	Normal
BLUETOOTH_ADMIN	Normal
ACCESS_COARSE_LOCATION	Tehlikeli (Dangerous)
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
CHANGE_WIFI_STATE*	Normal
INTERNET	Normal
GET_TASKS*	-
AUTH_SERVICE	-
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
READ_PHONE_STATE	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CAMERA	Tehlikeli (Dangerous)
VIBRATE	Normal

Tablo 5.1: Mi Fit 1 uygulama izinleri - Devam

İzinler	Koruma Seviyesi (Protection Level)
FLASHLIGHT	Normal
SYSTEM_ALERT_WINDOW*	İmza (Signature)
GET_ACCOUNTS	Tehlikeli (Dangerous)
MOUNT_UNMOUNT_FILESYSTEMS	-
READ_LOGS*	-
WAKE_LOCK	Normal
WRITE_SETTINGS	İmza (Signature)
CALL_PHONE*	Tehlikeli (Dangerous)
REORDER_TASKS	Normal
MIPUSH_RECEIVE	İmza|Sistem (SignatureOrSystem)
GAME_SERVICE_PERMISSION	-
READ_STEPS	-
UPDATE	-

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.1' de görülmektedir. Bu izinler güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 6 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle Mi hesabına sahip olmak gerekmektedir. Mi hesabı uygulama üzerinden açılabildiği gibi internetten de açılabilmektedir. Oturum açma işlemi için ise, eğer Mi hesabı telefon numarası ile açıldıysa telefon numarası ve parola ile, e-mail ile açıldıysa e-mail ve parola ile giriş yapılmaktadır. Ayrıca oturum açma işlemi öncesinde hizmet ve gizlilik şartları belgesi onaylanmak zorundadır.

- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/Uygulama_dosyası/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- mnt/sdcard/ dizini altında mi_file ve mili_log.txt isimli iki dosya oluşturulduğu görüldü. Uygulama tarafından alınan logların mili_log.txt dosyasına yazıldığı görüldü.
- mili_log.txt dosyası içerisinde kişisel veriler, kullanıcı ve cihaz ID değerleri gibi kritik bilgilerin kayıt altına alındığı görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.

Ağ Trafiği Analizi

- Uygulama üzerinden Mi hesabı açmak için girilen verilerin, oturum açmak için kullanılan kullanıcı adı, parola bilgilerinin, Mi hesabı üzerinden buluta aktarılan kişisel ve sağlık verilerinin TLSV1.2 kullanılarak şifreli bir şekilde iletildiği görüldü.
- Uygulamanın oturum açma ve buluta eşleme işlemi öncesinde SSL sertifika kontrolü yaptığı görüldü.

5.1.2 Mi Band Notify & Fitness

Resmi uygulama marketten edinilmiş bir uygulamadır. Akıllı telefona bir bildirim alındığında titrer ve belirlenen bir renk telefon ekranında belirir. SMS, Whatsapp mesajları veya kayıp çağrılar için bu renk kişiselleştirilebilir. Widget ile adımlar ve pil durumu kontrol edilebilir. Uyandırma özelliği kullanılarak sabah uyanmak için titreşim özelleştirilebilir. Kalp hızı görüntüleme özellikleriyle elektronik tablo oluşturulabilir, düşük veya yüksek kalp hızında uygulamanın alarm vermesi sağlanabilir [61].

Tersine Mühendislik

Tablo 5.2: Mi Band Notify & Fitness uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
BLUETOOTH	Normal
BLUETOOTH_ADMIN	Normal
WAKE_LOCK	Normal
RECEIVE_BOOT_COMPLETED*	Normal
READ_PHONE_STATE	Tehlikeli (Dangerous)
PROCESS_OUTGOING_CALLS	Tehlikeli (Dangerous)
SET_ALARM	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CHECK_LICENSE	-
READ_CONTACTS*	Tehlikeli (Dangerous)
BILLING	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
INTERNET	Normal
BODY_SENSORS	Tehlikeli (Dangerous)
RECEIVE**	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.2' de görülmektedir. Bu izinler güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 2 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulama MAC adresi üzerinden bilekliği tanımaktadır. Fakat herhangi bir MAC kontrolü yapılmamaktadır. Manuel olarak da istenilen değerler girilip programa erişilebilmektedir. Fakat geçerli bir MAC adresi olmadığından bileklikten herhangi bir veri çekmek mümkün olmamaktadır.

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır. Bileklik Bluetooth üzerinden uygulamaya eşleştirildiğinde kullanılabilmektedir. Uygulama bilekliği MAC adresi üzerinden tanımaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/Uygulama_dosyası/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- mnt/sdcard/miband isimli bir dizin ve altında da log.txt ve settings.bak dosyalarının oluşturulduğu görüldü.
- Uygulama tarafından alınan logların log.txt dosyasına yazıldığı görüldü.
- log.txt dosyası içerisinde kişisel veriler, cihaz MAC ID değerleri gibi kritik bilgilerin açık bir şekilde kayıt altına alındığı görüldü.

Ağ Trafiği Analizi

- Uygulamanın ücretsiz versiyonu olduğundan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- Uygulamanın ücretsiz versiyonunda herhangi bir SSL sertifika kontrolü yapılmadığı görüldü.

5.1.3 Mi Fit 2

Resmi uygulama marketten edinilmiş olan Mi Fit ile zamandan bağımsız olarak sağlık ve fitness verileri ayarlanabilir, görüntülenebilir ve takip edilebilir. Ayrıca uyku kalitesi de görüntülenebilir ve takip edilebilir [62].

Tersine Mühendislik

Tablo 5.3: Mi Fit 2 uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
BLUETOOTH	Normal
BLUETOOTH_ADMIN	Normal
ACCESS_COARSE_LOCATION	Tehlikeli (Dangerous)
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
CHANGE_WIFI_STATE*	Normal
INTERNET	Normal
GET_TASKS*	-
AUTH_SERVICE	-
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
READ_PHONE_STATE	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CAMERA	Tehlikeli (Dangerous)
VIBRATE	Normal
FLASHLIGHT	Normal
SYSTEM_ALERT_WINDOW*	İmza (Signature)
GET_ACCOUNTS	Tehlikeli (Dangerous)
MOUNT_UNMOUNT_FILESYSTEMS	-
READ_LOGS*	-
WAKE_LOCK	Normal
WRITE_SETTINGS	İmza (Signature)
CALL_PHONE*	Tehlikeli (Dangerous)

Tablo 5.3: Mi Fit 2 uygulama izinleri - Devam

İzinler	Koruma Seviyesi (Protection Level)
REORDER_TASKS	Normal
MIPUSH_RECEIVE	Tehlikeli|İmza|Sistem (Dang|Sig|System)
GAME_SERVICE_PERMISSION	-
READ_STEPS	-
UPDATE	-
ACCESS_BLE_SETTINGS	-
BROADCAST_STICKY	Normal
RECEIVE_BOOT_COMPLETED*	Normal
BLE_IMMEDIATE_ALERT	-
HONOR_RECEIVE	İmza|Sistem (SignatureOrSystem)
HONOR_SEND	İmza|Sistem (SignatureOrSystem)
CONFIG	Tehlikeli|İmza|Sistem (Dang|Sig|System)
MAPS_RECEIVE	İmza|Sistem (SignatureOrSystem)
READ_GSERVICES	-

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.3' de görülmektedir. Bu izinler güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 7 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle Mi hesabına sahip olmak gerekmektedir. Mi hesabı uygulama üzerinden açılabildiği gibi internetten de açılabilmektedir. Oturum açma işlemi için ise, eğer Mi hesabı telefon numarası ile açıldıysa telefon numarası ve parola ile, e-mail ile açıldıysa e-mail ve parola ile giriş yapılmaktadır.

Ayrıca oturum açma işlemi öncesinde hizmet ve gizlilik şartları belgesi onaylanmak zorundadır.

- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/Uygulama_dosyası/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- mnt/sdcard/ dizini altında miband ve mili_log.txt isimli iki dosya oluşturulduğu görüldü. Uygulama tarafından alınan logların mili_log.txt dosyasına yazıldığı görüldü.
- mili_log.txt dosyası içerisinde kişisel veriler, uygulama, kullanıcı ve cihaz ID değerleri gibi kritik bilgilerin açık bir şekilde kayıt altına alındığı görüldü.

Ağ Trafiği Analizi

- Uygulama üzerinden Mi hesabı açmak için girilen verilerin, oturum açmak için kullanılan kullanıcı adı, parola bilgilerinin, Mi hesabı üzerinden buluta aktarılan kişisel ve sağlık verilerinin TLSV1.2 kullanılarak şifreli bir şekilde iletildiği görüldü.
- Uygulamanın oturum açma ve buluta eşleme işlemi öncesinde SSL sertifika kontrolü yaptığı görüldü.

5.1.4 Tweaked

MI BAND kullanıcıları tarafından geliştirilen Tweaked ile zamandan bağımsız olarak sağlık ve fitness verileri ayarlanabilir, görüntülenebilir ve takip edilebilir. Ayrıca uyku kalitesi de görüntülenebilir ve takip edilebilir [63].

Tersine Mühendislik

Tablo 5.4: Tweaked uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
BLUETOOTH	Normal
BLUETOOTH_ADMIN	Normal
ACCESS_COARSE_LOCATION	Tehlikeli (Dangerous)
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
CHANGE_WIFI_STATE*	Normal
INTERNET	Normal
GET_TASKS*	-
AUTH_SERVICE	-
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
READ_PHONE_STATE	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CAMERA	Tehlikeli (Dangerous)
VIBRATE	Normal
FLASHLIGHT	Normal
SYSTEM_ALERT_WINDOW*	İmza (Signature)
GET_ACCOUNTS	Tehlikeli (Dangerous)
MOUNT_UNMOUNT_FILESYSTEMS	-
READ_LOGS*	-
WAKE_LOCK	Normal
WRITE_SETTINGS	İmza (Signature)
CALL_PHONE*	Tehlikeli (Dangerous)

Tablo 5.4: Tweaked uygulama izinleri - Devam

İzinler	Koruma Seviyesi (Protection Level)
REORDER_TASKS	Normal
MIPUSH_RECEIVE	Tehlikeli|İmza|Sistem (Dang|Sig|System)
READ_STEPS	-
UPDATE	-
BROADCAST_STICKY	Normal
RECEIVE_BOOT_COMPLETED*	Normal
CONFIG	Tehlikeli|İmza|Sistem (Dang|Sig|System)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.4' de görülmektedir. Bu izinler güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 7 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle Mi hesabına sahip olmak gerekmektedir. Mi hesabı uygulama üzerinden açılabildiği gibi internetten de açılabilmektedir. Oturum açma işlemi için ise, eğer Mi hesabı telefon numarası ile açıldıysa telefon numarası ve parola ile, e-mail ile açıldıysa e-mail ve parola ile giriş yapılmaktadır. Ayrıca oturum açma işlemi öncesinde hizmet ve gizlilik şartları belgesi onaylanmak zorundadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/ Uygulama_dosyası/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.

- mnt/sdcard/ dizini altında mili_log.txt isimli iki dosya oluşturulduğu görüldü. Uygulama tarafından alınan logların mili_log.txt dosyasına yazıldığı görüldü.
- mili_log.txt dosyası içerisinde kişisel veriler, kullanıcı ve cihaz ID değerleri gibi kritik bilgilerin kayıt altına alındığı görüldü.

Ağ Trafiği Analizi

- Uygulama üzerinden Mi hesabı açmak için girilen verilerin, oturum açmak için kullanılan kullanıcı adı, parola bilgilerinin, Mi hesabı üzerinden buluta aktarılan kişisel ve sağlık verilerinin TLSV1.2 kullanılarak şifreli bir şekilde iletildiği görüldü.
- Uygulamanın oturum açma ve buluta eşleme işlemi öncesinde SSL sertifika kontrolü yaptığı görüldü.

5.1.5 Güvenlik İncelemesi Uygulama İzinleri

Güvenlik incelemesi yapılan uygulamaların tüm izinleri Tablo 5.5' de toplu olarak görülmektedir.

Tablo 5.5: Güvenlik incelemesinde karşılaşılan uygulama izinleri

İzinler	Koruma Seviyesi	MiFit1	Mi Band Notify	MiFit2	Tweaked
BLUETOOTH	Normal	X	X	X	X
BLUETOOTH_ADMIN	Normal	X	X	X	X
ACCESS_COARSE_LOCATION	Tehlikeli	X		X	X
ACCESS_FINE_LOCATION*	Tehlikeli	X		X	X
ACCESS_NETWORK_STATE	Normal	X	X	X	X
CHANGE_WIFI_STATE*	Normal	X		X	X
INTERNET	Normal	X	X	X	X
GET_TASKS*	-	X		X	X
AUTH_SERVICE	-	X		X	X
WRITE_EXTERNAL_STORAGE	Tehlikeli	X	X	X	X
ACCESS_WIFI_STATE	Normal	X		X	X

Tablo 5.5: Güvenlik incelemesinde karşılaşılan uygulama izinleri - Devam

İzinler	Koruma Seviyesi	MiFit1	Mi Band Notify	MiFit2	Tweaked
READ_PHONE_STATE	Tehlikeli	X	X	X	X
READ_EXTERNAL_STORAGE	Tehlikeli	X		X	X
CAMERA	Tehlikeli	X		X	X
VIBRATE	Normal	X		X	X
FLASHLIGHT	Normal	X		X	X
SYSTEM_ALERT_WINDOW*	İmza	X		X	X
GET_ACCOUNTS	Tehlikeli	X		X	X
MOUNT_UNMOUNT_FILESYSTEMS	-	X		X	X
READ_LOGS*	-	X		X	X
WAKE_LOCK	Normal	X	X	X	X
WRITE_SETTINGS	İmza	X		X	X
CALL_PHONE*	Tehlikeli	X		X	X
REORDER_TASKS	Normal	X		X	X
MIPUSH_RECEIVE	İmza|Sistem	X			
GAME_SERVICE_PERMISSION	-	X		X	
READ_STEPS	-	X		X	X
UPDATE	-	X		X	X
RECEIVE_BOOT_COMPLETED*	Normal		X	X	X
PROCESS_OUTGOING_CALLS	Tehlikeli		X		
SET_ALARM	Normal		X		
CHECK_LICENSE	-		X		
READ_CONTACTS*	Tehlikeli		X		
BILLING	Tehlikeli		X		
BODY_SENSORS	Tehlikeli		X		
RECEIVE**	Tehlikeli		X		
ACCESS_BLE_SETTINGS	-			X	
BROADCAST_STICKY	Normal			X	X
BLE_IMMEDIATE_ALERT	-			X	
HONOR_RECEIVE	İmza|Sistem			X	

Tablo 5.5: Güvenlik incelemesinde karşılaşılan uygulama izinleri - Devam

İzinler	Koruma Seviyesi	MiFit1	Mi Band Notify	MiFit2	Tweaked
HONOR_SEND	İmza|Sistem			X	
CONFIG	Tehlikeli|İmza|Sistem			X	X
MAPS_RECEIVE	İmza|Sistem			X	
READ_GSERVICES	-			X	
MIPUSH_RECEIVE	Tehlikeli|İmza|Sistem			X	X

5.2 Mobil Sağlık Uygulamaları Güvenlik Testleri

Çalışma kapsamında, MI BAND cihazının mobil uygulamalarından farklı olarak, resmi uygulama marketten ve üçüncü parti uygulama marketlerden olmak üzere toplam 15 adet mobil sağlık uygulaması analiz edildi. Yapılan analizler sonucunda uygulamaların veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği tespit edildi. Yerel depolama alanlarının kullanım öncesi temiz olduğu görüldü. Ayrıca iki uygulama hariç diğer uygulamalarda sertifika kontrolünün yapılmadığı tespit edildi. Uygulamaların yeteneklerine göre farklı seviyelerde çeşitli izinlere sahip olduğu görüldü. Her uygulamanın sahip olduğu izinler tablolar halinde (Tablo 5.6 – Tablo 5.20) gösterildi. Uygulamada en çok karşılaşılan izinler ile güvenlik ve mahremiyetin sömürülmesinde etkili on izin yukarıda kısaca açıklandı. Bazı uygulamalarda ise kritik verilerin kayıt altına (loglama) alındığı görüldü.

Tüm uygulamaların detaylı test sonuçları aşağıda verilmiştir.

5.2.1 Healthiply Professionals

Resmi uygulama marketten edinilmiş olan Healthiply Professionals doktorlar, hastaneler, sağlık tesisleri ve sağlık hizmet vericileri için tasarlamış bir uygulamadır. Hastaların sağlık verilerini depolama, randevularını yönetme, hatırlatma gönderme, gerektiğinde verileri başka kişilerle paylaşma ve sağlık verilerine her yerden ulaşabilmeyi sağlamaktadır [64].

Tersine Mühendislik

Tablo 5.6: Healthiply Professionals uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
GET_ACCOUNTS	Tehlikeli (Dangerous)
USE_CREDENTIALS	Tehlikeli (Dangerous)
READ_PHONE_STATE	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CAMERA	Tehlikeli (Dangerous)
READ_CALENDAR*	Tehlikeli (Dangerous)
WRITE_CALENDAR*	Tehlikeli (Dangerous)
SEND_SMS*	Tehlikeli (Dangerous)
CALL_PHONE*	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.6' da görülmektedir. Bu izinler güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 3 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle e-mail adresi ve parola ile kayıt oluşturulması gerekmektedir. Oturum açma işlemi için ise kullanıcı adı ve parola ile giriş yapılmaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/Uygulama_dosyası/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- mnt/sdcard/Picture dizininde kullanıcının uygulamaya yüklediği fotoğraflara erişilebilir olduğu görüldü. Bu fotoğraflar telefondan silinip, uygulamada oturum açıldığında sunucudan getirilmekte fakat cihaza kaydedilmemektedir.

- Kullanıcı adı ve parola bilgileri lokalde tutulmamaktadır.
- data/data/Uygulama_dosyası/databases dizini bulunmamaktadır.
- Yeni kayıt açan hastaların, tüm bilgilerinin açık bir şekilde kayıt altına (loglama) alındığı görüldü. Kullanıcının kendi hesabı üzerinde yaptığı değişiklikler (telefon numarası güncelleme vb.) sırasında kullanıcı adı ve parola bilgilerinin açık bir şekilde loglandığı görüldü. Sonuç olarak yapılan bütün aktiviteler (ilk başlangıçtaki oturum açma bilgileri hariç) detaylı ve açık bir şekilde loglanmaktadır.

Ağ Trafiği Analizi

- Kullanıcı adı, parola bilgilerinin ağ üzerinde açık bir şekilde iletildiği görüldü.
- Kayıtlı hasta verilerinin ağ üzerinde açık bir şekilde taşındığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.2 mMR

mMR resmi uygulama marketten edinilmiş bir uygulamadır. SAP sertifikalı mobil sağlık veri kaydedicisidir. Uygulama hastane sistemine entegre olarak hastaların bütün bilgilerine ve sonuçlarına erişip yönetebilmektedir [65].

Tersine Mühendislik

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.7' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulama hastane tarafında kurulmuş olan bir sunucu ile entegre çalışmaktadır. Oturum açmak için ise kimlik bilgisi ve jeton (token) değeri gerekmektedir. Bizim

Tablo 5.7: mMR uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
GET_ACCOUNTS	Tehlikeli (Dangerous)
READ_PHONE_STATE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
ACCESS_NETWORK_STATE	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)

elimizde bu bilgiler olmadığından uygulama sadece öğrenme (training) modunda test edilebildi.

- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama training modda kullanıldığında herhangi bir dizinin altına bir şey yazılmadığı görüldü.
- Training modda kullanılan uygulamanın logları incelendiğinde kullanıcı adının açık bir şekilde kayıt altına alındığı görüldü.

Ağ Trafiği Analizi

- Training modda tüm veriler localden getirildiği için ağ üzerinde herhangi bir veri akışı olmadığı görüldü.
- Training modda sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.3 NFC Medic

Resmi uygulama marketten edinilmiştir. NFCMedic, akıllı telefon yada web sitesi üzerinden sağlık kaydı oluşturmayı sağlamaktadır. Bu sağlık kaydı, kişilerin acil durumda ihtiyaç duyabileceği bilgileri içermektedir. Uygulama ile acil durumlarda SOS çağrısı

yapılabilmektedir. Ayrıca NFC uyumlu telefonlardan bu bilgiler NFC kartlarına yazdırılabilmektedir [66].

Tersine Mühendislik

Tablo 5.8: NFC Medic uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CALL_PHONE*	Tehlikeli (Dangerous)
CAMERA	Tehlikeli (Dangerous)
INTERNET	Normal
READ_PHONE_STATE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
ACCESS_NETWORK_STATE	Normal
NFC	Normal
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
ACCESS_COARSE_LOCATION	Tehlikeli (Dangerous)
SEND_SMS*	Tehlikeli (Dangerous)
RECEIVE_SMS*	Tehlikeli (Dangerous)
READ_SMS	Tehlikeli (Dangerous)
WRITE_SMS	Tehlikeli (Dangerous)
DISABLE_KEYGUARD	Normal
WAKE_LOCK	Normal
INTERACT_ACROSS_USERS_FULL	İmza (Signature)
READ_EXTERNAL_STORAGE	Normal

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.8' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 3 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle e-mail adresi, parola ve telefon numarası ile kayıt oluşturulması gerekmektedir. Fakat telefon numarasının geçerli bir numara olup olmadığının kontrolü yapılmamaktadır. Oturum açma işlemi için ise kullanıcı adı ve parola ile giriş yapılmaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulamanın kullanıcı adı ve parola bilgileri lokalde tutulmamaktadır.
- Uygulamada data/data/Uygulama_dosyası/databases dizini bulunmamaktadır.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Kayıtlı hasta verilerinin, kullanıcı adı ve parola bilgilerinin şifreli olarak iletildiği görüldü. Fakat kullanıcının profil resminin bulunduğu URL' in açıktan gittiği görüldü. Bu URL adres çubuğuna yazıldığında resmin geldiği görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- Kullanıcı adı olarak "1' or '1'='1" ifadesini verilip, parolada doğru bir parola verildiğinde oturum açma işleminin gerçekleştiği görüldü. Bu durum, parolanın kaba kuvvet saldırılarına maruz kalabileceği anlamına gelmektedir.
- User ID değeri ele geçirilmiş bir kullanıcının verileri, oturum açmış başka bir kullanıcı tarafından görülebileceği tespit edildi.
- İnput alanlarının cache tutmadığı görüldü.

5.2.4 Patient Chart

Resmi uygulama marketten edinilmiş bir uygulama olan VirtalHub Chart, doktorlar, hemşireler, eczacılar ve yardımcı sağlık çalışanları için geliştirilmiştir. Hastane sistemine

entegre olabildiğinden hastaların sağlık verilerine kolayca erişim sağlamaktadır. Grafikler çıkartarak ilgili veriler hakkında bilgi vermektedir. Hasta verileri ile VitalHub tablosunu kullanabilmek için, hastane de VirtalHub sunucusunun yüklü olması gerekmektedir [67].

Bu uygulama mobil cihazda VirtalHub Chart olarak isimlendirilirken uygulama markette Patient Chart olarak isimlendirilmiştir.

Tersine Mühendislik

Tablo 5.9: VirtalHub Chart uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
INTERNET	Normal
ACCESS_NETWORK_STATE	Normal

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.9'de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulama hastane tarafında kurulmuş olan bir sunucu ile entegre çalışmaktadır. Oturum açmak için ise kimlik bilgisi ve jeton (token) değeri gerekmektedir. Bizim elimizde bu bilgiler olmadığından uygulama sadece öğrenme (training) modunda test edilebildi.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama training modda kullanıldığında herhangi bir dizinin altına bir şey yazılmadığı görüldü.
- Training modda kullanılan uygulamanın logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Training modda tüm veriler localden getirildiği için ağ üzerinde herhangi bir veri akışı olmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.5 Zibdy Health

Resmi uygulama marketten indirilen Zibdy Health, sağlık verilerinin tek bir noktadan yönetilmesi için tasarlanmıştır. Farklı hastanelerde bulunan bilgilerin tek bir noktada toplanmasını ve istenilen her yerde görüntülenmesini sağlamaktadır. Ayrıca kullanılan ilaçlar için bir liste hazırlama imkânı tanımakta ve ilaçlar için hatırlatıcısı özelliği bulunmaktadır [68].

Tersine Mühendislik

Tablo 5.10: Zibdy Health uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
CAMERA	Tehlikeli (Dangerous)
INTERNET	Normal
FLASHLIGHT	Normal
READ_CONTACTS*	Tehlikeli (Dangerous)
GET_ACCOUNTS	Tehlikeli (Dangerous)
USE_CREDENTIALS	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
RECEIVE_BOOT_COMPLETED*	Tehlikeli (Dangerous)
READ_PHONE_STATE	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.10' da görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 3 tanesini barındırmaktadır.

- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle kullanıcı adı, e-mail adresi ve parola ile kayıt oluşturulması ve bir anlaşma onaylanması gerekmektedir. Oturum açma işlemi için ise kullanıcı adı ve parola ile giriş yapılmaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra data/data/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulamanın kullanıcı adı ve parola bilgileri lokalde tutulmamaktadır.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Kayıtlı hasta verilerinin, kullanıcı adı ve parola bilgilerinin şifreli olarak iletildiği görüldü.
- SSL sertifika kontrolü yapıldığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.6 Yalova Devlet Hastanesi Uygulaması

Resmi uygulama marketten edinilmiş bir uygulama olan Yalova Devlet Hastanesi Uygulaması ile hastane sistemine kayıtlı tüm laboratuvar sonuçlarına, radyoloji görüntülerine erişilebilmektedir. Sonuçlar onaylandığında anlık olarak bildirim gelmektedir. Bu sonuçlar uygulama üzerinden görüntülenebilmekte ve bir başkası ile paylaşılabilmektedir. Hatta hastanedeki herhangi bir yazıcıya gönderilerek çıktısı alınabilmektedir. Ayrıca

hastanedeki randevu alınan poliklinikler listelenebilmekte, numaratör ile entegre çalışabildiğinden sıra numarası ve tahmini muayene saati online olarak takip edilebilmektedir [69].

Tersine Mühendislik

Tablo 5.11: Yalova Devlet Hastanesi uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
CAMERA	Tehlikeli (Dangerous)
INTERNET	Normal
FLASHLIGHT	Normal
C2D_MESSAGE**	İmza (Signature)
RECEIVE**	Tehlikeli (Dangerous)
GET_ACCOUNTS	Tehlikeli (Dangerous)
WAKE_LOCK	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
VIBRATE	Normal
SEND**	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.11' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle TC kimlik numarası, anne adı, baba adı, e-mail adresi, doğum tarihi, doğum yeri vb. kişisel bilgiler ile kayıt oluşturulması gerekmektedir. Parola, girilen telefon numarasına mesaj olarak gönderilmektedir. Oturum açma işlemi için ise TC kimlik numarası ve parola ile giriş yapılmaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.

- Uygulamaya kayıt olup kullanabilmek için Yalova Devlet Hastanesin de hasta kaydı bulunması gerekmektedir. Uygulamaya girilen TC kimlik numarası hastanede kayıtlı olan TC kimlik numarası ile eşleştirilip kontrol edilmektedir. Bizim Yalova Devlet Hastanesin de bir kaydımız bulunmadığından uygulama aktif olarak kullanılıp test edilemedi.
- Kayıt oluşturma sırasında incelenen loglama işleminde herhangi bir kritik bilginin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Kayıt işlemi sırasında girilen bütün verilerin, oturum açma sırasında girilen TC kimlik numarası ve parola bilgilerinin açık bir şekilde iletildiği görüldü.
- SSL sertifika kontrolü yapıldığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.7 Diagnose

Resmi uygulama marketten edinilmiştir. Diagnose, tıp doktorları ve tıp öğrencileri için tasarlanmıştır. Tanı, teşhis ve tedavisi onaylanmış bazı hastalıkların bilgilerini içerir. Ön tanı sırasında, hastanın şikayetleri ve laboratuar değerlerine göre teşhis konulmasına bununla birlikte tedavi yöntemi için de doktorlara yardımcı olur [70].

Tersine Mühendislik

Tablo 5.12: Diagnose uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
ACCESS_NETWORK_STATE	Normal

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.12' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.

- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.8 Healty Files

Resmi uygulama marketten edinilmiş bir uygulamadır. Healty Files, sağlık dosyalarının (fotoğraflarını, vs.) depolanmasını sağlar. Tıbbi kayıtları ve hassas kişisel sağlık verilerini içermektedir. Bu verilerin güvenli ve kategorize edilmiş bir şekilde tutulmasını, gerektiği zaman doktora mail ile gönderilmesini sağlar [71].

Tersine Mühendislik

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.13' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Tablo 5.13: Healty Files uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
CAMERA	Tehlikeli (Dangerous)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
ACCESS_NETWORK_STATE	Normal

- Uygulama emulatörde ve test cihazında çalışmadığından Depolama ve Ağ Trafiği analizleri yapılamamıştır.

5.2.9 Pedometer

Üçüncü parti uygulama marketten edinilmiş bir uygulamadır. Pedometer, atılan adım sayısını kaydeder ve yakılan kalori miktarını, mesafeyi, yürüyüş süresini ve saatlik hızı gösterir.

Tersine Mühendislik

Tablo 5.14: Pedometer uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
CAMERA	Tehlikeli (Dangerous)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_WIFI_STATE	Normal
WAKE_LOCK	Normal
ACCESS_NETWORK_STATE	Normal

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.14' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden hiç birisi bulunmamaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için sadece bir kullanıcı adı yazılıp giriş yapılmaktadır. Oturum açmak için herhangi bir parola bilgisine gerek duyulmamaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama kullanıldıktan sonra data/data/cache dizini altında tutulan verilerin şifreli olduğu görüldü.
- Uygulama içerisinde çekilen fotoğrafların mnt/sdcard/Android dizini altında tutulduğu görüldü.
- Uygulamada alınan yedeklerin mnt/sdcard dizini altında uygulamanın adında oluşturulan dosyada herkesin erişimine açık olarak tutulduğu görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamanın cihaz ve uygulama verilerini açık bir şekilde ilettiği görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.

5.2.10 Smart Medical

Üçüncü parti uygulama marketten edinilmiş bir uygulama olan Smart Medical, tıp öğrencileri için geliştirilmiş bir uygulamadır. Uygulamanın sahip olduğu güncel veritabanı ile hastaların şikâyetlerine göre ilgili alanlar doldurulup ön tanı konulmasına yardımcı olmaktadır. Ayrıca video desteği ile nasıl muayene edilebileceği de anlatılmaktadır [72].

Tersine Mühendislik

Tablo 5.15: Smart Medical uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_COARSE_LOCATION	Tehlikeli (Dangerous)
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
READ_CALENDAR*	Tehlikeli (Dangerous)
WRITE_CALENDAR*	Tehlikeli (Dangerous)
BILLING	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.15' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 2 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.

5.2.11 Health Records

Üçüncü parti uygulama marketten edinilmiş bir uygulamadır. Yapısında bulunan sağlık kartı (Health Card) sağlık bilgilerinin depolanması ve istenildiği zaman bilgilerin incelenebilmesi için kullanılır. Health Records tıbbi testlerin saklanmasında ve ilaçların zamanında alınarak sağlık takviminin devamlılığında yardımcı olur. Tıbbi hesap makinesi (Medical Calculator) günlük kalori alımını, vücut ağırlık indeksini ve ideal vücut ağırlığını hesaplamaya olanak sağlar [73].

Tersine Mühendislik

Tablo 5.16: Health Records uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
CAMERA	Tehlikeli (Dangerous)
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
VIBRATE	Normal
RECEIVE_BOOT_COMPLETED*	Normal
BILLING	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.16' da görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 1 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.

- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.12 Medical & Health Records Caddy

Üçüncü parti uygulama marketten edinilmiş bir uygulama olan Medical & Health Records Caddy, sağlık çalışanları için tasarlanmış bir uygulamadır. Hasta ile ilgili yapılması gerekenleri, notları, hastanın kayıtlarını, kullandığı ilaçları, resimleri ve doktorun eklemek istediği bilgileri zaman ve mekandan bağımsız olarak paylaşabilmesine olanak sağlar [74].

Tersine Mühendislik

Tablo 5.17: Medical & Health Records Caddy uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
READ_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
WAKE_LOCK	Normal
BILLING	Tehlikeli (Dangerous)
C2D_MESSAGE**	İmza (Signature)
RECEIVE**	Tehlikeli (Dangerous)
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)
GET_ACCOUNTS	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.17' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 1 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır. Ancak dışarıda bulunun sunucuya veri aktarımı yapılmak istenirse, o zaman bir hesap açılması gerekmektedir.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü. Yalnız dışarıya veri gönderilmek istenilen bir durumda açılan hesap üzerinden şifreli olarak veri iletimi yapıldığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tutmadığı görüldü.

5.2.13 My Medical History 1

Üçüncü parti uygulama marketten edinilmiş bir uygulamadır. Bu uygulama ile doktor randevuları, kullanılan ilaçlar, alerjik rahatsızlıklar ve ameliyatlar gibi tüm tıbbi geçmiş kayıt altında tutulabilir [75].

Tersine Mühendislik

Tablo 5.18: My Medical History 1 uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
READ_CALENDAR*	Tehlikeli (Dangerous)
WRITE_CALENDAR*	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.18' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 1 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde takvime işlenen verilerin açık bir şekilde kayıt altına alındığı, ayrıca girilen verilere tekrar bakılmak istendiğinde not kısmının tekrar açık bir şekilde kayıt altına alındığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.

5.2.14 WebMD

Üçüncü parti uygulama marketten edinilmiş bir uygulamadır. Yapısında bulunan WebMD Belirti Denetleyici (WebMD' s symptom checker); ilaçlar ve tedaviler, ilkyardım bilgisi ve il sağlık kurumu listeleriyle sağlık bilgisine ve/veya acil durumlarda ihtiyaç duyulduğunda zamandan bağımsız olarak mobil destek sağlar [76].

Tersine Mühendislik

Tablo 5.19: WebMD uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
INTERNET	Normal
WRITE_EXTERNAL_STORAGE	Tehlikeli (Dangerous)
CALL_PHONE*	Tehlikeli (Dangerous)
ACCESS_NETWORK_STATE	Normal
CAMERA	Tehlikeli (Dangerous)
WAKE_LOCK	Normal
ACCESS_FINE_LOCATION*	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.19' da görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 2 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için herhangi bir kullanıcı oluşturmaya gerek duyulmamaktadır. Fakat bir şeyler kaydedilmek istenildiğinde e-mail, parola ve doğum tarihi bilgileriyle hesap oluşturulup oturum açılması gerekmektedir.
- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.

- Kullanıcı adı ve parola bilgileri lokalde tutulmamaktadır.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya gönderilen verilerin şifreli olarak iletildiği görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tuttuğu görüldü.

5.2.15 My Medical History 2

Üçüncü parti uygulama marketten edinilmiş bir uygulamadır. Bu uygulama sayesinde cep telefonunda sağlık geçmişiyle ilgili veriler kolaylıkla taşınabilir. Veri girişi, düzenleme veya istenildiğinde görüntüleme yapılabilir. Girilen veriler şifre koruması altındadır [77].

Tersine Mühendislik

Tablo 5.20: My Medical History 2 uygulama izinleri

İzinler	Koruma Seviyesi (Protection Level)
RECEIVE_BOOT_COMPLETED*	Normal
SEND_SMS*	Tehlikeli (Dangerous)

- Uygulamanın, işlevi için talep ettiği izinler Tablo 5.20' de görülmektedir. Bu izinler içerisinde güvenlik ve mahremiyetin sömürülmesinde etkili olan 10 tehlikeli izinden 2 tanesini barındırmaktadır.
- Uygulamada kod karmaşıklaştırma işlemi yapılmamıştır.

Depolama Analizi

- Uygulamayı kullanabilmek için öncelikle e-mail adresi ve parola ile kayıt oluşturulması gerekmektedir. Oturum açma işlemi için ise sadece parola ile giriş yapılmaktadır.

- Uygulama kullanılmadan önce bakılan data/data, data/app ve mnt/ dizinlerinin temiz olduğu görüldü.
- data/data/Uygulama_dosyası/databases altında bulunan veritabanlarına parolasız erişim sağlanabildiği ve tablolarda bulunan verilerin çekilebildiği görüldü.
- Uygulama üzerindeki bütün veriler, kullanıcı adı parola dahil açık bir şekilde data/data/Uygulama_dosyası /shared_prefs altında tutulduğu görüldü.
- Uygulama kullanıldıktan sonra logları incelendiğinde herhangi bir kritik verinin kayıt altına alınmadığı görüldü.

Ağ Trafiği Analizi

- Uygulamadan dışarıya herhangi bir veri iletimi yapılmadığı görüldü.
- SSL sertifika kontrolü yapılmadığı görüldü.
- İnput alanlarının cache tuttuğu görüldü.

5.2.16 Mobil Sağlık Uygulama İzinleri

Güvenlik testlerinde karşılaşılan bütün izinler Tablo 5.21 ve Tablo 5.22' de toplu olarak gösterilmiştir.

Tablo 5.21: Mobil sağlık uygulamalarında karşılaşılan uygulama izinleri - 1

İzinler	Koruma Seviyesi	Healthiply Professionals	mMR	NFC Medic	Patient Chart	Zibdy Health	Yalova Devlet Hastanesi	Diagnose	Healty Files
INTERNET	Normal	X	X	X	X	X	X	X	X
GET_ACCOUNTS	Tehlikeli	X	X	X		X	X		
USE_CREDENTIALS	Tehlikeli	X				X			
READ_PHONE_STATE	Tehlikeli	X	X	X		X			
ACCESS_NETWORK_STATE	Normal	X	X	X	X	X		X	X
WRITE_EXTERNAL_STORAGE	Tehlikeli	X	X	X	X		X		X
CAMERA	Tehlikeli	X		X		X	X		X
READ_CALENDAR*	Tehlikeli	X							
WRITE_CALENDAR*	Tehlikeli	X							
SEND_SMS*	Tehlikeli	X		X					
CALL_PHONE*	Tehlikeli	X		X					
ACCESS_WIFI_STATE	Normal		X	X					X
READ_EXTERNAL_STORAGE	Tehlikeli		X	X					
NFC	Normal			X					
ACCESS_FINE_LOCATION*	Tehlikeli			X		X			
ACCESS_COARSE_LOCATION	Tehlikeli			X					
RECEIVE_SMS*	Tehlikeli			X					
READ_SMS	Tehlikeli			X					
WRITE_SMS	Tehlikeli			X					
DISABLE_KEYGUARD	Normal			X					
WAKE_LOCK	Normal			X			X		
INTERACT_ACROSS_USERS_FULL	İmza			X					
FLASHLIGHT	Normal				X		X		
READ_CONTACTS*	Tehlikeli				X				
RECEIVE_BOOT_COMPLETED*	Normal					X			
C2D_MESSAGE**	İmza						X		
RECEIVE**	Tehlikeli						X		
VIBRATE	Normal						X		
SEND**	Tehlikeli						X		
BILLING	Tehlikeli								

Tablo 5.22: Mobil sağlık uygulamalarında karşılaşılan uygulama izinleri - 2

İzinler	Koruma Seviyesi	Pedometer	Smart Medical	Health Records	Medical Health Records	Caddy	My Medical History 1	WebMD	My Medical History 2
INTERNET	Normal	X	X	X	X			X	
GET_ACCOUNTS	Tehlikeli				X				
USE_CREDENTIALS	Tehlikeli								
READ_PHONE_STATE	Tehlikeli								
ACCESS_NETWORK_STATE	Normal	X	X	X	X			X	
WRITE_EXTERNAL_STORAGE	Tehlikeli	X	X	X	X			X	
CAMERA	Tehlikeli	X		X				X	
READ_CALENDAR*	Tehlikeli		X				X		
WRITE_CALENDAR*	Tehlikeli		X				X		
SEND_SMS*	Tehlikeli								X
CALL_PHONE*	Tehlikeli							X	
ACCESS_WIFI_STATE	Normal	X							
READ_EXTERNAL_STORAGE	Tehlikeli	X		X	X				
NFC	Normal								
ACCESS_FINE_LOCATION*	Tehlikeli		X			X		X	
ACCESS_COARSE_LOCATION	Tehlikeli		X						
RECEIVE_SMS*	Tehlikeli								
READ_SMS	Tehlikeli								
WRITE_SMS	Tehlikeli								
DISABLE_KEYGUARD	Normal								
WAKE_LOCK	Normal	X				X		X	
INTERACT_ACROSS_USERS_FULL	İmza								
FLASHLIGHT	Normal								
READ_CONTACTS*	Tehlikeli								
RECEIVE_BOOT_COMPLETED*	Normal			X		X			X
C2D_MESSAGE**	İmza					X			
RECEIVE**	Tehlikeli								
VIBRATE	Normal			X					
SEND**	Tehlikeli								
BILLING	Tehlikeli		X	X		X			

5.3 Güvenli Mimari Tasarım ve Geliştirme Gereksinimleri

Verilmiş olan bilgiler ve yapılmış olan çalışmalar sonucunda, tasarlanacak bir WBAN sisteminin WBAN ve WBAN sunucu katmanları ve geliştirilecek olan mobil sağlık uygulamaları için bazı temel güvenlik gereksinimleri belirlendi.

5.3.1 WBAN ve WBAN Sunucu Katmanları Güvenlik Gereksinimleri

WBAN ve WBAN sunucu katmanlarının tasarım ve geliştirme için bazı temel güvenlik gereksinimleri Tablo 5.23' de verilmiştir.

Tablo 5.23: WBAN ve WBAN sunucu katmanları güvenlik gereksinimleri

No	Güvenlik Gereksinimleri
GK1	Bilgi ve farkındalık eksikliğinden kaynaklanacak güvenlik zafiyetlerine karşı kullanıcılara mutlaka eğitim verilmelidir.
GK2	Kullanılan cihazlara (sensör, WBAN sunucusu) izinsiz fiziksel erişimden doğabilecek güvenlik problemlerine karşı kullanıcılar bilgilendirilmelidir.
GK3	Akıllı sensörler ve WBAN sunucusu arasında yapılacak kablosuz iletişim için şifreleme, kimlik doğrulama gibi güvenlik kontrollerini sağlayan teknolojiler seçilmelidir.
GK4	Veri iletimi yapılmadan önce, veriler güçlü şifreleme algoritmaları ile şifrelenmeli ve şifreli bir kanal üzerinden gönderilmelidir.
GK5	Akıllı sensörler ve WBAN sunucusu üzerinde koşan yazılımlar güvenli yazılım geliştirme süreçlerinden geçmeli ve güvenlik testleri mutlaka yapılmalıdır.
GK6	WBAN sunucusu olarak kullanılan cihaz üzerine ya başka uygulama kurulmamalı ya da eğer kurulacaksa o uygulamaların da güvenlik testleri yapılmalıdır.
GK7	Sensörlere ve WBAN sunucusuna erişimlerde mutlaka kimlik doğrulama ve yetkilendirme yapılmalıdır.

Tablo 5.23: WBAN ve WBAN sunucu katmanları güvenlik gereksinimleri - Devam

No	Güvenlik Gereksinimleri
GK8	Sensörlerin konfigürasyonları kullanılan sisteme uygun olarak yapılmalıdır.
GK9	Veri iletiminde kullanılan ağın servis dışı bırakma saldırılarına karşı korunaklı olması sağlanmalıdır.
GK10	Veri iletimi için kullanılan ağın dinlenmesi ve manipüle edilmesine karşı güvenliği sağlanmalıdır.
GK11	WBAN sunucusu olarak kullanılan cihazın çalınması veya kaybolması riski değerlendirilip depolanan verinin kritikliğine göre yedekleme, bir süre sonra yok etme gibi önlemler alınmalıdır.
GK12	WBAN sunucusu olarak kullanılan cihazın diskinde meydana gelebilecek hatalara karşı önlem alınmalıdır.

5.3.2 Mobil Sağlık Uygulamaları Güvenlik Gereksinimleri

Mobil sağlık uygulamaları geliştirmek için bazı temel güvenlik gereksinimleri Tablo 5.24' de verilmiştir.

Tablo 5.24: Mobil sağlık uygulamaları güvenlik gereksinimleri

No	Güvenlik Gereksinimleri
GK1	Geliştirilecek mobil uygulamalar için gerekli izinler talep edilmelidir. Gereğinden fazla talep edilen izinlere onay verilmemelidir.
GK2	Yalnızca uygulamanın iş ihtiyacıyla kullanacağı veri toplanmalı, gereksiz veri toplanmamalıdır. Uygulama minimum yetki talep ederek çalışmalıdır.

Tablo 5.24: Mobil sağlık uygulamaları güvenlik gereksinimleri - Devam

No	Güvenlik Gereksinimleri
GK3	Geliştirilmiş olan mobil uygulamanın kodları kod karmaşıklaştırma işleminden geçirilmelidir.
GK4	Uygulamada kişisel sağlık verileri tutulacağı için mutlaka bir kimlik doğrulama işlemi yapılmalıdır.
GK5	Hassas veri cihaz üzerinde tutulmamalı, cihaz üzerinde tutulan tüm verinin 3. kişilerce kontrolsüz olarak değiştirilebileceği göz önünde bulundurulmalıdır. (Örneğin; SQLite)
GK6	Uygulamanın işi tamamlandığında hassas veri (GPS izleme bilgisi vb.) cihaz üzerinden silinmelidir.
GK7	Geçici olarak olsa bile hassas veri 3. kişi ya da uygulamalar tarafından erişilebilir yerlerde tutulmamalıdır.
GK8	Hassas veri SDCard vb. dış depolama alanlarında saklanmamalıdır.
GK9	Uygulama arkada bir sunucu ile haberleşip verileri orada tutacak ise mutlaka kullanıcıdan onay alınmalıdır. Aksi halde mahremiyet ihlal edilmiş olur.
GK10	Uygulamada kullanılan veritabanlarına parolasız erişime izin verilmemelidir.
GK11	Uygulama mobil uygulama güvenlik gereksinimleri göz önüne alınarak geliştirilmeli ve güvenlik testleri mutlaka yapılmalıdır.
GK12	Uygulama logları kritik verileri içermemelidir.
GK13	Uygulama üzerinde tutulan veriler güçlü şifreleme algoritmaları ile şifrelenmeli ve şifreli bir kanal üzerinden gönderilmelidir.
GK14	Uygulama sertifika kontrolü yapmalıdır.

Tablo 5.24: Mobil sağlık uygulamaları güvenlik gereksinimleri - Devam

No	Güvenlik Gereksinimleri
GK15	Uygulama, uygulamaya ilişkin trafiğin proxy üzerinden iletilmemesi ve proxy üzerinde HTTPS trafiğin açılarak incelenmesini önlemek amacıyla, sertifika iğneleme/sabitleme (certificate pinning) kullanmalıdır.
GK16	Tüm istekler ve tüm alt etki alanları (subdomain) için "HTTP Strict Transport Security" (Strict-Transport-Security: max-age=15724800) başlığı bulunmalı, uygulamanın sunucu ile güvensiz HTTP protokolü üzerinden erişime geçmesi engellenmelidir.
GK17	Uygulama Jailbreak yapılmış veya Root'lanmış cihazlar üzerinde yalnızca kullanıcının riskleri okuyup anladığını açıkça beyan etmesi durumunda çalıştırılabilmelidir.
GK18	Sunucu konfigürasyonları güvenli bir şekilde yapılandırılmalı, tüm işletim sistemi, web sunucu ve diğer uygulama bileşen yamaları güncel olmalıdır.
GK19	Denial of Service ataklarına karşın belirli bir süre içerisinde belirli bir kişi/IP'den gelebilecek maksimum istek sayısı sınırlandırılmalıdır.
GK20	Otomatize edilmemesi gereken özellikle herkese açık login vb. ekranlarda CAPTCHA kullanılmalıdır.

Bölüm 6

Sonuç ve Gelecek Çalışmalar

Tez çalışması kapsamında WBAN teknolojisinin her katmanına detaylı tehdit analizi yapılmıştır. Yapılan analizin sonucu WBAN sistem tasarımları yapılırken güvenlik konusunun üzerinde daha fazla durulması gerektiğini göstermiştir. WBAN teknolojilerinde kullanılan kablosuz ağlar, bu teknolojinin birçok güvenlik zafiyeti barındırmasına neden olmaktadır.

Çalışma kapsamında WBAN teknolojisini temsil eden Proof of Consept (PoC) bir sistem incelenmiştir. Giyilebilir medikal cihazlardan olan MI BAND 1S edinilerek haberleşmede kullandığı Bluetooth teknolojisi güvenlik açısından analiz edilmiştir. Analiz sonucunda cihazın Bluetooth Version 4.0 BTLE teknolojisini kullandığı ve yapılan saldırılara karşı savunmasız olduğu görüldü.

MI BAND cihazının sahip olduğu WBAN sisteminin mobil uygulamalarının ve uygulama marketlerden kolay şekilde edinilebilen mobil sağlık uygulamalarının güvenlik testleri Tersine Mühendislik, Depolama Analizi ve Ağ Trafiği başlıkları altında gerçekleştirildi.

MI BAND cihazının kullandığı resmi uygulama marketinden Mi Fit 2 ve Mi Band Notify & Fitness uygulamaları indirilerek incelendi. Ayrıca Mi Fit uygulamasının üçüncü parti olarak MI BAND kullanıcıları tarafından geliştirilen bir versiyonu (Tweaked) ve cihazın üretici firmasının internet sitesinden dağıtılan versiyonu (Mi Fit 1) da incelendi. Yapılan analizler sonucunda dört uygulamanın da veritabanlarına parolasız erişim gerçekleştirildi. Bu veritabanlarında bulunan verilerin çekilebildiği; ayrıca uygulamaların kritik verileri kayıt altına aldığı (loglama) görüldü. Uygulamalarda kod karmaşıklaştırma işlemi yapıldığı ve yerel depolama alanlarının kullanım öncesi temiz olduğu görüldü.

Mi Fit uygulamasının üç farklı versiyonu (Mi Fit 1, Mi Fit 2, Tweaked) kendi arasında değerlendirildiğinde bulundurdukları uygulama izinleri genellikle ortaktır. Fakat diğer ikisinden farklı olarak, sadece Mi Fit 2 uygulamasının barındırdığı izinler de bulunmaktadır. Ayrıca güvenlik ve mahremiyetin sömürülmesinde etkili olan on tehlikeli izinden 6 tanesi üçünde de bulunmaktadır. RECEIVE_BOOT_ COMPLETED izni Mi Fit 2 ve Tweaked' de bulunurken Mi Fit 1' de bulunmamaktadır. Üç uygulamada da ortak olarak Mi hesabı ile oturum açılmakta, sertifika kontrolü yapılmakta ve Mi sunucularına yapılan veri iletimi şifreli olarak sağlanmaktadır. MI BAND uygulamalarına giriş yapılırken bir politikaya onay verilmesi gerekmektedir. Ancak kişisel sağlık verilerinin, uygulamanın sunucusuna gönderilmesinde yeni bir onay istememektedir. Bu durumun mahremiyeti ihlal ettiği düşünülmektedir.

Mi Band Notify & Fitness uygulaması ise kritik on izinden ikisi olan RECEIVE_BOOT_ COMPLETED ve READ_CONTACTS izinlerini barındırmaktadır. Uygulamayı kullanabilmek için herhangi bir kullanıcı hesabı istememektedir. Fakat MAC adresi üzerinden MI BAND eşleşmesi gerekmektedir. Bu eşleşme işlemi manuel olarak da yapılabilmektedir. Sertifika kontrolü yapılmamaktadır. Sömürülmeye yatkın olan GCM fonksiyonu için oluşturulmuş izinlerden RECEIVE iznini barındırmaktadır. İncelemede uygulamanın ücretsiz versiyonu kullanıldığından dışarıya herhangi bir veri iletimi yapılmadığı görülmüştür.

Çalışma kapsamında resmi uygulama marketten ve üçüncü parti uygulama marketlerden olmak üzere toplam 15 adet mobil sağlık uygulaması analiz edildi. Yapılan analizler sonucunda uygulamaların veritabanlarına parolasız erişim gerçekleştirildi. Bu veritabanlarında bulunan verilerin çekilebildiği görüldü. Yerel depolama alanlarının kullanım öncesi temiz olduğu görüldü. Ayrıca sertifika kontrolünün de yapılmadığı tespit edildi. Uygulamaların yeteneklerine göre farklı seviyelerde çeşitli izinlere sahip olduğu görüldü. Özellikle bazı uygulamaların talep ettiği izinlerden dolayı mahremiyeti ihlal edebileceği düşünülmektedir. Örneğin; uygulamanın kullanıldığı cihazın nerede olduğuna dair lokasyon bilgisini almaya yarayan izne sahip olan uygulamalar olduğu görüldü. Bazı uygulamaların örneğin SEND SMS izni ile kullanıcının bilgisi olmadan telefonundan SMS gönderebilme iznine sahip olduğu tespit edildi. Kullanıcının bilgisi olmadan dışarıya arama yapılabilmesini sağlayan, kullanıcının takviminde kayıtlı olan verilere erişip günlük programına müdahale edip takibini yapabilen, uygulamanın yüklü olduğu cihazın

kişilerine erişip okuyabilen ayrıca kişi eklemesi yapabilen uygulama izinlerinin de bulunduğu görüldü.

Sömürülmeye yatkın olan GCM fonksiyonu için oluşturulmuş izinlerden RECEIVE, SEND, C2D_MESSAGE izinlerini barındıran uygulamaların olduğu tespit edildi.

Tersine Mühendislik işlemlerinde gerçek koda ulaşmayı zorlaştıran kod karmaşıklaştırma işlemi sadece Pedometer, Health Records uygulamalarında yapılmıştır. Kod karmaşıklaştırma işlemi yapılamamış olan uygulamaların gerçek kodlarına kolaylıkla ulaşıldı.

Bazı uygulamaları kullanabilmek için email, kullanıcı adı, parola vb. kişisel bilgiler ile hesap oluşturmak gerekmektedir. Oturum açma işlemi için ise kullanıcı adı ve parola ile kimlik doğrulaması yapılmaktadır. Ancak bazılarında herhangi bir hesap oluşturma ve kimlik doğrulama işlemi yapılmadan uygulama kullanılabilmektedir.

Kullanıcı adı, parola bilgileri dâhil kişisel sağlık verilerinin yerel depolama alanında açık bir şekilde tutulduğu uygulamaların olduğu görüldü. Bu durumun gizlilik prensibine aykırı olduğu bilinmektedir.

Bazı uygulamaların kişisel sağlık verilerini logladığı görüldü. Bu durum uygulama loglarına erişen herkesin kişisel sağlık verilerine ulaşmasına izin vermektedir.

Uygulamalardan ikisi olan WebMD ve Zibdy Health uygulamalarının internet üzerinden yaptıkları veri iletiminin şifreli olduğu görüldü. Ayrıca veri iletimini açık olarak yapan uygulamaların yanında hiç iletim yapmayan uygulamalar da bulunmaktadır.

Yapılan çalışmalara ek olarak gelecekte aşağıda belirtilen çalışmalarda yapılabilir.

Tıbbi medikal cihazlardan olan uzaktan yönetilebilir insülin pompası, kan basınçölçeri, kalp pili, defibrilatör gibi cihazlar günlük hayatta kullanılmaktadır. Güvenlik özelliklerinin ortaya çıkarılması ve geliştirilmesi açısından böyle bir çalışma bu cihazlarda da uygulanmalıdır.

Çalışma kapsamında sadece WBAN ve WBAN sunucu katmanı değerlendirilmiştir. Ayrıca WBAN Mimarisinde bulunan Medikal Sunucu Katmanı ve bu katmanın içerdiği Hastane Bilişim Yönetim Sisteminin de güvenlik özellikleri incelenmelidir.

Kablosuz vücut alan ağlarını kullanan medikal cihazların bu şekilde bir çalışmayla değerlendirilmesi sonucu, WBAN sisteminde bulunan her katmanının güvenlik gereksinimleri

detaylı olarak elde edilmiş olacaktır. Bu güvenlik gereksinimlerine uygun olarak tasarlanacak veya geliştirilecek olan tıbbi cihazlar kişisel sağlık verilerinin korunmasını sağlayarak kullanım kalitesini artıracaktır.

Kaynaklar

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *Comm. Mag.*, 40(8):102–114, August 2002. ISSN 0163-6804. doi: 10.1109/MCOM.2002.1024422. URL http://dx.doi.org/10.1109/MCOM.2002.1024422.

[2] H. Alemdar and C. Ersoy. Wireless sensor networks for healthcare: A survey. *Comput. Netw.*, 54(15):2688–2710, October 2010. ISSN 1389-1286. doi: 10.1016/j.comnet.2010.05.003. URL http://dx.doi.org/10.1016/j.comnet.2010.05.003.

[3] S. Gyula, M. Miklós, L. Ákos, B. György, K. Branislav, N. András, P. Gábor, S. János, and F. Ken. Sensor network-based countersniper system. In *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 1–12, New York, NY, USA, 2004. ACM. ISBN 1-58113-879-2. doi: 10.1145/1031495.1031497. URL http://doi.acm.org/10.1145/1031495.1031497.

[4] J. Yick, B. Mukherjee, and D. Ghosal. Analysis of a prediction-based mobility adaptive tracking algorithm. In *2nd International Conference on Broadband Networks, 2005.*, pages 753–760 Vol. 1, Oct 2005. doi: 10.1109/ICBN.2005.1589681.

[5] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff. Wireless sensor networks for flash-flood alerting. In *Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on*, volume 1, pages 142–146, Nov 2004. doi: 10.1109/ICCDCS.2004.1393370.

[6] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh. Deploying a wireless sensor network on an active volcano. *IEEE Internet Computing*, 10(2):18–25, March 2006. ISSN 1089-7801. doi: 10.1109/MIC.2006.26.

[7] G. K. Kevin and R. P. David. *Global aging: The challenge of success*, volume 60. Population Reference Bureau Washington, DC, USA, 2005.

[8] Department of Economic United Nations and Population Division Social Affairs. World population ageing: 1950-2050, 2002. URL `http://www.un.org/esa/population/publications/worldageing19502050/`.

[9] U.S. Department of Health National Institute on Aging, National Institutes of Health, Human Services, and World Health Organization. Global health and aging, 2011. URL `http://www.nia.nih.gov/sites/default/files/global_health_and_aging.pdf`.

[10] V. Stanford. Using pervasive computing to deliver elder care. *IEEE Pervasive Computing*, 1(1):10–13, Jan 2002. ISSN 1536-1268. doi: 10.1109/MPRV.2002.993139.

[11] T. McFadden and J. Indulska. Context-aware environments for independent living. In *Proceedings of the 3rd National Conference of Emerging Researchers in Ageing*, pages 1–6. Citeseer, 2004.

[12] JA. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Lin, S. Son, R. Stoleru, and A. Wood. Wireless sensor networks for in-home healthcare: Potential and challenges. In *High confidence medical device software and systems (HCMDSS) workshop*, pages 2–3, 2005.

[13] M. Patel and J. Wang. Applications, challenges, and prospective in emerging body area networking technologies. *IEEE Wireless Communications*, 17(1):80–88, February 2010. ISSN 1536-1284. doi: 10.1109/MWC.2010.5416354.

[14] S.K.S Gupta. Safe and dependable bio-sensor networking for pervasive healthcare dept. computer science and engineering, 2008. URL `http://impact.asu.edu/~mcn/Presentations/AYUSHMAN_BIOMED_ASU_Jan_2008_FINAL.ppt`.

[15] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58, February 2010. ISSN 1536-1284. doi: 10.1109/MWC.2010.5416350.

[16] Ş. Baş. Kişisel alan ağları ve giyilebilir bilgisayarların kullanımıyla gerçekleştirilecek bir hasta izleme sistemi önerisi. Master's thesis, Ege Üniversitesi, 2011.

[17] H. F. Rashvand, V. T. Salcedo, E. M. Sanchez, and D. Iliescu. Ubiquitous wireless telemedicine. *Communications, IET*, 2(2):237–254, 2008.

[18] R. Bults, K. Wac, A. Van Halteren, D Konstantas, V. Jones, and I. Widya. Body area networks for ambulant patient monitoring over next generation public wireless networks. In *3rd IST Mobile and Wireless Communications Summit*, pages 27–30, 2004.

[19] IEEE standard for local and metropolitan area networks - part 15.6: Wireless body area networks. *IEEE Std 802.15.6-2012*, pages 1–271, Feb 2012. doi: 10.1109/IEEESTD.2012.6161600.

[20] P. Dinkar, A. Gulavani, S. Ketkale, P. Kadam, and S. Dabhade. Remote health monitoring using wireless body area network. *International Journal of Engineering and Advanced Technology (IJEAT) ISSN*, 2249:8958, 2013.

[21] J. A. Gutierrez, E. H. Callaway, and R. L. Barrett. *Low-rate wireless personal area networks: enabling wireless sensors with IEEE 802.15. 4*. IEEE Standards Association, 2004.

[22] D. Geer. Users make a beeline for zigbee sensor technology. *Computer*, 38(12): 16–19, Dec 2005. ISSN 0018-9162. doi: 10.1109/MC.2005.422.

[23] U. Varshney. Using wireless technologies in healthcare. *International Journal of Mobile Communications*, 4(3):354–368, 2006.

[24] Bluetooth SIG. A look at the basics of bluetooth wireless technology, 2011. URL `https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics`.

[25] C. Odabaş, İ. Pehlivan, S. Demircioğlu, M. Gezer, and İ. Coşkun. Kablosuz Ağ Şifreleme Yöntemlerinin Karşılaştırılması. URL `http://www.emo.org.tr/ekler/8ca46a09ab755ee_ek.pdf`.

[26] D. M. Gezgin and F. Büyüksaraçoğlu Sakallı. *Kablosuz ağ teknolojileri ve şifreleme*, volume 1. Paradigma Yayınları, 2014.

[27] D. M. Gezgin and E. Buluş. Kablosuz Erişim Noktalarında Kullanılan Güvenlik Standartları. In *1.Uluslararası 5.Ulusal Meslek Yüksekokulları Sempozyumu*, 2009.

[28] Bluetooth SIG. Security, classic. URL `https://developer.bluetooth.org/TechnologyOverview/Pages/Security.aspx`.

[29] Bluetooth SIG. Bluetooth technology basics, 2011. URL `https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics`.

[30] J. Padgette, K. Scarfone, and L. Chen. *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology (Special Publication 800-121 Revision 1)*. CreateSpace Independent Publishing Platform, USA, 2012. ISBN 147816896X, 9781478168966.

[31] *BSI-Standard 100-1: Information Security Management Systems (ISMS)*. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.

[32] E. Başaranoğlu and G. Alkan. Farklı bir kaba kuvvet saldırı aracı: Crowbar (levye), 2014. URL `http://www.bilgiguvenligi.gov.tr/sizma-testleri/farkli-bir-kaba-kuvvet-saldiri-araci-crowbar-levye.html`.

[33] M. Baykara, R. Daş, and İ. Karadoğan. Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In *1st International Symposium on Digital Forensics and Security*, pages 231–239, 2013.

[34] Y. Vural and Ş. Sağıroğlu. Kurumsal bilgi güvenliği ve standartlari üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 23(2), 2008.

[35] S. Dilek and S. Özdemir. Sağlık hizmetleri sektöründe kablosuz algılayıcı ağlar. *Bilişim Teknolojileri Dergisi*, 7(2), 2014.

[36] Microsoft. The stride threat model, 2005. URL `https://msdn.microsoft.com/library/ms954176.aspx`.

[37] D. R. Zhang, C. J. Deepu, X. Y. Xu, and Y. Lian. A wireless ecg plaster for real-time cardiac health monitoring in body sensor networks. In *2011 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pages 205–208, Nov 2011. doi: 10.1109/BioCAS.2011.6107763.

[38] A. Volmer and R. Orglmeister. Wireless body sensor network for low-power motion-tolerant syncronized vital sign measurment. In *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3422–3425, Aug 2008. doi: 10.1109/IEMBS.2008.4649941.

[39] T. Falck, J. Espina, J. P. Ebert, and D. Dietterle. Basuma - the sixth sense for chronically ill patients. In *International Workshop on Wearable and Implantable*

Body Sensor Networks (BSN'06), pages 4 pp.–60, April 2006. doi: 10.1109/BSN.2006.12.

[40] C. s. Jang, D. G. Lee, and J. w. Han. A proposal of security framework for wireless body area network. In *Security Technology, 2008. SECTECH '08. International Conference on*, pages 202–205, Dec 2008. doi: 10.1109/SecTech.2008.32.

[41] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle. Security for pervasive medical sensor networks. In *Mobile and Ubiquitous Systems: Networking Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International*, pages 1–10, July 2009. doi: 10.4108/ICST.MOBIQUITOUS2009.6832.

[42] C. Li, A. Raghunathan, and N. K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, pages 150–156, June 2011. doi: 10.1109/HEALTH.2011.6026732.

[43] W. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE*, pages 12–17, June 2012. doi: 10.1145/2228360.2228364.

[44] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 129–142, May 2008. doi: 10.1109/SP.2008.31.

[45] L. C. Silva, M. Perkusich, H. O. Almeida, A. Perkusich, M. A. M. Lima, and K. C. Gorgônio. A baseline patient model to support testing of medical cyber-physical systems. In Indra Neil Sarkar, Andrew Georgiou, and Paulo Mazzoncini de Azevedo Marques, editors, *MedInfo*, volume 216 of *Studies in Health Technology and Informatics*, pages 549–553. IOS Press, 2015. ISBN 978-1-61499-564-7.

[46] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz. A biometric-based security for data authentication in wireless body area network (wban). In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pages 998–1001, Jan 2013.

[47] S. N. Ramli, R. Ahmad, and M. F. Abdollah. Electrocardiogram (ecg) signals as biometrics in securing wireless body area network. In *Internet Technology and*

Secured Transactions (ICITST), 2013 8th International Conference for, pages 536–541, Dec 2013. doi: 10.1109/ICITST.2013.6750259.

[48] Android Developer. Android sdk, 2016. URL `http://developer.android.com/sdk/index.html#downloads`.

[49] Genymotion, 2016. URL `https://www.genymotion.com/features/`.

[50] Portswigger. Burp suite, 2016. URL `https://portswigger.net/burp/`.

[51] Wireshark, 2016. URL `https://www.wireshark.org/download.html`.

[52] Xiaomi. Mi band 1s, 2016. URL `http://www.mi.com/en/miband/#01`.

[53] O. Topgül. Vezir project, 2016. URL `https://github.com/oguzhantopgul/Vezir-Project`.

[54] A. Balakrishnan and C. Schulze. Code obfuscation literature survey. *CS701 Construction of compilers*, 19, 2005.

[55] Android Developer. Android permission. URL `http://developer.android.com/guide/topics/manifest/permission-element.html`.

[56] I. Lewis D. Galpin. Google I/O 2012 - Ten Things Game Developers Should Know, 2012. URL `https://www.youtube.com/watch?v=WDDgoxvQsrQ`.

[57] Google Developers. Architectural overview, 2016. URL `https://developers.google.com/cloud-messaging/gcm#lifecycle`.

[58] Android Developer. Manifest permission, 2016. URL `http://developer.android.com/reference/android/Manifest.permission.html`.

[59] M. Ryan. Bluetooth: With low energy comes low security. In *Proceedings of the 7th USENIX Conference on Offensive Technologies*, WOOT'13, pages 4–4, Berkeley, CA, USA, 2013. USENIX Association. URL `http://dl.acm.org/citation.cfm?id=2534748.2534754`.

[60] Xiaomi. Mi fit, 2016. URL `http://app.mi.com/detail/68548`.

[61] Mc Group. Mi band notify & fitness, 2016. URL `https://play.google.com/store/apps/details?id=com.mc.miband1`.

[62] Xiaomi Technology. Mi fit, 2016. URL https://play.google.com/store/apps/details?id=com.xiaomi.hm.health.

[63] MIUI Device Team. Tweaked, 2016. URL http://en.miui.com/thread-53761-1-1.html.

[64] Healthiply. Healthiply professionals, 2016. URL https://play.google.com/store/apps/details?id=com.health.doc.

[65] KloudData Inc. mMR, 2016. URL https://play.google.com/store/apps/details?id=com.klouddata.mmr.main.

[66] NFC MEDIC. Nfc medic, 2016. URL https://play.google.com/store/apps/details?id=com.gn4me.apps.NFCMedic2.

[67] VitalHub Corp. Patient chart, 2016. URL https://play.google.com/store/apps/details?id=com.vitalhub.vitalchart.

[68] Zibdy Inc. Zibdy health, 2016. URL https://play.google.com/store/apps/details?id=com.zibdy.VPB.client.

[69] Tıpnet Yazılım. Yalova devlet hastanesi uygulaması, 2016. URL https://play.google.com/store/apps/details?id=com.yalovadh.monaca.

[70] Diagnose Software Inc. Diagnose, 2016. URL https://play.google.com/store/apps/details?id=com.DiagnoseSoftware.diagnose.

[71] Greenway Family Practice. Healty files, 2016. URL https://play.google.com/store/apps/details?id=com.healthfilesapp.mobileandroid.

[72] Smart Medical Apps. Smart medical, 2016. URL https://apkpure.com/smart-medical-apps-h-p/com.smartmedicalapps.checklist.

[73] AvvaStyle. Health records, 2016. URL https://apkpure.com/health-records/com.AvvaStyle.medcard.

[74] Caddy. Medical & health records caddy, 2016. URL https://apkpure.com/medical-health-records-caddy/com.medicalcalculations.

[75] Tanya White. My medical history, 2016. URL https://apkpure.com/my-medical-history/com.droidcasa.tanyawhite.

[76] LLC WebMD. Webmd, 2016. URL `https://apkpure.com/webmd-for-android/com.webmd.android`.

[77] LifeGuard Global Ltd. My medical history, 2016. URL `https://apkpure.com/my-medical-history/com.pirolor.steven.medhitory`.