Akıllı Ev Sistemlerinde Güvenlik Zafiyetleri ve Önlemleri

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

Burak ÖZDEMİR
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:

Prof. Dr. Ensar Gül .....
(Tez Danışmanı)

Dr. Öğretim Üyesi Hüseyin Yüce .....

Dr. Öğretim Üyesi İhsan Çiçek .....

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

ONAY TARİHİ: 29.08.2019

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Burak ÖZDEMİR, başlığı, 'Akıllı Ev Sistemlerinde Güvenlik Zafiyetleri ve Önlemleri' 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: 29.08.2019

Security Vulnerabilities and Precautions in Smart Home Systems

Burak ÖZDEMİR

Abstract

Nowadays, there is a huge increase in the use of smart home systems with widespread use of IoT devices. Vulnerabilities found in smart home systems has become more important than ever. In this study, a smart home was modeled and tested for vulnerabilities and the results were analyzed. While selecting the devices to be used in the model, market share, usage rate, price performance ratio and availability of these devices were taken into consideration. The smart home system consists of an intelligent electrical outlet, a main management console, a security alarm system and a baby monitoring camera devices. The selected devices were subjected to security tests for the most commonly used vulnerabilities. These tests include attacks on wireless network vulnerabilities, man-in-the-middle attacks, and distributed decommissioning attacks. Security weaknesses were detected in all tested devices. The use of strong passwords, the use of a separate network for devices, changing default ports, the monitoring of authorization and event log records are recommended to ensure users' own security. On the other hand, the manufacturers should take the most basic security measures such as the use of difficult passwords, not using the default password, two-factor verification, encrypted data traffic, authority management and similar security measures.

Keywords: Information Security, Smart Home, Security Vulnerability, Security Precautions

Akıllı Ev Sistemlerinde Güvenlik Zafiyetleri ve Önlemleri

Burak ÖZDEMİR

Öz

Günümüzde yaygınlaşan nesnelerin interneti cihazlarıyla birlikte akıllı ev sistemlerinin kullanımında büyük bir artış yaşanmaktadır. Akıllı ev sistemlerinde ortaya çıkan güvenlik açıkları birçok güvenlik sorununu beraberinde getirmektedir. Bu çalışmada bir akıllı ev sistemi örnek modeli oluşturularak güvenlik testleri uygulanmış, sonuçları gözlemlenmiş ve elde edilen bulgulara yer verilmiştir. Oluşturulan örnek modelde kullanılacak cihazlar seçilirken pazar payı, kullanım oranı, fiyat performans başarısı ve elde edilebilme kolaylıkları göz önünde bulundurulmuştur. Örnek akıllı ev sistemi; akıllı elektrik prizi, ana yönetim konsolu, akıllı güvenlik alarm sistemi, güvenlik ve bebek izleme kamerası cihazlarından oluşmaktadır. Seçilen cihazlara en yaygın kullanılan zafiyet açıklıklarına yönelik güvenlik testleri uygulanmıştır. Bu testler kablosuz ağ zafiyetlerine yönelik saldırı, ortadaki adam saldırısı, dağıtık servis dışı bırakma saldırısı testlerinden oluşmaktadır. Test edilen cihazların tamamında güvenlik zafiyetleri tespit edilmiştir. Kullanıcıların kendi güvenliklerini sağlamak adına güçlü şifre kullanımı, cihazlara ayrı bir ağ kullandırma, varsayılan portları değiştirme, yetki ve olay günlük kayıtlarının takibi ve diğer önlemlerin alınmasının gerekliliği vurgulanmıştır. Üreticilerin ise en temel güvenlik önlemleri olan zorlu şifre kullanımı, varsayılan şifreyi kullandırmama, iki faktörlü doğrulama, şifreli veri trafiği, yetki yönetimi ve buna benzer güvenlik önlemlerini alması gerektiği tespit edilmiştir.

Anahtar Sözcükler: Akıllı Ev Sistemleri, Güvenlik Zafiyetleri, Güvenlik Önlemleri, Bilgi Güvenliği

Teşekkür

Tez çalışmam boyunca desteğini ve motivasyonunu esirgemeyen değerli hocam Prof. Dr. Ensar Gül 'e, çalışmalarım sırasında destekleriyle beni cesaretlendiren değerli dostlarım Ömer Ünsal ve Yusuf Topal'a teşekkürü bir borç bilirim.

Tez ve ders sürecinde hoşgörü ve sevgisini eksik etmeyen sevgili eşim Mehtap Özdemir'e, varlığıyla beni güçlendiren ve onur duyduğum sevgili kızım Elif Özdemir'e, hayatım boyunca her anlamda desteklerini sürekli hissettiğim çok değerli aileme şükranlarımı ve teşekkürlerimi sunarım.

İçindekiler

Şekil Listesi

Kısaltmalar

IOT	**I**nternet **O**f **T**hings (Nesnelerin İnterneti)
MiTM	**M**an **i**n **T**he **M**iddle (Ortadaki Adam Saldırısı)
DDOS	**D**istributed **D**enial **O**f **S**ervice (Dağıtık Servis Dışı Bırakma Saldırısı)
SSL	**S**ecure **S**ockets **L**ayer (Güvenli Soket Katmanı)
AES	**A**dvanced **E**ncryption **S**tandard (Gelişmiş Şifreleme Standardı)
MAC	**M**essage **A**uthentication **C**ode (Mesaj Doğrulama Kodu)
ABD	**A**merika **B**irleşik **D**evletleri
BLE	**B**luetooth **L**ow **E**nergy

Bölüm 1

Giriş

Akıllı ev sistemleri; bir ana yönetim cihazına bağlı olan, az enerji tüketen sensör veya küçük akıllı cihazların günümüzde insan hayatını daha konforlu bir hale getirmek, enerji tasarrufu ve ortam güvenliğini sağlamak için geliştirilmiş uzaktan yönetilebilen, programlanabilen sistemlerdir.

Günümüzde teknoloji ile birlikte akıllı sistemler hızla gelişmekte ve canlıların olduğu veya olmadığı her ortamda kullanılmaktadır. Gartner araştırma şirketinin son yıllarındaki raporlarına göre, gelişmekte olan teknolojilerle ilgili beklentilerin en tepe noktasında 'nesnelerin interneti' konusu gelmektedir [1]. İnsanların en çok vakit geçirdiği mekânlar, evler ve iş yerleri olduğu için başlangıçta ev veya çalışma hayatıyla ilgili yaşamı kolaylaştıran çözümler sağlama amacı taşımaktadır. Nesnelerin interneti olarak adlandırılan bu cihazların evlerde kullanımı ile evler akıllı bir şekilde yönetilebilmektedir ve bu teknoloji sayesinde akıllı ev kavramı oluşmaktadır.

Sabah güneşin doğuşuyla açılan veya akşam hava kararkdığında kapanan perde ve panjurlar, ortamı ayarlanan hava sıcaklığına getirmek için hava sıcaklığını ölçerek çalışan ısıtma ve soğutma sistemleri, hava kirliliğini ve nem miktarını ölçen akıllı cihazlar, akıllı aydınlatma sistemleri, duman, gaz ve su sensörleri, akıllı eğlence sistemleri, akıllı elektrik prizleri gibi cihazlar akıllı ev sistemlerini oluşturmaktadır.

Bir akıllı ev sisteminde mevcutta kullandığımız elektronik aletlerin ve cihazların sadece akıllı hareket etmeleri yeterli olmamaktadır. Akıllı ev konsepti, hayatımıza konfor, kolaylık ve güvenlik sağlamak amacıyla birçok fiziksel nesnenin bu ortama akıllı olarak katılması ile sağlanmaktadır. Yapılabilecekler sadece hayal gücü ile sınırlıdır. Örneğin bir kişi evden çıkmadan önce aklına gelip gökyüzüne bakması ve gökyüzünün bulutlu olduğunu görüp yağmur yağacak mı diye merak ettiği bir anda hava tahminlerine bakıp buna karar vermesi vaktini almaktadır. Fakat evde bulunan bir şemsiyenin hava tahmininde yağmur gözüküyorsa üzerinde bir küçük ışık yanması kişinin evden çıkmadan şemsiyeyi almasını hatırlatmakta ve hayatına kolaylık, konfor katmaktadır [2].

Gelişen bu teknolojileri göz önünde bulundurduğumuzda akıllı ev sistemlerinin önümüzdeki birkaç yıl içinde cep telefonu gibi gündelik hayatımızın içinde vazgeçilmez bir rolü olacağı kaçınılmaz bir gerçektir. Hemen hemen her alanda bir çözümü ve kullanım alanı bulunan bu akıllı ev sistemlerinin, topladığı verileri paylaşımda bulunması kullanıcı gizliliği ve mahremiyeti açısından çeşitli problemleri ortaya sermektedir. Bu akıllı cihazların siber saldırılara karşı güvenlik seviyelerine bakıldığında maalesef üreticilerinin yeteri kadar güvenli bir sistem kurmayı önemsemedikleri görülmektedir. Son yıllarda ortaya çıkan güvenlik açıklıkları ve olası herhangi bir güvenlik açığına maruz kalan kullanıcı sayısının fazlalığı bilgisayar korsanları açısından cezbedici bir ortam oluşturmaktadır.

Bu akıllı cihazlar yeni gelişmekte olan bir teknolojinin ürünü olmasından dolayı henüz bir standart çerçevesinde geliştirilmemektedir. Bundan dolayı pazarda bulunan akıllı cihaz üreticilerinin, güvenlikten daha çok ticari düşünceler içinde olduğu bir gerçektir. Bu sebeple akıllı cihazlar güvenlik yönünden birçok eksikliklere sahiptir. Ucuz bir teknoloji olmamasından dolayı fiyatları ve maliyetleri daha çok artacağından, üretim aşamasında sıkı güvenlik tedbirleri uygulanamamaktadır. Sıkı güvenlik tedbirleri uygulandığında da maliyetleri artacağı için satışları ve popülariteleri olumsuz yönde etkileneceğinden maalesef güvenliğe çok fazla önem verilmemektedir.

Kullanılan ağ trafiğinin şifrelenmesi ve kimlik doğrulama güvenlik önlemleri gibi temel güvenlik önlemleri dahi kullanılmadığı için güvenlik sağlanamamaktadır. Önümüzdeki

yıllarda bu teknolojinin daha çok ortamda kullanılacağı ve insanların büyük bir çoğunluğunun ilgisini çekeceği göz önünde bulundurulduğunda, güvenlik önlemleri alınarak siber saldırılara karşı en kısa sürede korunaklı olunması gerekmektedir.

Statista araştırma firmasının raporuna göre dünya genelinde akıllı ev cihazları pazar hacmi 2018 yılında 53.2 milyar dolar olarak gerçekleşmiştir ve 2023 yılında 145.4 milyar dolara yükselmesi tahmin edilmektedir [3]. Kullanım fazlalığı siber saldırılar için cazip bir ortam oluşturmakta ve gün geçtikçe daha cazip bir hal almaktadır. En çok yapılan siber saldırılardan biri olan DDOS (Dağıtık Servis Dışı Bırakma Saldırısı) gibi saldırılarda kullanılan zombi bilgisayarlar günümüzde yerlerini, internet of things olarak adlandırılan akıllı sistemlere bırakmaktadır. Bunun en büyük sebeplerinin başında gelen varsayılan şifrelerin değiştirilmemiş olması, güçlü parola doğrulama altyapılarının kullanılmaması gibi etkenlerdir.

Geçtiğimiz günlerde ABD de gerçekleşen ve dünya genelini etkileyen, büyük çaplı yankı uyandıran bir siber saldırı sonucunda yüzlerce internet sitesinin yanı sıra popüler birçok sosyal medya sayfasına erişim sağlanamamıştır. Siber saldırı hakkında yapılan incelemede saldırının DYN IPM DNS servis sağlayıcısına yapılan dağıtık hizmet reddi (DDoS) saldırısı olduğu anlaşılmıştır. Bu siber saldırıyı diğerlerinden farklı kılan nokta ise saldırganların kullandıkları yöntemlerdeki farklılık olmuştur. Bu tip saldırılarda kullanılan bilgisayarlar yerine alışılmışın dışında bir durum gerçeklemiş ve akıllı ev sistemlerinin bir parçası olan akıllı kameralar kullanılmıştır. Siber saldırıda Mirai ismi verilen kötücül bir yazılım kullanan saldırganlar, bu saldırı sonucunda daha önceden bu yazılım sayesinde yapılan 620GB lık veri trafiği rekorunu da kırmayı başardıkları gözlemlenmiştir [4]. Mirai, sıkça kullanılan ve yaygın olan şifreleri deneyerek şifre kırma konusunda çok başarılı olmakta ve cihazlara erişim sağlayabilmektedir. Bu sayede güçlü kimlik doğrulaması olmayan akıllı cihazlar ele geçirilerek siber saldırılarda kullanılmaktadır.

Akıllı ev sistemlerini uzaktan kontrol etmek için kullanılan mobil cihazların büyük bir çoğunluğu SSL bağlantısı kullanmamaktadır. Kimlik doğrulama yöntemleri ya çok temel bir şekilde kullanılmakta ya da hiç kullanılmamaktadır. Genel anlamda web üzerinden

yönetim ve erişim sağlanabildiği için web uygulamalarının sahip olduğu tüm açıklıklara sahip olma riski barındırmaktadır. Güçlü şifre kullanımı zorunlu tutulmamakta, iki faktörlü doğrulama neredeyse hiçbirinde desteklenmemektedir. Kullanıcı hesaplarını koruma adına geçici erişim engelleme ya da kullanıcı engelleme gibi güvenlik önlemleri desteklenmemektedir. Yazılım güncellemeleri imzalanmış ve şifrelenmiş bir şekilde güvenli olarak sunulmamaktadır.

Günümüzde söz ettiğimiz güvenlik açıklıkları ve siber saldırılar yaygın bir şekilde bilinmesine ve kullanılmasına rağmen akıllı ev sistemlerinde güvenlik anlamında yeterli hassasiyetin gösterilmediği ve önlemlerin yeterli düzeyde alınmadığı gözükmektedir. Bu tip akıllı cihazların uygulanabilirliği açısından, boyut olarak küçük olmaları ve uzun süre aktif olarak çalışabilmeleri için enerji tüketimi konusunda cimri olmaları gerektiği kaçınılmaz bir gerçek olsa da, bu şartlar dahilinde en temel güvenlik tedbirlerinin dahi yeterli düzeyde alınmadığı gözlemlenmektedir.

Bu tezde günümüzde kullanılan akıllı ev sistemi cihazlarının çeşitliliği, kullanıldığı alanlar, kullanımla birlikte toplanan veri ve bilgiler incelenerek olası bir siber saldırı sonucunda kullanılabilirliği etkileyen, bireysel ve toplumsal zarara sebep olabilecek saldırı çeşitleri araştırılacaktır. Bu saldırıların bazı örnek modeller üzerinde ne tür etkiler verdiği test edilerek sonuçları gözlemlenecektir. Hayatımızı kolaylaştıran ve konfor sağlayan akıllı ev sistemlerine yapılacak siber saldırılar karşısında maksimum seviyede korunmak ve kullanılabilirliğin devamını sağlamak için üreticiler ve kullanıcılar tarafından yapılması gereken güvenlik tedbirlerinin neler olduğu incelenecektir.

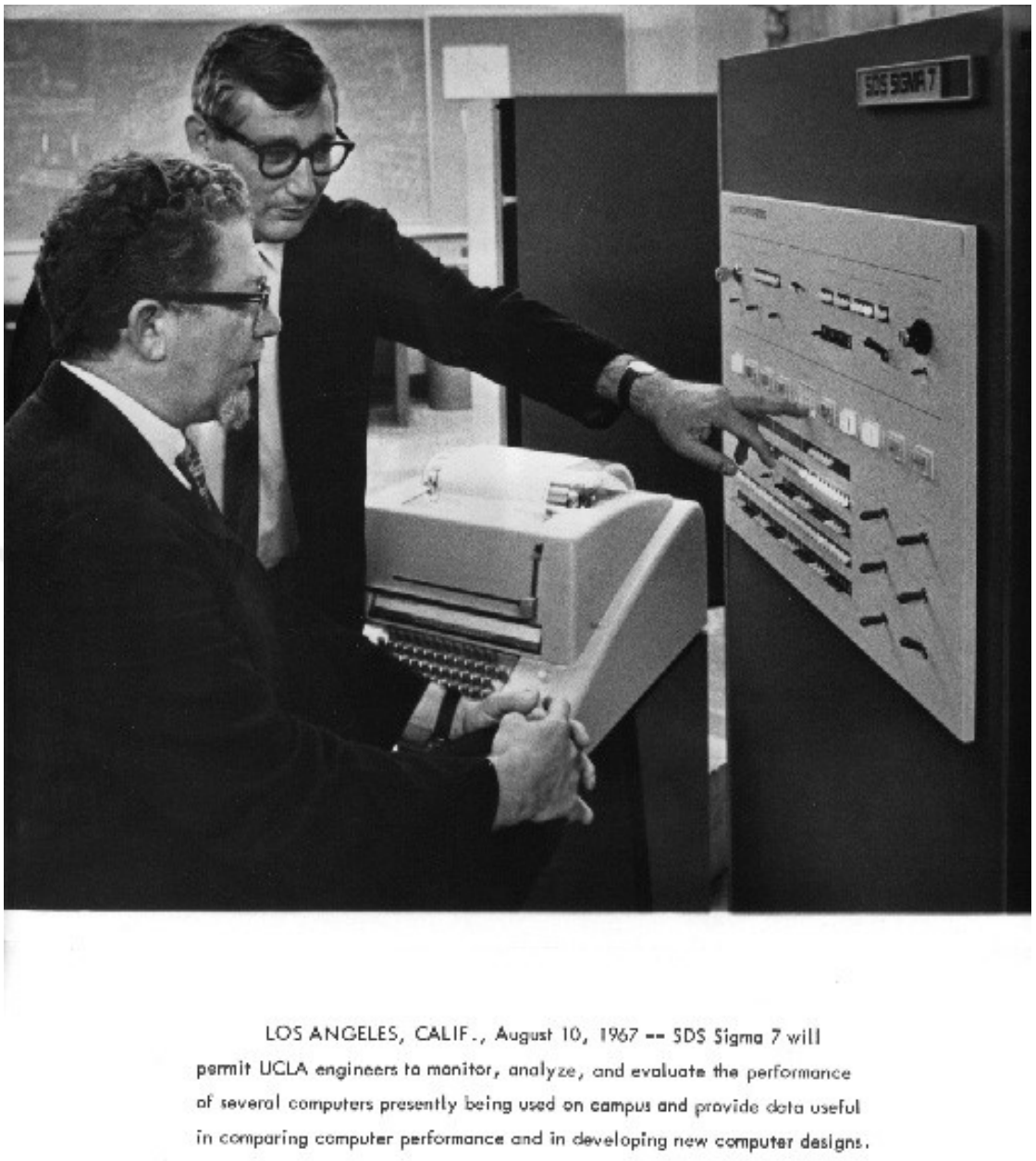
Bölüm 2

Temel Bilgiler

2.1 Nesnelerin İnterneti (Internet Of Things)

Fiziksel nesnelerin birbirleri veya daha büyük sistemler ile belirli bir protokol kapsamında haberleşmesi sonucu oluşan iletişim ağına nesnelerin interneti adı verilmektedir [5]. Nesnelerin interneti teknolojisinin temeli 1800'lerde fiziksel bir hareket olmaksızın frekanslar ve kablolar üzerinden iletişim kurmayı sağlayan telgraf, faks makinesi ve radyo gibi cihazların icadına dayanmaktadır.

Nesnelerin interneti teknolojisini var eden unsur, nesnelerin üzerlerinde bulunan sensörler sayesinde topladıkları milyonlarca veriyi birbirleri ile iletişim kurarak aktarmaları ve bu verileri anlamlı bir hale getirerek çalışmalarıdır. İnternet Protokolü'nü (IP) kullanan ilk ağ Amerika Birleşik Devletleri Savunma Bakanlığı için geliştirilmiş ARPANET adı verilen bir ağdır. ARPANET ağı internet teknolojisinin temeli olarak kabul edilmektedir. Bu ağ üzerinden ilk olarak 1969 yılında, bilgisayar aracılığı ile ilk mesaj başarılı bir şekilde gönderilmiştir [6].



Şekil 2.1: ARPANET geliştirilmiş ağında kullanılan 32 bit bilgisayara ait görüntü [7]

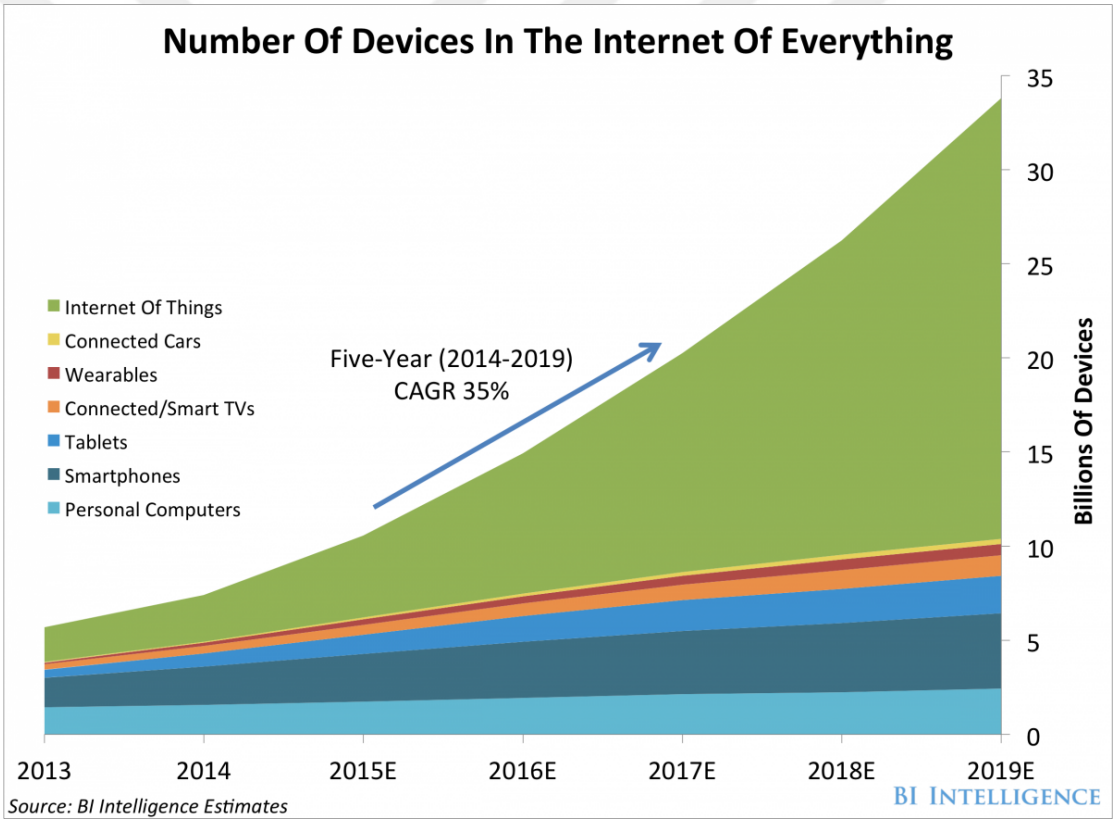
Günümüzde iletişim sadece insanlar arasında kurulmamakta, nesneler ürettikleri verileri birbirlerine aktararak kendi aralarında anlamlı bir iletişim kurabilmektedirler. Hatta makinelerin birbirleri arasında iletişim kurması (machine to machine veya m2m) günümüzün sıkça kullanılan kavramlarından biri haline gelmiştir. Birçok teknoloji firması özellikle endüstri faaliyetlerinde kullanmak üzere yeni ürünler geliştirmek için machine to machine üzerinde çalışarak yeni projeler geliştiren ekipler kurmaktadır.

Nesnelerin interneti kavramı ilk olarak 1999 yılında Kevin Ashton tarafından telaffuz edilmiştir. Kevin Ashton bir firmaya yaptığı sunumda RFID adı verilen radyo frekansı ile tekil veya toplu olarak ürün tanımlama yapmak için kullanılacak teknolojinin adından nesnelerin interneti olarak söz etmiştir [8]. Henüz nesnelerin interneti kavramı ortaya atılmadan önce, ilk örneği 1991 yılında Cambridge Üniversitesi'nde yaşanmıştır. Üniversitede çalışan 15 akademisyen bulundukları oda dışında olan bir kahve makinesinin durumunu görebilmek, kahvenin olup olmadığını anlayabilmek için kameralı canlı bir sistem kurarak, kahve makinesinin fotoğrafını dakikada üç kez çekip bilgisayar ekranına gönderen bir sistemi hayata geçirmişlerdir [9]. Kısa bir süre sonra bilgisayarların ve internet teknolojisinin yaygınlaşması ile birlikte bu kahve makinesinin görüntüsünü internet üzerinden web ortamına koyarak, herkesin görüntüleyebileceği şekilde yayınlamaya başlamışlardır. Sembolik olarak 10 yıl boyunca internet üzerinden yayını yapılan kahve makinesinin görüntüsü 2001 yılında internet üzerinden kaldırılmıştır. Bu sistemin gerçek zamanlı oluşu ve cihazların aralarında otomatik gerçekleşmesi nesnelerin interneti kavramının ilk örneği olarak tarihte yerini almıştır.

Şekil 2.2: Kahve makinesinin internet üzerinden kamera ile canlı izlenen görüntüsü[9]

Günümüzde etrafımızdaki birçok nesnenin internete bağlı olduğu ve internetin insan hayatında neredeyse hava, su kadar önemli olduğu zamanlara doğru ilerlemekteyiz. Gün geçtikte internet bağlantı maliyetleri düşmekte ve bununla beraber internet kullanımı, internete kablosuz bağlanan sensörlerle donatılmış cihazların sayısı artmaktadır. Akıllı telefon ve internet kullanımı inanılmaz bir hızla artarken nesnelerin interneti teknolojisinin hayatımızda daha fazla rol alacağı kaçınılmaz bir gerçektir.

Business Insider araştırma raporuna göre 2008 yılında dünyadaki insan sayısından daha fazla internete bağlı cihaz bulunurken bu sayı 2015 yılında 10 milyara ulaşmıştır ve aynı raporun tahminlerine göre 2020 yılında dünyada 34 milyar internete bağlı cihaz bulunması beklenmektedir. Başka bir açıdan bakılacak olursa 2025 yılında pazar büyüklüğünün 13 trilyon dolara ulaşması tahmin edilmektedir [10]. 2020 yılında akıllı ev sistemlerinde kullanılan 20 adet IOT cihazının üzerindeki sensörler aracılığıyla üreteceği veri trafiğinin 2008 yılında dünyadaki tüm internet trafiğinden daha fazla olacağı tahmin edilmektedir. Bu kadar çok cihazın gelecekte benzersiz bir kimliğe sahip olup her yerden erişilebilir olmasını sağlamak adına, IPv6 protokolüne geçiş bu teknolojinin gelişmesinin ve önündeki önemli bir engelin kaldırılmasını sağlayacaktır.



ŞEKIL 2.3: Dünyada internete bağlı cihaz sayısının yıllara göre tahmini artış grafiği[11]

Milyarlarca akıllı nesnenin birbirleriyle bağlantı halinde olarak sensörleri aracılığı ile üretilen çok yüksek veri trafiğinin anlamlandırılması ve kullanıcılar adına kararlara varılmasını sağlamakta bu nesnelere düşen görevler arasında yer almaktadır. Tüm akıllı cihazlar toplanan bu veriler ile beslenerek daha akıllı bir hale gelmek üzere programlanmaktadır. Son yıllarda sensörlerle üretilen bu verilerin gerçek zamanlı işlenmesi ve

makine öğrenimi (machine learning) alanındaki gelişmelerle birlikte nesnelerin interneti daha ön planda olmaktadır. Günümüzde hızla gelişmekte olan bir diğer teknolojide yapay zeka teknolojisidir. Yapay zeka teknolojisi ile nesnelerin interneti teknolojisi iç içe kullanıldığında gelecekte en önemli danışmanlarımız hatta birçok günlük işimizde karar vericilerimiz olarak yer alacaklardır.

Sanayi devrimi olarak adlandırılan endüstri 4.0 kavramının temeli nesnelerin interneti teknolojisinde yatmaktadır. Bu teknoloji sayesinde fabrikaların üretim bantlarında ya da güç gerektiren taşıma , işleme gibi süreçlerde akıllı robotlar kullanılmaktadır. Akıllı robotlar üzerlerinde bulunan sensörler ve bu sensörlerden gelen veririnin işlenip anlamlandırıldığı yazılımları sayesinde fabrikalarda işçilerden daha çok tercih edilmektedir. Fabrikalar yakın bir gelecekte işçilik anlamında insanlardan arınacağı, insanların sadece kontrol aşamalarında yer alacağı bir yapıya doğru ilerlemektedir.

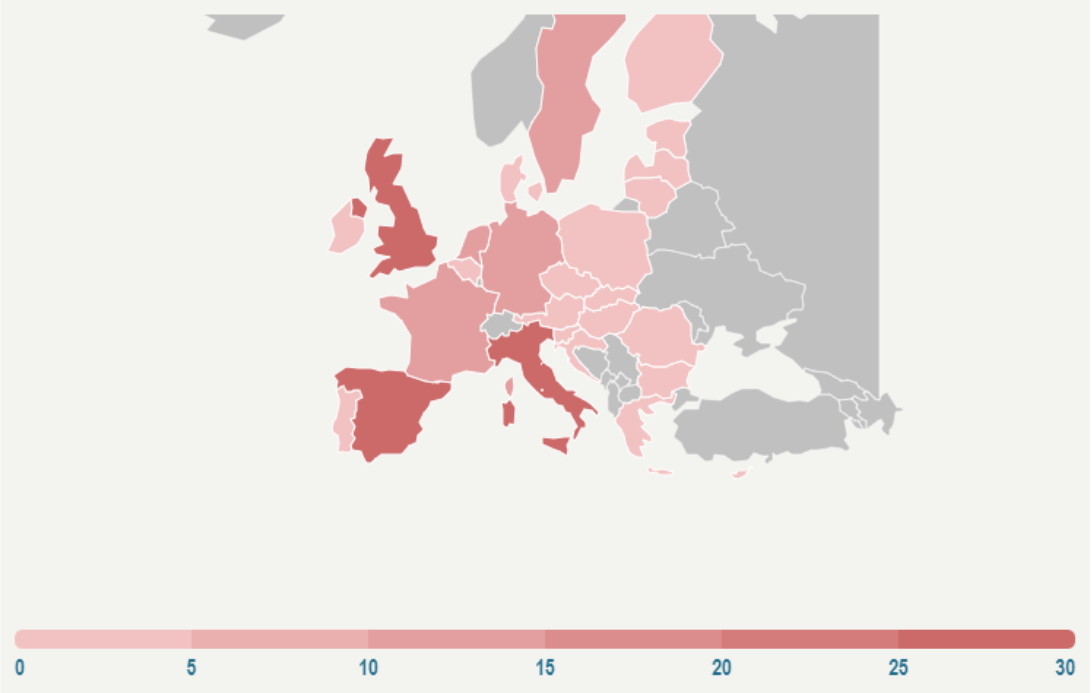
Nesnelerin interneti teknolojisi hayat kalitesini arttırmak, hayatı kolaylaştırmak, zamanın tasarruflu kullanılabilmesini sağlamak, verimi arttırmak, bilgi edinebilmeyi, konforu ve güvenliği sağlamak amaçlarıyla insanın olduğu ya da olmadığı hemen hemen her alanda kullanılabilir bir hale gelmektedir.

Nesnelerin interneti teknolojisinin en popüler kullanım alanlarından biri de şehirler ve evlerdir. Bu teknoloji sayesinde şehirler ve evler akıllı olarak adlandırılmaktadır. Şehirlerde kullanımı genellikle yoğun olan metropollerde olmaktadır. Nüfus açısından kalabalık olan şehirlerde trafiği rahatlatmak, hayatı kolaylaştırmak, zamandan tasarruf sağlamak, enerji verimliliğini arttırmak ve kamu güvenliğini sağlamak amacıyla nesnelerin interneti teknolojisi kullanılmaktadır. İnsanlar akıllı cihazlar sayesinde yönlendirilerek şehrin daha yaşanabilir bir alan olması sağlanmaktadır. Trafik sıkışıklığında sürücülere boş olan alternatif yollar hakkında bilgi verilebilmektedir. Toplu ulaşım araçlarının durağa ne zaman geleceği, o an nerede olduğu ve yaklaşık ne kadar sürede hangi durağa ulaşacağı konusunda bilgiler verilebilmektedir. Bu sayede trafik tıkanıklıkları ve hava kirliliği daha düşük düzeyde tutulmaktadır. Şehir su isale şebekesinde bulunan sensörler sayesinde sızıntı, tıkanıklık gibi durumlar analiz edilerek hızlı müdahale sağlanmaktadır.

Sokak lambaları sensörler sayesinde hava karardığında otomatik olarak yanmakta yönetim ve enerji verimliliği açısından birçok faydalar sağlanmaktadır.

Şehirlerde insana hizmet noktasında da kamu bu teknolojiden faydalanmaktadır. Hasta verileri yapay zeka üzerinde işlenerek daha iyi teşhis ve kişilere özel tedavi imkanı sağlanmaktadır. Bakıma muhtaç insanlar robotik sağlık hizmeti ve hızlı uyarı sistemleri ile bakım gözetimi altında evlerinde güvence alında yaşayabilmektedir. Kamu güvenliğini sağlamak amacıyla sensör ve kameralar gerçek zamanlı olarak taranmakta, yüz algılama, plaka okuma gibi takip sistemleri kullanılmaktadır. Akıllı çöp konteynerleri sayesinde çöp kutularının doluluk oranları, yaklaşık ne kadar sürede dolacakları gibi bilgiler takip edilerek çöp araçları en ideal şekilde bu çöpleri toplamak için yönlendirilebilmektedir. Otoparkların doluluk oranları mobil uygulamalar ve uyarı levhalarında gösterilerek sürücüler boş otopark noktalarına yönlendirilebilmektedir.

Avrupa bölgesel kalkınma fonu akıllı şehirleri oluşturabilmek için Avrupa da büyük yatırımlar yapmaktadır. Gelecekte şehirler daha kalabalıklaştığında bu altyapıları sağlamak için yatırımları yapmanın daha zor olacağı düşünülmektedir [12]. Avrupa da şimdiden şehirlerin bu teknolojileri ne kadar kullandıklarına bakılarak akıllılık seviyeleri ölçülmektedir.



Şekil 2.4: Avrupa şehirlerinin akıllılık seviyelerine göre grafiği [12]

Dünyada popüler olan ve bir anlamda gereklilik haline gelmiş bu teknoloji üzerinde kamu bu denli yatırım yaparken, bireyler akıllı şehirlerin bir parçası olan evlerini de akıllı bir hale getirmek adına yatırımlar yapmaktadır. Özellikle son yıllarda verinin online olarak gerçek zamanlı işlenmesi ve makine öğrenimi (machine learning) alanındaki gelişmeler sayesinde bu teknoloji daha da ön plana çıkmaktadır. Bireyler vakitlerinin büyük bir çoğunluğunu geçirdikleri evlerini takip edebilmek, yönetebilmek ve yaşadıkları bu alanlarla adete bir iletişim halinde olabilmeyi istemektedir.

2.2 Akıllı Ev Sistemleri

Evlerde bulunan bazı cihaz ve eşyaların uzaktan izlenebilmesi, programlanabilmesi ve bir ağ ile birbirine bağlı olarak yönetilebilmesini sağlayan sistemler akıllı ev sistemleri olarak adlandırılmaktadır. Akıllı ev sistemleri teknolojisinin amacı, onu kullanan bireylerin güvenli, tasarruflu bir şekilde yaşam standartlarını yükseltmektir. Akıllı ev sistemlerinin altındaki teknoloji, endüstrinin birçok alanındaki kontrol sistemlerinin kişiye özel

ihtiyaç ve istekleri karşılayabilecek şekilde gündelik hayata uyarlanması ile oluşmaktadır.

Akıllı ev kavramı ilk olarak 1984 yılında Amerikan Ev İnşacıları Derneği (American Association of House Builder) tarafından kullanılmıştır. Ancak bu teknolojinin temelleri, 1960 yıllının başlarında meraklılar tarafından, kablolu evler (wired homes) adıyla geliştirilen evlerde atılmıştır [13]. Günümüze kadar yapılan farklı çalışmalarda ev otomasyonu, zeki yapılar, yapı otomasyon sistemi, entegre ev sistemleri gibi terimler akıllı ev terimi yerine kullanılmıştır [14] [15].

İnsanların evlerinde hayatlarını kolaylaştırmak, daha güvenli, daha konforlu ve daha tasarruflu bir yaşama sahip olmalarını sağlamak üzere akıllı evler tasarlanmaktadır. Evlerimizde kullandığımız televizyon, kahve makinesi, elektrik süpürgesi, buzdolabı, çamaşır ve bulaşık makineleri, müzik sistemleri ve bunlar gibi daha birçok cihaz gelişen teknoloji sayesinde hayatımızı kolaylaştırmak için çeşitli değişimler geçirmiştir [16]. Kullandığımız birçok cihazın bu değişimler sayesinde verimliliği ve kalitesi artacaktır.

Akıllı ev sistemini oluşturan cihazların ekosistemi teknoloji açısından kontrol edilebilir, programlanabilir ve yapay zekaya sahip teknolojiler olarak üç kategoriye ayrılabilir.

Kontrol Edilebilir Cihazlar

Evde bulunan cihazları çeşitli kumanda ve komut ile kontrol edebilmeyi sağlamaktadır. Örneğin içinde bulunduğumuz odanın ışıklarını açmak istediğimizde bir kumanda, el çırpması veya ses komutu ile bunu sağlayabiliriz. Bu teknolojide o an orda bulunmak ve bir komut vermek gerekmektedir.

Programlanabilir Cihazlar

Bu kategori altındaki cihazlar zamana ve çeşitli sensörlerden aldıkları bilgilere göre hareket edebilmektedir. Bu cihazlar kullanıcısı tarafından bir senaryo doğrultusunda

da programlanabilmektedir.

Yapay Zekaya Sahip Cihazlar

Bu cihazlar programlanabilir cihazlardan farklı olarak topladıkları çeşitli bilgiler neticesinde bazı kararlar alarak senaryoları kendileri oluşturabilmektedir. Kullanıcının davranışlarını analiz ederek buna göre yorumlayıp bir sonraki adım için en doğru kararı vermeye çalışmaktadırlar. Örneğin eve geliş zamanınızı daha önceki geliş zamanlarınıza göre tahmin ederek, gelmeden önce evi her zaman kullandığınız ısı derecesinde ısıtarak ya da soğutarak gerekli konforu sağlamaktadırlar.

Aile bireylerinin davranışları sırasında düşünmeleri gereken bazı işlemler akıllı ev otomasyonu sistemi tarafından otomatikleştirilip yapılabilmektedir. Örnek olarak bir aile bireyinin evden çıkarken ev otomasyon sistemine vereceği tek bir komut ile aşağıdaki işlemler sırasıyla art arda gerçekleşebilmektedir.

- Aydınlatma sistemleri kapatılacak,
- Televizyon, müzik seti gibi eğlence sistemleri kapatılacak,
- Isıtma ve soğutma sistemleri kapatılacak,
- Su ısıtma cihazı, çay makinesi ya da kahve makinesi gibi aygıtlar kapatılacak,
- Ütü gibi aletlerin elektriği kesilecek,
- Akıllı güvenlik alarmı devreye sokulacak,
- Akıllı güvenlik kamerası hareket anında bildirim gönderecek şekilde ayarlanacak

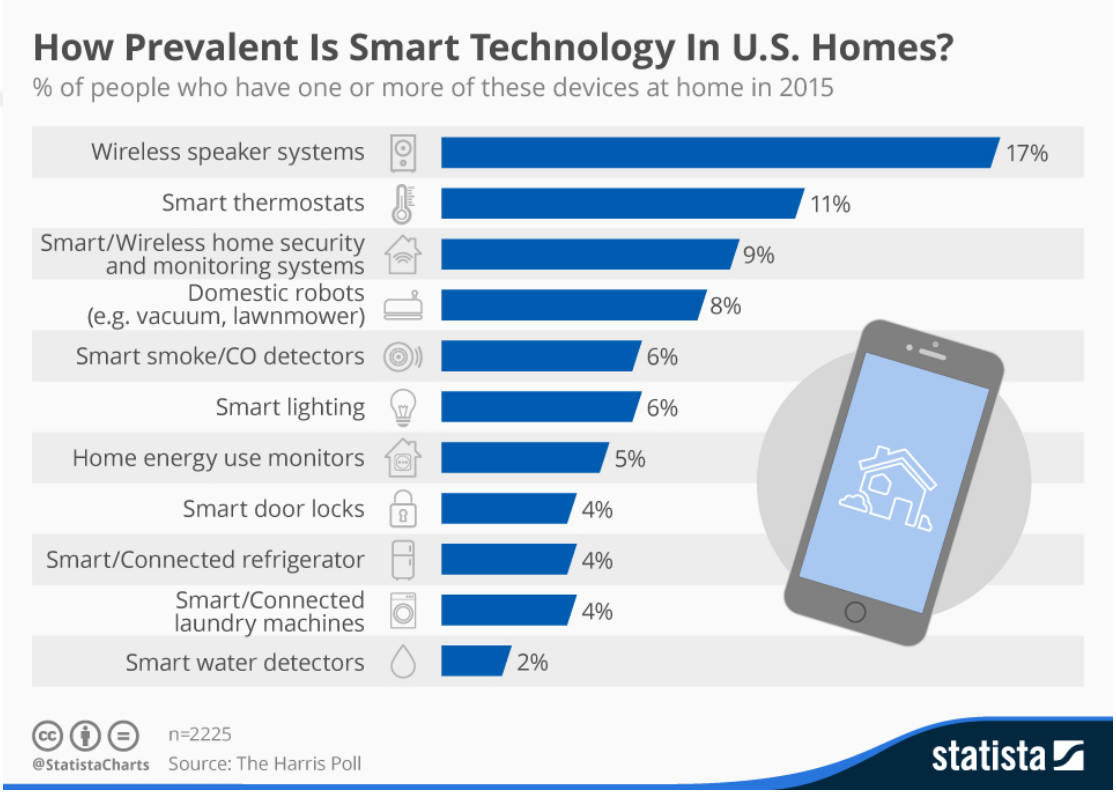
Bireyin kontrol etmesi ve yapması gereken tüm bu işlemleri unutması gibi unsurlar olmadan tek bir evden ayrılma komutu ile otomatik olarak yapılabilmektedir. Ev otomasyon sistemi tüm bu işlem adımlarını birçok komutu arka arkada ilgili akıllı ev aletlerine göndererek yapabilmektedir. Akıllı ev sisteminin sağladığı kolaylıklardan biri olan birçok işlemi arka arkaya gerçekleştirme işlemine akıllı ev sistemlerinde senaryolandırma adı

verilmektedir. Tüm bu senaryoların bir ev otomasyon sistemiyle yapılması ile gereksiz enerji tüketimi en az indirilmiş olacaktır. Bu sayede kullanılan elektronik cihazlar ve aydınlatma sistemlerinin kullanım ömürleri de artacaktır. Bu işlemler akıllı ev sistemi kullanıcılarına hem tasarruf hem de konfor sağlamaktadır.

Akıllı ev sistemi ile yapılabilecek bazı örnek senaryolar aşağıda sıralanmaktadır.

- Sabah uyandığınızda ya da ayarladığınız saatte panjur veya perdeleriniz otomatik olarak istediğiniz seviyede açılabilir, odanız istediğiniz sıcaklık derecesine getirilebilir, çayınız veya kahveniz hazırlanabilir,
- Sensörler yardımıyla evde olmadığınız algılanarak evdeki ısıtma soğutma ve aydınlatma sistemleri kapatılarak enerji tasarrufu yapılabilir, akıllı güvenlik alarmı devreye sokularak ev güvenliği sağlanabilir.
- Uzun seyahatlerde her gün planlanan saatte evin panjurları açılarak evin güneş ışığı alması sağlanabilir, havalandırma sistemleri açılarak ev havalandırılabilir, bahçe sulama sistemi çalıştırılarak bahçe sulanabilir.
- Evde olmadığınız zamanlarda bazı aydınlatmalar sanki kullanıyormuş gibi açılabilir, perdeler gece ve gündüz farkına göre kapatılıp açılabilir, müzik seti açılarak ses sayesinde evde olduğunuz izlenimi verilerek hırsızlara karşı caydırıcı bir etki yaratılabilir.
- Evin içindeki sensörler yardımıyla gaz kaçakları tespit edilerek gaz kesilebilir, su baskını tespit edilerek su vanaları kapatılabilir, duman dedektörleri ile yangın tespit edilerek yangın söndürme sistemleri devreye sokulabilir, kullanıcıya veya ayarlanmış itfaiye gibi yerlere bilgi gönderilebilir.
- Bahçedeki nem sensörleri ile toprağın kuruluk oranı tespit edilerek bitkilere, çiçeklere gerektiği kadar su verilebilir.
- Geceleri sadece bulunduğumuz odalardaki aydınlatma sistemleri gerektiği oranda açılarak hem tasarruf sağlanabilir hem de lambaların ömürleri uzatılabilir.
- Sensörler yardımıyla güneşin batışı algılanarak evin panjurlarının kapatılması ve aydınlatma sisteminin açılması sağlanabilir.

The Harris Poll isimli ABD'deki kamuoyu araştırma şirketi 2015 yılında yaptığı bir araştırmada ABD halkının yüzde 88 inin akıllı ev sistemlerini çok pahalı bulduğunu, fiyatlar düştüğünde kullanmayı düşünen yüzde 37 lik bir kesim olduğunu ortaya koymuştur. Aynı araştırmada akıllı ev teknolojisinin cihaz bazlı olarak ne kadar yaygın olduğu araştırılmıştır. Bu araştırmanın sonucuna göre en yaygın akıllı ev cihazının kablosuz hoparlör sistemi olduğu tespit edilmiştir. Kullanıcıların yüzde 17'si evlerinde kablosuz hoparlöre sahipken, bunu yüzde 11 ile akıllı termostat, yüzde 9 ile akıllı ev güvenlik sistemleri takip etmiştir [17].



Şekil 2.5: 2015 yılında akıllı ev sistemlerinin cihaz bazlı kullanılma oranları [17]

Akıllı ev sistemlerinin kullanıcılara sağladığı faydaların başında seyahat sırasında ya da evde bulunulmadığı durumlarda, uzaktan akıllı cihazları kontrol edebilme kabiliyeti gelmektedir. Bu özellik bazı durumlarda çok önemli ve faydalı olabilmektedir. Örneğin Kasım 2015 tarihinde Güney Avustralya'da çıkan büyük bir yangın bölgede bulunan birçok eve, araziye ve doğal yaşama ciddi zararlar vermiştir. Charles Darwin Üniversitesi'nde rektör yardımcısı olan Profesör Simon Maddocks olayı haberlerden öğrendikten sonra bölgede bulunan evinin güvenlik kameralarına bağlanarak, gördüğü dumanlardan yangının kendi evine yaklaştığını öğrenmiştir. Olay anında binlerce kilometre uzakta olan

profesör çaresizce bahçe sulama sistemini cep telefonundaki yönetim uygulamasından tam kapasite sulama yapacak şekilde çalıştırmış ve alevlerin evine sıçramasını engellemiştir. Bu sayede evini ve arazisini yangınlardan kurtarmıştır[18].

Şekil 2.6: Prof. Simon Maddocks'ın yangını akıllı ev kamerası ile görüntülemesi [18]

Kendi kendine hareket etmesini sağlayan birçok sensör ve toz algılayıcısı ile otonom çalışan, şarjı bittiğinde kendini şarj edebilen elektrik süpürgeleri geliştirilmiştir. Televizyonlar, müzik sistemleri için uzaktan kumandalar üretilmiş, internet üzerinden medya içeriklerine erişim sağlayabilme yetenekleri geliştirilmiştir. Kahve makineleri için zamanlayıcı ve ısı ayarlama teknolojileri geliştirilmiştir. Beyaz eşya olarak adlandırılan makinelere farklı program seçenekleri, otomatik miktar ayarlayarak çalışma özellikleri getirilmiştir. Şimdi ise akıllı ev sayesinde tüm bu teknolojik gelişmeleri bir adım ileri götürerek, tüm cihazların yapay zeka sayesinde bizim alışkanlıklarımızı öğrenebilmeleri, buna göre otonom çalışabilmeleri ve internet üzerinden uzaktan kontrol edilebilmeleri amaçlanmaktadır.

2.2.1 Akıllı Elektrik Sistemleri

Uzaktan kontrol edilebilen akıllı prizler veya elektrik hattına bağlı röle barındıran bazı cihazlar yardımı ile kullanılabilmektedir. Akıllı elektrik sistemleri sayesinde tasarruf sağlamanın yanı sıra, açık unutulmuş olabilecek elektrikli soba, fırın, ütü gibi tehlike oluşturacak cihazlar kapatılarak evin yangına karşı güvenliği sağlanabilmektedir.

Hemen hemen bütün elektrikli cihazlar kullanılmadığı zamanlarda bile prize bağlı olduklarında çok düşük miktarlarda da olsa mutlaka elektrik tüketmeye devam etmektedirler. Örneğin multimedya, tv ve ses sistemi gibi cihazlar kullanıcının kumanda ile açabilmesi için çalışmadıkları zamanlarda uyku modunda tetiklenmeyi beklemektedirler ve elektrik tüketmektedirler. Bu cihazların elektrikleri akıllı elektrik sistemleri sayesinde, ev otomasyonunda uygulanabilecek senaryolar ile kullanılmadığı zamanlar tespit edilerek tamamen elektrikleri kesilebilir ve bu sayede elektrik tüketimi sıfıra indirilebilir.

Kullanıcılar akıllı ev otomasyonu üzerinde evden çıkış modu gibi modlar oluşturarak çalışmasının gerekmediği tüm elektrikli cihazların elektriğini tamamen kesebilir, bu sayede hem yangına karşı güvenlik hem de elektrik tasarrufu elde edebilir. Aynı zamanda evden çıkış sırasında cihazların açık olup olmadıklarını kontrol etmek gibi durumlarda ortadan kalkacağı için zaman tasarrufu da sağlamaktadır.

Akıllı elektrik prizleri ve akıllı sayaçlar sayesinde tüketim verileri grafiklendirilebilir, hangi elektrikli cihazın ne kadar elektriği hangi saat aralıklarında tükettiği gibi bilgiler kullanıcılar tarafından kolayca raporlandırılabilir. Tüketim verilerini raporlar sayesinde inceleyerek kullanıcılar, elektrik tüketim alışkanlıklarını değiştirebilmek için otomasyon üzerinde programlamalar yaparak tasarruf elde edebilir.

2.2.2 Akıllı Aydınlatma Sistemleri

Aydınlatma sistemleri içinde yer alan tüm ışık kaynakları, lambalar kullanıcıların kullanım alışkanlıklarına göre programlanabilmektedir. Kullanım alışkanlıklarına göre sonsuz senaryolar programlanabilmektedir. Örneğin kullanıcı film izlerken tüm aydınlatma

sistemlerinin kapalı olmasını ya da ortamın loş olmasını sağlayabilmektedir. Kitap okurken sadece kitap okuma köşesinde bulunan lambaderin açık olmasını diğer ışıkların kısık olarak çalışmasını sağlayabilmektedir. Yemek yerken yemek masasının aydınlatmasının en yüksek seviyede olmasını, yemek haricinde buraya etki eden aydınlatma sistemlerinin çalışmamasını sağlayabilmektedir. Bunun gibi daha birçok farklı örnekle akıllı ev otomasyonu sayesinde aydınlatma sistemleri kullanıcılara tasarruf imkanı ve konfor sunmaktadır.

Evden ayrılma veya eve geliş gibi durumlar kontrol edilebilmektedir. Evde kimse kalmadığı durumlar hareket sensörleri yardımı ile veya akıllı ev sistemine kullanıcıların talimat vermesi ile tespit edilerek aydınlatma sistemlerinin tamamı veya istenilenleri kapatılabilmektedir. Kullanıcı eve geç bir saatte geldiğinde kapıyı uzaktan kumanda ederek açabilir ve bu sayede evde bulunan aydınlatma elemanları açılarak kullanıcının karanlık bir eve girmemiş olması sağlanabilmektedir [19].

Evde bulunan hareket sensörleri sayesinde kullanıcının ev içindeki hareketlerine göre aydınlatma sistemleri ayarlanabilmektedir. Kullanıcı bu sayede ev içinde gezerken ışıkları kontrol etmek durumunda kalmamış olur ve elektrik tüketiminden tasarruf sağlayabilir.

Özellikle bahçe aydınlatma sistemleri gibi dış aydınlatmalar ışık miktarını ölçen sensörler yardımı ile güneşin batması durumunda otomatik olarak açılabilir, güneşin doğması ile otomatik kapanabilir. Aynı şekilde ışık miktarını ölçen sensörler olmadan da güneşin doğuş ve batış zamanına göre kullanıcı tarafından programlanabilir ve bu sayede ışık kaynakları otomatik olarak kapanıp açılabilir.

Aydınlatma sistemleri aynı zamanda birer güvenlik sistemi elemanı gibi evde olunmadığı durumlarda, kapı önünde bir hareket tespit edilmesi halinde ya da zaman programlı olarak açılabilir bu sadece hırsızlara karşı caydırıcı bir etki sağlayabilir.

2.2.3 Akıllı Isıtma, Soğutma, İklimlendirme ve Havalandırma Sistemleri

Evdeki sıcaklık miktarını, nem miktarını ve hava kalitesini ölçen sensörler sayesinde oluşturulan akıllı ev otomasyonunun bir parçasıdır. Odalarda bulunan akıllı termostatlar sayesinde sıcaklık miktarı ölçülenebilir. Hava sensörleri sayesinde de hava kalitesi ve havadaki nem miktarı ölçülebilir. Evlerde bulunan merkezi ya da bölgesel ısıtma veya soğutma sistemleri sayesinde evde bulunan tüm odaların en uygun şekilde derecelendirilmesi sağlanmaktadır.

Bölgesel ısıtma veya soğutma sistemleri, ev otomasyonu sayesinde en çok kullanılanişl odaları en uygun şart ve maksimum konforda derecelendirmek için kullanılabilir. Evde bulunan odaların güneş ışığını doğrudan ve ne kadar süre aldığına bakılarak yapılan programlamalar ya da sensörlerden gelen verilerin işlenmesi sayesinde odaların dereceleri istenilen seviyede tutulmuş olmakta, güneş ışığından en yüksek seviyede faydalanılmış olmaktadır.

Hava kalitesi havada bulunan oksijen miktarı hesap edilerek, istenilen seviyenin altına düşmesi durumunda havalandırma sistemleri otomatik açılabilir veya kullanıcıya havalandırma yapması yönünde uyarılar verilebilir. İnsan sağlığı ve konfor açısından akıllı ev otomasyonu sayesinde fayda sağlanabilmektedir.

Akıllı oda termostatları ısıtma yapılırken evlerde bulunan kombileri doğalgazın en verimli tüketileceği sıcaklıkta çalıştırabilmektedirler. Bu sayede gereksiz ısıtmanın önüne geçilerek doğalgazdan tasarruf edilmesi sağlanmaktadır. Akıllı oda termostatları sayesinde kullanıcı evde olduğunda evin sıcaklığının sabit tutulmasını sağlayabilmektedir. Gece saatlerinde evdekilerin üşümeden en uygun ısıda yatabilmeleri için evin sıcaklığını hissetmeyecekleri kadar düşürebilmektedir. Evden ayrılma durumunda, eve dönüşte evin ısısının kolayca istenilen değere çıkmasını sağlayabilecek kadar değişmesine müsaade ederek tasarruf sağlanabilmektedir.

2.2.4 Akıllı Perde, Panjur Sistemleri

Evlerde bulunan panjur ve perdeler tek tek veya gruplama yapılarak oda bazlı ya da tümü kapanıp açılacak şekilde senaryolandırılabilir, kontrol edilebilir. Güneş ışığından en çok ve verimli şekilde yararlanılabilmesi için programlandırılabilir. Bu sayede ısıtma ve soğutma sistemlerinin de çalışma sürelerinde etkin rol oynayabilir.

Fırtına durumunda tek bir komut ile çok hızlı bir şekilde pencerelerin tamamının kapatılması sağlanabilir. Bu sayede ısı kaybı ve fırtına sebebiyle eve gelebilecek zararlardan en aza indirilebilmektedir.

Kullanıcıların oluşturduğu seçenekler sayesinde işlem adımları arda arda kolayca uygulanabilmektedir. Örneğin gündüz film izlenmek istendiğinde ortam ışığının azaltılması için film izleme seçeneğini çalıştırılabilir ve bu işlem senaryosu sayesinde ortam ışıkları otomatik olarak azaltılabilir. Kullanıcı ev otomasyonunu film izleme seçeneğine getirdiğinde panjur veya perdeler kapatılarak, ortamın ışığının azaltılması sağlanabilmektedir.

2.2.5 Akıllı Güvenlik Sistemleri

Akıllı güvenlik sistemleri evde olunan veya olunmayan durumlarda ev halkının güvenliğini sağlamak üzere tasarlanmışlardır. Akıllı güvenlik sistemi içerisinde birçok farklı sensor ve cihaz bulunabilmektedir.

Kapı ve pencerelere yerleştirilen manyetik kontaklar sayesinde hangi kapı ve pencerenin ne zaman açılıp kapandığı gibi bilgiler toplanabilir, bu verilere göre değerlendirmeler yapılabilir. Hareket sensörleri ve ev içindeki kameralar sayesinde evin hangi odalarında ne zaman bir ihlalin olduğu tespit edilebilir. Bunların neticesinde alarm sistemleri çalıştırılabilir ve ev halkına veya kolluk kuvvetlerine bildirim gönderilmesi sağlanabilir.

Uygun konumlara yerleştirilen kameralar sayesinde evde bulunulmayan zamanlarda hareket anında görüntüler elde edilerek kullanıcının cep telefonuna bu görüntüler gönderilebilir. Kameralar sayesinde tüm ihlaller evden farklı bir ortama kaydedilebilir, görüntülerin güvenliği sağlanabilir.

Akıllı güvenlik sistemlerinin normal güvenlik sistemlerine oranla daha çok fayda sağladığı kısımlar, ihlallerin nerelerde olduğunun tespiti ve caydırıcılık sağlamalarıdır. İstenilen durum yabancıların biz evde yokken eve girmemelerini sağlamaktır. Geleneksel güvenlik sistemleri yabancılar eve girdikten sonra veya hırsızlık anında alarm sistemini çalıştırarak bir güvenlik sağlamaya çalışmaktadırlar. Ancak akıllı güvenlik sistemleri sayesinde, kötü niyetli kişilerin evde birinin olup olmadığını anlaması zorlaştırılmaktadır. Evde bulunan aydınlatma sistemleri, panjur, perde sistemleri gibi sistemler evde birisi olduğunda çalıştığı şekilde çalışmaya devam ederek hırsızlara karşı bir caydırıcılık sağlamaktadırlar. Örneğin uzun süreli seyahatlerde uygulanan senaryolar ile evde bulunan müzik sistemi günün belirli saatlerinde devreye girerek ses olmasını sağlayabilir, günün belirli saatlerinde aydınlatma sistemleri açılıp kapatılabilir, gece ve gündüz olması durumuna göre panjur, perde sistemleri kapatılıp açılabilir, bu sayede ev biz yokken sanki evde biri yaşıyormuş gibi dışarıdan gözükebilir.

Sıvı tespit sensörleri sayesinde evde su basması durumunda sıvı algılanabilir ve su borusu valfi kapatılarak su akışı kesilebilir ve su basması engellenebilir. Gaz sensörü sayesinde evde kullanılan gazdan herhangi bir sızıntı veya kaçak olması durumunda gaz valfi gaz borusundaki gazı keserek herhangi bir yangını engelleyebilir.

Akıllı güvenlik sistemi sayesinde evde herhangi bir duman tespit edildiğinde sistem yangının sönmesi için gerekli senaryonun adım adım uygulanmasını sağlayabilir. Örneğin duman tespiti sonrasında gaz akışını keserek gazın tehlike oluşturmasını engelleyebilir, hava tahliye fanlarını çalıştırarak dumanın evden atılmasını sağlayabilir, siren sistemleri ve mobil aygıtlara gönderilen bildirimler sayesinde kullanıcının durumdan haberdar olması sağlanabilir.

Havuz bulunan evlerde yüzme bilmeyen küçük çocukların havuza düşmesi ihtimali ebeveynleri tedirgin eden bir durumdur. Bu gibi istenmeyen durumların oluşmaması için havuzlara eklenen su hareket sensörü gibi sensörler sayesinde havuza girilmeyen zamanlarda havuz alarm moduna getirilebilir. Havuz alarm modundayken havuza girilme anında alarm sistemi devreye sokulabilir ev halkına bilgilendirme yapılabilir. Bu sayede hem küçük çocukların havuza düşmesi durumunda müdahale edilebilir hem de seyahat halindeyken istenmeyen yabancı misafirlerin havuza girişinden haberdar olunabilir.

2.3 Akıllı Ev Sistemlerinde Kullanılan İletişim Teknolojileri

Akıllı ev sistemlerde kullanılan nesnelerin interneti olarak adlandırılan cihazların birbirleri ile çalışabilmesinde kilit rol oynayan iletişim protokolleridir. Bu protokoller sayesinde cihazlar arasında iletişim kurulmaktadır. Bu protokollerin vazgeçilmez bazı özelleri olması gerekmektedir. İletişim menzili, güç tüketim verimliliği, güvenlik ve hızlı iletişim en önemli konulardır. Bu konular doğrultusunda birçok farklı protokol geliştirilmiş ve geliştirilmeye devam etmektedir.

Özellikle güç tüketim konusu en önemli konulardan biridir. Cihazlar genellikle bir güç kaynağına bağlı olmadan evin farklı noktalarına konumlandırılabilir ve kolaylıkla konumları değiştirilebilmelidir. Dolayısıyla bir güç kaynağına bağlı olmadan pil teknolojisi ile beslenebilir olmaları önemlidir. Bu durumda ne kadar az güç tüketerek çalışırlarsa o kadar uzun süre kullanılabilir olmaktadırlar. Sürekli pil değiştirmek kullanıcının konforunu ve cihazların sürekli kullanılabilir olmasını etkilemektedir.

Protokollerde verinin şifreli ve güvenli bir şekilde gönderilmesi de önemli olan konulardan biridir. Sensörler elde ettikleri verileri iletirken bu verilerin bütünlüğünü ve doğruluğunu teyit edecek şifreleme yöntemleri ve güvenli bağlantı seçeneklerini kullanmalıdır. Protokollerde aranan bir diğer özellik sensörlerin topladıkları verileri en hızlı ve veri yapısı bozulmadan en kayıpsız şekilde ana yönetim konsoluna ya da diğer cihazlara iletmesidir. Bu sayede toplanan veriler anlık işletilebilir ve gerekli adımlar sırasıyla yapılabilir.

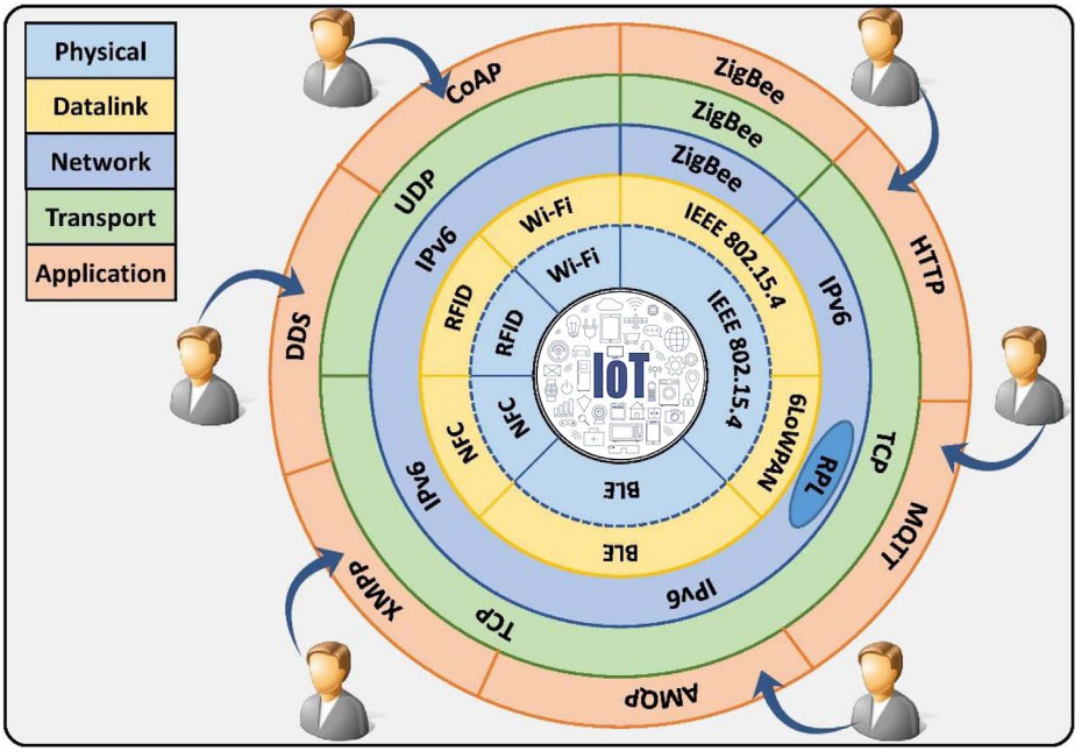
İletişim protokollerinin ortaya çıkmasında IEEE 802.15.4 standardı önemli bir rol oynamaktadır. Bu standartta iletişim noktadan noktaya ve yıldız topolojisi kullanılarak dizayn edilmiştir. Merkezde iletişimi koordine eden bir koordinatör cihaz bulunmaktadır. Diğer cihazlar bu koordinatör cihaz ile noktadan noktaya bağlantı kurarak iletişimi sağlamaktadırlar. Bu standart düşük hızda ve düşük güç tüketimine uygun ortamlarda sistemin çalışabilmesini sağlamaktadır.

Smart home applications		*Requirements*							*Recommended wireless technology*
		Low power	*Low cost*	*Security*	*Range*	*Topology*	*Network density*	*Throughput*	
Home automation	*Lighting*	+-	+	+-	PAN/LAN	p2p, star, mesh	+	Low	ZigBee, BLE, Bluetooth, Z-Wave, ANT, WiFi HaLow, WiFi
	HVAC	+-	+-	+-	PAN/LAN	p2p, star, mesh	+-	Low	ZigBee, BLE, Bluetooth, Z-Wave, ANT, WiFi HaLow, WiFi
	Security	+-	+	+	PAN/LAN	p2p, star, mesh	+	Low, upper medium	- ZigBee, BLE, Bluetooth, Z-Wave, WiFi HaLow, ANT, WiFi (low) - Bluetooth, WiFi (upper medium)
Energy management		-	+-	+	LAN	p2p, star	+-	Low	ZigBee, WiFi, WiFi HaLow, Bluetooth, Z-Wave, BLE, ANT
Entertainment		+-	+-	+-	PAN/LAN	p2p, star	+-	Upper medium, high	- Bluetooth, WiFi (upper medium) - WiFi (high)
Wearables		+	+	+-	BAN/PAN	p2p, mesh	-	Low	BLE, ZigBee, Z-Wave, Bluetooth

Şekil 2.7: Cihazlara bağlı olarak önerilen kablosuz teknolojiler [20]

Şekil 2.7. de kablosuz iletişim teknolojilerinin kullanım alanlarına bağlı olarak uygunluklarına göre sıralanmış bir tablosu yer almaktadır. Bu tabloda kablosuz iletişim teknolojileri güç tüketimleri, maliyetleri, güvenlik düzeyleri, verimlilikleri ve kullanım alanlarına göre teknolojileri analiz edilerek listelenmiştir. Örneğin aydınlatma sistemleri, ısıtma soğutma ve iklimlendirme sistemleri gibi akıllı ev teknolojileri için zigbee ve bluetooth

uygunken, güvenlik kameraları gibi yüksek veri trafiği gerektiren durumlarda wifi iletişim teknolojisinin kullanımı daha uygun olmaktadır [20].



Şekil 2.8: Akıllı ev sistemlerinde kullanılan iletişim teknolojileri ve protokolleri (Değiştirilerek alınmıştır.) [21]

Zigbee, Z-wave, bluetooth ve wifi gibi iletişim teknolojileri akıllı ev sistemlerinde kullanılan cihazların temel teknolojilerini oluşturmaktadır. Akıllı ev sistemlerinin güvenliğini ve kullanılabilirliğini doğrudan etkileyen bu iletişim teknolojileri bu bağlamda kilit rol oynamaktadır. Akıllı ev sistemlerinde en çok kullanılan kablosuz iletişim teknolojileri olan zigbee, z-wave, bluetooth ve wifi teknolojileri detaylı olarak incelenecektir.

2.3.1 Z-wave ve Zigbee

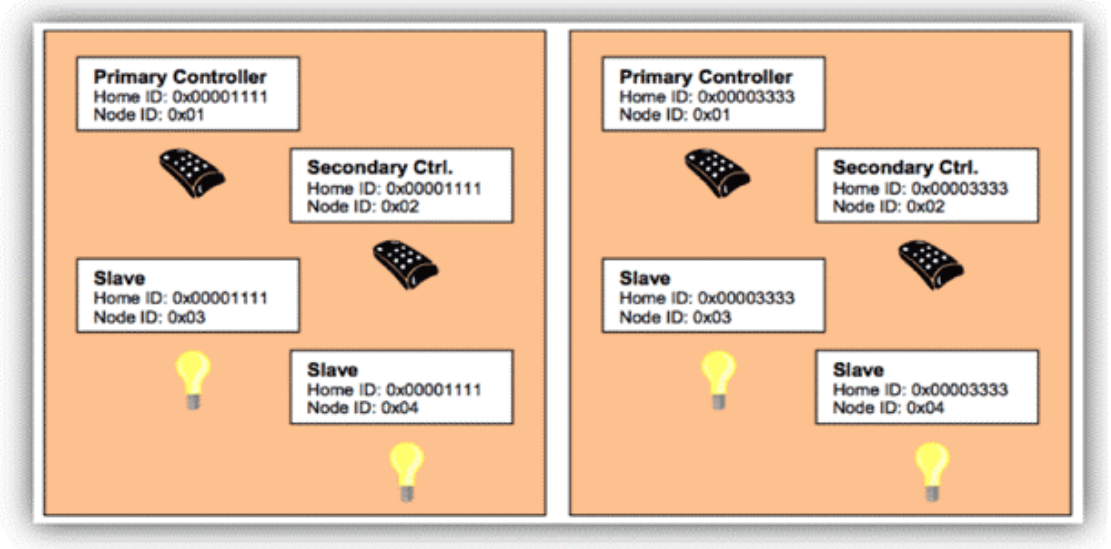
Zigbee IEEE 802.15.4 standardını kullanan bir iletişim protokolüdür. Düşük güç tüketimi ve düşük oranda veri iletimi için uygun bir protokoldür. Herhangi bir veri alışverişi olmadığı durumlarda cihazları ve koordinatör cihazı uyku modunda bekleterek bu sayede çok düşük oranlarda güç tüketimi kullanabilmektedir.

Zigbee, bluetooth ve wifi gibi 2.4 GHZ ISM frekans bandını kullanmaktadır. Aynı ortamda kullanılan wifi ve bluetooth sayesinde aynı frekans bandını kullandığı için yoğun parazite maruz kalabilmektedir. Z-wave akıllı ev sistemlerinde kullandığı frekans nedeniyle daha çok tercih edilmektedir. Avrupa da 868 MHz RFID bandını kullanmaktadır. RFID radyo frekansı sayesinde zemin ve duvar gibi engellerden kolayca geçebilen bir protokoldür.

Temel olarak iki güvenlik algoritması kullanmaktadır. Bunlar İleri Düzeyde Şifreleme Standartı AES ve Mesaj Denetleme Kodu MAC algoritmalarıdır. Zigbee sistemlerinde İleri düzey şifreleme tekniği AES 128 bit olarak kullanılmaktadır. Ayrıca zigbee sistemlerinde doğrulama tekniği kullanılmaktadır, bu teknik sayesinde iletilen mesajın doğru yere iletilip iletilmediği kontrol edilebilmektedir. Doğrulama tekniği sayesinde saldırganın aygıtı başka bir aygıtmış gibi göstermesi önlenebilmektedir [22].

Zigbee kısa mesafede birbirine bağlanacak ve iletişim kuracak birçok cihazda düşük güç tüketim avantajı sayesinde tercih edilmektedir. Zigbee aynı zamanda maliyeti düşük, uygulanabilirliği ve gelişletilebilmesi kolay bir kablosuz haberleşme protokolüdür.

Z-wave kısa gecikmelerle küçük veri paketleri göndermek için geliştirilmiş bir iletişim teknolojisidir. İletişim menzili 30 metreye kadar çıkabilmektedir. Z-wave kullanılan ağlarda iki kimlik tanımlaması olmaktadır. Bunlar ortam kimliği ve cihaz kimliğidir. Ortam kimliği, sadece o ağda bulunan cihazlar arasında kullanılan kimlik bilgisidir ve aynı ağdaki cihazların başka cihazlarla iletişim kurmasını engellemek için kullanılır. Cihaz kimliği ise her cihazın kendisine ait benzersiz bir kimlik bilgisidir. Cihaz kimlikleri aynı olsa bile farklı ortam kimliklerine sahip cihazlar farklı networkte çalışmaktadır ve birbirleri ile çakışmamaktadır [23].



ŞEKIL 2.9: Z-wave cihaz kimliklerine göre farklı ağlarda çalışma şekilleri [23]

Bu protokolde cihazlar, iletişim kurmak için ağ anahtarı kullanmaktadırlar. Z-wave ağına yeni bir cihaz eklenmek istendiğinde cihazlar arasında ağ anahtarı paylaşılmaktadır. Gönderilen ilk paketler şifrelenmemiş ve saldırganların açık bir şekilde yakalayabileceği paketlerdir. Bu paketler içinde ortam ve cihaz kimliklerini barındıran paketlerdir [24].

2.3.2 Wireless (Wifi)

Wifi IEEE 802.11 protokolüne bağlı olarak standartlaştırılmış bir kablosuz iletişim teknolojisidir. Wifi çok yüksek bant genişliğinde veri iletimi yapabilirken yüksek enerji tüketimi nedeniyle genellikle bina ve açık alanlarda internete bağlanmak için kullanılmaktadır. Sadece wifi tabanlı bir akıllı ev sistemi geliştirilebileceği gibi akıllı ev sistemlerinin merkez kontrol noktalarını kontrol etmek ya da belirli görevler içinde kullanılabilen bir kablosuz iletişim teknolojisidir.

Wifi açık alanda 300 metre menzil mesafesine kadar çıkabilmektedir. Frekans olarak 2.4 Ghz ve 5 Ghz frekans değerlerinde çalışabilmektedir.

Genellikle yüksek veri iletimi gerektiren durumlarda akıllı ev sistemlerinde en çok tercih edilen iletişim teknolojisidir. Video akışı gibi güvenlik kameralarının ihtiyaç duyduğu yüksek veri iletimi durumlarında ve dosya transfer durumlarında yüksek veri iletimi sayesinde en uygun seçenek olmaktadır. Wifi teknolojisi en çok kullanılan akıllı ev sistemlerinin güvenliğinde çok önemli bir konumda rol oynamaktadır. Akıllı ev sistemi oluşturulurken kullanılan sensörler wifi teknolojisini kullanmasalar bile akıllı ev sisteminin ana omurgası olan yönetim cihazı genellikle wifi teknolojisini kullanmaktadır. Kablosuz ağ bağlantısı için kullandığımız wifi tüm ağ bağlantımızı ve bu bağlantıyı kullanan tüm aygıtlarımızı tehdit edebilecek bir konumda bulunmaktadır.

Akıllı ev sistemlerine wifi üzerinden gelebilecek tehditler Rusya bilgi güvenliği veri bankası tarafından aşağıdaki şekilde listelenmektedir [25].

- Yetkilendirilmiş bir kablosuz aygıtın tekrar yetkilendirilebilmesi tehditi,
- Kablosuz kanal üzerinden sisteme yetkisiz erişim sağlanabilmesi tehditi,
- Ağ üzerinde aktarılan verinin kablosuz ağ sayesinde ele geçirilebilmesi tehditi,
- Kimlik doğrulama prosedürünün atlanarak kablosuz ağa bağlantı tehditi,
- Kablosuz bağlantı yapan cihazın veya kablosuz bağlantı erişim noktasının (access point) değiştirilme tehditi,
- Kablosuz cihaz sahibi hakkında kişisel bilgilerin ele geçirilmesi tehditi

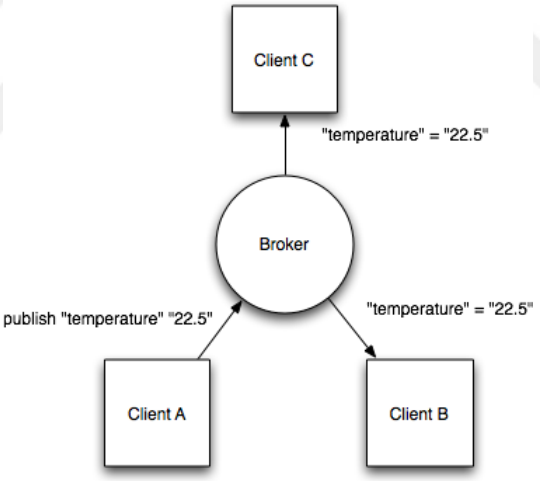
2.3.3 Bluetooth

Bluetooth, 1994 yılında Ericsson firması tarafından geliştirilmiştir. Mobil cihazlar arasında kullanılan RS-232 ye alternatif olarak kablosuz iletişimi sağlamak için geliştirilmiş bir teknolojidir. Bluetooth 2.4 GHZ ISM frekans bandında çalışmakta ve veri aktarım hızı 54 mbps ye kadar çıkabilmektedir. Geliştiriciler enerji verimliliği için çalışmalarında veri aktarım hızını 0.3 mbps ye düşürerek güç tüketimini olabildiğince aşağıya çekmeyi başarmışlardır. Bu düşük güç tüketimli bluetooth modeline Bluetooth Low Energy adını vermişlerdir [26].

2.3.4 MQTT (Message Queuing Telemetry Transport)

Mesaj gönderme odaklı bir haberleşme protokolüdür. Cihazlardan birinden üretilen veri mesaj olarak öncelikle haberleşme trafiğini kontrol eden yönetici cihaza (broker) gönderilmektedir. Haberleşme trafiğini kontrol eden yönetici tarafından da abone olan aygıtlara online olduklarında mesaj iletilebilmektedir. MQTT asenkron (eş-zamansız) iletim yapan bir haberleşme protokolüdür.

MQTT ilk olarak IBM tarafından geliştirilmiş fakat şuan açık olan bir standarttır. Gizliliği sağlamak için veri TCP bağlantısı SSL / TLS ile şifrelenerek iletilmektedir. Düşük menzilli, düşük güç kullanan ve düşük bellekli yapılarda cihazlar arası haberleşme protokolü olarak kullanılmaktadır. Mesaj iletim hızı gerçek zamanlı olarak milisaniye sürelerde gerçekleşmektedir.



Şekil 2.10: MQTT mesaj iletim ağı grafiği [27]

Kullanım alanlarından bir örnek vermek gerekirse Facebook online mesajlaşma uygulaması olan Facebook Messenger da MQTT protokolünün sağladığı özellikleri kullanmaktadır [28].

2.4 Akıllı Ev Sistemlerinde Güvenliğin Önemi

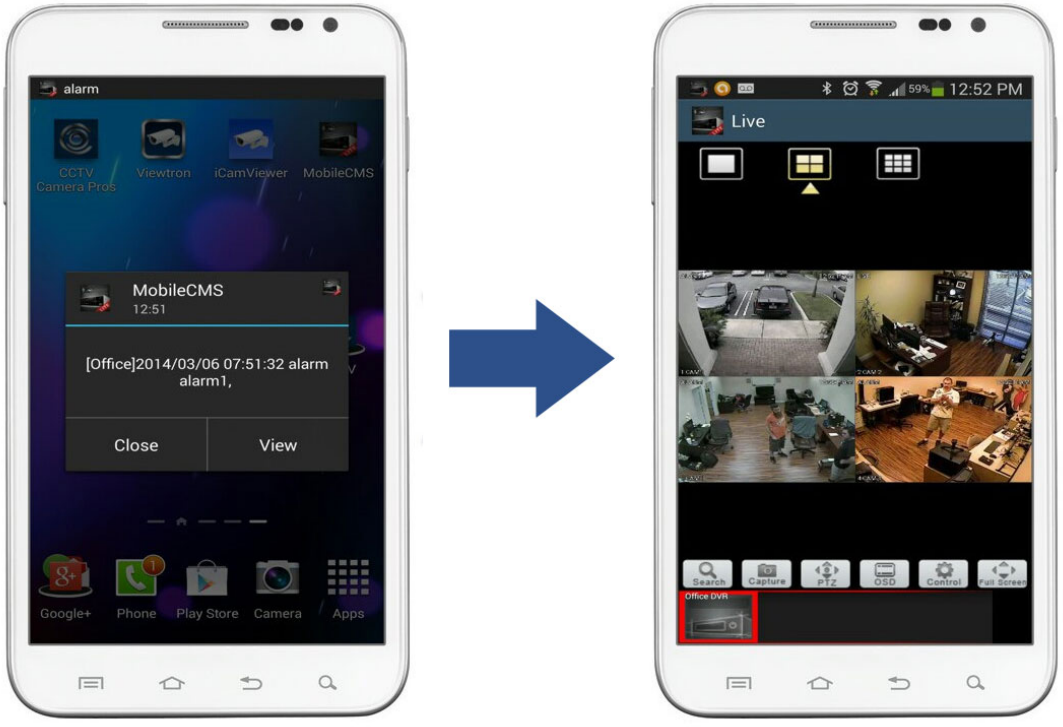
İnsanlar varoluş gereği evlerinde aile bireyleri ile birlikte mahremiyet çerçevesi içinde huzurlu ve konforlu şekilde yaşamayı arzulamaktadırlar. Evlerimizin temel özelliklerinden birisi herkes tarafından dışardan erişilebilir olmaması ve bizim mahremiyetimizi sağlamalarıdır. Mahremiyetimiz ve gizliliğimiz için evlerimizin içinin ve evdeki yaşantımızın dışarıdan gözükmemesini sağlamaya çalışmaktayız. Evlerimizde kullandığımız perde ve panjurlar bunun en büyük örneklerinden biridir. Her bireyin kendine ait başkaları tarafından bilinmesini ve görünmesini istemediği mahrem yönleri, davranışları vardır. Kişiler bu mahremiyetlerini sağlayabildiklerinde huzurlu olmaktadır.

Teknolojinin yaygınlaşması ile insanlar, hayatı kolaylaştırmak ve konfor sağlamak için teknolojiyi hemen hemen hayatın birçok yerinde aktif olarak kullanmaya başladılar. Bununla birlikte özellikle son yıllarda insanlar evlerinde akıllı ev sistemlerini kullanmaktadırlar. Başlangıçta güvenlik için kullanılan kamera, hareket sensörü gibi temel güvenlik cihazları artık akıllı bir nesnelerin interneti aygıtına dönüşmektedir. Tüm bu akıllı ev cihazlarının sağladığı sayısız nimetin yanı sıra bu cihazların güvenliği gözden kaçırılmaması gereken bir konudur.

Evlerde mahremiyeti temel olarak perdelerimizi kapatarak sağlamaktayız. Aslında burada ki temel mahremiyet riski dışardan evimizi görebilecek sınırlı kişilerin görmemesini sağlamaktır. Salonumuzun ortasına bakan bir güvenlik kamerasının üzerinde bulunan zafiyet sayesinde, dışarıdan sayısını dahi tahmin edemeyeceğimiz kişiler salonumuzun mahremiyetini bozabilmektedir. Burada ihlal edilen aslında sadece mahremiyet değildir. Bu kişilerin bu görüntüleri ne amaçlarla kullanacağı tahmin edilememektedir. Somut olarak o an kamerayı kimin izlediğini bilmediğimiz için aslında bu tip cihazların güvenliklerini çoğu zaman göz ardı edilmektedir.

Eskiden evlerin ve iş yerlerinin güvenliğini sağlamak için kullanılan analog güvenlik kameraları ip güvenlik kameralarına oranla daha güvenli bir yapıdaydı. Fakat bu kameralar

sadece yerel depolama kayıt ünitelerine bağlanarak kamera görüntülerini oraya depolamaktaydı. Bu durum kullanıcılar için fiziksel bir güvenlik riski oluşturmaktaydı. Hırsızlar güvenlik kameralarını gördüklerinde bu kameraların kayıt ünitelerini bularak, onlara zarar veriyor ya da onları da çalışıyor ve bu şekilde güvenlik kameralarının içindeki kendi görüntülerini imha etmiş oluyorlardı. Bu gibi durumlarda geriye dönük inceleme çoğu zaman yapılamamakta ve güvenlik ihlallerini tespit etmek amacı ile bulunan güvenlik kameraları hiçbir işe yaramamaktadır. Gelişen teknoloji ile birlikte analog güvenlik kameraları yerlerini ip kameralara bırakmışlardır. İp güvenlik kameraları güvenlik görüntülerini fiziksel olarak orada olmayan başka bir ortama ya da bulut bir depolama alanına kayıt edebilmektedir. Kullanıcılar istediklerinde internet üzerinden mobil uygulamalar ya da web sayfalarından bu görüntülere erişip canlı olarak görüntüleri izleyebilmektedir. Hatta ip kameralar hareket analizi yapıp bir ihlal olduğunu tespit ederek, sadece bu güvenlik ihlaline ait görüntüleri kullanıcıların mobil cihazlarına bildirim şeklinde göndererek kullanıcıları bilgilendirebilmektedir.

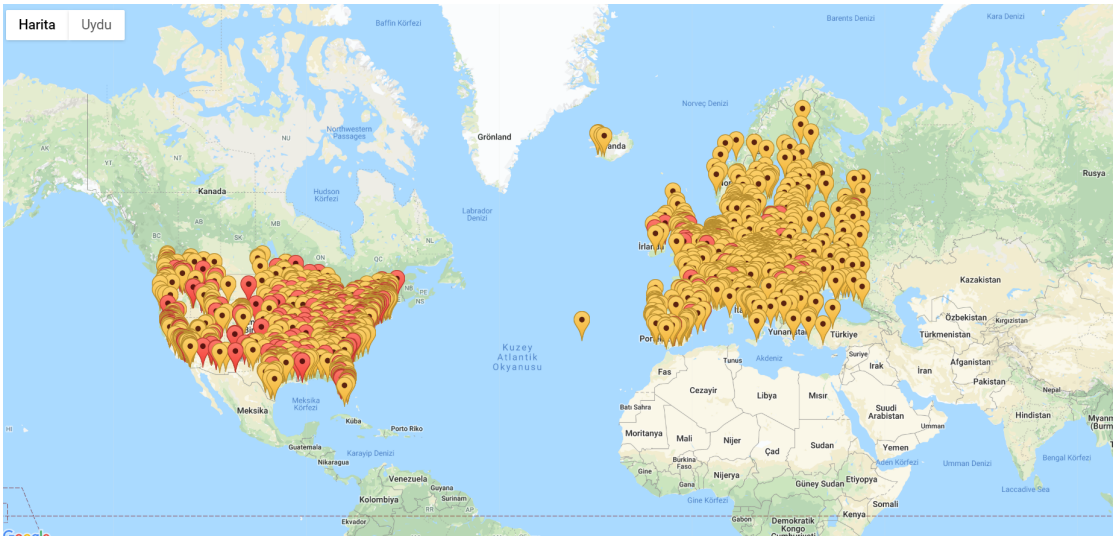


Şekil 2.11: Akıllı güvenlik kamerasının mobil uygulama üzerinden hareket yakalama bildirimi [29]

Kullanıcıların kullanımını kolaylaştırmak için yapılan bir takım kolaylık çoğu zaman güvenlik ihlaline sebep olmaktadır. İp güvenlik kameraları tak çalıştır tarzında kurgulandıkları için kullanıcılar tarafından daha sonra güvenlik ayarları yapılmadığı taktirde ciddi güvenlik açıklıklarına sebebiyet vermektedirler. Kameraların varsayılan olarak verilen şifreleri değiştirilmediği takdir de internet üzerinden anonim olarak izlenebilir hale gelmektedirler.

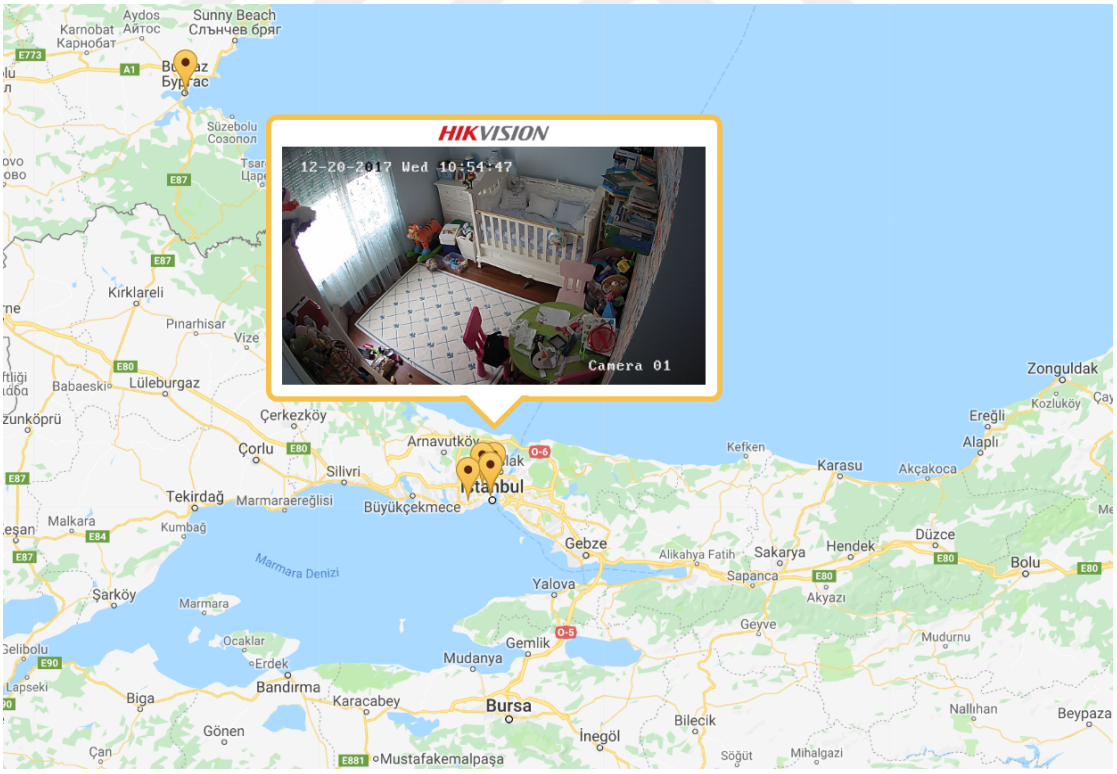
Akıllı ev sistemleri içinde en çok tercih edilen ürünlerden biri de akıllı televizyonlardır. Akıllı televizyonlar birçok uygulama barındırmakta ve usb üzerinden multimedya görüntülerini açabilmektedir. Bu sayede barındırdığı uygulamalar ya da usb üzerinden bilgisayar korsanları tarafından ele geçirilebilmektedir. Bazı akıllı televizyonların üzerinde bulunan mikrofon ve kamera kullanıcının bilgisi olmadan bilgisayar korsanları tarafından aktif edilerek ortamın görüntü ve ses kaydı alınabilmektedir. Bunun yanı sıra akıllı televizyonların içlerinde barındırdıkları bilgisayar, bilgisayar korsanlarının kullandığı fidye yazılımları tarafından ele geçirilebilir ve televizyonun tekrar kullanılabilir hale getirilmesi için fidye talebinde bulunulabilir [30].

2014 sonrası üretilen bütün Hikvision ve aynı firma tarafından üretilen diğer akıllı güvenlik kameralarında yetkilendirilmiş bir kullanıcı olmadan oturum açma sayfaları atlanarak akıllı kameralara yönetici olarak oturum açmayı sağlayan bir zafiyet bulunduğu 2017'de tespit edilmiştir. Akıllı güvenlik kameralarının ip adreslerine '?auth=YWRtaW46MTEK' uzantısı eklenerek güvenlik kameraları ele geçirilebilmiştir. Bu zafiyet sayesinde dünyada kullanılan aynı zafiyete sahip bütün akıllı güvenlik kameraları ele geçirilmiş ve bulundukları konumlara göre bir harita oluşturulmuştur [31].



Şekil 2.12: Ele geçirilen akıllı güvenlik kameralarının bulunduğu konumlara ait harita[31]

Yönetimi ele geçirilen akıllı güvenlik kameralarının görüntüleri kaydedilerek harita üzerindeki konumlara yerleştirilmiştir.



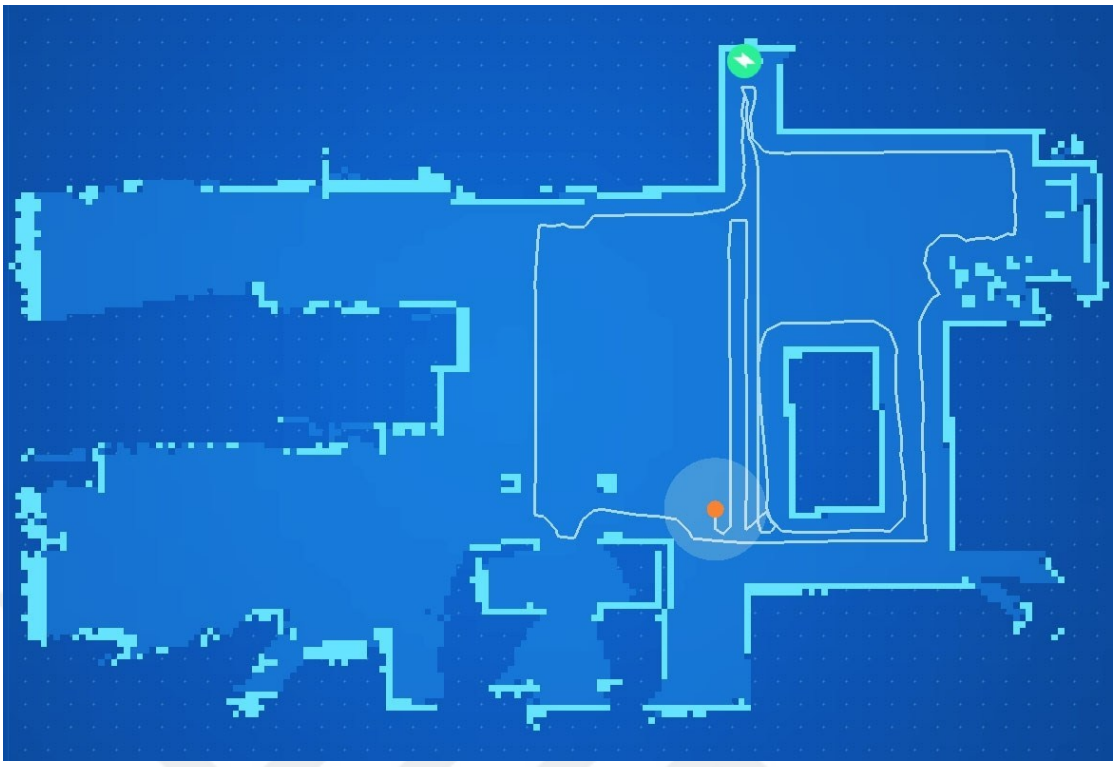
Şekil 2.13: Ele geçirilen akıllı güvenlik kameralarından birine ait örnek görüntü [31]

Kaspersky Labs tarafından 2014 yılında evlerde kullanılan akıllı tv ve depolama cihazlarından birkaçına güvenlik açıklığı testi uygulanmıştır. Bu test sonuçlarına göre kullanıcıların mahremiyetini tehdit edebilecek ciddi güvenlik zafiyetleri tespit edilmiştir. Cihazların çok basit varsayılan şifrelere sahip oldukları, bu şifreleri düz metin şeklinde depoladıkları ve yanlış yetki izinlerine sahip oldukları tespit edilmiştir. Akıllı televizyonlara ortadaki adam saldırısı (man in the middle) yapılarak televizyonun üretici firmasının sunucuları ile televizyon arasındaki trafiğin şifreli olmadığı gözlemlenmiştir. Bu zafiyet dolandırıcılara, televizyonun market uygulaması üzerinden uygulama satın alınırken kredi kartı bilgilerinin ele geçirilmesinin yolunu açmaktadır. Akıllı televizyonun kullandığı küçük resimler ve pencere araçları (widget) şifreli bağlantı olmadan, sunucu tarafından sağlandığı için bu içerik ortadaki adam saldırısı ile değiştirilebilmektedir. Bu sayede içeriklerin içine zararlı java kodları enjekte edilerek akıllı televizyon bu java kodunu çalıştırdığında ele geçirilebilmektedir [32].

Gelişen teknoloji ile birlikte süpürgenin yerini yavaş yavaş alan akıllı robot süpürgeler evlerde kullanılmaya başlamıştır. Bu akıllı robot süpürgelerin çalışma mantığı odanın bir köşesinde bulunan şarj istasyonunda şarj olduktan sonra ayarlanan zamanlarda oda ya da ev içinde dolaşarak altında bulunan kollar ve çekiş gücüyle tozları süpürmektir. Akıllı robot süpürge odalar arasında dolaşırken evde bulunan eşyalara çarpmamak için eşzamanlı yerelleştirme ve haritalama (SLAM) teknolojisi kullanmaktadır. Bu teknoloji sayesinde evlerin birer haritasını çıkartmaktadır. Bunun yanı sıra üzerinde bulunan düşük çözünürlüklü kamera ile hangi odanın ne için kullanıldığını ayırt edebilmektedir. Akıllı ev sistemleri teknolojisinde bir süpürge olarak kullanılan bir robot bile birçok kritik bilgi barındırmaktadır.

Akıllı robot süpürge üreticilerinden Roomba nın yöneticisi akıllı robot süpürgelerinin evlerde çalışarak oluşturduğu harita verilerini akıllı ev sistemi teknolojisi geliştirmekte birlikte çalıştıkları firmalara satacaklarını açıklamıştır [34].

Akıllı kapı kilitleri, akıllı ev sistemleri kullanıcılarının anahtar taşıma zorunluluğunu ve anahtar kaybetme endişelerini ortadan kaldırdığı için tercih ettikleri bir akıllı ev sistemi cihazıdır. Bu cihazların kullanıldıkları konum gereği evin fiziksel güvenliğinin en önemli



Şekil 2.14: Bir akıllı robot süpürgenin oluşturduğu örnek ev haritası [33]

elemanlarından biri olmaktadırlar. Akıllı kapı kilitleri aynı zamanda kullanıcının evde olup olmadığını, ne zaman eve geldiğini ya da ne zaman evden ayrıldığını takip etmek amacıyla da kötü niyetli kişiler tarafından ilk olarak incelenecek akıllı cihazlardan biridir. Akıllı kapı kilitlerinde bulunan herhangi bir zafiyet sayesinde kapı kilitlenemeyebilir, kilitlenen kapı açılabilir ve hatta kötü niyetli kişiler evin sahibi gibi eve girip çıkabilir.

Araştırmacı elektrik mühendisi olan Anthony Rose ve Ben Ramsey test ettikleri farklı markalardaki 16 akıllı kapı kilidinin 12 tanesini buldukları zafiyetler sayesinde yetkisiz bir şekilde açmayı başarmışlar. Yaptıkları inceleme sonucunda bu kilitleri açmanın çok zor olmadığını ortaya koymuşlardır. Elde ettikleri sonuçlara göre bazı modeller şifreleri düz metin olarak iletmekte oldukları için bir bluetooth veri yakalama cihazı ile bu şifreler ele geçirilebiliştir. Bazı cihazlara düz metin olarak gönderilen veri sayesinde de mevcut şifrelerin değiştirilebildiğini bu sayede cihaz kullanıcılarının kapıyı sökerek kilidin pilini çıkarmaktan başka bir şekilde şifreyi sıfırlayamadıklarını gözlemlemişlerdir. Şifreleme standartlarına sahip olan bazı kapı kilitlerinin ise hatalı şifreleme standardında bir veri gönderildiğinde arıza durumuna geçtiklerini ve kapı kilidinin arıza durumunda açıldığını gözlemlemişlerdir. Burada var olan vahim durum ise bu güvenlik açıklıklarının

tespiti değil, bu zafiyetleri üretici firmalara raporladıklarında bu raporların dikkate alınmamasıdır. Hatta bazı firmalar tarafından yapılan geri dönüşlerde bulunan zafiyetin bilindiğinin fakat bulunla ilgili bir geliştirme veya bir işlem yapılmayacağı söylenmiştir [35].

Akıllı ev sistemlerinde kullanılan cihazların çoğu her zaman açık şekilde ve internete sürekli bağlı haldedirler, dolayısıyla internet üzerinden veya fiziksel olarak yakın konumdayken potansiyel saldırılara karşı her zaman açık durumdadırlar. Herhangi bir zafiyetin varlığı ve bu zafiyetin bilgisayar korsanları tarafından keşfedilmesi sonucunda istenmeyen durumlar oluşabilmektedir. Zafiyeti kullanan bilgisayar korsanı tarafından akıllı ev sistemlerine erişim engellenebilir, bilgisayar korsanı olan kötü niyetli kişiler tarafından sistemde var olan kritik veriler ele geçirilebilir, akıllı ev sistemi başkasının kontrolüne geçebilir ve cihaz sahibinin o kişi olması sağlanılabilir, akıllı ev sisteminin tümüne ya da akıllı ev sisteminin bazı cihazlarına zarar verilerek cihazlar kullanılmaz hale getirilebilir. Bunların yanı sıra bir model üzerinde keşfedilen bir zafiyet sayesinde aynı üretici firmanın ürettiği aynı cihazların ya da aynı zafiyeti barındıran farklı cihazlarının tespiti ile cihazların birçoğuna erişilerek toplumsal zararlara sebebiyet verilebilir. Örneğin bir kapı kilidinin bir zafiyet sonucu açılabildiği tespit edilirse bu kapı kilidini kullanan aynı mahalledeki kullanıcıların tümüne çok kısa bir süre içerisinde zarar verilerek toplumsal bir olaya sebebiyet verilebilir.

ABD nin Springfield şehrinde yaşayan Marcus, bluetooth ile kontrol edilebilen bir akıllı kapı kilidini bir tablet üzerinde bulunan sesli asistan yardımı ile sesli komutlar göndererek açıp kapatabildiği bir akıllı ev sistemi kurmuştur. Burada bulunan ses tanıma teknolojisinin zafiyeti sayesinde komşusu evin dışından akıllı sesli asistana kapıyı açması için bağırmış ve akıllı asistan bu sesi evin sahibinin sesi olarak algılayıp kapının kilidini açmıştır [36].

Akıllı ev sistemlerinde sistemin her bir elemanı olan cihaz veya sensörler aracılığı ile birçok kişisel veri toplanmakta ve işlenmektedir. Akıllı ev sistemlerinde güvenliğin önemi konusunda bu kişisel verilerin gizliliği gelmektedir. Bu kişisel veriler kullanıcının kullanım alışkanlıklarının yanı sıra evde olup olmadığı gibi bilgileri de barındırmaktadır.

Ayrıca bu kişisel veriler sadece kötü niyetli bilgisayar korsanlarının iştahını kabartmamaktadır. Aynı zamanda kurumsal firmaların birçoğunun hiçbir ücret ile elde edemeyeceği çok önemli ve kritik tüketici verilerini barındırmaktadır. Örneğin akıllı bir televizyon üzerinde izleme alışkanlıklarımız, kayıt detaylarımız, uygulama marketini kullandıysak banka işlemleri veya kredi kartı detaylarımız, konum verimiz gibi bazı kişisel verilerimiz yer almaktadır. Alarm sisteminde konum verimiz, evin boş veya dolu olduğu, yaklaşık olarak eve gidiş geliş saatlerimiz gibi kişisel verilerimiz bulunmaktadır. Akıllı elektrik sistemlerinden konum verimiz, kullanım alışkanlıklarımız, evin boş veya dolu olduğu bilgisi, tüketim miktarlarımız gibi kişisel veriler yer almaktadır. Tüm bu kişisel verilerimizin tamamı kritik bir öneme sahiptir ve kötü niyetli kişiler tarafından ele geçirilmesi durumunda kötü sonuçlara sebebiyet verebilmektedir.

Mahremiyet ihlallerinin yanı sıra kötü niyetli kişiler tarafından hırsızlık gibi durumlarda da güvenlik açıklıkları kullanılabilir. Örneğin şu sonuçlar oluşabilir;

- Kapı kilidi açılarak eve girilebilir.
- Alarm sistemleri devre dışı bırakılarak etkisiz hale getirilebilir.
- Güvenlik kameralarına girilerek görüntüler ele geçirilebilir.
- Güvenlik kameralarının kayıt yapması engellenebilir, yapılan kayıtlar silinebilir.
- Hareket sensörlerinden ya da kullanım verilerinden evde birinin olup olmadığı veya ne kadar süredir evde olmadığı tespit edilebilir.
- Kullanıcıların kullanımını etkileyen zararlar verilerek akıllı ev sistemlerini kullanmaları engellenebilir.
- Akıllı elektrik sistemlerine müdahale edilerek kapalı olması gereken cihazlar açılabilir ya da açık olması gereken cihazlar kapatılabilir.
- Akıllı aydınlatma sistemlerine müdahale edilerek elektrik tüketimi arttırılabilir.
- Fırın, ütü gibi yüksek enerji kullanan cihazlar uzun süre yüksek güçte çalıştırılarak yangın gibi sonuçların oluşması sağlanabilir.
- Yüksek enerji kullanan bütün elektrikli aletler aynı anda çalıştırılarak elektrik sistemine toplumsal veya bireysel bazda zararlar verilebilir.

Yukarıdaki örneklerin sayısı arttırılabildiği gibi akıllı ev sistemi kullanan ve kullandığı akıllı ev sistemine ait bilinen zafiyetleri olan cihazların tespiti de günümüzde mümkün olmaktadır.

Gelişen teknoloji ile birlikte ortaya çıkan Shodan gibi arama motorları interneti tarayarak internete açık olan sistemleri, cihazları, aygıtları tespit edip bunları bağlantı noktasına, türüne, coğrafi konumuna ve servis bilgisine göre sınıflandırmaktadır. Buradan elde edilen bilgiler sayesinde temel kullanım bilgisine sahip olup çok profesyonel olmayan kullanıcılar bile, içinde zafiyet bulunan birçok canlı sistemi tarayıp bu sistemlere ait raporları görebilmektedir.

Bölüm 3

İlgili Çalışmalar

Ali 2018, IoT tabanlı akıllı ev sistemlerinde siber ve fiziksel güvenlik açıklığı değerlendirmesi yapmak için veri tabanı, fiziksel doküman ve insan gibi farklı bilgi varlıklarını tutmaya ve değerlendirmeye odaklanan OCTAVE (operationally critical threat, asset, and vulnerability evaluation) Allegro metodolojisini kullanarak IoT tabanlı akıllı evlerin çeşitli güvenlik zafiyetlerini göstermek, ev sakinlerine bu riskleri sunmak ve tanımlanan riskleri hafifletmeye yönelik yapılacak çalışmaları araştırmıştır. Çalışma kapsamında akıllı ev sistemlerine ilişkin 10 adet bilgi varlığı, bunlara ait olası güvenlik tehditleri, olası etkiler (yaklaşık 15 adet) ve risk puanları belirlenmiştir. Ardından gerçek dünya ve literatür desteği ile bu tehditlere ilişkin olası hafifletme aksiyonları belirlenmiştir. Buna göre en yüksek risk puanını siber güvenlikle ilgili olan kullanıcı kimlik bilgileri, mobil kişisel veri ve kullanıcı uygulamaları almıştır [37].

Apthorpe 2017, uyku monitörü, iç mekan güvenlik kamerası, bir ağ çoğaltıcı ve akıllı ev asistanını (a Sense sleep monitor, a Nest Cam Indoor security camera, a WeMo switch and an Amazon Echo) Raspbian Jessie işletim sistemi çalıştıran Rasberry Pi3 model B cihazına bağlayıp (802.11n kablosuz erişim noktası olarak) akıllı ev cihazlarının gittiği DNS adreslerini bir laboratuvar ortamı kurup dinleyerek akıllı evde yaşayan insanların hareketlerini tahmin etmişlerdir. 4 cihazın da hangi işlemi yaparken ne kadar veri gönderdiğini tespit ederek bu tahminlemeyi yapmışlardır. Nest kameranın canlı görüntü aktarımı esnasında 10.000 ile 48.000 byte arasında veri gönderdiği, ev sakininin yatağa gittiğinde 50.000 byte civarında veri gönderdiği, ağ çoğaltıcı açıldığında 70.000, kapandığında 0'a

yakın miktarda byte gönderdiği, akıllı ev asistanının soruya cevap verdiğinde 70.000 byte civarında veri gönderdiği elde edilen bulgular arasındadır. Araştırmacılar, akıllı ev sahipleri için gelecekte kullanıcı dostu bir trafik izleyen çözüm geliştirmeyi planlamaktadır [38].

Gai 2018, 7 akıllı ev cihazına (akıllı TV, akıllı ev sinema sistemi, akıllı su ısıtıcısı, akıllı buzdolabı, akıllı termostat, akıllı ışıklandırma, akıllı güvenlik kamerası) yapılabilecek 14 saldırı türünü ve 11 güvenlik zafiyetini literatür araştırması desteği ile kategorilendirmiştir. Buna göre akıllı ev cihazlarının en fazla şifrelenmemiş servis, DDoS, zayıf şifre altyapısı, firmware versiyonunun güncel olmayışı ve iki faktörlü yetkilendirmenin olmayışı gibi zafiyetlerle saldırı alabileceği tespit edilmiştir [39].

Jia 2018, bir akıllı ampul (TP-LINK LB100) ve akıllı ev asistanındaki (Google Home) zafiyetleri bulmak için 58.714 paketi inceleyerek 6 farklı saldırı senaryosunu uygulamıştır. Bu senaryolarda kendi zararlı sunucusunu, yazılımını ve SSL sertifikasını kullanarak ortadaki adam (Man in the Middle), yan kanal, veri dinleme (sniffing) gibi yöntemleri uygulamıştır. Herhangi bir cihaz firmware bilgisi olmadan yapılan senaryolar sayesinde ampulü açıp kapatmaya, aydınlatma seviyesini değiştirmeye, kullanıcının ev konumuna, kullanıcının ses geçmişine, akıllı ev asistanının root yetkisine, düz metin olarak TP-LINK'in yetkilendirme jetonuna (token), ampulün kullanıcı adı ve şifresine erişilmiştir [40].

Lee 2014, akıllı evlerde güvenliği sağlamak adına 10 tane akıllı ev cihazındaki yonga seti türü, işletim sistemi, ağ protokolü, frekans gibi çeşitli özellikleri ve bunlar üzerinde yapılabilecek olası saldırıları kategorilendirmiştir. Buna göre fiziksel, veri bağlantısı, ağ, taşıyıcı ve uygulama katmanı olmak üzere 5 adet saldırı yapılabilecek katmanı ve bunlar üzerindeki saldırı türleri sıralanmıştır. Örnek olarak fiziksel katmana jamming ve tampering, veri linki katmanına KillerBee, GTS saldırısı, geri çekme manipülasyonu (Back-off manipulation), ACK saldırısı gibi saldırı türleri kategorilendirilmiştir [41].

Ling 2017, bir akıllı priz (Edimax SP-2101W) üzerinde yapılan güvenlik zafiyeti taraması için cihaz tarama, kaba kuvvet, taklitçilik (spoofing) ve firmware saldırısı olmak üzere 4 saldırı türü yapılandırılmış ve gerçek dünyadaki 5 akıllı prize uygulanmıştır. Elde edilen

bulgulara göre savunma stratejileri belirlenmiştir. Bu stratejiler ise güvenli iletişim ağı, prizler ile sunucular arasında ortak yetkilendirme, saldırı tespit sistemi (IDS), anti-bot mekanizması ve veri bütünlüğünün korunmasından oluşmaktadır [42].

Aktaş 2013, akıllı ev cihazlarına güvenli uzak bağlantı için iki farklı SIP (Session Initiation Protocol) bağlantı modeli önermiş ve bu modelleri yaygınca kullanılan 7 güvenlik tehdidine karşı değerlendirmiştir. İlk SIP modeli için, kullanıcı kaydı için HTTP Digest Kimlik Doğrulaması ve veri gizliliği için İnternet Protokolü Güvenliği (IPSec) tüneli kullanılırken, ikinci modelde güvenli kimlik denetimi için Taşıma Katmanı Güvenliği (TLS), bağlantı sırasında veri gizliliğini sağlamak için Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP) çözümleri kullanılmıştır. Bu iki model; dinleme (eavesdropping), değiştirme (modification), aradaki adam (Man-in-the-Middle), tekrar paket gönderme (replay), şifre tahmini (password guessing), sızdırma (spoofing) ve dağıtık servis dışı bırakma (DDos) olmak üzere 7 yaygın saldırı yöntemiyle test edilmiş ve elde edilen bulgulara yer verilmiştir [43].

Wurm 2016, iki adet kişisel ve endüstriyel olarak kullanılan IoT cihazlarında yapmış olduğu güvenlik analizleri ile cihazları ele geçirebilmiştir. İlk cihaz olan Haier SmartCare akıllı ev otomasyon sisteminin ilk olarak donanım ve işletim sistemi incelemesi yapılmıştır. Cihazdaki işlemcinin Android ve Linux işletim sistemlerini desteklediği ve seri haberleşme protokollerinden olan Universal Asynchronous Receiver Transmitter (UART) kullandığı tespit edilmiştir. UART ve USB cihazı kullanılarak önyükleme (boot) zafiyetinden faydalanarak işletim sistemi kabuğuna (shell) erişim sağlanmıştır. Daha sonra işletim sistemi kabuğundan erişilen DES şifrelemesine sahip yönetici parolası kaba kuvvet saldırısı ile 5 saatte ele geçirilmiştir. Yönetici parolası port taraması üzerinden telnet girişinde kullanılmış ve sonrasında ağ trafiği dinlenmiştir. Bu sayede aygıt yazılımı güncellemesinde kullanılan düz metin haldeki HTTP bağlantısı tespit edilmiştir. İkinci cihaz olan endüstriyel akıllı sayacın (Itron Centron) EEPROM dosyası üzerinden cihaz kimlik numarasına erişip kimlik numarasını değiştirmiştir. Başka bir sayaçta bulunan yeni kimlik numarası ile diğer cihazın enerji tüketim bilgisine erişilmesiyle beraber, sayacın enerji tüketim değerleri de diğer cihazdan alınmaktadır. Bu sayede enerji hırsızlığı, enerji hattına aşırı yüklenme gibi saldırılar yapılabilmektedir. Çalışmada UART

konsoluna erişimin kısıtlanması, daha iyi hash algoritmasının kullanılması, dosya sisteminin şifrelenmesi, EEPROM dosyasına erişimin engellenmesi çözüm önerileri olarak tespit edilmiştir [44].

Rafferty 2018, akıllı ev cihazları için geleneksel güvenlik duvarı ve antivirüs yazılımlarının yeterli olmayacağını öne sürerek akıllı çok ajanlı bir iş birliği modeli geliştirilmiş ve örnek olay çalışması yapmıştır. Geliştirilen model; ajanların karar vermesi, iş birliği yapması ve ortak güvenlik amaçlarını başarmak için ajanların programlanması için geliştirilen İnançlar-İstekler-Niyetler (Beliefs, Desires, and Intentions-BDI) yazılım modelini kullanmaktadır. Model, 3 katman ve 4 fonksiyondan oluşmaktadır. Model; akıllı cihaz, iş birliği ve bulut servis katmanı olmak üzere 3 katmandan oluşmaktadır. Fonksiyonlar ise inanç revizyon fonksiyonu, seçenek oluşturma fonksiyonu, filtreleme fonksiyonu ve aksiyon seçim fonksiyonundan oluşmaktadır. Örnek olay çalışması ise bir akıllı güvenlik kamerası üzerinde gerçekleştirilmiştir. Ajanların akıllı güvenlik kamerasının bir botnet aktivitesinde kullanılıp kullanılmadığını algılaması, bir alarm üretmesi ve bir aksiyon alması sağlanmıştır [45].

Bölüm 4

Materyal ve Yöntem

4.1 Materyal

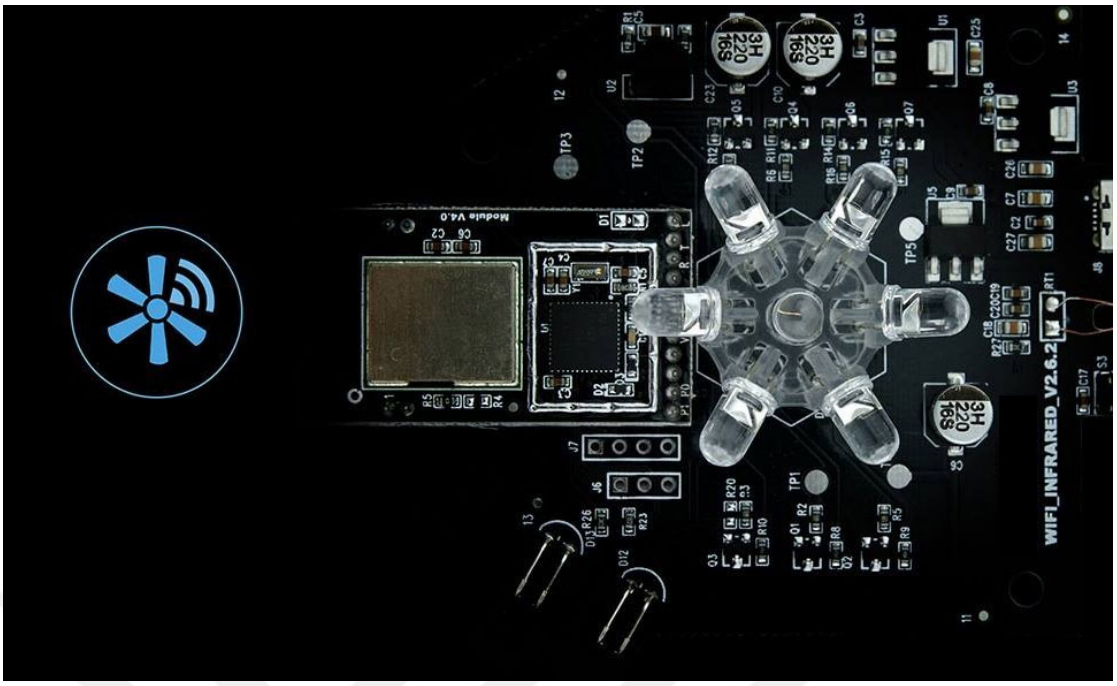
Akıllı ev sistemi projesi hazırlamak için akıllı ev sistemlerinde temel olan ürünler bir araya getirilerek akıllı ev modeli oluşturulmuştur. Oluşturulan bu akıllı ev modeli güvenlik zafiyetlerinin araştırılması için bir test ortamı olarak kullanılmıştır. Güvenlik zafiyet testleri yapılacak olan cihazlar seçilirken akıllı ev sistemleri kategorisinde pazar payları, kullanım oranları ve fiyat performans başarılarına göre, elde edilebilme kolaylıkları göz önünde bulundurulmuştur.

Akıllı ev sistemleri genellikle bir ana yönetim konsolu ve bu konsola bağlanabilen veri gönderebilen ve bu konsol üzerinden ya da internet yardımıyla kontrol edilebilen diğer akıllı ev cihazları bulunmaktadır. Akıllı ev modelinde ana yönetim konsolu, uzaktan kontrol edilebilen akıllı priz, kablosuz güvenlik ve bebek izleme kamerası, akıllı güvenlik alarm sistemi ve bu alarm sistemine bağlı olarak hareket sensörü, kapı pencere sensörü kullanılarak akıllı ev sistemi modeli oluşturulmuştur.

4.1.1 Akıllı Ev Sistemi Ana Yönetim Konsolu

Test için geliştirilen akıllı ev modelinde kullanılan akıllı ev sistemi ana yönetim konsolu, sensör ve diğer akıllı ev aygıtlarının yönetimini sağlayan akıllı ev sisteminin merkez cihazıdır. Yönetim konsolu yapılan görev ve işlemlerin zamanlayıcıya göre işlem sırasını gerçekleştiren cihazdır. Girilen talimat doğrultusunda işlem zamanlayıcısı belirtilen işlemleri zamanında otomatik olarak adım adım komut göndererek gerçekleştirmektedir. Üzerinde dahili bulunan termometre ile bulunduğu ortam ısısını ölçerek bu ısıya göre de verilen komutları gerçekleştirebilmektedir. Örneğin ısı 20 derecenin altına düştüğünde ısıtıcıyı aç, 20 derece üzerine çıktığında kapat veya 23 derecenin üzerine çıktığında klimayı aç gibi talimatları bulunduğu ortamın ısı derecesine göre gerçekleştirilebilir.

Uzaktan kumandalı tüm aygıtları kontrol edebilmek için üzerinde kızılötesi ve radyo frekansı alıcı ve vericiler bulunmaktadır. Bu alıcı ve vericiler 360 derece her yöne bakacak şekilde yerleştirilmiştir, bu sayede gönderilen ya da alınan sinyalin ulaşmama sorunu en aza indirilmektedir.



Şekil 4.1: Akıllı ev ana yönetim konsolu kablosuz sinyal şeması [46]

Ana yönetim konsolunun üzerinde tanımlı olan birçok uzaktan kumandalı cihaz olduğu gibi kullanıcısı istediği takdirde yeni ve farklı uzaktan kumandaları cihaza tanımlayabilmektedir. Konsolun ilk kurulumu yapılmak için açıldığında konsol üzerinden şifresiz kendi adında bir kablosuz ağ bağlantısı paylaşmaktadır. Bu ağa bağlanan mobil cihaz üzerinde bulunan mobil uygulamasına otomatik olarak konsolun tanımlaması yapılmış olur. Bu adımda kendi kablosuz ağ sinyali kesilmekte ve evin kablosuz ağ bağlantı adı ve şifresi girilerek artık konsolun bu kablosuz ağa bağlanması sağlanmaktadır. Tanımlaması bu şekilde yapılan ana yönetim konsolu daha sonrasında mobil uygulama üzerinden aynı kablosuz ağa bağlı olarak ya da internet üzerinden yönetilebilmektedir.

4.1.2 Akıllı Priz

Kullanılan model uzaktan kontrol edilebilen, tak çalıştır olarak ifade edilen kolay kuruluma sahip bir akıllı elektrik prizidir. İlk kurulumunda akıllı prizin üretici firması tarafından geliştirilmiş mobil uygulama vasıtası ile akıllı priz kurulumu yapılabilmektedir. Kurulum aşamasında cihazın bağlanacağı wireless ağına daha önceden bu ağa bağlı olan telefon üzerinden mobil uygulama ile bağlanılacak wireless ağının yayın adı ve şifre

bilgileri gönderilerek akıllı prizin kurulumu tamamlanmaktadır. Daha sonra mobil uygulama üzerinden aynı ağa bağlı durumda ya da internet üzerinden dünyanın herhangi bir yerinden priz kullanılabilmektedir. Uygulama üzerinden priz açılıp kapatılabilmekte, o anki açık kapalı durumunun ne olduğu görüntülenebilmekte veya priz üzerinde bulunan gece lambası kontrol edilebilmektedir. Aynı şekilde priz üzerinde bulunan buton yardımı ile fiziksel şekilde de priz kontrol edilebilmektedir.

Akıllı priz bir kablosuz ağ ile eşleştirilmediğinde üzerinde bulunan mavi durum ledi hızlı bir şekilde yanıp sönerek cihazın kurulmadığını kuruluma hazır olduğunu göstermektedir. Cihaz kablosuz ağ ile eşleştirildiğinde üzerinde bulunan mavi led sönmekte ve cihaz hazır duruma geçmektedir. Kurulum tamamlandıktan sonra üzerinde bulunan led priz açıkken yanmakta, priz kapalı durumda iken sönmektedir. Cihazın bu şekilde açık ya da kapalı durumda olduğu anlaşılabilmektedir. Cihazın bağlı olduğu kablosuz ağ bağlantısı kesildiğinde mavi led yavaş bir şekilde yanıp sönmektedir.

4.1.3 Akıllı Güvenlik Alarm Sistemi

Evin güvenliğini sağlamak için kullanılan akıllı güvenlik alarm sistemi; alarm yönetim cihazı, kapı pencere sensörü, hareket sensörü ve uzaktan kumandadan oluşmaktadır. Kapı pencere sensörü konumlandırıldığı yerde kapı veya pencere, açıldığı ya da kapandığı zaman alarm yönetim cihazına ilgili durumu 433 mhz radyo frekansı olarak göndermektedir. Aynı şekilde hareket sensörü de konumlandırıldığı yerde herhangi bir hareket algıladığında bu durumu yönetim cihazına 433 mhz radyo frekansı olarak göndermektedir. Kumanda ise mobil uygulama üzerinden işlem yapmadan fiziksel bir tuş imkanı sunarak alarm sistemini devreye alabilmekte, devre dışı bırakabilmekte, seçilen sensöre göre devrede olmasını sağlayabilmektedir.

Alarm yönetim cihazının ilk kurulumda mobil uygulama üzerinden bağlanabileceği kablosuz ağ adı ve şifresi girilerek o kablosuz ağa bağlanması sağlanmaktadır. Sonrasında alarm yönetim cihazı aynı kablosuz ağ üzerinden ya da internet üzerinden kontrol edilebilmektedir.

4.1.4 Kablosuz Güvenlik, Bebek İzleme Kamerası

Kablosuz olarak ağa bağlanabilen uzaktan kontrol edilebilen bir güvenlik kamerasıdır. Üzerinde bulunan dahili mikrofon ve hoparlör sayesinde kullanılan mobil uygulaması ile karşı tarafla çift yönlü iletişime geçilebilmektedir. Tüm görüntülerin kaydını üzerinde bulunan hafıza kartına, aynı ağda bulunan depolama alanlarına ya da bulut depolama alanlarına yapabildiği gibi sadece hareket algılandığı takdirde de kayıt yapabilmektedir. Gece görüş özelliği, 360 derece her yöne dönebilme özelliği bulunmaktadır. Bu kontroller kameranın mobil uygulaması üzerinden veya internet tarayıcısı üzerinden ip adresine erişilerek de yapılabilmektedir.

Kamera satın alındığında tak çalıştır şeklide kullanıma hazır durumda gelmektedir. Cihazın üzerinde bulunan benzersiz kimlik bilgisi veya barkod kullanılarak yine cihaz üzerinde bulunan kullanıcı adı ve parola ile kameraya erişilebilmekte, ayarları yapılandırılabilmekte ve görüntüler kaydedilebilmektedir. İnternet üzerinden kameraya erişebilmek için kameranın kutusunda ya da kameranın üzerinde bulunan benzersiz kimlik bilgisi ile birlikte kullanıcı adı ve parolayı bilmek gerekmektedir. Güvenlik, bebek izleme kamerasının diğer teknik özellikleri ve sahip olduğu sertifikalar şekil 4.2.' de gösterilmektedir.

Catalogue	Type	Parameters
Features	View by phone	Support Android ,Iphone/Ipad Free APP
	View on PC	support windows system
	Monitor Advantage	Support IPhone、Android、Computer monitor. Miscrosoft certification plugin, no virus risk.
	Sever cluster	Using Cloud PnP servier cluster, Intelligent application and super stable
	UID Technology	UID scan technology applied, easy to operate, and highly confidential.
	Easy operation	Plug & Play, technology, penetration degree can be 99%,applicable toany complex network surroundings. Easy operation: 1. plug the cable and power line, 2.install computer software, scan code to add camera.
	Super Client	1,4,9,16,25,36, 64,81-channel , no user limited , centralized monitor
System	Operation system	Embedded Linux OS
	System security	Supports account, password authority management
	DDNS	Free need ddns
Collection	Image sensor	1/4inch 0.3 Megapixel line by line CMOS sensor
	SNR	≥50dB
	Minimum Illumination	0.3Lux
	Lens	Standard:3.6mm
Video	Compression Format	M-jpeg
	Resolution	VGA（640×480）/QVGA(320×240)
	Maximum frame rate	30fps
	Bit Rate	32Kbps～4Mbps can be set
	IR	10 Φ5mm LEDs IR Distance: 10 m
	IR CUT	IRCut Built-in,there is no color cast and more sharp at nightvision.
Audio	Encode formats	ADPCM
	Input	1 Channel Internal -48dB Microphone
	Output	1 Channel Line out(3.5mm phone jack)&Internal speaker(8Ω1W)
Memory	Memory Socket	Automatic pop-up slot for TF/Micro SD card
	View by SD Card	Remote browsing, PC Software,Android&Iphona /Ipad APP
Network	Socket	RJ-45 10/100Mb self-adaptable Ethernet slot
	WIFI	WIFI 802.11 b/g/n
	Visitors Online	Support 4 visitors viewing on line at the same time
P/T	Control Method	Pan:355°,Tilt:90°(speed can be set)Highest speed:70°/s
Alarm	Alarm Detection	Support motion detecting
Physical index	Power	DC 5V2A
	Comsumption	<6W
	Temperature	-10~50℃
	Humidity	10%~85%
	Weight	Gross:800g （Note: in kind prevail）
	Package size	210*200*130mm (L*W*H)
Certification	Certificate	ISO FCC CE RoHS

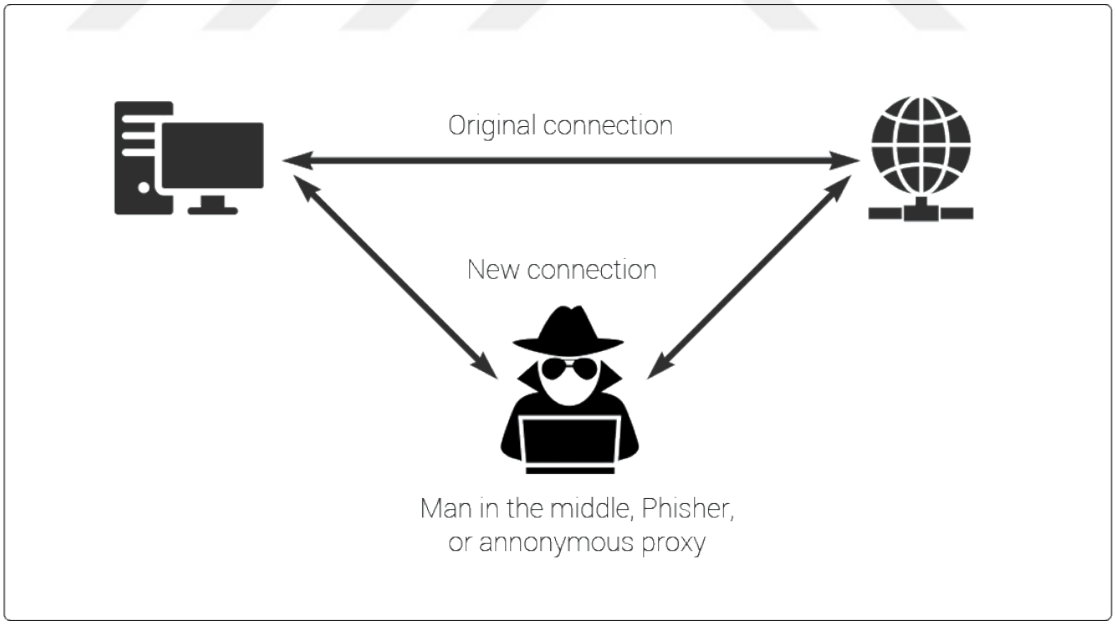
Şekil 4.2: Kablosuz güvenlik,bebek izleme kamerası teknik özellikleri [47]

4.2 Yöntem

Bu tezde örnek akıllı ev modeli olarak oluşturulan akıllı ev sistemine yapılan güvenlik testleri için kullanılan bazı yöntemler aşağıda açıklanmaktadır. Literatür taramasındaki çalışmalar da göz önünde bulundurularak zafiyet taramasında yapılacak testler belirlenmiştir. [39] [40] [42] [43] Bu çalışmada ortadaki adam ve dağıtık servis dışı bırakma saldırıları ile birlikte kablosuz ağ ve aygıt güncelleme (firmware) zafiyeti araştırılmıştır.

4.2.1 Ortadaki Adam Saldırısı (Man in The Middle)

Ortadaki adam (man in the middle) saldırıları ağ yönlendirme anahtarı cihazlarının temel özelliği olan anahtarlama mekanizmasını kandırma şeklinde gerçekleştirilmektedir. Birbirleri ile doğrudan bağlantılı olan iki taraf arasındaki trafiğin bilgisayar korsanı üzerinden geçerek iletilmesi ile yapılmaktadır. Bilgisayar korsanı şifrelenmemiş olarak geçen trafiği dinlemek veya değiştirerek iletmek için bu yöntemi kullanmaktadır [48].



Şekil 4.3: Ortadaki Adam Saldırısı Bağlantı Şeması [49]

Ağ yönlendirme anahtarı ile hedef olarak belirlenen cihaz ya da bilgisayara ait tüm trafik bilgisayar korsanı üzerinden transparan geçecek şekilde yönlendirilebilmektedir. Geçen

paketleri wireshark gibi bazı yazılımlar ile görüntüleyebilmekte ve kayıt edilebilmektedir. Kayıt edilen paketlerin içerisinden trafik şifrelenmeden iletiliyorsa hassas verilere erişim sağlanabilmektedir. Paketler içerisinde kullanıcı adı ve parola gibi kritik verilere de ulaşılabilmektedir.

4.2.2 Dağıtık Servis Dışı Bırakma Saldırısı (DDOS)

Dağıtık servis dışı bırakma saldırısı gibi saldırılarda bir cihazın veya internet sitesinin altyapısında olan ağ kaynağı için geçerli kapasite sınırlarından faydalanılmaktadır. Dağıtık servis dışı bırakma saldırısı yapılan cihazın kapasitesinden fazla talep gönderilmesi sonucunda gerçekleşmektedir [50]. Cihazın ağ kaynağına birden çok istek göndererek bu istekleri işleme kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlamaktadır. Saldırı anında uygulama kullanılan port üzerinden sürekli bağlantı açmaktadır. Zaman aşımına uğrayan bağlantılar yerine hemen yeni bir bağlantı açarak çok kısa süre içinde paket sayısını aşırı arttırarak maksimum bağlantı limitini doldurabilmektedir. Saldırgan tarafından gönderilen paketler sayesinde cihazı asıl kullanan kullanıcının gönderdiği komutlara cevap verememektedir. Bu yöntem kullanılarak cihazın kullanımına engel olunabilmektedir.

Bölüm 5

Bulgular

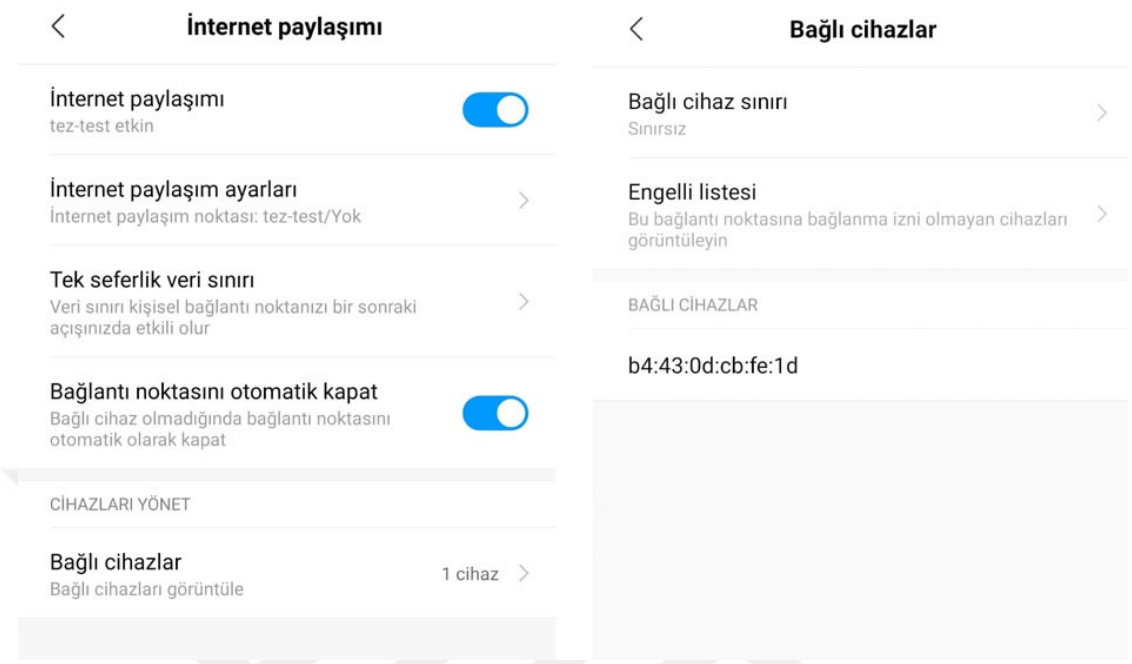
5.1 Akıllı Priz Zafiyet Bulguları

Akıllı prizler fiziksel, kablosuz ağ ve internet üzerinden kontrol edilebilmektedir. Akıllı ev sistemlerinin temelinde kablosuz ağ bağlantısı kullanıldığı için ilk olarak kablosuz ağ zafiyetleri üzerinden test edilmiştir. Diğer bir yöntem olarak ortadaki adam saldırısı (man-in-the-middle) ile paketler yakalanarak test edilmiştir. Bu testlerin yanı sıra dağıtık servis dışı bırakma saldırısı (Ddos) durumunda cihazın davranışları incelenerek kullanımı etkileyen bir durumun oluşup oluşmadığı test edilmiştir. Akıllı prizin aygıt yazılımı (firmware) güncelleme aşamasında doğrulanmamış yazılım yüklenebilme durumu incelenmiştir. Aşağıdaki başlıklarda akıllı prize yapılan güvenlik testlerinin bulgularına yer verilmiştir.

5.1.1 Kablosuz Ağ Zafiyeti

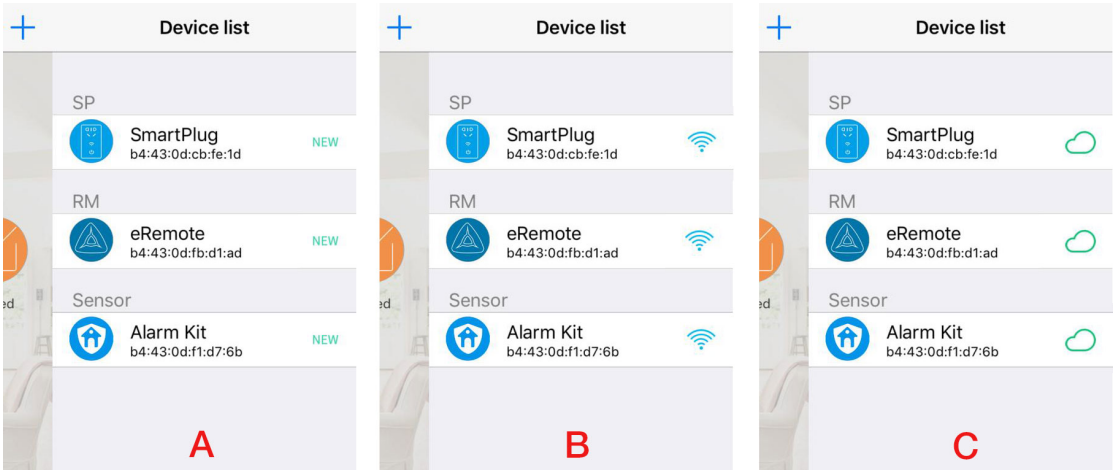
Kablosuz ağa bağlı durumda ve cihaz kullanılabilir olduğunda, bağlı olduğu kablosuz ağ yayını kesilmiş ve cihazın aynı kablosuz ağ yayınını tekrar bağlanmak için aradığı gözlemlenmiştir. Cihazın tekrar bağlanması için aynı kablosuz ağ ismine sahip olan fakat şifresi olmayan farklı bir modem üzerinden kablosuz bağlantı oluşturulmuş ve cihazın otomatik olarak bu yeni kablosuz ağa bağlandığı gözlemlenmiştir. Burada bulunan kablosuz ağ zafiyeti sayesinde akıllı prizin kontrol edilmek üzere bağlı olduğu kablosuz ağın sadece ismini kontrol ettiği fakat kablosuz ağın şifresini bir doğrulama aracı olarak kullanmadığı

gözlemlenmiştir.



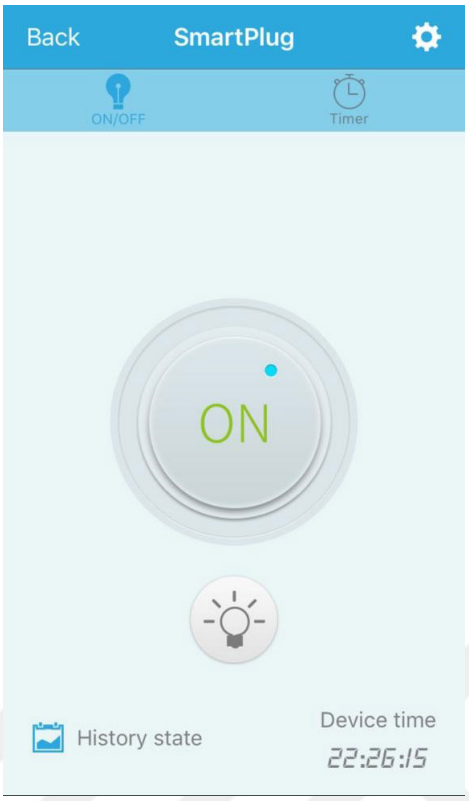
Şekil 5.1: Oluşturulan kişisel erişim noktasına cihazın doğrulama yapmadan bağlanması

Akıllı priz ile aynı ağ bağlantısına bağlı olan mobil cihaz, üzerinde bulunan uygulama ile akıllı prizi yönetilebilmektedir. Burada herhangi bir eşleştirme ya da doğrulama yapmadığı gözlemlenmiştir. Akıllı prizi yönetmek için aynı ağa bağlı olan mobil cihaz üzerinde akıllı prizin mobil uygulamasına sahip olmanın yeterli olduğu gözlemlenmiştir. Akıllı prizin mobil uygulaması açıldığında aynı yerel ağ üzerinde bulunan akıllı prizin otomatik olarak uygulama üzerine mac adresi ile eklendiği görülmüştür. Uygulama herhangi bir şifre, benzersiz kimlik, qr kod ya da bunlar gibi başka hiçbir bilgi istememektedir. Uygulama üzerine eklenen akıllı ev cihazları bulut yapı sayesinde dünyanın herhangi bir yerinden kontrol edilebilmektedir. Bu zafiyet sayesinde akıllı priz ile aynı ağa sadece bir kere bağlı olmanın o cihazın kontrolünü ele geçirebilmek için yeterli olduğu anlaşılmıştır. Cihazın kontrolünü ele geçiren kötü niyetli kişinin bundan sonra bulut üzerinden herhangi bir yerde ve zamanda akıllı prizi kontrol edilebileceği gözlemlenmiştir.



Şekil 5.2:
a) Akıllı priz ile aynı ağ bağlantısına bağlanınca akıllı prizin uygulama üzerine otomatik olarak eklendiği durum
b) Akıllı priz ile aynı ağ bağlantısına bağlı şekilde akıllı prizin uygulama üzerinden yönetilebildiği durum
c) Akıllı priz ile aynı ağ bağlantısı kesilse dahi bir kez tanımlandığı için bulut üzerinden kontrol edebilmenin devam ettiği durum

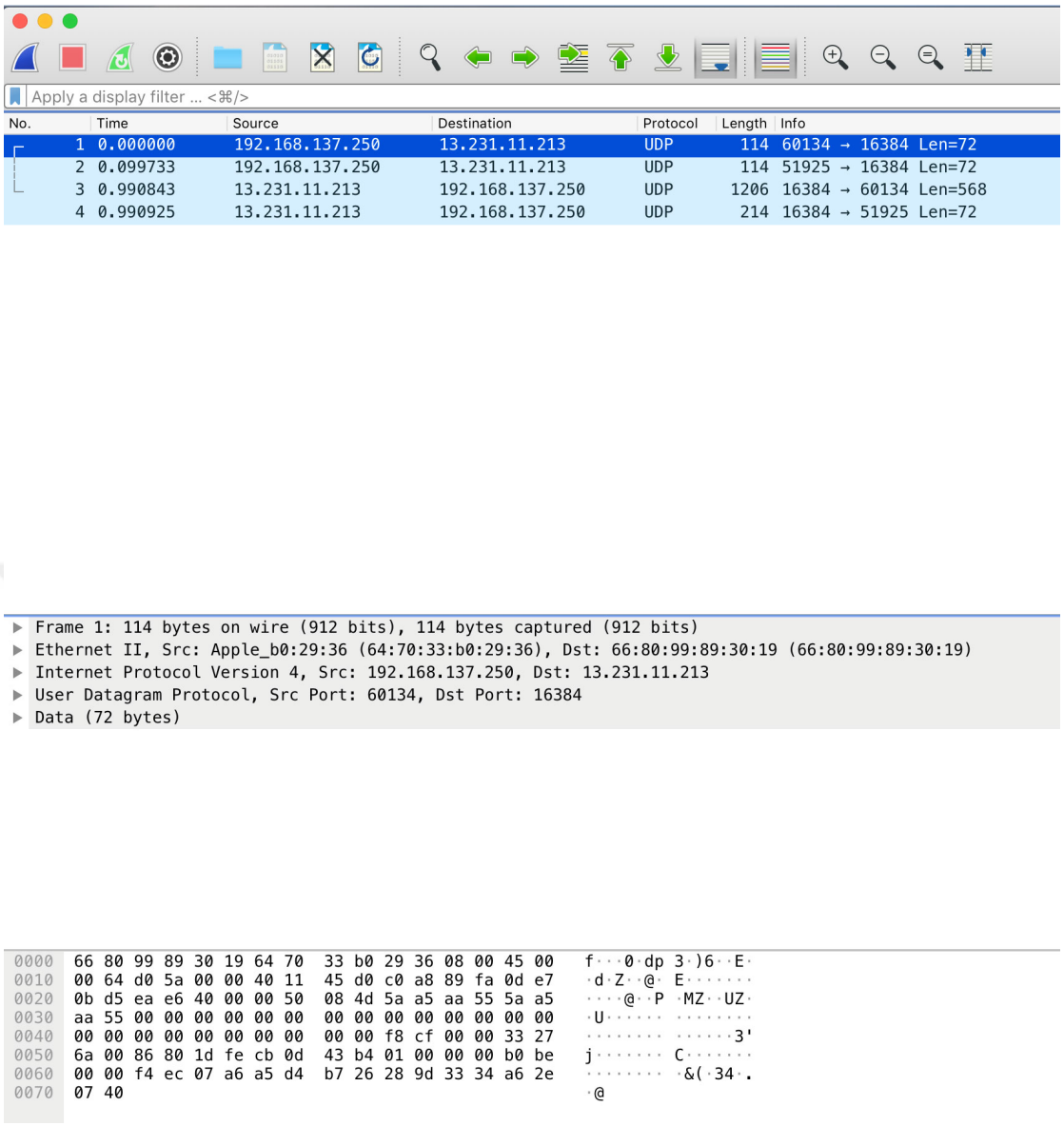
Aynı akıllı priz birden çok mobil aygıt üzerinden mobil uygulaması ile kontrol edilebilmektedir. Akıllı prizin yönetimine sahip olan cihaz sınırı bulunmamaktadır. Akıllı prizin yönetimine sahip olan cihazların listesi herhangi bir yerde bulunmamakta ve bu yönetime sahip kullanıcılar asıl kullanıcısı tarafından kontrol edilememektedir. Bu eksiklik nedeniyle akıllı priz sahibi cihazının kontrolünü elinde bulunduran kişileri görüntüleyememekte ve bundan haberdar olamamaktadır. Akıllı prizin bir başka mobil aygıt üzerine yönetilebilir olarak eklenmesi sonucunda daha önce yönetebilme kabiliyetine sahip olan mobil aygıtlara bilgi ya da bildirim gönderilmediği gözlemlenmiştir. Bu yönetebilme kabiliyetine sahip cıhazları yetkisizleştirebilmenin akıllı prizi sıfırlamaktan başka türlü mümkün olmadığı tespit edilmiştir.



Şekil 5.3: Akıllı prizin gerçek sahibi yönetebilmeye devam etmektedir ve cihaz yönetiminin başkası tarafından ele geçirildiğinin farkında değildir.

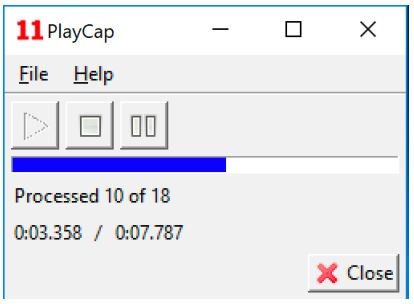
5.1.2 Ortadaki Adam Saldırısı ile Paket Yakalama

Örnek akıllı ev modeli üzerinde uygulanan testte akıllı prize mobil uygulama üzerinden açma ve kapatma komutları gönderilmiştir. Bu aşamada ortadaki adam saldırısı gerçekleştirilerek wireshark aracı ile gönderilen paketler analiz edilmiştir. Analiz edilen paketler doğrultusunda akıllı prizi açma ve kapatma komutunu içeren veri paketleri kopyalanmıştır.



Şekil 5.4: Wireshark uygulaması ile ortadaki adam saldırısı yapılarak elde edilen komut paketlerinin yakalanmasına ilişkin ekran görüntüsü

Kopyalanan açma ve kapatma komutları tekrarlama saldırısı (replay attack) yapmak için PlayCap uygulaması ile akıllı prize tekrar gönderilmiştir. Cihaza tekrar gönderilen paketler sonucunda cihazın açıldığı ve kapandığı tespit edilmiştir. Paketler tekrar gönderilerek cihaza erişim sağlanabilmektedir.

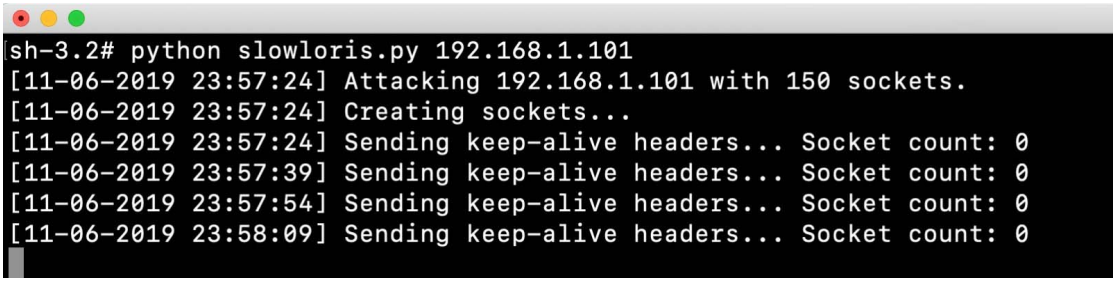


ŞEKIL 5.5: Yakalanan paketlerin PlayCap uygulaması ile tekrarlama saldırısı (replay attack) yapılarak tekrar gönderilmesine ilişkin ekran görüntüsü

Cihaza gönderilen paketlerde oturum kontrolü yapılmadığı tespit edilmiştir. Bu yöntem ile bir defaya mahsus ortadaki adam saldırısı yapılsa dahi internet üzerinden akıllı priz yönetilebilmektedir. Bilinmeyen herhangi bir kablosuz ağa bağlandığımızda ağda bulunan kötü niyetli bir kişi tarafından bu paketler dinlenebilmektedir.

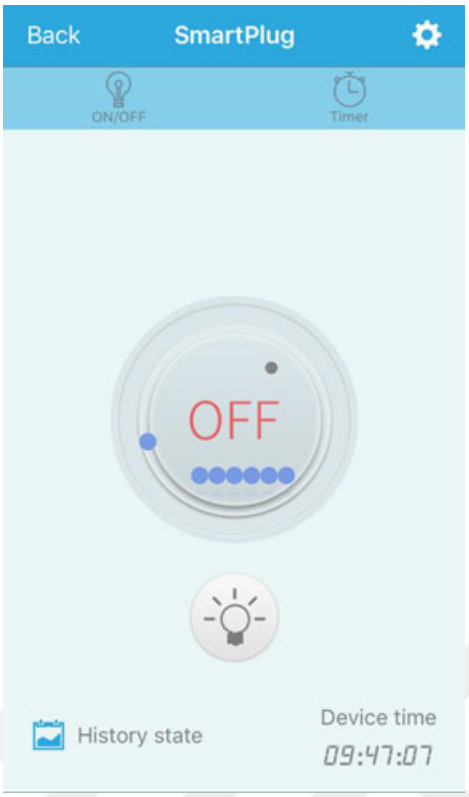
5.1.3 Dağıtık Servis Dışı Bırakma Saldırısı

Akıllı ev örnek modelinde yapılan testlerde akıllı priz ile aynı ağda bulunan kötü niyetli bir saldırgan cihaza sürekli paket göndermesi işlemi test edilmiştir. Test sonucunda saldırganın cihazı servis dışı bırakabildiği tespit edilmiştir. Slowloris python yazılımı ile yapılan dağıtık servis dışı bırakma saldırısında akıllı prizin gönderilen isteklere cevap veremediği ve mobil uygulamadan gönderilen komutları çalıştıramadığı tespit edilmiştir.



ŞEKIL 5.6: Slowloris Python yazılımı dağıtık servis dışı bırakma saldırı ekran görüntüsü

Mobil uygulama dağıtık servis dışı bırakma saldırısı esnasında sürekli olarak yükleniyor ekranı görseli çıkararak kullanıcıya sanki internet problemi yüzünden cihaza erişilemiyormuş izlenimi vermiştir.



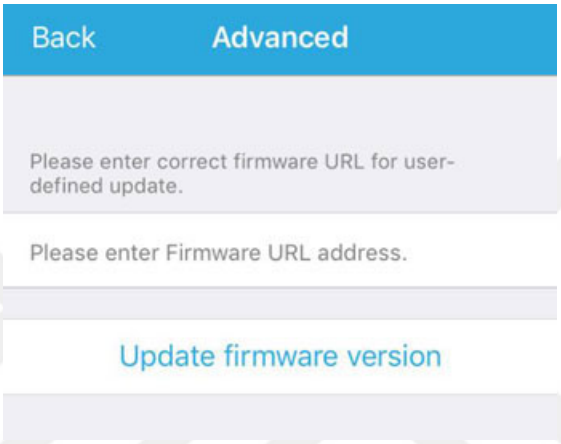
Şekil 5.7: Komut gönderilirken uygulama yanıt verememektedir. Yükleniyor işaretine ait ekran görüntüsü

Dağıtık servis dışı bırakma saldırısı yapılmaya devam ederken bir ara mobil uygulama üzerinden akıllı prizi kapatma komutu gönderilebilmiştir. Mobil cihaz üzerinde bulunan uygulamanın bu komut sonrasında herhangi bir hata vermediği gözlemlenmiştir. Fakat gönderilen komut akıllı priz tarafından algılanmadığı ve herhangi bir işlem yapılmadığı tespit edilmiştir. Telefonda bulunan uygulama herhangi bir hata vermediği için kullanıcıya işlem yapılmış ve akıllı priz kapatılmış olarak görülmüştür. Mobil uygulamanın akıllı prizi kapanmış olarak göstermesine rağmen prizin kapanmadığı açık olduğu ve üzerinde bulunan elektronik cihazlara elektrik vermeye devam ettiği gözlemlenmiştir.

5.1.4 Doğrulanmamış Firmware Yüklenebilme Zafiyeti

Akıllı ev sistemi modeli için kullanılan akıllı prizin aygıt yazılımı (firmware) güncellemesi mobil uygulama üzerinden yapılabilmektedir. Yazılım güncelleme kısmında birden fazla

seçenek bulunmaktadır. Yazılım güncelleme aşamasında istenilen bir internet adresi üzerinden doğrulanmamış yazılım güncellenmesi yüklenebilmektedir. Saldırganlar tarafından oluşturulan zararlı yazılım güncellemesi yöntemi ile akıllı ev sistemi ele geçirilebilir ve uzaktan yönetilebilir. İçeriği ile oynanmış bir aygıt yazılımı yükleme sonrasında cihaz üzerinde arka kapı bağlantısı oluşturularak kötü niyetli kişiler tarafından cihazın uzaktan yönetimi ele geçirilebilir. Bu tez kapsamında zararlı yazılım geliştirilerek uygulanmadığı için bir saldırı yöntemi olarak test edilmemiş, zafiyet bulgusu olarak ele alınmıştır.



Şekil 5.8: Mobil uygulama üzerinde internet adresi girilerek doğrulama yapmadan aygıt yazılımı yükleme ekranı

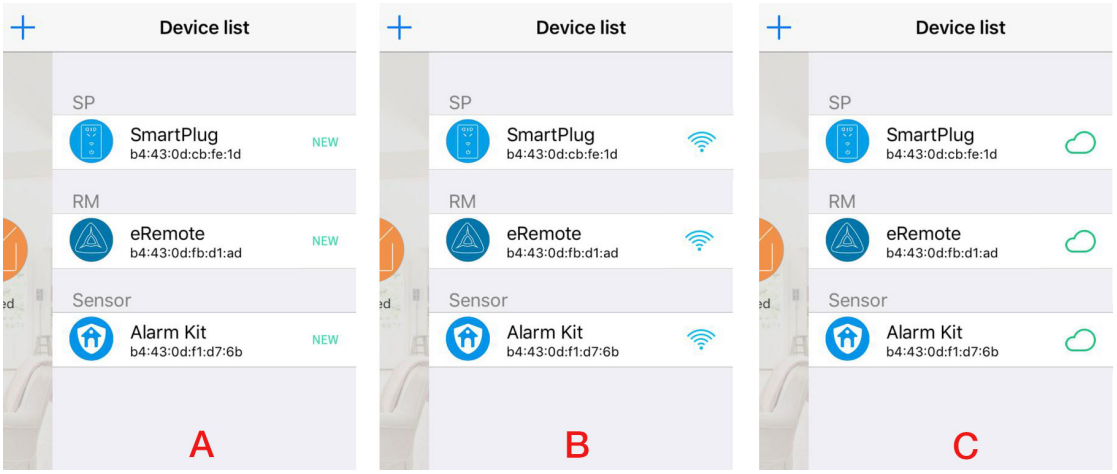
5.2 Akıllı Ev Sistemi Ana Yönetim Konsolu Zafiyet Bulguları

Akıllı ev sistemi ana yönetim konsolları kablosuz ağ ve internet üzerinden kontrol edilebilmektedir. Akıllı ev sistemlerinin temelinde kablosuz ağ bağlantısı kullanıldığı için ilk olarak kablosuz ağ zafiyetleri üzerinden test edilmiştir. Diğer bir yöntem olarak ortadaki adam saldırısı (man-in-the-middle) ile paketler yakalanarak test edilmiştir. Bu testlerin yanı sıra dağıtık servis dışı bırakma saldırısı (Ddos) durumunda cihazın davranışları incelenerek kullanımı etkileyen bir durumun oluşup oluşmadığı test edilmiştir. Ana yönetim konsolu aygıt yazılımı (firmware) güncelleme aşamasında doğrulanmamış yazılım yüklenebilme durumu incelenmiştir. Aşağıdaki başlıklarda ana yönetim konsoluna yapılan güvenlik testlerinin bulgularına yer verilmiştir.

5.2.1 Kablosuz Ağ Zafiyeti

Ana yönetim konsolunun kablosuz ağ bağlantısı kesildiğinde akıllı prizde olduğu gibi bir kablosuz ağ doğrulama zafiyetinin bulunmadığı tespit edilmiştir. Bağlandığı kablosuz ağın aynı isimde ve şifrede olduğunu kontrol ettiği aksi durumda başka bağlantılara bağlanmadığı gözlemlenmiştir.

Ana yönetim konsolu ile aynı ağ bağlantısına bağlı olan mobil cihaz, üzerinde bulunan uygulama ile ana yönetim konsolunu yönetilebilmektedir. Burada herhangi bir eşleştirme ya da doğrulama yapmadığı gözlemlenmiştir. Ana yönetim konsolunu yönetmek için aynı ağa bağlı olan mobil cihaz üzerinde ana yönetim konsolunun mobil uygulamasına sahip olmanın yeterli olduğu gözlemlenmiştir. Ana yönetim konsolu mobil uygulaması açıldığında aynı yerel ağ üzerinde bulunan Ana yönetim konsolunun otomatik olarak uygulama üzerine mac adresi ile eklendiği görülmüştür. Uygulama herhangi bir şifre, benzersiz kimlik, qr kod ya da bunlar gibi başka hiçbir bilgi istememektedir. Uygulama üzerine eklenen akıllı ev cihazları bulut yapı sayesinde dünyanın herhangi bir yerinden kontrol edilebilmektedir. Bu zafiyet sayesinde ana yönetim konsolu ile aynı ağa sadece bir kere bağlı olmanın o cihazın kontrolünü ele geçirebilmek için yeterli olduğu anlaşılmıştır. Cihazın kontrolünü ele geçiren kötü niyetli kişinin bundan sonra bulut üzerinden herhangi bir yerde ve zamanda ana yönetim konsolunu kontrol edilebileceği gözlemlenmiştir.



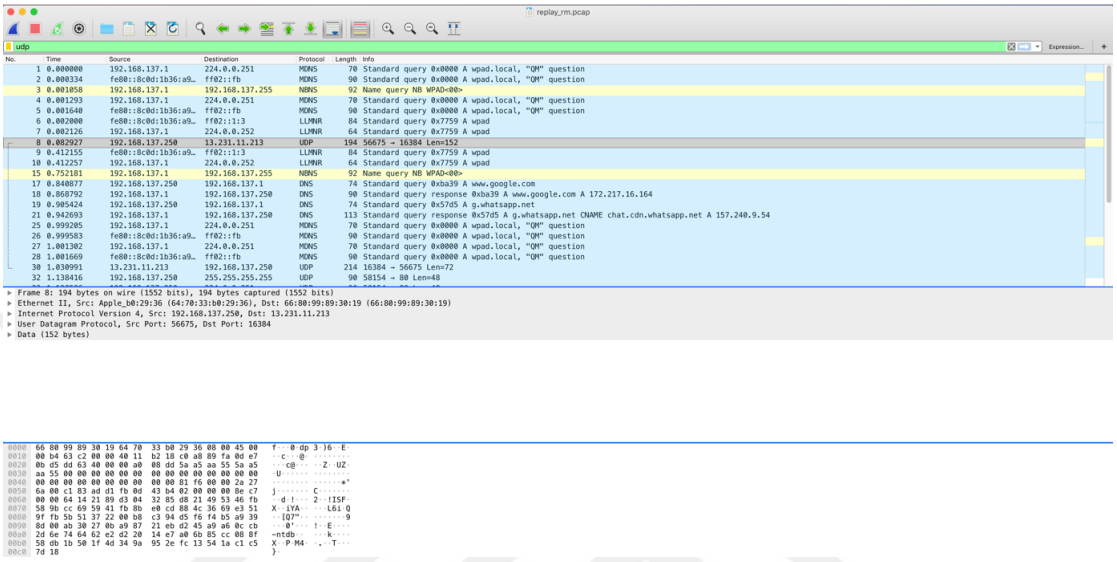
Şekil 5.9:
a) Ana yönetim konsolu ile aynı ağ bağlantısına bağlanınca ana yönetim konsolunun uygulama üzerine otomatik olarak eklendiği durum
b) Ana yönetim konsolu ile aynı ağ bağlantısına bağlı şekilde ana yönetim konsolunun uygulama üzerinden yönetilebildiği durum
c) Ana yönetim konsolu ile aynı ağ bağlantısı kesilse dahi bir kez tanımlandığı için bulut üzerinden kontrol edebilmenin devam ettiği durum

Aynı ana yönetim konsolu birden çok mobil aygıt üzerinden mobil uygulaması ile kontrol edilebilmektedir. Ana yönetim konsolunun yönetimine sahip olan cihaz sınırı bulunmamaktadır. Ana yönetim konsolunun yönetimine sahip olan cihazların listesi herhangi bir yerde bulunmamakta ve bu yönetime sahip kullanıcılar asıl kullanıcısı tarafından kontrol edilememektedir. Bu eksiklik nedeniyle ana yönetim konsolu sahibi, cihazının kontrolünü elinde bulunduran kişileri görüntüleyememekte ve bundan haberdar olamamaktadır. Ana yönetim konsolu, bir başka mobil aygıt üzerine yönetilebilir olarak eklenmesi sonucunda daha önce yönetebilme kabiliyetine sahip olan mobil aygıtlara bilgi ya da bildirim gönderilmediği gözlemlenmiştir. Bu yönetebilme kabiliyetine sahip cıhazları yetkisizleştirebilmenin ana yönetim konsolunu sıfırlamaktan başka türlü mümkün olmadığı tespit edilmiştir. Ana yönetim konsolunu yönetme yetkisi bulunan kişi tüm akıllı ev aygıtlarını yönetebilme yetkisine de sahip olmaktadır. Bu zafiyet sayesinde tüm akıllı ev sistemi kötü niyetli kişiler tarafından ele geçirilebilmektedir.

5.2.2 Ortadaki Adam Saldırısı ile Paket Yakalama

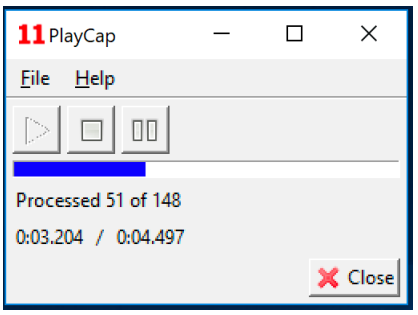
Örnek akıllı ev modeli üzerinde uygulanan testte ana yönetim konsoluna mobil uygulama üzerinden televizyon kumandası yönetimi gerçekleştirilmiştir. Televizyon yönetimi

için televizyon açma, televizyon kapatma, ses açma, ses kapatma ve kanal değiştirme komutları telefon üzerinden gönderilmiştir. Bu aşamada ortadaki adam saldırısı gerçekleştirilerek wireshark aracı ile gönderilen paketler analiz edilmiştir. Analiz edilen paketler doğrultusunda televizyon açma ve televizyon kapatma paketleri kopyalanmıştır.



ŞEKIL 5.10: Wireshark uygulaması ile ortadaki adam saldırısı yapılarak elde edilen komut paketlerinin yakalanmasına ilişkin ekran görüntüsü

Kopyalanan paketler tekrarlama saldırısı (replay attack) yapmak için PlayCap uygulaması ile ana yönetim konsoluna tekrar gönderilmiştir. Gönderilen paketler doğrultusunda televizyonun açıldığı tespit edilmiştir. Televizyon yönetimi için diğer tüm komutlar da test edilmiştir. Yakalanan paketlerin tekrar gönderilmesi sonucunda tüm komutların kullanılabildiği tespit edilmiştir. Cihaza gönderilen paketlerde oturum kontrolü yapılmadığı tespit edilmiştir.



ŞEKIL 5.11: Yakalanan paketlerin PlayCap uygulaması ile tekrarlama saldırısı (replay attack) yapılarak tekrar gönderilmesine ilişkin ekran görüntüsü

Bu yöntem ile bir defaya mahsus ortadaki adam saldırısı yapılsa dahi internet üzerinden ana yönetim konsolu yönetilebilmektedir. Bilinmeyen herhangi bir kablosuz ağa bağlandığımızda ağda bulunan kötü niyetli bir kişi tarafından bu paketler dinlenebilmektedir. Paketler tekrar gönderilerek cihaza erişim sağlanabilmektedir.

5.2.3 Dağıtık Servis Dışı Bırakma Saldırısı

Akıllı ev örnek modelinde yapılan testlerde ana yönetim konsolu ile aynı ağda bulunan kötü niyetli bir saldırgan cihaza sürekli paket göndermesi işlemi test edilmiştir. Test sonucunda saldırganın cihazı servis dışı bırakabildiği tespit edilmiştir. Slowloris python yazılımı ile yapılan dağıtık servis dışı bırakma saldırısında ana yönetim konsolunun gönderilen isteklere cevap veremediği ve mobil uygulamadan gönderilen komutları çalıştıramadığı tespit edilmiştir.

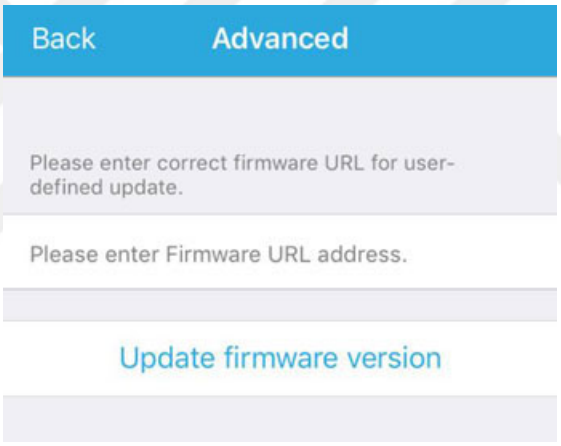
```
sh-3.2# python slowloris.py 192.168.1.100
[26-06-2019 21:45:15] Attacking 192.168.1.100 with 150 sockets.
[26-06-2019 21:45:15] Creating sockets...
[26-06-2019 21:45:16] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:45:32] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:45:48] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:46:04] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:46:20] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:46:36] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:46:51] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:47:06] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:47:21] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:47:36] Sending keep-alive headers... Socket count: 0
[26-06-2019 21:47:51] Sending keep-alive headers... Socket count: 0
```

Şekil 5.12: Slowloris python yazılımı ile ana yönetim konsoluna dağıtık servis dışı bırakma saldırısı düzenlenmiştir.

Dağıtık servis dışı bırakma saldırısı yapılırken ana yönetim konsoluna mobil uygulama üzerinden televizyonu kapatma komutu gönderilmiştir. Mobil cihaz üzerinde bulunan uygulamanın bu komut sonrasında herhangi bir hata vermediği gözlemlenmiştir. Fakat gönderilen komut televizyon tarafından algılanmadığı ve herhangi bir işlem yapılmadığı tespit edilmiştir. Mobil cihazda bulunan uygulama herhangi bir hata vermediği için kullanıcıya işlem yapılmış ve televizyon kapanmış olarak görülmüştür. Bu saldırı yöntemi ile kullanıcının akıllı ev sistemi kullanımı engellenmiştir.

5.2.4 Doğrulanmamış Firmware Yüklenebilme Zafiyeti

Akıllı ev sistemi modeli için kullanılan ana yönetim konsolu aygıt yazılımı (firmware) güncellemesi mobil uygulama üzerinden yapılabilmektedir. Yazılım güncelleme kısmında birden fazla seçenek bulunmaktadır. Yazılım güncelleme aşamasında istenilen bir internet adresi üzerinden doğrulanmamış yazılım güncellenmesi yüklenebilmektedir. Saldırganlar tarafından oluşturulan zararlı yazılım güncellemesi yöntemi ile akıllı ev sistemi ele geçirilebilir ve uzaktan yönetilebilir. İçeriği ile oynanmış bir aygıt yazılımı yükleme sonrasında cihaz üzerinde arka kapı bağlantısı oluşturularak kötü niyetli kişiler tarafından cihazın uzaktan yönetimi ele geçirilebilir. Bu tez kapsamında zararlı yazılım geliştirilerek uygulanmadığı için bir saldırı yöntemi olarak test edilmemiş, zafiyet bulgusu olarak ele alınmıştır.



Şekil 5.13: Mobil uygulama üzerinde internet adresi girilerek doğrulama yapmadan aygıt yazılımı yükleme ekranı

5.3 Akıllı Güvenlik Alarm Sistemi Zafiyet Bulguları

Akıllı güvenlik alarm sistemi fiziksel, kablosuz ağ ve internet üzerinden kontrol edilebilmektedir. Akıllı ev sistemlerinin temelinde kablosuz ağ bağlantısı kullanıldığı için ilk olarak kablosuz ağ zafiyetleri üzerinden test edilmiştir. Diğer bir yöntem olarak ortadaki adam saldırısı (man-in-the-middle) ile paketler yakalanarak test edilmiştir. Bu testlerin yanı

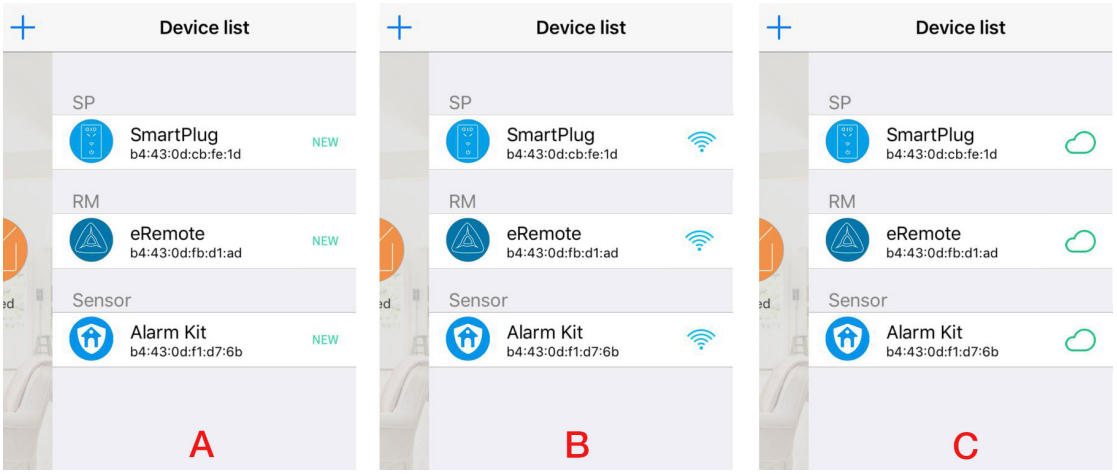
sıra dağıtık servis dışı bırakma saldırısı (Ddos) durumunda cihazın davranışları incelenerek kullanımı etkileyen bir durumun oluşup oluşmadığı test edilmiştir. Alarm sisteminin aygıt yazılımı (firmware) güncelleme aşamasında doğrulanmamış yazılım yüklenebilme durumu incelenmiştir. Aşağıdaki başlıklarda alarm sistemine yapılan güvenlik testlerinin bulgularına yer verilmiştir.

5.3.1 Kablosuz Ağ Zafiyeti

Alarm sistemin de kablosuz ağ bağlantısı kesildiğinde akıllı prizde olduğu gibi bir kablosuz ağ doğrulama zafiyetinin bulunmadığı tespit edilmiştir. Bağlandığı kablosuz ağın aynı isimde ve şifrede olduğunu kontrol ettiği aksi durumda başka bağlantılara bağlanmadığı gözlemlenmiştir.

Alarm sistemi ile aynı ağ bağlantısına bağlı olan mobil cihaz, üzerinde bulunan uygulama ile alarm sistemini yönetilebilmektedir. Burada herhangi bir eşleştirme ya da doğrulama yapmadığı gözlemlenmiştir. Alarm sistemini yönetmek için aynı ağa bağlı olan mobil cihaz üzerinde alarm sisteminin mobil uygulamasına sahip olmanın yeterli olduğu gözlemlenmiştir. Alarm sisteminin mobil uygulaması açıldığında aynı yerel ağ üzerinde bulunan alarm sisteminin otomatik olarak uygulama üzerine mac adresi ile eklendiği görülmüştür. Uygulama herhangi bir şifre, benzersiz kimlik, qr kod ya da bunlar gibi başka hiçbir bilgi istememektedir. Uygulama üzerine eklenen akıllı ev cihazları bulut yapı sayesinde dünyanın herhangi bir yerinden kontrol edilebilmektedir. Bu zafiyet sayesinde alarm sistemi ile aynı ağa sadece bir kere bağlı olmanın o cihazın kontrolünü ele geçirebilmek için yeterli olduğu anlaşılmıştır. Cihazın kontrolünü ele geçiren kötü niyetli kişinin bundan sonra bulut üzerinden herhangi bir yerde ve zamanda alarm sistemi kontrol edilebileceği gözlemlenmiştir.

Aynı alarm sistemi birden çok mobil aygıt üzerinden mobil uygulaması ile kontrol edilebilmektedir. Alarm sisteminin yönetimine sahip olan cihaz sınırı bulunmamaktadır. Alarm sisteminin yönetimine sahip olan cihazların listesi herhangi bir yerde bulunmamakta ve bu yönetime sahip kullanıcılar asıl kullanıcısı tarafından kontrol edilememektedir. Bu eksiklik nedeniyle alarm sistemi sahibi cihazının kontrolünü elinde bulunduran kişileri



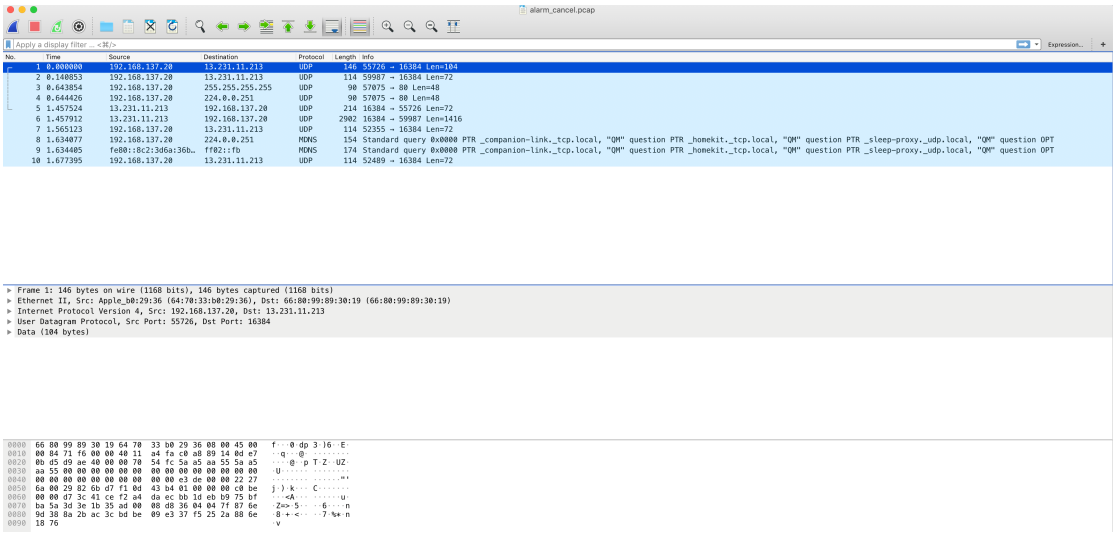
Şekil 5.14:
a) Alarm sistemi ile aynı ağ bağlantısına bağlanınca alarm sisteminin uygulama üzerine otomatik olarak eklendiği durum
b) Alarm sistemi ile aynı ağ bağlantısına bağlı şekilde alarm sisteminin uygulama üzerinden yönetilebildiği durum
c) Alarm sistemi ile aynı ağ bağlantısı kesilse dahi bir kez tanımlandığı için bulut üzerinden kontrol edebilmenin devam ettiği durum

görüntüleyememekte ve bundan haberdar olamamaktadır. Alarm sisteminin bir başka mobil aygıt üzerine yönetilebilir olarak eklenmesi sonucunda daha önce yönetebilme kabiliyetine sahip olan mobil aygıtlara bilgi ya da bildirim gönderilmediği gözlemlenmiştir. Bu yönetebilme kabiliyetine sahip cıhazları yetkisizleştirebilmenin alarm sistemini sıfırlamaktan başka türlü mümkün olmadığı tespit edilmiştir.

5.3.2 Ortadaki Adam Saldırısı ile Paket Yakalama

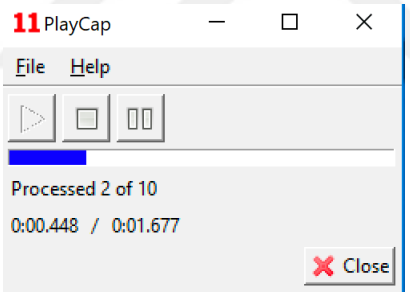
Örnek akıllı ev modeli üzerinde uygulanan testte mobil uygulama üzerinden alarm sisteminin yönetimi gerçekleştirilmiştir. Alarm sisteminin yönetimi için alarm sistemini devreye sokma ve alarm sistemini devre dışı bırakma komutları telefon üzerinden gönderilmiştir. Bu aşamada ortadaki adam saldırısı gerçekleştirilerek wireshark aracı ile gönderilen paketler analiz edilmiştir. Analiz edilen paketler doğrultusunda alarm sistemini devreye sokma ve alarm sistemini devre dışı bırakma paketleri kopyalanmıştır.

Kopyalanan paketler tekrarlama saldırısı (replay attack) yapmak için PlayCap uygulaması ile alarm sistemine tekrar gönderilmiştir. Gönderilen paketler doğrultusunda



Şekil 5.15: Wireshark uygulaması ile ortadaki adam saldırısı yapılarak elde edilen komut paketlerinin yakalanmasına ilişkin ekran görüntüsü

alarm sisteminin devre dışı kaldığı tespit edilmiştir. Yakalanan paketlerin tekrar gönderilmesi sonucunda tüm komutların kullanılabildiği tespit edilmiştir. Cihaza gönderilen paketlerde oturum kontrolü yapılmadığı tespit edilmiştir.

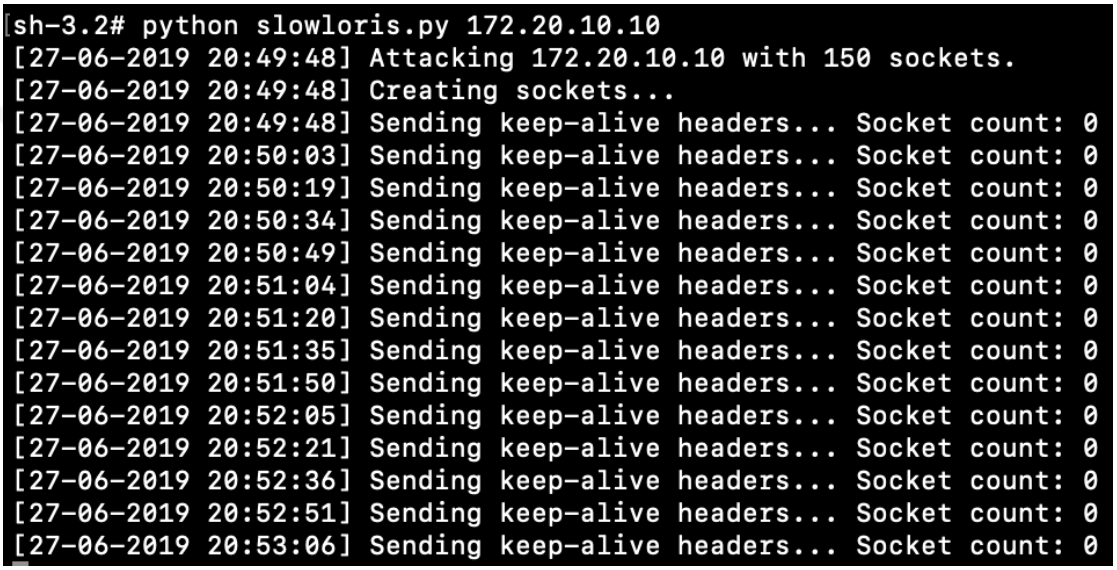


Şekil 5.16: Yakalanan paketlerin PlayCap uygulaması ile tekrarlama saldırısı (replay attack) yapılarak tekrar gönderilmesine ilişkin ekran görüntüsü

Bu yöntem ile bir defaya mahsus ortadaki adam saldırısı yapılsa dahi internet üzerinden alarm sistemi uzaktan yönetilebilmektedir. Bilinmeyen herhangi bir kablosuz ağa bağlandığımızda ağda bulunan kötü niyetli bir kişi tarafından bu paketler dinlenebilmektedir. Paketler tekrar gönderilerek cihaza erişim sağlanabilmektedir.

5.3.3 Dağıtık Servis Dışı Bırakma Saldırısı

Akıllı ev örnek modelinde yapılan testlerde alarm sistemi ile aynı ağda bulunan kötü niyetli bir saldırgan cihaza sürekli paket göndermesi işlemi test edilmiştir. Test sonucunda saldırganın cihazı servis dışı bırakabildiği tespit edilmiştir. Slowloris python yazılımı ile yapılan dağıtık servis dışı bırakma saldırısında alarm sisteminin gönderilen isteklere cevap veremediği ve mobil uygulamadan gönderilen komutları çalıştıramadığı tespit edilmiştir.



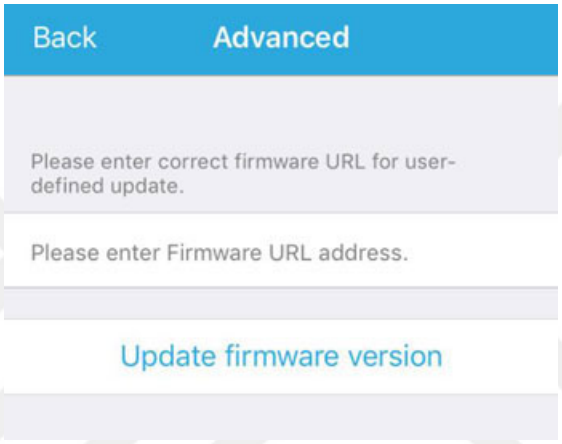
Şekil 5.17: Slowloris python yazılımı ile dağıtık servis dışı bırakma saldırısı düzenlenmiştir.

Dağıtık servis dışı bırakma saldırısı yapılırken alarm sistemine mobil uygulama üzerinden alarm sistemini devreye sokma komutu gönderilmiştir. Mobil cihaz üzerinde bulunan uygulamanın bu komut sonrasında herhangi bir hata vermediği gözlemlenmiştir. Fakat gönderilen komut sonrasında alarm sisteminin devreye girmediği gönderilen komutun algılanmadığı tespit edilmiştir. Mobil cihazda bulunan uygulama herhangi bir hata vermediği için kullanıcıya işlem yapılmış ve alarm sistemi devreye girmiş olarak görülmüştür.

5.3.4 Doğrulanmamış Firmware Yüklenebilme Zafiyeti

Akıllı ev sistemi modeli için kullanılan akıllı alarm sistemi yazılımı (firmware) güncellemesi mobil uygulama üzerinden yapılabilmektedir. Yazılım güncelleme kısmında

birden fazla seçenek bulunmaktadır. Yazılım güncelleme aşamasında istenilen bir internet adresi üzerinden doğrulanmamış yazılım güncellenmesi yüklenebilmektedir. Saldırganlar tarafından oluşturulan zararlı yazılım güncellemesi yöntemi ile akıllı ev sistemi ele geçirilebilir ve uzaktan yönetilebilir. İçeriği ile oynanmış bir aygıt yazılımı yükleme sonrasında cihaz üzerinde arka kapı bağlantısı oluşturularak kötü niyetli kişiler tarafından cihazın uzaktan yönetimi ele geçirilebilir. Bu tez kapsamında zararlı yazılım geliştirilerek uygulanmadığı için bir saldırı yöntemi olarak test edilmemiş, zafiyet bulgusu olarak ele alınmıştır.



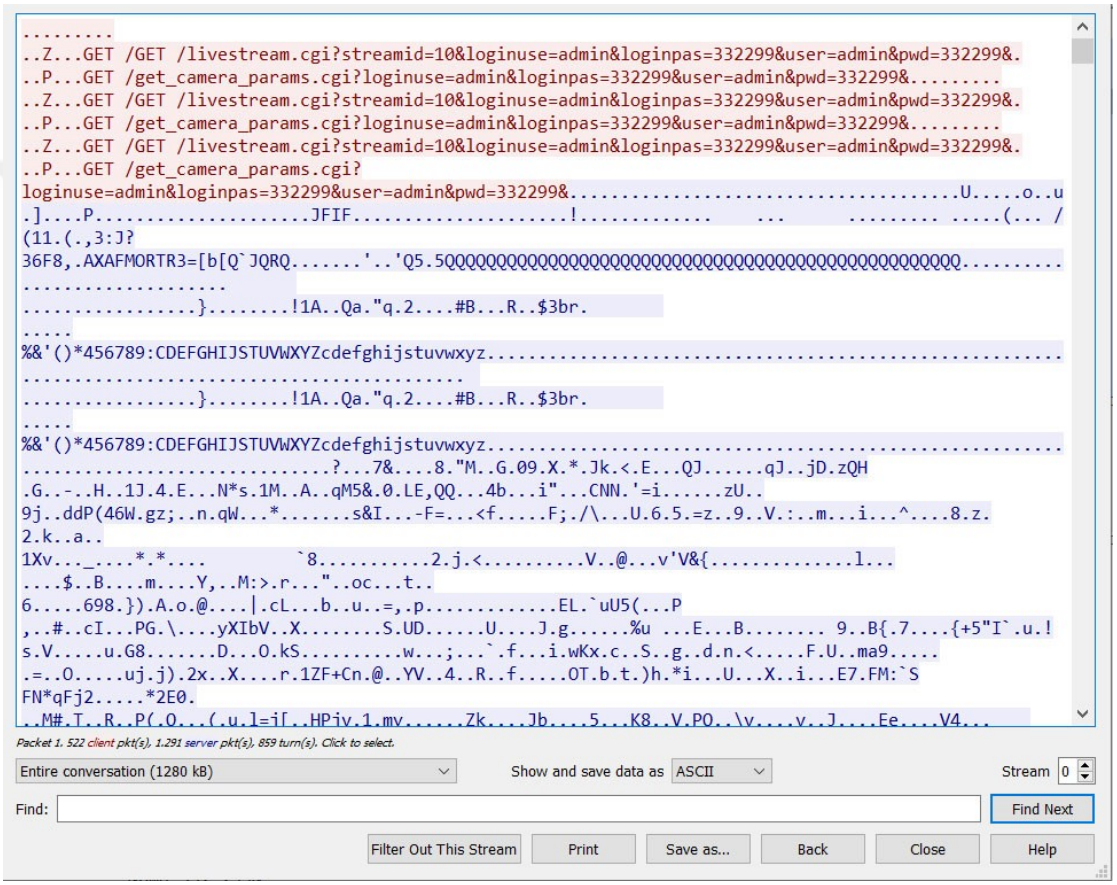
Şekil 5.18: Mobil uygulama üzerinde internet adresi girilerek doğrulama yapmadan aygıt yazılımı yükleme ekranı

5.4 Güvenlik ve Bebek İzleme Kamerası Zafiyet Bulguları

Akıllı güvenlik kamerasına diğer akıllı ev cihazlarına yapılan kablosuz ağ zafiyeti testleri yapılmış bu testler sonucunda zafiyet bulgusu bulunamamıştır. Dağıtık servis dışı bırakma saldırısı yapıldığı sırada akıllı güvenlik kamerasına bağlanılmış, görüntü izlenmiş ve kamera hareket ettirilerek kullanılmıştır. Bu denemeler sırasında akıllı güvenlik kamerasının dağıtık servis dışı bırakma saldırılarından kullanımını etkileyen bir zafiyeti olmadığı tespit edilmiştir.

5.4.1 Ortadaki Adam Saldırısı ile Paket Yakalama

Telefon uygulaması üzerinden güvenlik kamerası canlı olarak izlenirken, aynı anda ortadaki adam saldırısı testi gerçekleştirilmiştir. Ortadaki adam saldırısı sırasında Wireshark aracı ile yakalanan veri paketleri incelenerek analiz edilmiştir. Analiz edilen paketlerde kameranın kullanıcı adı ve parolasının gönderilen veri paketlerinin her birinde açık metin olarak herhangi bir şifreleme algoritması kullanılmadan gönderildiği tespit edilmiştir.



Şekil 5.19: Akıllı güvenlik kamerasının gönderdiği paket ortadaki adam saldırısı ile yakalanarak içeriği görüntülenmiştir.

Gönderilen veri paketlerinde geçen

```
'loginuse=admin&loginpas=332299&user=admin&pwd=332299&.'
```

satırı akıllı güvenlik kamerasının kullanıcı adı ve şifresini açık metin olarak göstermektedir. Ortak kullanıma sahip herhangi bir kablosuz ağa bağlı kullanıcı kamerasının görüntülerini izlemek istediğinde aynı ağda bulunan kötü niyetli bir kişi tarafından bu veri paketleri yakalanarak analiz edilebilir. Analiz edilen veri paketlerinde kameranın kullanıcı adı ve parolasının açık metin olarak gönderilmesi sonucunda saldırgan kamera izleme uygulamasını kullanarak kamerayı uzaktan kontrol edebilmekte ve izleyebilmektedir. Kameranın birden fazla kişi tarafından aynı anda veya farklı zamanlarda izlenmesinde herhangi bir sorun oluşmadığı ve bununla ilgili olay kayıtlarının kullanıcının görüntüleyebileceği şekilde tutulmadığı tespit edilmiştir. Bu sebeplerden dolayı asıl güvenlik kamerasının sahibi olan kullanıcı evinde kullandığı kameranın başkaları tarafından ele geçirildiğini anlayamamaktadır.

5.4.2 Hatalı Oturum Yönetimi ve Kritik Bilgi İfşası Zafiyeti

Bu çalışmada [51] yapıldığı gibi 'loginuse ve loginpass' parametresi kameranın web erişim paneline boş gönderildiğinde oturum kontrolünün atlatıldığı ve oturumun başlatıldığı tespit edilmiştir. Web sayfası üzerinden ip adresine gönderilen parametre

```
'http://192.168.1.105:81/system.ini?loginuse&loginpas'
```

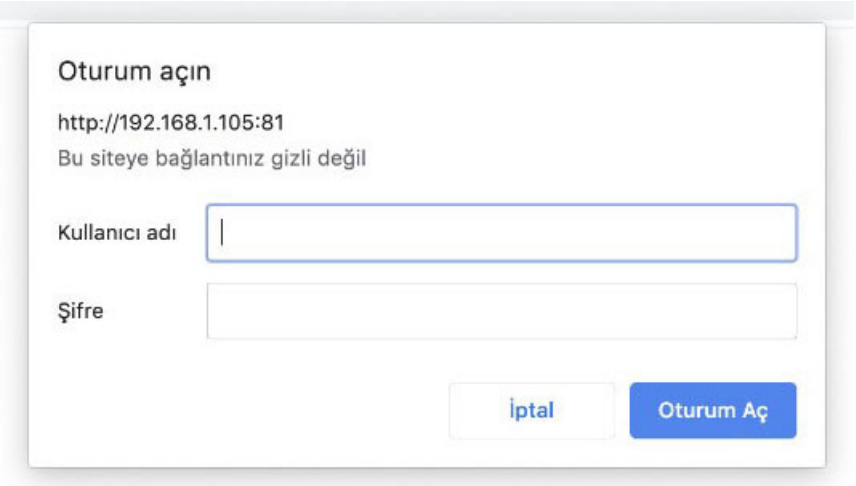
şeklindedir. Oturum kontrolünü atlattıktan sonra 'system.ini' dosyasının içeriğine erişilebilmektedir. Bu dosyada kablosuz ağın kullanıcı adı ve parolası, kameranın kullanıcı adı ve parola bilgilerinin açık metin olarak tutulduğu tespit edilmiştir. Kötü niyetli bir saldırgan bu bilgileri alarak kamerayı uzaktan izleyebilmektedir ve yönetebilmektedir.

```
sh-3.2# curl 'http://192.168.1.105:81/system.ini?loginuse&loginpas'|xxd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5020  100  5020    0     0  50586      0 --:--:-- --:--:-- --:--:-- 50707
00000000: 5653 5443 3138 3632 3539 474b 464d 4500  VSTC186259GKFME.
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 4950 4341 4d00 0000 0000 0000 0000 0000  IPCAM...........
---
00000760: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000770: 0000 0000 6164 6d69 6e00 0000 0000 0000  ....admin.......
00000780: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000790: 0000 0000 3638 3432 3234 0000 0000 0000  ....332299......
000007a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
---
00000900: 0000 0000 0000 0000 6275 7261 6b6b 0000  ........burakk..
00000910: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000920: 0000 0000 0000 0000 0000 0000 0000 0000  ................
---
00000a30: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a40: 0000 0000 0000 0000 0000 0000 6275 7261  ............bura
00000a50: 6b6b 3638 3432 3234 0000 0000 0000 0000  kk123456........
00000a60: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Şekil 5.20: Akıllı güvenlik kamerası system.ini dosya içeriği

5.4.3 Kaba Kuvvet Saldırısı

Akıllı güvenlik kamerasının 81 portu üzerinden web ara yüzüne erişilmiştir. Akıllı kameranın basit oturum başlatma yöntemi kullandığı tespit edilmiştir. Basit bir oturum başlatma yöntemi olduğu için gönderilen kullanıcı adı ve parolaların insan bilgisayar ayrımı için kullanılan test (captcha) şeklinde kaba kuvvet saldırılarını engelleyici bir özelliği bulunmamaktadır. İnsan bilgisayar ayrımı testi bulunmadığı için kaba kuvvet saldırısı yapılabilmektedir.



Şekil 5.21: Akıllı güvenlik kamerası oturum açma ekranı

5.5 Zafiyetler Sonucu Olası Senaryolar

Senaryo 1: Akıllı ev modelinde kullanılan akıllı prize sahip bir kullanıcının kablosuz ağı kesilerek oluşturulan aynı isimdeki ikiz şifresiz kablosuz ağa prizin bağlanması sağlanabilir. Bu şekilde akıllı priz ile aynı ağ bağlantısı üzerinde olan kötü niyetli kişi akıllı prizi ele geçirebilir. Kablosuz ağ modem düşürme saldırısı (airodump-ng) ile kablosuz ağın yeniden başlatılması sağlanabilir.Bir diğer yöntem olarak şebeke elektriği sigortadan kapatılıp tekrar açılarak akıllı prizin kablosuz ağdan önce açılması sağlanabilir. Kablosuz ağ tekrar başlayana kadar şifresiz ama aynı kablosuz ağ adına sahip ikiz kablosuz yayın yapılarak başkantısı kesilen cihazın yeni kablosuz ağa bağlanması sağlanabilir.

Senaryo 2: Akıllı ev modelinde kullanılan ana yönetim konsolu, akıllı priz ve akıllı alarm sistemine sahip bir kullanıcı kafe ya da havalimanı gibi kablosuz internetin ortak kullanım alanlarından internete erişerek, akıllı cihazını kontrol etmek istediğinde oluşturduğu veri paketleri bağlı bulunduğu ağ üzerinden gönderilmektedir. Aynı ağa bağlı kötü niyetli bir kişi o sırada ağ üzerinde ağ dinlemesi yapabilir ya da ortadaki adam saldırısı için mevcutta bulunan kablosuz ağ bağlantısını taklit ederek gönderilen paketlerin internete kendi üzerinden geçmesini sağlayabilir. Bu şekilde elde ettiği paketleri analiz ederek bunların akıllı cihazı kontrol etmek için kullanılan paketler olduğunu anlayabilir. Bu paketleri toplayıp, kaydederek akıllı cihazın kontrolünü yetkisiz bir şekilde internet

üzerinden yapabilir, yönetimini ele geçirebilir.

Senaryo 3: Akıllı priz üzerinde bulunan röle ile prizin elektrik bağlantısını açıp kapatmaktadır. Senaryo 2 de ki gibi bu paketleri yakalanan kötü niyetli kişi zarar vermek için sürekli yakaladığı bu paketleri akıllı prize internet üzerinden gönderilebilir ve akıllı prizin sürekli açılıp kapanarak bozulmasını sağlayabilir. Bu esnada asıl akıllı prizin kullanıcısının prize erişimini talep çoğunluğu sebebiyle engelleyebilir. Bireysel bir zarara ve kullanımı etkilemeye sebep olabilir.

Senaryo 4: Senaryo 3 de anlatılan bir şekilde saldırı gerçekleştirildiğinde akıllı prize o esnada bağlı olan elektronik cihazın sürekli elektrik gelip gitmesine bağlı olarak bozulmasına sebep olabilir. Bu bağlı olan cihazın ütü, su ısıtıcısı, elektrikli ısıtıcı gibi yüksek enerji çeken bir cihaz olması durumunda olası yangın çıkma riskleri bulunmaktadır. Çıkan olası bir yangın durumunda aynı bina ya da aynı mahalle yangından etkilenebilir. Bu şekilde bireysel zarar, kullanımı engelleme ve toplumsal zarara sebebiyet verebilir.

Senaryo 5: Akıllı ev sisteminin yönetimini ele geçiren kötü niyetli bir kişi akıllı ev sistemini yönetme yetkilerini mobil uygulama üzerinden başkalarıyla da paylaşabilmektedir. Kötü niyetli kişiler deep web gibi yerlerde bu yetkileri satabilir.

Senaryo 6: Akıllı güvenlik kamerası kötü niyetli kişiler tarafından shodan benzeri arama motorları ile tespit edilerek oturum atlama yöntemi ya da kaba kuvvet saldırısı ile şifresi ele geçirilebilir. Sonrasında kamera izlenebilir, yönetilebilir ve başkalarının kontrolü altında DYN dns servis sağlayıcısına yapılan saldırı [4] gibi saldırılarda botnet olarak kullanılabilir.

Bölüm 6

Sonuç ve Öneriler

Oluşturulan örnek akıllı ev modelinde kullanılan akıllı ev sistemi cihazlarının olası bir siber saldırı sonucunda ne tür etkiler verdiği ve güvenlik zafiyetleri barındırıp barındırmadığı test edilerek incelenmiştir. Kullanıcı kitlesi yüksek olan akıllı ev cihazları seçilerek, bu cihazların olası zafiyetler kullanılarak yapılabilecek siber saldırı sonucunda kullanılabilirliği etkileyen, bireysel ve toplumsal açıdan oluşturabileceği zararlar araştırılmış ve ortaya konmuştur. Kullanılan örnek modellerin tamamında yapılan testler sonucunda zafiyetler tespit edilmiştir. Bu durumlarla ilgili olası senaryolar yazılarak nelerin yapılabileceği örneklendirilmiştir.

Yapılan testler sonucunda çok temel olan güvenlik tedbirlerinin dahi alınmadığı tespit edilmiştir. Üretilen akıllı ev sistemlerinin piyasaya sürülmeden önce güvenlik testlerinin yapılmadığı ve bazı durumlar karşısında ne tür etkiler vereceğinin araştırılmadığı gözlemlenmiştir.

Kullanılan örnek modellerin aygıt yazılım (firmware) sürümlerinin son olarak yayınlanan versiyonlarda olduğu ve bu tez kapsamında araştırıldığı zamana kadar bu zafiyetlerin tespit edilmediği, edilse dahi herhangi bir tedbir alınmadığı tespit edilmiştir.

Akıllı ev sistemleri teknolojisinin henüz yeni bir teknoloji olduğu, kullanım oranının hızla arttığı ve yaygınlaştığı, Iot cihaz sayısının 2020 yılında 34 milyara ulaşacağı göz önünde bulundurulduğunda gelecekte güvenlik zafiyetlerinin çok ciddi problemlere yol açacağı

kaçınılmaz bir gerçektedir. Bununla ilgili olarak üretici, kullanıcı ve devletlerin tedbir almaları ve çözüm üretmeleri gerekmektedir [10].

Hayatımızı kolaylaştıran ve konfor sağlayan akıllı ev sistemlerine yapılacak siber saldırılar karşısında maksimum seviyede korunmak ve kullanılabilirliğin devamını sağlamak, bunun yanı sıra çalışma kapsamında oluşturulan olası senaryolara çözüm için üreticiler ve kullanıcılar tarafından alınması gereken güvenlik tedbirlerinin neler olduğu aşağıda sıralanmıştır.

- **Varsayılan şifre kullanımı ve politikası;** Akıllı ev sistemi cihazlarının fabrika çıkışı olarak üzerinde gelen, kullanım kılavuzlarında ve internette bulunan hatta bazı cihazların üzerine etiketle yazılmış olan varsayılan şifreleri değiştirmek cihazı kullanmadan önce ilk yapılması gereken işlemdir. Üreticiler, kullanıcıların cihaz kurulumu yaptıktan sonra bu ilk kurulumla gelen varsayılan şifreleri değiştirmek için kullanıcıların karşısına mesajlar çıkartmalı ya da bu varsayılan şifreyi değiştirmeye kullanıcıları zorunlu tutmalıdır. Üreticiler cihazlara varsayılan şifre olarak 1234, 8888 gibi tek sayıdan oluşan veya ardışık basit şifreler koymamalıdır. Cihazlar tak çalıştır olarak adlandırılan kolay kuruluma sahip ürünler olduğu için her ürün benzersiz bir şifre ile şifreli bir şekilde satılmalı, şifre kullanıcıya ürün ile birlikte verilerek ilk kurulum sonrası değiştirmeye mecbur bırakılmalıdır.

- **Güçlü şifre kullanımı;** Kullanıcılar akıllı ev sistemi cihazlarının parolalarını belirlerken güçlü ve tahmin edilmesi güç parolalar kullanmalıdır. Günümüzde kullanılan IOT cihazlarının çoğu sadece rakam ile parola vermeyi kabul etmektedir. 6 Haneli bir parola koyduğunuzu düşünürsek 1.000.000 parola denemesi gerekmektedir. Web sayfalarına yapılan parola saldırılarında ortalama 1 saniyede 4 parola denenebildiği göz önünde bulundurulursa ortalama 5 saatte bu basit parolalar tespit edilebilmektedir. Üreticiler büyük harf, küçük harf, sembol ve rakam içermeyen parola koyabilmeyi engellemeli ve kullanıcıların güçlü parolalar koymasını zorunlu hale getirmelidir. Parola giriş ekranlarına yanlış parola deneme sınırları koymalı belli bir denemeden sonra süre beklemeli deneme ya da insan bilgisayar ayrımı için kullanılan test (captcha) şeklinde kaba kuvvet saldırılarını engelleyici yazılımlar kullanmalıdır.

- **Kullanıcı yetkilendirme ve yetki yönetimi;** Üreticiler tüm akıllı ev cihazlarının yönetim panellerinde ya da mobil uygulamalarında kullanıcı yetkilerini ayarlayabilme modülleri geliştirmelidir. Akıllı ev cihazlarını yönetme yetkisine sahip olan kullanıcılara ait mobil cihazların listesi mobil uygulama üzerinden yönetici olan kullanıcıya gösterilmelidir. Cihazları yönetebilme yetkisine sahip olan kullanıcılar mobil uygulama üzerinde yetki seviyelerine göre yönetici ve görüntüleyici gibi yetkilendirilebilmelidir. Yetki seviyeleri farklı kullanıcı hesapları açılabilmelidir. Yönetici olan kullanıcı bu liste üzerinde yetkisi olan cihazların yetkisini düzenleyebileceği, kaldırabileceği ve geçici olarak engelleyebileceği bir yapı ile yönetim listesini yönetebilmelidir. Akıllı cihazlara erişim yetkisi olan diğer hesapların bu yetkiye ne zaman sahip olduklarını görebilmeli ve yetkisini kaldırdığı anda sistem üzerinden atılmalarını sağlayabilmelidir.

- **İki faktörlü doğrulama kullanımı;** Üreticiler tarafında yapılacak geliştirme ile kullanıcı hesaplarında iki faktörlü doğrulama kullanılmalıdır. Kullanıcının eriştiği cihaz kayıt edilmeli farklı bir cihazdan erişmek isterse cihaz üzerinden oturum açabilmesi için iki faktörlü doğrulama adımlarını tamamlayarak yetkili bir kullanıcı olduğunu teyit etmelidir. İkinci faktör olarak cep telefonu numarasına gönderilecek bir sms, bir mail üzerinden gönderilecek benzersiz kod ile birlikte bir akıllı ev cihazının cihaz kimliği kullanılabilir.

- **Akıllı ev için özel ağ ve misafir ağı kullanımı;** Akıllı ev sistemlerinin güvenliği açısından kullanıcıların alması gereken en önemli ve ilk önlemlerden biri de kablosuz ağlar için farklı bir vlan kullanmaktır. İnternete erişim için kullandığımız ortak olan kablosuz ağ yerine akıllı ev cihazlarının kullanımı için farklı bir kablosuz ağ oluşturmak ve bu kablosuz ağı sadece onların kullanmasını sağlamak gerekmektedir. Misafirler için de misafir ağı oluşturarak geçici olarak internetimizi paylaşmak istediğimiz ziyaretçilerimizin bu ağı kullanmalarını sağlamak, bu tez kapsamında tespit edilen kablosuz ağ zafiyetlerini de önleyebilmektedir.

- **Aygıt yazılımı ve uygulama güncelleme politikası;** Cihazlar kurulum sonrasında üretici firma tarafından yayınlanan aygıt yazılım (firmware) güncellemeleri ile kullanmadan önce son yayınlanan versiyona güncellenmelidir. Üretici firmalar kullanıcı geri dönüşleri, yapılan test ve analizler sonucuna göre tespit edilen zafiyet,hata ve yazılım sorunlarını kullanıcıların yükleyebilmesi için yayınlayacakları aygıt yazılım

güncellemeleri ile gidermelidir. Yeni bir aygıt yazılım güncellemesi yayınlandığında kullanıcıların bundan haberdar olabilmesi ve kolayca güncelleyebilmesi için kullanıcılara otomatik güncelleme bildirimleri çıkararak gerekli uyarılarda bulunulması gerekmektedir. Kullanıcılar bu güncellemeleri ertelemek istese dahi ileri bir zamanda otomatik kurulum onayı alarak kullanıcıları bu güncellemeleri yüklemeye zorlamalıdır. Üreticiler aygıt yazılım güncellemesinde olduğu gibi mobil uygulamalarında sık sık geliştirme ve hata giderme yaparak güncelleştirmelidir. Üreticiler cihazların aygıt yazılım güncellemesi yükleme seçeneklerini doğrulama olmadan üçüncü kaynaklar tarafından yüklenebilecek şekilde yapılandırmamalıdır. Üretici firmaya ait güvenli ve yedekli sunucular üzerinden doğrulanmış aygıt yazılım sürümlerini yükleyebilecek şekilde bir yapıda aygıt yazılım güncelleme işlemleri gerçekleştirilmelidir.

- **Trafiğin ssl sertifikası ile şifrelenerek kullanımı;** Akıllı ev sistemleri kontrolü için kullanılan tüm trafiğin ssl sertifikası ile şifrelenmesi gerekmektedir. Üretici bulut kontrol için kendi sunucusu üzerinden göndereceği tüm trafiği ssl sertifikaları ile şifreleyerek yapmalıdır. Kullanıcılar kendi statik ip adresleri üzerinden gerçekleştireceği akıllı kamera kayıtları gibi trafikleri kendilerinin temin edeceği ssl sertifikalar ile şifrelenmesini sağlamalıdır.

- **Cihaz tanımlamada doğrulama politikası;** Bu tez kapsamında oluşturulan akıllı ev modelinde test edilen cihazlar mobil uygulama üzerine aynı ağa bağlı olma durumunda otomatik olarak tanımlanabiliyor. Cihazların mobil uygulama üzerine tanımlanabilmesi için cihazın benzersiz kimliğini bilmek, cihaz üzerinde daha önce yetkisi olan kullanıcılardan eş zamanlı onay almak, cihazlar üzerinde oturum açmak için tanımlı kullanıcı hesapları olması gerekmektedir. Herhangi bir şekilde aynı ağa bağlı olan kullanıcılara cihazların otomatik olarak yönetim yetkisini vermek çok ciddi bir zafiyet sorunudur.

- **Mac filtrelemesi kullanımı;** Kablosuz ağ bağlantısına bağlanan cihazların mac adreslerine göre erişim izni verilmesi kablosuz ağ güvenliğini arttırmaktadır. Modem üzerinden ağ için mac adres filtrelemesi açılmalıdır. Bu sayede sahte erişim noktası saldırısı ile ya da başka bir şekilde kablosuz ağ şifresi ele geçirilmiş olsa dahi kablosuz ağa kötü niyetli bilgisayar korsanları bağlanamayacaklardır.

- **Kablosuz ağ doğrulaması;** Kablosuz ağa bağlanan akıllı ev cihazlarının bağlandıkları kablosuz ağı doğrulaması gerekmektedir. İlk kurulumdan sonra kendi hafızasında tuttuğu kablosuz ağa ait isim ve şifre bilgisini doğrulama için kullanarak aynı ağa tekrar bağlanabilmeli, şifresi farklı olan diğer kablosuz ağlara bağlanmaması gerekmektedir.

- **Kullanılan portların değiştirilmesi;** Akıllı ev cihazlarının kullandığı varsayılan portların kullanıcılar tarafından başka portlarla değiştirilmesi güvenlik için bir önlemdir. Örneğin akıllı güvenlik kamerası için varsayılan port yerine 1025 ile 65535 aralığında bir port girilerek görüntü izleme uygulaması üzerinde bu yeni girilen portlara göre değişiklik yapılarak port güvenliği kullanıcı tarafından sağlanmış olmaktadır.

- **Jeton kullanarak benzersiz paket üretimi;** Cihazlara gönderilen veri paketleri her seferinde benzersiz ve rastgele oluşturulan bir değer ile üretilmiş jeton (token) kullanmalıdır. Bu sayede paketi ele geçiren bir bilgisayar korsanı paketi tekrar gönderme saldırısı ile akıllı ev aygıtına tekrar gönderse bile paket geçersiz olacağı için herhangi bir işlem yapılmayacaktır.

- **Paket içeriğinin hash ve şifreli kullanım politikası;** Test edilen akıllı güvenlik kamerası kullanıcı adı ve şifre bilgilerinin yanı sıra bağlı olduğu kablosuz ağ ismi ve şifresini düz metin (clear text) olarak iletişim paketlerinde kullanmaktadır. Üretici tarafından zafiyetli bir şekilde planlanan bu veri iletişim fonksiyonunun şifreli olması gerekmektedir. Bunun gibi bilgiler ilk eşleştirme paketinde şifreli bir şekilde gönderilmeli daha sonraki iletişimin devamında gönderilen paketlerde hash olarak gönderilmelidir. Bu sayede kötü niyetli kişilerin paketleri ele geçirmesi durumunda bile şifreyi çözmeleri çok zor olacaktır.

- **Dağıtık servis dışı bırakma saldırılarına karşı önlem;** Cihazların dağıtık servis dışı bırakma saldırılarına maruz kaldığı durumlarda istekleri karşılayamadığını tespit eden bir hata mekanizması olması gerekmektedir. Cihazlar taleplerin çok olduğu durumlarda bu talepleri karşılayamayacağını yönetici olan kullanıcıya bildirmelidir. Kullanıcı bu saldırı altındaki cihaza bir komut gönderdiğinde talep yoğunluğu altındaki cihazın farkına varmayabilir ve yaptığı işlemin gerçekleştiğini zannedebilir.

- **Olay günlüğü kayıtlarının incelenmesi ve takibi;** Akıllı ev sistemi cihazlarının olay günlüğü kayıtlarını (log) yetkisiz erişimin olup olmadığını anlamak için belirli aralıklarla kullanıcının kontrol etmesi gerekmektedir. Herhangi bir yetkisiz erişim durumunda ne tür işlemlerin yapıldığı bu kayıtlar sayesinde tespit edilebilmektedir.

- **Fiziki erişimlere karşı alınması gereken tedbirler;** Akıllı ev sistemi cihazlarına fiziki erişim olması durumunda cihazlar sıfırlanarak kullanım engellenebilir. Alarm sistemi, kamera gibi cihazlar etkisiz hale getirilebilir. Üzerinde bulunan hafıza kartına kayıt yapan güvenlik kameralarının üzerinde bulunan hafıza kartları çalınarak güvenlik görüntüleri yok edilebilir. Bunun gibi durumlar için bu tip cihazların kolay erişilebilir olmaması ve korunaklı bölmelerde bulunması önemlidir.

- **Çoklu yayın akışının kullanılmıyorsa kapatılması;** Akıllı kameralar üzerinde bulunan canlı yayın akışını çoklu yayın (multicast) olarak aktarmaya yarayan özelliği, eğer kamera görüntülerini farklı depolama aygıtlarına kaydetmiyorsak devre dışı bırakmamız gerekmektedir.

- **Anonim bağlantıların kapatılması;** Akıllı güvenlik kameralarında bulunan anonim bağlantıların kapalı olması gerekmektedir. Aksi halde kamera internet üzerinden kullanıcı oturumu açmadan yayın yapan kameralar tarzında çalışacak ve görüntülerin başkaları tarafından izlenmesini sağlayacaktır.

- **Gerçek zamanlı yayın doğrulamasının açılması ve port değişikliği;** Akıllı güvenlik kameralarında bulunan gerçek zamanlı yayın protokolunun doğrulama özelliği bazı güvenlik kameralarında varsayılan olarak kapalı gelmektedir. Bu doğrulama güvenliğinin açık olması ve varsayılan olarak gelen 554 portunun kullanıcılar tarafından değiştirilmesi kamera görüntülerinin güvenliği açısından önemlidir.

- **UPNP özelliğinin kapatılması;** Modem ve yönlendirici (router) üzerinde bulunan UPNP veya Universal Plug and Play özellikleri devre dışı bırakılmalıdır. Akıllı ev sistemi gibi ağ cihazlarının kolayca algılanması için geliştirilen bu özellik çok ciddi güvenlik açıklıkları ve hatalar barındırmaktadır. Zararlı yazılımlar sayesinde internet trafiğimiz bazı ip adreslerine bu özelliğin zafiyeti ile yönlendirilebilmektedir [52].

Her ne kadar kullanıcı ve üreticilere bu güvenlik zafiyetlerini gidermek için birçok görev düşse de üretici ve kullanıcıların haklarını gözetmek, gerekli olduğu durumlarda denetlemek ve bununla ilgili standartlar belirlemek uluslararası organizasyon ve devletlerin alması gereken sorumluklardandır.

Bu tez kapsamında yapılan örnek akıllı ev modelinde kısıtlı imkanlardan dolayı yapılamamış ancak gelecek çalışmalarda yapılması durumunda yararlı sonuçlar elde etmeye yarayacak çalışma örnekleri aşağıda belirtilmiştir.

- Akıllı ev cihazı kategorisinde olan bu tez kapsamında kullanılmayan diğer akıllı ev cihazlarının aynı saldırılar karşısında vereceği sonuçlar analiz edilmeli ve çıkan sonuçlar ilgili sonuçlarla karşılaştırılmalıdır.
- Akıllı ev cihazlarının yazılımları aygıt yazılım güncelleme zafiyeti ile doğrulanmamış şekilde değiştirildiğinde, akıllı ev cihazlarının dağıtık servis dışı bırakma (Ddos) saldırısı gibi saldırılarda kullanılabilirliği, botnet olarak verebilecekleri zararlar araştırılmalıdır.

Kaynaklar

[1] Gartner. Gartner top 10 strategic technology trends for 2018. Url, Gartner, https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/, Ekim 2017. Retrieved 4 Temmuz 2018.

[2] M. H. Gonzalez, CISA, CRISC, and J. Djurica. Internet of things offers great opportunities and much risk. *Isaca Journal*, 2, 2015.

[3] Statista. Smart home report 2019. *Statista*, page 183, Aralık 2018.

[4] The Associated Press. Hackers used internet of things devices to cause fridays massive ddos cyberattack. Url, CBC News, https://www.cbc.ca/news/technology/hackers-ddos-attacks-1.3817392, Ekim 2016. Retrieved 9 Mart 2019.

[5] L. Gökrem and M. Bozuklu. Nesnelerin interneti yapılan Çalışmalar ve ülkemizdeki mevcut durum. *Gaziosmanpaşa Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Mekatronik Mühendisliği Bölümü*, Aralık 2016.

[6] UCLA Edu. Ucla. Url, UCLA Press Release, http://newsroom.ucla.edu/portal/ucla/Internet-Began-35-Years-Ago-at-5464.aspx, Eylul 2004. Retrieved 19 Kasım 2018.

[7] G. Estrin and Professor Emeritus. Url, UCLA Computer Science Department, https://www.cs.ucla.edu/history/. Retrieved 17 Temmuz 2019.

[8] Solidworks. Url, Solidworks, https://www.solidworks.com/sw/resources/internet-of-things.htm. Retrieved 13 Nisan 2019.

[9] Q. Stafford-Fraser. Url, University of Cambridge, Department of Computer Science and Technology, https://www.cl.cam.ac.uk/coffee/qsf/coffee.html, Mayıs 1995. Retrieved 23 Mayıs 2019.

[10] Business Insider Intelligence. Url, Business Insider Intelligence, https://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-4-28, Nisan 2016. Retrieved 28 Mayıs 2019.

[11] J. Greenough. Url, BI Intelligence, https://www.businessinsider.com/internet-of-everything-2015-bi-2014-12, Nisan 2015. Retrieved 17 Temmuz 2019.

[12] K. Congar. Url, http://tr.euronews.com/2017/02/28/avrupa-nin-akilli-sehir-leri, Şubat 2017. Retrieved 19 Mayıs 2019.

[13] R. Harper. *Inside the Smart Home.* Springer, London, 2003.

[14] S. P. Pande and Prof.P. Sen. Home automation system for disabled people using. *IOSR Journal of Computer Science (IOSR-JCE)*, pages 76–80, 2014.

[15] J. L. Fernandez, D. P. Losada, and E. P. Domonte. An integrated and low cost home. Technical report, XV WORKSHOP OF PHYSICAL AGENTS, LEON (SPAIN), Haziran 2014.

[16] E. Özçekiç. Akıllı ev sistemleri. Master's thesis, Beykent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2005.

[17] N. McCarthy. Url, Statista, https://www.statista.com/chart/3857/smart-technology-in-us-homes/, Ekim 2015. Retrieved 3 Ocak 2019.

[18] K. Banks. Url, NT News, https://www.ntnews.com.au/news/northern-territory/cdu-prof-turned-on-sprinkler-system-from-smart-phone-to-save-his-home-from-raging-fire-ball-in-remote-sa-town/news-story/e25ff9fd4efdb6b795d4c23d5aa165f1, Kasım 2015. Retrieved 20 Mart 2019.

[19] J. Gerhart. *Home Automotion and Wiring.* 1999.

[20] O. Horyachyy. *Comparison of Wireless Communication Technologies used in a Smart Home: Analysis of wireless sensor node based on Arduino in home automation scenario.* Blekinge Tekniska Högskola Faculty of Computing, 2017.

[21] B. S. Nathali ans M. Khan and K. Han. Towards sustainable smart cities a review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, 38:697,713, 2018.

[22] İTÜ Bilgi İşlem Daire Başkanlığı. Url, İTÜ Bilgi İşlem Daire Başkanlığı, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/zigbee, Eylül 2013. Retrieved 18 Aralık 2018.

[23] Vesternet Ltd. Url, Vesternet, https://www.vesternet.com/pages/understanding-z-wave-networks-nodes-devices, 2012. Retrieved 23 Haziran 2019.

[24] K. Hoskins. Security vulnerabilities in z-wave home automation protocol. Technical report, Tufts University Department of Computer Science, 2016.

[25] N. Y. Parotkin and V. V. Zolotarev. Information security of iot wireless segment. Technical report, Reshetnev Siberian State University of Science and Technology Krasnoyarsk, 2018.

[26] Chip. Kablosuz dünyaya hazırlık. *Chip*, 02:54,62, 2002.

[27] T. Jaffey. Url, Eclipse, https://www.eclipse.org/community/eclipse-newsletter/2014/february/article2.php, Haziran 2014. Retrieved 16 Temmuz 2019.

[28] L. Zhang. Building facebook messenger. Url, Facebook, https://www.facebook.com/notes/facebook-engineering/building-facebook-messenger/10150259350998920, Ağustos 2011. Retrieved 14 Nisan 2019.

[29] M. Haldas. Url, Security Camera and Video Surveillance Blog, https://videos.cctvcamerapros.com/security-mobile-app/push-notification-android-dvr-viewer.html, Mart 2014. Retrieved 17 Temmuz 2019.

[30] M. Maciej. Url, Zur GIGA, https://www.giga.de/extra/tv/specials/smart-tv-hacken-was-geht-was-geht-nicht/, Ocak 2017. Retrieved 2 Şubat 2019.

[31] IPVM Team. Url, IPVM, https://ipvm.com/reports/hik-hack-map, Ocak 2018. Retrieved 4 Nisan 2019.

[32] P. Gaur. Dark side of your living room. Technical report, Tech And Trends, 2014.

[33] J. Roberts. Url, Vacuums Guide, https://www.vacuumsguide.com/privacy-robot-vacuum-cleaners/, Ağustos 2017. Retrieved 9 Temmuz 2019.

[34] Techinside. Url, Techinside, https://www.techinside.com/robot-supurge-evinizin-haritasini-satacak/, Temmuz 2017. Retrieved 29 Mayıs 2019.

[35] P. Wagenseil. Url, Tom's Guide, https://www.tomsguide.com/us/bluetooth-lock-hacks-defcon2016,news-23129.html, Ağustos 2016. Retrieved 26 Nisan 2019.

[36] A. Tilley. Url, Forbes, https://www.forbes.com/sites/aarontilley/2016/09/21/apple-homekit-siri-security/, Eylül 2016. Retrieved 3 Haziran 2019.

[37] B. Ali and A. İ. Awad. Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 3(18), Mart 2018.

[38] N. Apthorpe, D. Reisman, and N. Feamster. A smart home is no castle privacy vulnerabilities of encrypted iot traffic. Technical report, 2018.

[39] A. Gai, S. Azam, B. Shanmugam, M. Jonkman, and F. De Boer. *Categorisation of security threats for smart home appliances.* School of Engineering and IT Charles Darwin University, 2018.

[40] Y. Jia, Y. Xiao, J. Yuy, X. Cheng, Z. Liangz, and Z. Wan. A novel graph-based mechanism for identifying traffic vulnerabilities in smart home iot. *Department of Computer Science, The George Washington University, Washington DC, USA*, 10.1109/INFOCOM.2018.8486369(978-1-5386-4128-6):1493–1501, Nisan 2018.

[41] C. Lee, L. Zappaterra, K. Choi, and H. Choi. Securing smart home: Technologies, security challenges, and security requirements. *Department of Computer Science, George Washington University*, 14(978-1-4799-5890-0):67–72, 2014.

[42] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu. Security vulnerabilities of internet of things: A case study of the smart plug system. *IEEE Internet of Things Journal*, 4(6):1899–1909, Dec 2017. ISSN 2327-4662.

[43] T. Aktaş. Securing sip communication for remote access to smart home networks. Master's thesis, Yeditepe Üniversitesi. Master of Science in Computer Engineering, İstanbul, Turkey, 2013.

[44] J. Wurm, K. Hoang, O. Arias, A. Sadeghi, and Y. Jin. Security analysis on consumer and industrial iot devices. *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016.

[45] L. Rafferty, F. Iqbal, S. Aleem, Z. Lu, S. Huang, and P. C. K. Hung. Intelligent multi-agent collaboration model for smart home iot security. In *2018 IEEE International*

Congress on Internet of Things (ICIOT), pages 65–71, July 2018. doi: 10.1109/ICIOT.2018.00016.

[46] Broadlink. Url, Broadlink, https://www.broadlink.com.tr/tr/broadlink-rmpro. Retrieved 3 Haziran 2019.

[47] AliBaba Group. Url, Aliexpress, https://www.aliexpress.com/item/1126775982.html. Retrieved 3 Temmuz 2019.

[48] A. Mallik, A. Ahsan, Md. M. Z. Shahadat, and J. Tsou. Man-in-the-middle-attack: Understanding in simple words. 3:77–92, 01 2019. doi: 10.5267/j.ijdns.2019.1.001.

[49] Securebox. Url, Comodo, https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/. Retrieved 17 Temmuz 2019.

[50] S. Atasever, İ. Özçelik, and Ş. Sağıroğlu. Siber terör ve ddos. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(1):227–233, 2019.

[51] P. Kim. Url, Github, https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html, Mart 2017. Retrieved 13 Temmuz 2019.

[52] C. Hoffman. Url, How to Geek, https://www.howtogeek.com/122487/htg-explains-is-upnp-a-security-risk/, Temmuz 2017. Retrieved 17 Temmuz 2019.