Avrupa Bilim ve Teknoloji Dergisi
Sayı 31 (Ek Sayı 1), S. 242-255, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 31 (Supp. 1), pp. 242-255, December 2021

Research Article

Otonom Araçlar İçin Siber Güvenlik Risklerinin Araştırılması ve Savunma Metotları

Cevat Özarpa[1*], İsa Avcı[2], Seyit Ali Kara[3]

[1*]Karabük Üniversitesi, Mühendislik Fakültesi, Makine Mühendisliği Bölümü, 78050, Merkez, Karabük (ORCID: 0000-0002-1195-2344),cevatozarpa@karabuk.edu.tr
[2] Karabük Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 78050, Merkez, Karabük (ORCID: 0000-0001-7032-8018),isaavci@karabuk.edu.tr
[3] Karabük Üniversitesi, Mühendislik Fakültesi, Makine Mühendisliği Bölümü, 78050, Merkez, Karabük (ORCID: 0000-0003-1275-1242), 2028129013@ogrenci.karabuk.edu.tr

(İlk Geliş Tarihi 8 Nisan 2021 ve Kabul Tarihi 21 Aralık 2021)

(**DOI:** 10.31590/ejosat.911468)

ATIF/REFERENCE: Özarpa, C., Avcı, İ., Kara, S.A. (2021). Otonom Araçlar İçin Siber Güvenlik Risklerinin Araştırılması ve Savunma Metotları. *Avrupa Bilim ve Teknoloji Dergisi*, (31), 242-255.

Öz

Dünyada dijital teknolojinin hızla gelişmesiyle birlikte, akıllı şehirler ve akıllı şebekelerde olduğu gibi akıllı ulaşım araçlarında da gelişmeler yaşanmıştır. Akıllı sistemlerin akıllı araçlara entegrasyonun ardından otonom araçların yaygınlaşmasıyla siber güvenliğin önemi daha da artmıştır. Konforlu, güvenilir ve zamandan tasarruf edilebilecek yolculuk ve taşımacılık için otonom araçların güvenlik zafiyetleri araştırılmıştır. Yapılan siber saldırıların 3 çeşit amacı vardır: sistemi kontrol eden yöneticiyi devre dışı bırakarak sistemin kontrolünü ele geçirmek, sistem çalışmasında gecikmelere neden olacak yoğunlukta çalışmasını sağlamak ve sistemin tamamen çökmesine neden olmak. Bu çalışmada kontrolün kullanıcıdan saldırgana nasıl geçebileceğini göstermek amacıyla 10 çeşit saldırı incelenmiştir. Bu saldırılar, GPS yanıltma, ara bellek taşması, istismar açıklık saldırıları, araya girme saldırısı, kötülcül yazılım saldırısı, hizmet kesintisi saldırısı, vekil sunucu saldırısı, sibil saldırısı, OBD Saldırısı ve ARP yanıltma saldırısıdır. Saldırıların yapılacağı mimaride temel otonom sistemler için gereksinim olan konum sensörleri, araç alt sistem denetleyicileri, kablosuz bağlantı araçları ve görüş sensörleri üzerinden yapılan saldırılar incelenmiştir. Ayrıca otonom araçların sistem mimarisi, siber saldırı yöntemleri, siber saldırı önlemleri ve son 5 yılda yapılmış akademik çalışmalar incelenerek analiz edilmiştir. Otonom araçlarda saldırıların sensör bilgilerinin toplandığı, araçların yönetildiği işlemciye yapıldığı tespit edilmektedir. Kablosuz bağlantıların otonom araç yönetiminde kullanıcıların isteği üzerine kullanılması beraberinde çokça açıklığı da getirmiştir. İşlemcide kullanılabilir açıklıkları azaltmak için, işlemcinin yapması gereken görevlerin azaltılarak, yapılması gereken çalışmanın diğer sensörler tarafından yapılması istenmektedir. Sistemin sahip olduğu tek işlemciye doğrudan erişimi kapatarak sistem açıklıklarının azaltılması yönünde çalışmalar yapılmaktadır. Akademisyenler ve otonom araç üreticileri araç mimarisini yöneten yazılım ve korunma yöntemleri üzerinde geliştirme çalışmalarına devam ettikleri görülmektedir. Bu çalışmada, kullanıcıların güvenlik işlemlerini kolaylaştıracak çalışmalar, bazı araçlar ve tedbirler incelenmiştir. Uzmanlar tarafından kullanılarak sistem IP'si hakkında bilgi sahibi olunabilecek, yetkisiz veya yabancı sistemleri tespit edebilecek olan NMAP, Maltego ve Metasploit araçları da incelenmiştir. Yaptığımız çalışmalar tamamıyla etik kurallar çerçevesinde yapılmıştır.

Anahtar Kelimeler: Otonom araçlar, Siber saldırılar, Siber risk analizi, Siber tehditler.

Survey of Cyber Security Risks and Defense Methods for Autonomous Vehicles

Abstract

With the rapid development of digital technology in the world, there have been developments in smart vehicles as well as in smart cities and smart grids. After the integration of smart systems with smart vehicles, the importance of cyber security is increasing with the spread of autonomous vehicles. In this study, security vulnerabilities of autonomous vehicles were investigated, especially for comfortable, reliable, and time-saving travel and transportation. The cyberattacks carried out in the research have 3 purposes. These are to take control of the system by disabling the administrator who controls the system, to make the system work intensively, to cause delays in the system operation, and cause the system to crash completely. In this study, 10 attack types are analyzed to show how control can pass from the user to the attacker. These are GPS spoofing, buffer overflow, exploit vulnerability attacks, Man-in-the-Middle attack, malware attack, DDoS attack, Proxy/Socks attack, Sybil attack, OBD attack, and ARP spoofing attack. The attacks made through position sensors, vehicle subsystem controllers, wireless connection devices, and image sensors, which are required for basic autonomous systems in the attack architecture, are examined. In addition, the system architecture of autonomous vehicles, cyberattack methods, cyber attack measures, and academic studies in the last 5 years have been examined and analyzed. It has been shown that attacks are made on the processor in which the sensor information is collected, and the vehicles are managed in autonomous vehicles. The use of wireless connections at the request of users in autonomous vehicle management has brought a lot of clarity. To reduce the

[*] Sorumlu Yazar: cevatozarpa@karabuk.edu.tr

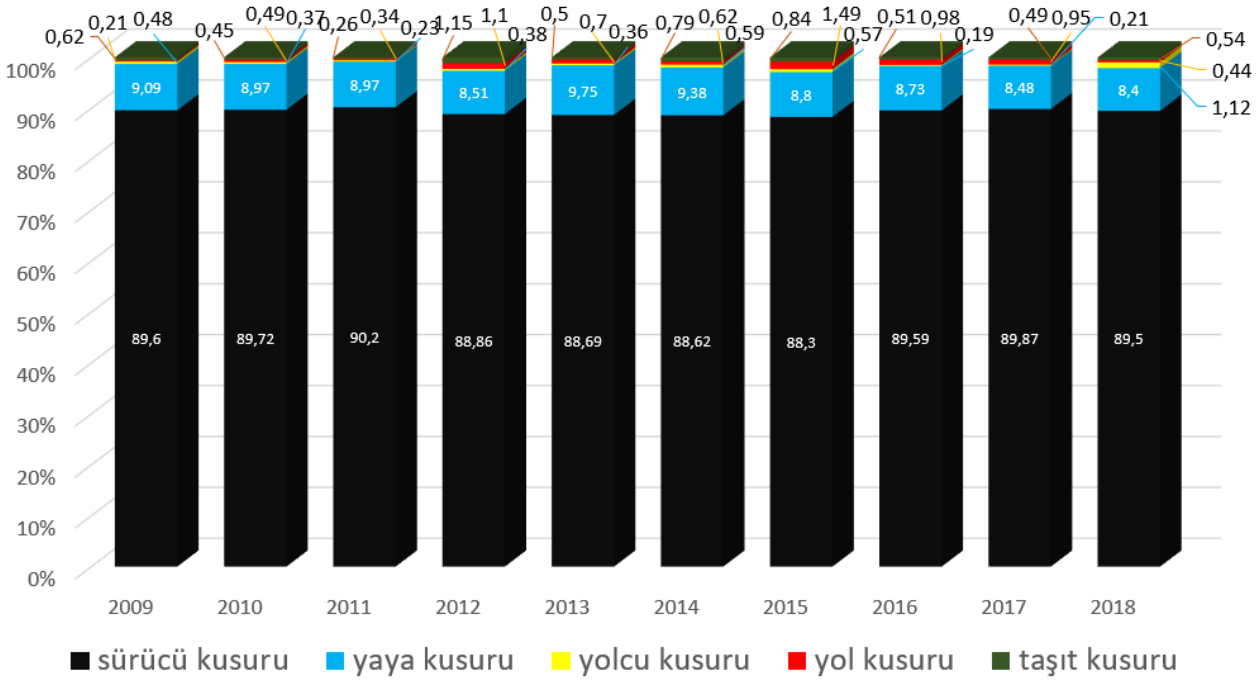
available openings in the processor, the tasks that need to be done by the processor are reduced and the work is required to be done by other sensors. It is tried to reduce system vulnerabilities by closing direct access to a single processor owned by the system. It has been observed that academics and autonomous vehicle manufacturers continue to work on the software and protection methods that manage the vehicle architecture. Studies, some tools, and measures that will facilitate the security processes of users have been examined. NMAP, Maltego, and Metasploit tools that can be used by experts to gain knowledge of system IP and detect unauthorized or foreign systems were also examined. Our work has been carried out completely within the framework of ethical rules.

Keywords: Autonomous vehicles, Cyber-attacks, Cyber risk analysis, Cyber treatment.

1. Giriş

Otomobil sektöründeki gelişmeler son dönemlerde otonom araçların kullanılmasını gündeme getirmiştir. Peki bu araçların kullanımı tamamıyla makinelerin eline verilirse siber saldırılara maruz kalmadan, dışarıdan müdahaleler ile araç kontrolünü kaybetmeden ne kadar güvenli yolculuk yapabiliriz? Bu araçların tarihi otomobillerin ilk zamanlarına dayanıyor. Aracın kumandayla kontrol edilmesi ve ilk otonom araç örneği 1925 yılında görülmüştür (Feng, 2019; Green, 1925). Teknolojinin hızla gelişmesi ve insan hayatına konfor olarak geri dönmesi otomobil teknolojilerinden de aynısının beklenmesine sebep olmuştur. Tarihte tekerleklerin buluşuyla tekerlekler üzerinde seyahat ve taşımacılık başlamıştır. 19. yüzyılda buharın ve 20. yüzyılda petrolün enerji olarak kullanılmasıyla devam etmektedir.

İlk araç örneklerinden kabul edilen Nicolas Joseph Cugnot tarafından 1769 yılında yapılmış olan buharlı araç, Paris'te Arts et Metiers Müzesi'nde sergilenmektedir. Yapılan araç dönem içerisinde ilgi çekememesinden dolayı ordu deposuna kaldırılmıştır (Bellu, 1998; Vers et al., 2019). 1791 yılında Ivan Kulibin tasarladığı araç volan, fren, vites kutusu ve rulman yataklıkları gibi özelliklere sahiptir. Ancak o dönem hükümet bu araçta bir gelecek görememiştir ve çalışmalara son verilmiştir. Oliver Evans, Richard Trevithick, Josef Bozek ve Walter Hancock buharla çalışan araç örnekleri yapmışlardır (Devichnick, 2017; Gridin, 2017). 1860' larda içten yanmalı motorlar tasarlanmıştır. Bu tasarımda motorlar gazyağı ile çalışmaktadır. 1884 yılında Karl Benz tarafından karbüratörlü 4 zamanlı motor yapılmıştır. 1889 yılında Rene Pabhard ve Emile Levassor 4 zamanlı Benz motorunu 4 kişilik bir araca bağlamışlardır (Eckermann, 2001; Milev et al., 2019).



Şekil 1. Trafik Kazaları Nedenleri İstatistik Tablosu (TÜİK, 2018)

Birçok buluş bu aracın üzerine eklenerek daha konforlu, daha hızlı ve daha güzel dış tasarıma sahip olan araçlar yapılmıştır. Fren sistemleri, direksiyon sistemleri, motor için su ile soğutma sistemleri, buji ile ateşleme sistemleri, subap sistemleri, toza ve yağmura karşı araç içerisindekileri korunması için düşünülmüş tasarımlar gibi (Coulibaly, 2007; Taymans et al., 2020).

Otomobillerde gelişim, yarışlarla daha da hızlı bir hal almıştır. 1894 yılında gerçekleştirilen Paris-Rouen bilinen ilk otomobil yarışıdır. Yarışlarda ilk öncelik hız ve araç hakimiyeti olduğundan süspansiyon, direksiyon, aerodinamik, tekerlekler, frenleme sistemleri ve motor performansı için yapılan gelişmeler hız kazanmıştır. Bilinen ve kabul edilebilecek ilk otonom otomobil Francis Houdina tarafından uzaktan kumanda ile kontrol edilmektedir (Esteban, 2019; Puiboube, 2000). 1956 yılında General Motors firması Firebird model araca telsiz sinyalleri ile otoyolda otomatik hareket etmesini sağlamışlardır (Kendi, 2017). Teknolojik yetersizlikler ve otomobil sektörünün insan hakimiyetine dayalı sürüş üzerine gelişmesi, otonom araçların 2004 yılına kadar insan kontrollü gitmesine ilerlemesine sebep olmuştur (Miller, 2014).

Otonom araçlarda gelişimler elektronik sensörlerin gelişimine bağlı olarak ilerlemiştir. Görüş sistemlerinin özellikle Lidar Sensörlerinin 1970' lerden 2000' lere kadarki süreçte havadan denizaltı tespiti için kullanımı ve karada haritalama, orman ve su araştırmalarında kullanılmasıyla gelişmiştir ve otonom araçlarda 2000' li yıllarda kullanılmaya başlamıştır.

Otonom araçlarda kullanlılan diğer bir sensör olan GPS, 1978 yılında ABD Savunma Bakanlığı tarafından kullanılmıştır (Congress, 2018). 24 adet uydunun atmosferde konumlandırılmasıyla kullanılır. GPS navigasyon, tarım ve madencilik gibi alanlarda kullanılmaktadır (Gps.gov, 2020; Haider & Khalid, 2017).

2004 yılında DARPA Grand Challenge açıklanmıştır. 2010 yılında Google firmasının da bu alanda çalışmasıyla birlikte otomobil üretici firmalar (General Motor, Ford, Volkswagen, Toyota ve Volvo) kendi araçlarını Google ile test etmeye başlamışlardır (Patterson et al., 2017). 2013 yılında seviye 1 ve seviye 2 türünde araçlarla trafikte testler yapılmıştır. 2014 yılında seviye 3 ve seviye 4 türünde araçlar San Francisco ve Seattle arasında test edilmiştir (Tunalı, 2019). Bu çalışmamızda 5. seviye tamamıyla otonom araçlarda var olan ve kullanıma müsait zafiyetler, alınabilecek önlemler ve yapılabilecek çalışmalar incelenmiştir.

Güvenlik zafiyetleri otonom araçlar üzerinde kontrol kayıplarına sebep olabilir, diğer yandan kullanımı zorlaştırabilir veya zarar görmemize sebep olabilir. Siber güvenlik zafiyetlerinden doğan ve akla gelecek ilk siber tehdit otomobilin insan kontrolü dışında belirli bir koordinata doğru hareket etmesidir. Siber saldırılar sonucunda otomobil çalınabilir veya otomobil içerisindekiler alıkonulabilir. Akla gelen ikinci tehdit, sistemin istenildiği gibi çalışmaması ve otomobilin ve/veya içerisindekilerin zarar görmesinin istenmesidir. Örnek olarak, saldırganlar tarafından yapılacak arabelleklerde taşma saldırıları ile sistem sensörleri çalışmaz hale gelebilir. Bu siber saldırı yöntemi ile trafik ışıklarını doğru algılanmaması, fren sisteminin devre dışı bırakılması ve/veya doğru frenleme yapılamaması gibi sorunlar ile karşılaşılabilir. Ayrıca radyo, koltuk ısıtmaları, klimalar, kalorifer, pencereler, tekerleklerle beraber süspansiyonlar gibi konfor amacıyla kullanılan ve geliştirilen tüm sistemler istem dışı kullanılabilir. Otomobillerin insan hayatında çok sık kullanılması, trafikte yaşanan kazaların %90'a yakınının insan kaynaklı olması Şekil 1' de gösterilmiştir ve teknolojik gelişmeler, otonom otomobillerin kullanımını desteklemektedir.

2. Otonom Araçlar

19. Yüzyılda hayatımıza giren otomobiller her açıdan farklı bir yere gelmiştir. İnsanların daha konforlu ve donanımlı araç isteğine çözüm olması amacıyla otonom araçların üretimi ve kullanımı yaygınlaşmaktadır. Bu araçlar günümüzde SAE J3016 standartlarına göre 6 kategoride incelenmektedir ve seviye 5 isimli 6. kategori tam otonom otomobil kategorisidir (European Union Agency for Network and Information Security (ENISA), 2017). Trafikte harcanacak zamandan tasarruf etmiş olunmaktadır. Artık düşünmemiz gereken konu şahsi güvenlik konusudur.

Bu nedenle tam otonom araçların internet ihtiyacı ve sistemin dışarıyla olan etkileşimi zafiyetleri ortaya çıkarmaktadır. Otonom araçlar sistem olarak temelde görüş sensörleri, konum sensörleri, kablosuz haberleşme sensörleri, araca ait parçaların denetim sensörlerine sahiptirler. Otonom olmayan araçlarla pek çok ortak yönü de vardır ve bunlar mekanik sistemleri; süspansiyon, direksiyon, tekerlekler, fren sistemleri ve araç iç donanımıdır. Gelecekte bu parçalarda değişmeler, hafiflemeler, kullanım kolaylığı sağlayacak eklemeler olsa da şu an için kullanılacak bir otonom araç hemen hemen bu özelliktedir (Molla & Electronik, 2018).

2.1. Otonom Araçlarının Faydaları ve Kullanım Alanları

İstatistiksel çalışmaların bizlere verdiği sonuçlara göre % 90' lık bir dilim insan hatalarından dolayı trafikte kaza olduğunu gösteriyor (TÜİK, 2018). Bu hataları azaltmak için sürücü kullanımı ve trafikte kural ihlalleri en aza indirmek istenmiştir.

Otonom araçlar insan hatalarına bağlı kazaların yaşanmaması istenen yerlerde, geniş arazilerde, çiftçilikte, sağlık sorunları sebebiyle standart araç kullanımında zorlanmalarda kullanımı düşünülen araçlardır (Pancorbo Crespo et al., 2019).

2.2. Otonom Araç Seviyeleri

Araçların her geçen gün elektrikli araçlara dönüştürülmesi isteği de otonom araçlarda tasarım değişikliklerine sebep olacaktır. Bu değişiklikler elektronik ve dijital parçaların küçük modellerinin, dayanıklı ve olabildiğince küçültülmüş mekanik parçaların bir araya gelmesi demektir. Bu doğrultuda yapılan çalışmalarla şu an için 6 ayrı seviye mevcuttur. Bunlar Seviye 0, Seviye 1, Seviye 2, Seviye 3, Seviye 4, Seviye 5 olarak isimlendirilirler (ENISA, 2017; Feng, 2019; Ustam, 2020).

2.2.1. Seviye 0: Otonom Olmayan Araçlar

Araç üzerinde, etrafında, içerisindeki sensör veya kameraların kullanım kontrolünde herhangi bir etkisi yoktur. Kullanım kontrolü yalnızca sürücünün elindedir.

2.2.2. Seviye 1: Sürüş Yardımlı Araçlar

Araçlar bazı sürüş yardım desteğiyle ilerleyebilir fakat bunlara rağmen kontrol yine de sürücüdedir. Adaptif hız sabitleyiciler, far açı sensörü, frenlemeye bağlı tekerleklerin hareketinin kesilmesi gibi etkiler söz konusudur.

Tablo 1. Otonom Araçların Sınıflandırması (Bezai et al., 2020; ENISA, 2017; Pancorbo Crespo et al., 2019)

Kategori	Otonomluk Seviyesi	İnsan Müdahalesi	Hakimiyet Kontrolü
Geleneksel	0 Manuel Kontrol Araçlar	Evet	Manuel Kullanılan araçlar
Akıllı	1 sürüş yardımlı araçlar	Evet/Hayır	Makine destekli insan kullanımlı araçlar
Akıllı	2 kısmi otonom araçlar	Evet/Hayır	Kararları insanlar verir kullanım araçtadır
Otonom	3 koşullu otonom araçlar	Evet/Hayır	Son kararı insanların verdiği araçlar
Otonom	4 yüksek otonom araçlar	Evet/Hayır	Acil durumlar dışında insanlar karar verir
Otonom	5 tam otonom araçlar	Hayır	İnsanların sadece acil durumları bildirirler

2.2.3. Seviye 2: Kısmi Otonom Araçlar

Araç, sürücü kontrolüyle çalışmaktadır ve ilerler ancak sürüş sistemi sisteme devredilebilir. Her an sürücü müdahale edecekmiş gibi tasarlanırlar. Bu seviyedeki araç modeli, şeritlerin belirgin

olduğu, düz ve kavisin az olduğu yollarda kontrolün araç beynine bırakılabileceği araç modelleridir. Bu model araçlarda yine de sürücüden direksiyondan tutması istenilmektedir.

2.2.4. Seviye 3: Koşullu Otonom Araçlar

Seviye 2' deki araç sensörlerine ve daha fazla sensöre sahiptirler. Bu araçlarda kontrol tamamıyla araca bırakılmaktadır. Sürücünün yola, etrafındaki araçlara, trafik uyarı levhalarına, ışıklara, yayalara dikkat etmesi gereken durumlarda sürücü önceden uyarılır.

2.2.5. Seviye 4: Yüksek Otonom Araçlar

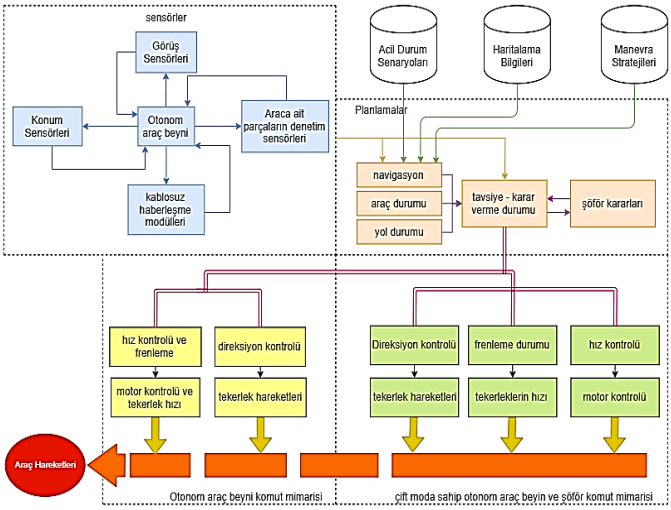
Araçların istenen noktaya gidebilmesi sürücü kontrolsüz mümkündür ve bu sürüş esnasında sürücüden kontrol beklenmez. Araç kendi kendini park edebilmektedir. Bu araçlarda yolcuların gidecekleri yerlere güvenle gidebilmeleri için sistem sensörleri tarafından kontrol edildiğinden beyin sensörlerden gelen veriler doğrultusunda en güvenli şekilde seyahat için tasarlanmışlardır. Bu araçlar aynı zamanda sıkışık trafik durumunda da kendine alternatif yollarla da rota çizerek yolcuları güvenle gidecekleri yerlere götürebilmektedir.

2.2.6. Seviye 5: Tam Otonom Araçlar

Seviye 5 olması gereken tüm sensörlerle tam donanımlı araçların seviyesidir. İnsan müdahalesi olmaksızın istenen noktaya yolcuları bırakabilmektedir. Öngörülere göre 2030 yılında 5. Seviye araçların trafikte olması düşünülmektedir (Molla & Electronik, 2018).

2.3. Otonom Araç Mimarisi

Araç donanımında en az mekanik parçalar kadar elektronik parçalar bulunmaktadır. Bunlar; radar, şerit takip sistemi, lidar sensörü, kızılötesi kamera, GPS, atalet ölçüm cihazı, tekerlek kodlayıcı, odometri, bilgisayar görüş sistemi, frenleme, hız kontrol ünitesi ve direksiyon olarak söylenebilir (José E. Naranjo, 2009). Araçların otonomluk seviyelerine göre kullanılan sensörlerde de değişmektedir. Genel olarak kullanıma bakılacak olursa araçların mimarisi birbirlerine çok yakındır. (İspir, 2019; Naranjo et al., 2009).



Şekil 2. Otonom Araç Mimarisi Örneği (Bezai et al., 2020; El-Rewini et al., 2020)

3. Otonom Araçlarda Siber Saldırı Yöntemleri ve Riskleri

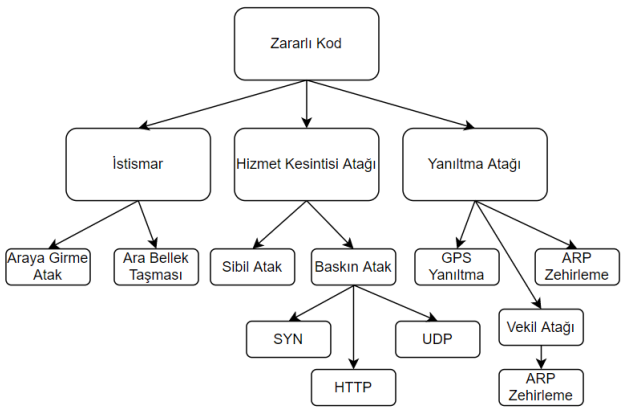
Siber saldırılar sistemi durdurmaya, kapatmaya veya tekrar çalıştırmamaya yöneliktir. Siber saldırı yapılmadan önce sistem ve sistem kullanıcıları hakkında bilgiler toplanır. Yapılacak saldırıda saldırılan sistemin şifreli veya şifresiz bir arayüzü olabilir. Kullanıcı arayüzünde şifre olmadığında yerel ağ ile kolayca erişim sağlayabilmektedir (Morimoto et al., 2018; Ünver, n.d.; Ünver vd., 2009).

3.1. Otonom Araçlarda Siber Saldırı Yöntemleri

Otonom otomobillerde yapılacak saldırılar sistemin bağlı olduğu kablolu ve kablosuz bağlantılar üzerinden yapılmaktadır. Siber saldırılarda amaç sistemin kullanımını kullanıcıdan ve yöneticiden düşürmektir. Saldırılar genellikle sistemin durdurulması, sonlanması, bir daha hiç çalışmaması gibi sistemi bloke edecek yazılımlar veya sistemi dinlemeye yönelik saldırılardır (Schmittner et al., 2016). Sistemdeki arabelleklere yapılacak saldırılarda ara bellek taşmaları vasıtasıyla kullanıcı girişlerinin bir önemi kalmaz ve sistem saldırganların kontrolüne geçer. Araç navigasyonuna yapılacak saldırılarla kullanıcının rota bilgileri değiştirilerek aracın farklı noktaya gitmesi veya sabit bir noktada kalması sağlanabilmektedir. Yapılacak saldırıların ve sistemin sahip olduğu zafiyetlerin dinlenmesi ise Exploits ile denetlenebilir. Zafiyetlerin kullanımı için saldırılacak sisteme payloadlar gönderilir. Payload zafiyetin saldırgan tarafından kullanılmasını sağlayacak zararlı saldırı kodlarıdır. Bu kodlar sistemin dinlenmesine bilgilerinin izin gerektirmeden başka makinelerle paylaşılmasına neden olmaktadır (Han et al., 2014; Sheehan et al., 2019).

3.1.1. İstismar (Exploit)

İşletim Sistemleri ve bazı programların güvenlik açıklarını keşfederek bu güvenlik açıklarını kötüye kullanma yöntemine istismar (exploit) denilmektedir. Yapılacak saldırılar içerisinde dinleme zafiyetler kullanılarak sistemde değişiklikler yapmamızı sağlayan saldırı araçlarındandır. Doğrudan sisteme sızma amaçlansa da güvenlik açıklıklarının bize sağlayacağı risklerin ne boyutta olduğunu göstermesi açısından kullanılır. Sistemler istismar edilerek sistem şifreleri görülebilir, sistemler hakkında bilgiler elde edilebilir.

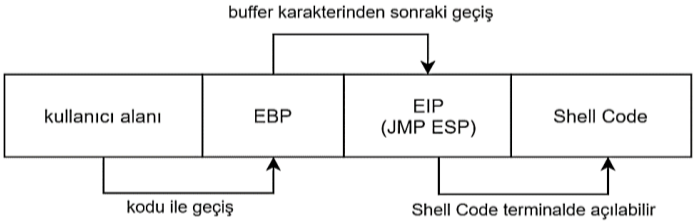


Şekil 3. Siber Saldırı Yöntemleri için Zihin Haritası

İstismar saldırıları sistemin olağan olarak çalışmasına engel olurlar ve sisteme dışardan kod göndererek sistemi normal olarak çalıştığına ikna ederler ve genelde yetkisiz erişim için kullanılmaktadır. Kullanım için açık kaynaklı kodlar kullanılır burada amaçlardan ilki art niyetli yazılımların kullanıma erişebilen diğer kullanıcılar tarafından fark edilmesi ve gerekirse müdahale edilebilmesidir, ikinci amaç ise keşfedilmemiş güvenlik açıklıklarının ne olduğudur. (Polat, 2016; Sweshsec, 2020).

3.1.2. Bellek Taşması (BufferOverFlow)

Sistem içerisinde bellekte aşırı yoğunluktan doğan zafiyet çeşididir. Bellek üzerinde statik ve dinamik değişkenlerin tutulduğu alanlar bulunmaktadır. Bu alanların kapasitelerinin üzerinde veri yüklenmesinden dolayı ortaya çıkmaktadır Saldırılar genelde C dilinde yazılmış buffer değişkeninde boyutların belirlenmesi ve belirlenen değişkenin boyutlarının üzerinde veri alması sonucu taşmalara sebep olacak kodlarla yapılırlar. Shell Code'a erişim mümkün olduğunda üzerinde değişiklikler yapılır (Altınkaynak, 2020). Otonom otomobillerde kullanıcı girişi komut ekranına geçişte kullanılır. Komut ekranında ise gidilmesi istenen yol tarifi mevcuttur. Bu tarife göre otomobilden kendisi gitmesi istenmektedir. Burada Bufferoverflow saldırısı ile bizler komut ekranında girilmiş olan bilgileri değiştirebilmekteyiz.



Şekil 4. JMP ESP Konumu

3.1.3. GPS Yanıltma (GPS Spoofing)

Sistemde bulunan radyo dalga sinyallerini kopyalayarak sahtelerinin üreten ve bu sinyalleri sisteme gönderen saldırı çeşididir. Sistemin gelen sinyallerin doğruluğuna bakmaksızın kabul etmesi zafiyetine dayanmaktadır. Yapılan saldırılarda kullanılan GPS dalga boyuna göre saldırıların kullanımı da şekillenmektedir. Bu saldırılar maliyeti yüksek ve donanım gerektiren bir saldırı türüdür (Jadoon et al., 2018; Parkinson et al., 2017). Saldırgan tarafından taklit edilecek esas sinyallerin taklit edilen sinyallere oranı 2 µs arttırılırsa veya 10 dB daha güçlü olduğunda saldırganın yapacağı saldırıların başarılı olacağı görülmüştür. Bu saldırıda saldırgan kullanıcının gideceği adres bilgisini değiştirilebilir. GPS yanıltma, 2 teknik ile saldırı yapılması mümkün olmaktadır. Bunlar, saldırının gizlemesi (covert capture) ve gizlememesi (overt capture) olarak verilmektedir (Çuhadar, 2017). Covert Capture'da saldırganın tespiti zordur ve Overt Capture saldırılarına göre pahalıdır. Overt Capture'da saldırgan tespit kaygısı yaşamadığından önce sistem sinyallerini bozmaktadır, ardından sisteme kendi sinyallerini yollamaktadır.

3.1.4. Hizmet Kesintisi Saldırısı (DDos-DoS Attack)

Hizmet kesintisi olan bu saldırı türü saldırı yapılacak sisteme cevap veremeyeceği kadar istek gönderilmesi sonucunda oluşmaktadır. Sistemin çok fazla istek alması artık kullanım dışı kalmasına sebep olacaktır. Sistemin çalışmaz hale getirilebilmesi için genellikle bant genişlikleri kullanılarak taşırma işlemi yapılmaktadır. Bu tarz saldırılar için yasa dışı kullanımı olan sunucular mevcuttur. Dağınık saldırı tekniğine sahiptir, IP adresleri farklı subnetlerde yer alabilir. Bu sayede tespiti ve önlenebilmesi çok zordur. Önemli hususlardan birisi de paketler ve boyutlarıdır. Bunun için 100 ile 1000 MB bağlantı için Tablo 1' e bakacak olursak ortalama TCP 60 byte, UDP 40 byte, http 400 byte olarak paket boyutlarını kabul edebiliriz (Jadoon et al., 2018; Parkinson et al., 2017).

3.1.4.1. SYN Taşması (SYN Flood)

SYN bağlantısı kurulacak olan cihaz veya internet bağlantısı için bağlantı kurma talep paketidir ve istek paketi olarak gönderilir. Gönderilen paketlere karşılık olarak SYN-ACK paketi alınır ve bu alınan ACK paketi ile sisteme bağlantı kurulmuş olunur. Eğer eş zamanlı pek çok SYN paketi farklı noktadan erişim için gönderilirse bu SYN Flood olmaktadır. Sistem çok fazla SYN paketi olmasından dolayı cevap veremez duruma gelir.

Tablo 2. 100-1000 MB Bağlantı Paketleri İncelemesi

Saldırı Tipi	**100 MB (pps, packet per second)**	**1000 MB (pps)**
SYN Flood	200.000 pps	2.000.000 pps
UDP Flood	400.000 pps	4.000.000 pps
HTTP Flood	32.000 pps	320.000 pps

3.1.4.2. HTTP Taşması (HTTP Flood)

HTTP portu web yayınları için 80. portu, güvenli web yayını için 443. portu kullanmaktadır. Bu durumdan dolayı bu portlar daima açıktır. HTTP Flood saldırıları da http protokolü aracılığıyla yapılmaktadır. Web servisinin kaç kişiye kadar hizmet verebileceğinin ölçütü olarak kullanılır. Sayfa yenileme gibi kullanımlarda http portuna giriş talep edildiğinden bu tarz saldırıları tespit etmek güçleşmektedir.

3.1.4.3. UDP Taşması (UDP Flood)

UDP sahip olduğu protokol itibariyle TCP' den farklı olarak 3'lü el sıkışma (3-way handshake) yapmamaktadır. Öncelik verilen konu güvenlik değil hızdır. Paket gönderiminin ardından paketin gönderildiği portun kontrolü yapılır. Portun kullanıcısının olup olmadığı denetlenir eğer var ise paket servise iletilir, eğer yoksa ICMP (hedefe ulaşılamıyor) olarak döner. Bu saldırılar yol bilgisi alınacak olan websiteleri üzerinde kullanılabilir. Bu kullanımlar otomobil beyni olarak kullanılan sistemlerin bilgi alamamasına ve otomobillerin harekete geçmemesine neden olacaktır.

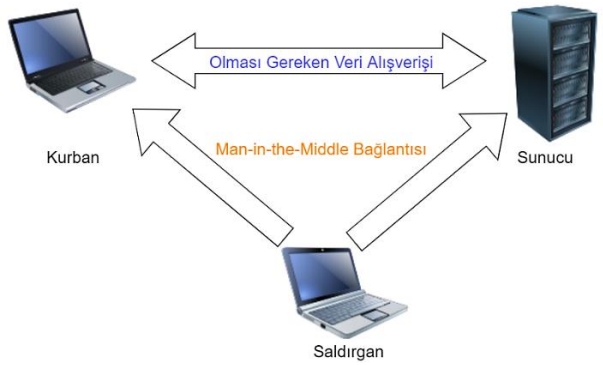
3.1.5. Ortadaki Adam Saldırısı (Man in the Middle)

Her sistem mantıksal ve fiziksel operatörlere sahiptir. Bunlar MAC ve IP protokolleridir. Bu protokoller hem güvenlik amacıyla tasarlanmıştır hem de internette gezinmelerde karışıklıkların önüne geçmek hedeflenmektedir. Yapılan aramaların IP karışıklıklarından dolayı arama yapan kişiler arasında çarpık gösterimidir. Problem olarak karşımıza çıkacak ilk sorun bizim mantıksal veya fiziksel protokollerimizin başka bilgisayarlar tarafından kullanılmasıdır. OWASP'a göre Man-in-the-Middle saldırısı çok tehlikelidir (Çıtak, 2020). Bunun temel sebebi HTTP protokollerinin güvenliksiz yapısıdır. Kurban ile sunucu rahatlıkla dinlenebilir ve manipüle edilmeye müsaittir. Oturum bilgileri,

çerezler, e-posta kullanımı gibi bazı kullanıcı girdileri bu saldırı durumunda tehlike altındadır. Sunucunun kurbana göndereceği her paket saldırganın terminalinden geçmektedir (Altınkaynak, 2020; Muratoğlu, 2020; OWASP, 2015).

3.1.6. Vekil Saldırısı (Proxy/Socks)

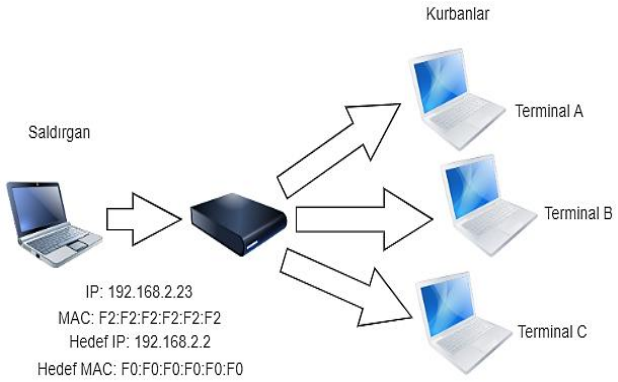
Proxy kullanmak demek IP adresinizi maskelemektir. Genelde IP adresini paylaşmak istemeyen kullanıcılar tarafından kullanılırlar. İnternette Proxy serverlar mevcuttur ve bunların pek çoğu ücretsiz olarak hizmet vermektedir. En sık kullanılan üç yaygın kullanımı bulunmaktadır. Bunlar; 4, 4a ve 5' tir. Her birinin kendine özgü kullanımı vardır. Kullanımda en yaygını ise 4' tür. Yalnızca IPv4 destekler ve hedef adres olarak 32 bit IP adresi belirtilebilir. 4a ise 4'e yapılmış bir ekleme ile kullanılabilir. Eğer IP adresi çözebilecek bir DNS sunucunuz yoksa faydalıdır. 5 ise IPv6, hostname desteği , UDP yönlendirme ve geliştirilmiş kimlik doğrulama desteğine sahiptir (Duan et al., 2006; Forshaw, 2018).



Şekil 5. Man-in-the-Middle Bağlantı Şeması

3.1.7. ARP Yanıltma (ARP Spoofing)

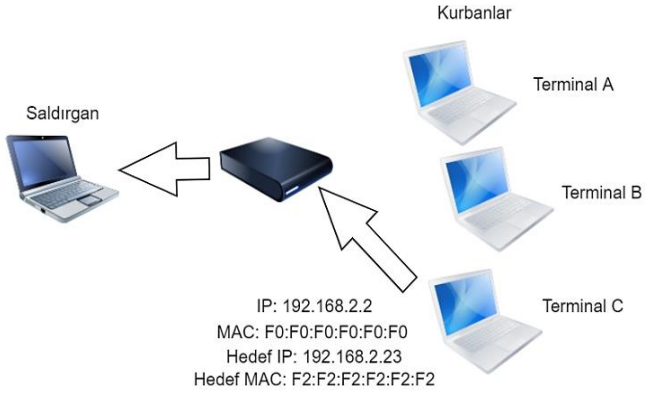
ARP, ethernet üzerinde IP trafiğini verimli yönlendirmek için kullanılır. IP ağları için fazlaca öneme sahiptir. Çalışma mantığı ise sunucuya bağlanmak isteyen terminalin kendine ait IP, MAC adreslerini ve hedef IP, MAC adreslerini ARP paketi olarak oluşturmasıdır Şekil 6 (Forshaw, 2018; Şimşek, 2020).



Şekil 6. Saldırgan ARP Paketi Göndererek Sorgulama Yapması

Şekil 6'da saldırgan tarafından Ethernet vasıtasıyla kullanıcılara ARP paketi gönderilmektedir. Ethernete bağlı kullanıcılar bu paketi almaktadır. Alınan pakete uygun IP ve MAC adresine sahip kullanıcılar geri dönüş yaparlar.

Şekil 7'de gelen pakete uygun içeriğe sahip kullanıcı geri dönüş sağlamıştır. Bu geri bildirim ile sistemde kullanılacak kurban belirlenmiş olunmaktadır.



Şekil 7. Saldırgana Gönderdiği Paket İçin C Terminalinden Cevap Gelmesi

3.1.8. Kötü Amaçlı Yazılım (Malware)

Kötü amaçlı yazılım (M*alicious software*) ifadesinin kısaltmasıdır. Sisteme zarar veren, onu durduran, bilgi sızdıran, manipüle eden veya onu kullanmaya yönelik hazırlanmış kötücül yazılımlardır (Çeliktaş, 2016; uzmanim.com, 2018; Uzmanim.com, 2018).

Kötü amaçlı yazılımlar grubuna virüs (virus), truva atı (trojan), arka kapı (backdoor), worm (solucan), reklam yazılımı (adware) gibi kötü amaçlı programlar girer. Kötücül yazılım olarak da bilinen malware, bilgisayar ve ağ üzerindeki herhangi bir sisteme sızmak ve zarar vermek için geliştirilen bir tip yazılımdır. Malware yazılımlar sadece sistemi yavaşlatmaz veya bilgi çalmazlar ve bazıları sisteminizin bir bot görevi görerek başkaları tarafından uzaktan kullanılmasına yol açarlar.

Malware virüslerinde içerisinde olduğu zararlı yazılımların genel adıdır. Farklı amaçlar için kullanılan çok sayıda malware yazılımlar bulunmaktadır.

3.1.8.1. Casus Yazılım (Spyware)

Yazılımcının kendi yazdığı programla, belirli reklamların kullanıcıya gösterilmesi mantığıyla çalışan Adware'den farklı olarak, kullanıcının ekranında belirli reklâmları görüntüleyip aynı zamanda takip ve kontrol mekanizması oluşturan programlara "Spyware" denir. Adware' den en belirgin farkı cihazda yapılan kişisel bilgi eklemeleri ve değişimleri daha önceden yazılım içerisine gömülmüş bir sunucuya, internete bağlandığınız zamanlarda gönderen programlardır.

3.1.8.2. Virüs

Virüsler birer programdır, kendi kendilerini kopyalarlar ve bir yerden bir yere bulaşırlar. Virüs bulaştığı sistemin çalışmasıyla otomatik olarak faaliyete geçer. Bir virüsün bir diğer dosyaya veya sürücüye geçmesi çok kolaydır. Sistemin yavaş çalışmasına, sistem bilgilerinin kopyalanmasına, sistemin başkaları tarafından dinlenmesine veya durmasına neden olabilir.

Tablo 3. Tehditlere Örnekler ve Risk Değerleri (European Union Agency for Network and Information Security (ENISA), 2017; Muratoğlu, 2020; Schmittner et al., 2016)

Yapılabilecek Saldırılar	Tehtitler	Etki	Minimum Uzmanlık	Önem
OS'ta bilinen Exploit açıkları veya uzaktan kontrol	Rootkit veya Trojan yüklenmesi	ECU kontrolünün kaybedilmesi	1	4
OS'ta bilinen Exploit açıkları veya BufferOverFlow	Yazılım Araçlarının Silinmesi	ECU kontrolünün azaltılmasıdır	1	2
Man-in-the-middle Attack	Kullanılacak Şifreyi Gizli Dinleme	Olması Gereken Bağlantıyı Ele Geçirilmesi	1	2
ECU ve Web Server arasında taviz ve DDoS Saldırısı	Gelen verileri kesme amacıyla sistemin durdurulması	ECU'nun durdurulması	1	3
İletişimde Man-in-the-middle attack	Web Server'a manipüle edici veri gönderme	Daha önceden hazırlanmış bakım verileri gereksiz bakıma neden olur	1	1
Malware ve Aynı anda çok fazla ECU'ya veri gönderme	OS veya uygulamaları geçici süreliğine devre dışı bırakır	Sistem fonksiyonlarının azalmasına depolama alanlarının azalmasına neden olur	2	0
OS'ta bilinen Exploit açıkları veya BufferOverFlow	Verilere yetkisiz erişim	ECU'nün Kullanımına veya Konfigürasyonuna erişim	1	1
İletişimde Man-in-the-middle attack	Aktarılan Verilere Yetkisiz Erişim	Belirli Erişim Kullanım Verisi	1	1
GPS Spoofing	Gelen GPS verilerinin değiştirilmesi	Belirlenecek rotada değişikliklere neden olur	1	1
Proxy/Socks Saldırısı	Saldırganın Kimliğinin gizli kalmasını sağlar	Sistem tarafından saldırganın adresi doğru belirlenemez	1	0
ARP Spoofing	Saldırganın Kimliğinin gizli kalmasını sağlar	Sistem saldırganın kimliğini doğru tanımlayamaz	1	0

3.1.8.3. Truva Atı (Trojan Horse)

Truva atları yararlı yazılımlar gibi görünen bilgisayar programlarıdır, ancak güvenliğinizi tehlikeye atarlar ve pek çok zarara yol açarlar. Yakın geçmişteki bir Truva atı, Microsoft güvenlik güncelleştirmeleri olduğu iddia edilen eklerin bulunduğu bir e-posta görünümündeydi, ancak ekteki dosyaların virüsten koruma ve güvenlik duvarı yazılımlarını devreden çıkarmayı hedefleyen virüsler olduğu ortaya çıkmıştır (Yüksek, 2014).

3.1.8.4. Tuzak Kapanları (Trap doors)

Tuzak kapısı ya da arka kapı, bir sistemin yazılımını yapan kişi tarafından, yazılımın içine gizli bir şekilde yerleştirilen bir virüs yazılımıdır. Bu programın çalıştığı bilgisayara virüsü yerleştiren kişinin, uzaktan erişim yöntemiyle sistem duvarlarını aşarak sızması mümkündür (Alioğlu, 2019; Vinnem & Utne, 2018).

3.1.8.5. Solucan (Worms)

Solucan, virüs gibi, kendisini bir sistemden diğerine kopyalamak için tasarlanmıştır ve bunu otomatik olarak yapar. İlk olarak, sistemde dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Sisteminize girdikten sonra kendi başına ilerleyebilir. Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir (Yaşar & Çakır, 2015).

Kötü niyetli yazılımların genel bir listesini yaparsak:

- Sisteminizi uzaktan yönetirler (remote control-uzaktan kumanda)
- Kişisel bilgilerinizi toplarlar (spyware-casus yazılım)
- Tuş kullanımınızı kaydederler (keyloggers-tuş kayıtçıları)
- Sisteminize sessizce girer ve tamamen ele geçirirler (rootkit-trojan)

Tablo 4. Saldırı Olasılık Parametreleri (ENISA,2017; Schmittner et al., 2016)

Parametreler	Puanlama			
	3	2	1	0
Yetenek	Acemi	Teknisyen	Hacker, Otomotiv Uzmanı	Birçok Alanda Uzman Ekip
Bilginin Kullanılabilirliği	Herkese açık bilgiler	Bakım veya müşteriler için bilgiler edinilebilir	Üretim İçin Bilgiler mevcut	ECU tedarikçilerinin edinebildiği bilgiler
Erişilebilirlik	Güvenilmeyen Ağlar ile daimî erişim	Özel ağlar ile daimî erişim veya güvenilmeyen ağlar ile kısmi erişim	Fiziksel olarak daimî erişim veya özel ağlarla kısmi erişim	Sadece fiziksel olarak erişilebilir
Gereken Ekipmanlar	Herkesin kullanımına açık IT cihazları	Herkese açık özel IT cihazları	Kişiye özel tescillenmiş IT cihazları	Çoklu Özel Tasarım, Tescilli IT cihazları

3.1.9. Sibil Atak (Sybil Attack)

Saldırganın saldırılan sisteme yanlış sinyaller göndererek sahte kimliklerle sistemin stabilitesini bozması ve kontrolü ele almak istemesidir. Trafikte olmayan araçları var gibi göstererek sistemin doğru çalışmamasına sebep olmaktadırlar (Luo et al., 2019; Sinai et al., 2014).

3.1.10. OBD Port Atak (OBD Port Attack)

Diyagnostik portu vasıtasıyla sisteme kablolu olarak sızma işlemidir. Sistemin işletim sistemi tekrar programlayarak sistem kontrol edilebilir.

3.2. Otonom Araçlarda Siber Güvenlik Riskleri

Otonom araçlarda sensörlerin kullanımı siber saldırılarla devre dışı bırakılabilir. Bu işlem ile sistemde geçici veya kalıcı hasarlar meydana gelebilir. İnsan kullanımından kaynaklı kazaların önüne geçebilmek için teknolojiden faydalanmak istenmektedir. Fakat bu siber tehditlerin beraberinde gelmesine sebep olmuştur. Kazaların siber saldırıların sonucunda olma olasılığı gözükmektedir (El-Rewini et al., 2020; Schmittner et al., 2016). Sahip olunan GPS Sensörü kendine has güvenlik zafiyeti olan GPS Spoofing ile kullanıcı kullanımının etkisiz kalmasına sebep olabilir. Gelen yanlış sinyaller ile sistem bulunduğu veya gideceği konumun lokasyonunu farklı algılayabilir (Çuhadar, 2017). Ortaya çıkan etkilerden diğeri yönlendirme sonucu oluşacak kazalardır. Yönlendirmeler için sistemi yönetme amacıyla Shell Code' lar kullanılabilir. Yapılacak saldırı kullanıcının yetkilerini ele geçirmeye yöneliktir. Shell Code sistemde assembly dilinde yazılmış birtakım kodlar tutmaktadır. Kodlarda yapılacak değişiklikler sistemin çalışmasında sorunlar meydana getirecektir. Bu kodlarda düzeltmeler yapılmadığı takdirde sistem daima başkalarının hakimiyetine açık kalacaktır. Frenleme ve direksiyon hakimiyeti kullanıcının elinden alınmış olacaktır. Aydınlatma sistemleri, Airbag sistemi ve diğer koruma araçları kontrol dışı kalacaktır (Taeihagh & Lim, 2019). Sistem yazılımının yeniden yüklemesi yapılıncaya kadar sistemde yönetim başkalarının elinde olacaktır. Tablo 3' de yapılabilecek saldırılar ve bunların oluşturdukları tehditler gösterilmişlerdir.

Tablo 5. Siber Güvenlik Ağırlık Sınıfları (European Union Agency for Network and Information Security (ENISA), 2017; Schmittner et al., 2016)

Ağırlık Sınıfı	Emniyet	Gizlilik	Maliyet	Performans
0	Yaralanmalar yok	Verilere yetkisiz erişim yok	Finansal kayıp yok	İşlemler üzerinde performans etkisi yok
1	Hafif veya orta dereceli yaralanmalar	Sadece Yapılandırma verileri	Düşük seviyede kayıplar	Etki operatör tarafından fark edilmez
2	Birden çok araçta orta derecede yaralanmalar	Kısmi veriler	Orta derecede kayıp	Birden çok araç için fark edilmeyen performans düşüşü
3	Ölümcül derecede yaralanmalar	Girişe etkisiz veri	Birden fazla araçta orta veya büyük hasar	Birden fazla araç için fark edilebilir performans kayıpları
4	Ölümle sonuçlanan yaralanmalar	Araçta bulunan ECU' lar için verilere erişim	Birden fazla araç için ağır kayıplar	Birden fazla araç için önemli derecede etki

3.3. Otonom Araçlarda Siber Saldırı Olasılık Parametreleri

Siber saldırıların sistem üzerideki hareketleri, siber saldırıların sisteme olan etkileri ve gereken uzmanlık seviyeleri Tablo 3' te gösterilmiştir. Yapılan literatür taramaları ve incelemeler neticisinde otonom araçlara karşı yapılabilecek saldırıların etkileri ve bu saldırılar için gereken donanım değerlendirilmiştir.

Çalışmada sahip olunan ve literatürde geçen zafiyetler değerlendirilerek Tablo 3'te ortaya çıkabilecek açıklıklar olarak verilmiştir. Puanlamalar Tablo 4 ve 5' teki saldırı değerlendirmeleri ve uzmanlık puanlarına göre yapılmıştır.

Tablo 6. Siber Saldırılar Tespit ve Önleme (ENISA, 2017; Muratoğlu, 2020; Schmittner et al., 2016)

Siber Saldırılar	Siber Saldırı Tespit	Önleme Teknikleri
GPS Yanıltma (GPS Spoofing)	Sinyalin yüksek çözünürlükte dijitalleştirilmesi ve analizi	Anti Jammer kullanımı
Araya Girme Saldırısı (Man-in-the-Middle)	Bağlantıların beklenmedik kopması ve bilinmeyen lokasyonlar üzerinden bağlantı	HTTPS üzerinden internet kullanımı ve çoklu kimlik doğrulama kullanımı
Bellek Taşması (Buffer OverFlow)	Veri yığını tahsis eden hücrelerin denetlenmesi	Değişikliklerin düzeltilmesi
Kötü Amaçlı Yazılım (Malware)	Anti-virüs yazılımların kullanımı	Anti-virüs yazılımlarının kullanımı, İşlemciyi formatlamak
ARP Yanıltma (ARP Spoofing)	Açık kaynaklı paket analizi yapan yazılımlar	Yeni ARP Paketleri belirlemek veya HTTPS ve SSH ile kanal şifreleme
Vekil Sunucu Saldırısı (Proxy/Socks Attack)	IP bağlantılarının taranmasında benzer veya bilinmedik IP bağlantılarının tesbit edilmesi	Kaynak yönlendirme opsiyonlarının pasifleştirilmesi veya ağda IP değiştirme kaldırılması
Hizmet Kesintisi Saldırıları (DDoS Attacks)	Sistemin sitelerle olan bağlantısının beklenmedik şekilde kopması ve değişim izni vermemesi	Sistemin bağlanılacağı sitenin alternatiflerine geçiş sağlanması
Sibil Atak (Sybil Attack)	Sistemde yoğunluğun olmadığı bilindiği halde aşırı yoğunluğun olması	Sensörlerden gelen bilgilerin işlemci tarafından görmezden gelinmesi

Tablo 4'te uzmanlık derecesinin küçüklüğü sistem saldırıları hakkındaki donanımla ters olacak şekilde numaralandırılmıştır. Tablo 5'teki tahribatın büyüklüğü tahribatla doğru orantılı olacak şekilde numaralandırılmıştır. Saldırının önem derecesi ise insani kayıpların, sistemdeki performans kayıplarının, sistemdeki mali zararların, sistemdeki veri sızıntılarının derecesini belirtmektedir. Tablo 4' te saldırı yapabilecek kişilerin uzmanlık seviyelerine göre puanlama yapılmıştır. Herkesin erişebileceği bilgi seviyesi en yüksek sayı olarak, alanında uzman kişilerin erişebileceği bilgi seviyesi en düşük sayı olarak gösterilmiştir. Tablo 3 ve Tablo 4' te sistem açıklıklarının bilinmesi halinde herkesin sistemde değişikliklere neden olabileceği gösterilmiştir.

3.4. Otonom Araçlarda Siber Güvenlik Ağırlık Sınıfları

Yapılacak veya yapılan saldırıların kullanıcılara yaşatacağı mağduriyet açısından Tablo 5' te sınıflandırmalar yapılmıştır. Verilecek olan kayıpların derecesi ağırlık sınıfı ile verilmek istenmiştir. Ağırlık derecesiyle verilecek olan kayıp doğru orantılıdır. Kullanıcıların can güvenliği kayıpları emniyet, şahsi bilgi kayıpları gizlilik, bütçesel kayıpları maliyet, sistem üzerindeki etkisi performans ile sınıflandırılmıştır.

Tablo 7. Siber Saldırıların Tespiti için Kullanılacak Araçlar (ENISA, 2017; Muratoğlu, 2020; Schmittner et al., 2016)

Saldırı Tespit Araçları	Tespit Yöntemleri	Bizlere Sunduğu Veri
Nmap	IP'lere bağlı portların taranması ile port açıklıkları hakkında bilgi sahibi olunmaktadır. Saldırıların yapılabileceği portlar tespit edilebilir.	Portların açıklık durumuna göre Open, Closed, Fıltered ve Unfiltered değerlerini bizlere vermektedir.
Maltego	Sistemin IP yollarında bağlı olduğu bağlantı noktalarının haritalamasını çıkararak IP yollarının haritalamasını çıkartır.	Sistemin sahip olduğu bağlantı yollarını bizlere sunar. Dış bağlantıların tamamı IP yolları ile gösterilirler.
Metasploit	Veritabanında bulunan sistem dinleme yolları ile sisteme bağlanılabilecek yolları dinlememizi sağlar.	Sistemin sahip olduğu zafiyetler bizlere sunulmaktadır.

4. Siber Saldırı Tespit Araçları ve Önleme Teknikleri

Siber saldırılara karşı çeşitli önlemler mevcuttur. Bu çalışmada incelemeler neticesinde üzerinde genel olarak durulacak önlemler sistemde kullanılacak tespit araçları olacaktır. Sistemde kullanılacak tespit araçlarının yanı sıra sistemin dış koruyucu sistemler tarafından da korunması sistemin daha güvenli olmasını sağlayabilmektedir. Çalışma içerisinde tespit araçlarından detaylı olarak bahsedilmiştir. Otonom sistemlerin kendilerinde yüklü olarak denetleme araçlarınında bulunması yapılacak denetlemelere kolaylık sağlayacaktır. Siber saldırıların önlenmesi için sistemin düzenli olarak denetlenmesi gerekmektedir. Bu denetlemeler port taramaları ile mümkündür (Marquez, 2010; Technical & Str, 2019). Bu çalışmamızda ele alacaklarımız port taramalarıdır. Yapılan saldırılar kontrolü ele almak olduğu varsayıldığından çalışmamızda araç hareketlerindeki değişimler denetlenerek kontrolün kaybedildiği fark edilecektir. Burada kullanılacak tarama teknikleri; NMAP, Maltego ve Metasploit' dur (Kennedy et al., n.d.; Singh, 2013).

Sistemde bulunan zararlı yazılımların silinmesi gerekmektedir. Zararlı yazılımları metasploit ile denetlemek mümkündür. Sistemlerin sahip olduğu tüm açıklıkların bulunduğu metasploit database vasıtası ile otomobillerin açıklıkları üzerinden denetleme yapılabilir ve tedbirleri alınabilir. Yapılan saldırılar fiziksel olarak bağlantı içermiyorsa kablosuz olarak bağlantılarda IP kullanılarak bağlantı gerçekleştirilebilir. IP hareketlerinin denetimi sistemde var olmadığı bilinen IP'lerin hareketi sonucu bize saldırganın kimliğini verebilir. Kullanılması gereken araç ise Nmap'tir. Nmap sistemin bağlı olduğu ağdaki tüm kullanıcı IP'lerini bize vermektedir. Elde edilecek IP' ler arasında yabancı IP' ler sistem tarafından maruz bırakılacakları paketlerle devre dışı kalabilmektedir.

4.1. Siber Saldırı Tespit Araçları

Saldırılar için sistem açıklıklarını bizlere bildirecek araçlarımız mevcuttur. Araçlarımızın kullanımı ile sistem açıklıkları fark edilerek giderilebilir. Kullanılabilir tespit ve denetleme araçları kullanımı ile sistemde güvenlik için kolaylıklar sağlayabilmektedir. Saldırı tespit araçlarımızın isimleri, tespit için yöntemleri ve bizlere sunduğu veriler Tablo 7' de gösterilmiştir. Çalışma boyunca Nmap, Maltego ve Metasploit incelemeleri yapılmıştır.

4.1.1. NMAP

Sistemlerde genel olarak bilinen 65.532 adet port mevcuttur. Bu portlarla kullanıcıların kullanımını kolaylaştıracak cihazlara ve yardımcı olacak dış bağlantılara erişim gerçekleştirilmektedir. Bu bağlantılar kullanılarak siber saldırılar gerçekleştirilmesine karşı NMAP ile tarama gerçekleştirilmektedir. NMAP kendisine özel olarak port belirtilmez ise en sık kullanılan 1000 portu taramaktadır. Burada dışarıdan gelecek bağlantılar ile IP adreslerinin taramaları sonucu yabancı, bilinmeyen bir IP kullanılarak sisteme bağlanma durumu denetlenmektedir. Sistemin tanınması da çok önemlidir çünkü kullanılacak tarama yönteminde sistemde bulunan tüm IP adresleri taranmaktadır.

NMAP' te varsayılan olarak TCP taraması yapılmaktadır (THT, 2020). Kullanıcının kendisine ait IP adresi ve sistemde yardımcı kullanılan IP adresleri open olarak sistemde görülebilir. Şekil 8' da görüldüğü gibi. Çıktı olarak Port, State ve Service bilgileri alınmaktadır.

- Port, port numarasını kullandığı protokolü gösterir.
- Servis (Service), port üzerinde çalışan servis isimlerini belirtir.
- Durum (State), portun open, closed veya filtered olduğunu gösterir.
- Açık (Open): portun erişilebilir olduğunu göstermektedir.
- Kapalı (Closed): portun erişilebilir olduğunu fakat üzerinde değişiklikler yapılamayacağını göstermektedir.
- Filtreli (Filtered): filtreleme portun filtreleme mekanizması tarafından engellendiği manasına gelmektedir. Portun açık veya kapalı olması durumuna dair bir bilgi yoktur.
- Filtresiz (Unfiltered): porta erişilebilir fakat açık veya kapalı olduğuna dair fikir yoktur.
- Açık Filtrelenmiş (Open Filtered): port açık veya filtrelenmiş olabilir. Bu durum çözümlenememiş.

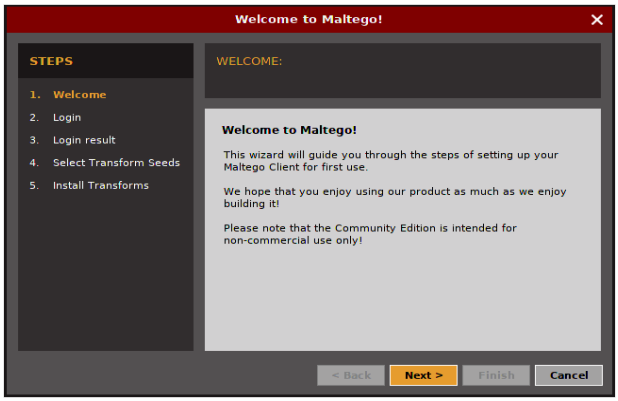
```
Nmap scan report for 10.0.2.2
Host is up (0.0016s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
```

Şekil 8. Nmap'te taranan bir IP'nin port sonuçları (Andress & Winterfeld, 2011; Çıtak, 2020).

Şekil 8' de 10.0.2.2 IP adresine bağlı cihazın taraması yapılmıştır. Gösterilen portlar arasında 3 port açıktır (Andress & Winterfeld, 2011; Çıtak, 2020).

4.1.2. Maltego

Saldırı yapılacak sistemler hakkında bilgi sahibi olmak önemlidir. Sistemler hakkında pasif ve aktif bilgiler toplayarak sistem hakkında yeterince bilgiye sahip olunmalıdır. Pasif bilgiler; hakkında bilgi toplanması istenen sistemin internet üzerinde sabit bulunan bilgilerdir. Arama motorları, sosyal paylaşım platformları, whois ve DNS sorgu siteleri, kişisel bilgi toplayan siteler bize bu bilgileri sağlayabilir. Aktif bilgiler; IP, sunucu ve servis sağlayıcılar üzerinden DNS ve alt alan adlarının edinilmesidir (Çelik, 2020). Maltego, sistemin aktif ve pasif bilgilerimi bize sunan araçtır. Paterva tarafından Java programlama dilinde geliştirilmiştir. Ücretsiz ve ticari sürümleri mevcuttur. Güvenlik alanında uzmanlar ve bu alanda kendini geliştirmek isteyenler tarafından açık kaynak bilgileri toplamak ve bu bilgileri analiz etmek için kullanılmaktadır(Andress & Winterfeld, 2011; Hai-Jew, 2014). Sistemin IP ve bağlantı bilgilerini verir. Tarama da kullanıcının bağlı olduğu tüm sistemler, aracılar, IP adresi veren bağlantılar, ağ bağlantıları, aktif veri gönderilen alıcılar, aktif veri alınan göndericilere dair tüm açık kaynaklı bilgiler, sistemin erişebildiği ve sisteme iletilen tüm bilgiler, websiteler, IPv4 adresleri, e-posta adresleri, domain adresleri ve URL adreslerini bizlere sunabilmektedir. Kendilerine ait websitelerinden alınan aktivasyon kodu ile kullanılabilir (Agus & Pratama, 2019; Ağyol, 2020; Hai-Jew, 2014; Maltego.com, 2020). Maltego' nun açılışında karşımıza çıkan ekran Şekil 9' da verilmiştir.



Şekil 9. MaltegoProgramı Açılış Ekran

4.1.3. Metasploits

2003 yılından beri geliştirilen, kendisine ait sistemde güvenlik açıklarının bulunmasını kolaylaştıran ve kontrolünün yapılmasını sağlayan açık kaynak kodlu bir platformdur. Metasploit 2.0 Perl, Metasploit 3.0 Ruby dilinde kodlanmıştır. Sistemlerde çalışan servis ya da uygulamaların güvenlik açıklarını bizlere sunar. Sahip olduğu Framework üzerinde 1400+ exploits, 800+ auxiliary modül, 400+ payload, 30+ encoder ve 8 nobs mevcuttur. Mevcut araçlarla saldırı, dinleme ve açıklık tespiti yapılabilir (Baggett, 2008; Singh, 2013). Metasploit Framework kendisine ait bir veritabanına sahiptir. Açıklıkların neler olduğu, nasıl kullanıldığı gibi bilgiler mevcuttur. Açıklıkların kullanımına kolaylık sağlaması için kullanımıda beraberinde açıklanmıştır. Bilgi toplama, açıklıkların tespiti, güvenlik noktalarından yetkiye gerek duymadan geçiş gibi bazı modüllerinde kullanım vardır. Kullanım kolaylığı sağlayacak metotlar şunlardır:

- İstismar (Exploits): Hedef alınan sistemde bulunan açıklıkları kullanarak sistemin servis dışı çalışmasına neden olacak sistem açıklıklarıdır. Exploits saldırıları sistemde çalışmayan veya Bug olarak nitelendirilen tüm açıklıkların kullanılması sonucu sistemin kullanım dışı kalmasına sebep olacak metotların kullanımıdır.
- Şifreleme (Encoder): Sistemde güvenlik noktalarında atlatma yapma amacıyla gerekli kriptolama işleminin yapılmasıdır.
- Payload: Sistem bağlantılarının dinlenmesi amacıyla yazılmış saldırı kodlarıdır. Webcam, speaker, bluetooth bağlantılar, wireless gibi sistem bağlantılarını dinleme ve izleme yapılabilir. Saldırı sonrası sistemde değişiklikler yapılabilir.
- Yedek (Auxiliary): Sistemde saldırı öncesi bilgi toplama amacıyla yapılan saldırılardır. Servis tespiti, port taramaları, zafiyet taramaları ve tüm istemciler için kullanılan araçlar bu başlık altında mevcuttur.
- Not Operasyonu (Nops): "Not Operation" bellek yerlerini öğrenme amacıyla bellekte yer dolduran bitler. Amaçları saldırı tespit etme ve sistemleri yanıltmak için kullanılır. Program ilerleme akışı değiştirilebilir ve rastgele bir yere atlanabilir.

Metasploit kendine özgü dosyalama sistemi özellikleri (Altınkaynak, 2020);

- Veri (Data): Datalar metasploit tarafından işlenebilir ve değiştirilebilirler
- Lib: Framework sisteminin ana yapı kütüphanesidir.
- Eklentiler (Plugins): Framework'ün tüm özelliklerini kullanabilen eklentidir.
- Araçlar (Tools): komut satırında çalışan yerine göre işlemleri halleden araçlardır.
- Dış (External): Harici kaynaklar, 3. Parti yazılımlar ve kaynak kodlardır.
- Dökümantasyon (Documentation): Framework'ü bilgilendirmek için kullanılan belgelerdir.

4.2 Otonom Araçlarda Siber Saldırıları Önleme Yöntemleri

Araç işlemci ağları, bilgisayar korsanlarının ulaşması zor olan kontrol birimleriydi ve fiziksel etkileşim olmadan kontrol mümkün değildi (McAfee, 2016). Fakat günümüzde fiziksel erişim olmadan da bu ağlara erişmek mümkün hale gelmiştir. Standartlaştırılmış işlemci yapısı ortak ağlarla birbirine bağlanmasının ardından sistemlerde doğan açıklıklarla bağlantı kablosuz olarakta mümkün olmaktadır. Bu saldırıları yapabilmek için en azından araç alt sistemleri uzmanı veya hacker olmak gerekmektedir.

İşlemci veri yollarına saldırı yapabilmek için hazırlanmış kötü amaçlı kodlar işlemciye yüklendiğinde sistemde kontrol mümkün olmaktadır. Sistemde bulunan dış müdahaleleri tespit edebilmek için sistemin belirli aralıklarla denetlenmesi gerekmektedir. Dış müdahalelerde sistem içerisinde bilinen IP hareketleri dışında IP hareketleri tespit edilmektedir. Sisteme saldırı yapılmadan önce alınması gereken önlemler oldukça önemlidir (Schmittner et al., 2016). Sisteme trojan ve rootkit gibi yüklemeler yapılabilmektedir. Sisteme konfigürasyon esnasında yanlış konfigürasyon yüklemesi yapılabilir.

Sistem kontrolünün kaybedilmesinden önce alınması gereken önlemler;

- Sistemin bağlı olduğu cihazların belirli aralıklarla denetlenmesi,
- Yetkisiz ve yanlış konfigürasyon verilerinin uygulanmasını önlemek,
- Bilinmeyen kaynaklardan gelen yazılım güncellemelerinin kabul edilmemesi,
- Sistemin kablolu ve kablosuz bağlantılarının sık sık denetlenmesi,
- Tablo 3' de bahsedilen açıklıkların kullanılmasına yönelik önlemler almak.

Sistem kontrolünün kaybedilmesinin ardından yapılması gerekenler;

- Nmap te IP' ler için port taramaları yapılmalıdır,
- Dış müdahaleler için açık olan portlar kapatılmalıdır,
- Maltego'da bağlantı yapılan noktalar için taramalar yapılmalıdır. Dış müdahale için açık olan bağlantılar kapatılmalıdır,
- Metasploit ile sistem açıklıkları için testler yapılmalıdır.

Sistemin kontrolünün kaybedilmesinin ardından sistemde denetlemeler yapılmalıdır. Denetimlerin yapılabilmesi için kullanılması gereken araçlar mevcuttur. Sisteme dışarıdan bağlantı sağlayabilecek olan tüm portlar taranmalıdır. Taramalarda amaç sisteme sızmak için kullanılan IP adreslerinin tespiti ve bunların sistem tarafından bertaraf edilmesidir. Taramalar için en çok tercih edilen araç Nmap aracıdır. Açılımı "Networking Mapping" Ağ Haritalamadır (Altınkaynak, 2020; Çıtak, 2020).

Sistemin internet üzerinden taramaları için ise Maltego aracı kullanılmaktadır. Nmap ve Maltego araçları bizlere bağlı olduğumuz serverları, ağları vermektedir. Bilinen bağlı cihazlar ve IP adresleri dışında sistemde bulunan cihazlar ve IP'ler sisteme giren yabancı sistemler olarak kabul edilirler. Sistemin açıklıklarının tespiti için kullanılan araç Metasploit Framework'tür. Herhangi bir sistem içerisinde bulunan açıklıklar Metasploit Framework içerisinde mevcuttur (Singh, 2013). Uzmanlar, yetkililer ve kendi güvenliğini sağlamak isteyen kullanıcılar bu araçları kullanarak sistemlerindeki açıklıkları ve sızmaları tespit edebilmektedirler.

Sistemde kontrolün kaybedilmesinin ardından yapılması gerekenler sistemin içerisinde açıklıkları keşfederek bu açıklıkların giderilmesi olmalıdır. Sistem bilgilerini bizlere verecek bazı araçlarımız mevcuttur. Siber güvenlikte kullanılan tarama araçları ile sistemde sızma testleri yapılarak sızma noktaları veya yazılımsal açıklıklar bulunabilir. Buna ilave olarak sızma noktaları üzerinden açıklıklarda giderilebilir.

5. Otonom Araçlarla İlgili Son 5 Yılda Yapılmış Çalışmalar

Otonom araçlarda haberleşme, veri iletimi ve dış bağlantıları üzerinde açıklıkların incelendiği akademik çalışmalar incelenmiştir. İncelenen çalışmalarda otonom araçların açıklıklarının kablosuz dış bağlantılar üzerinden olduğu görülmüştür. Saldırılarda sistem açıklıklarının kontrolün

kaybedilmesine sebep olan alanlarda düzeltmeler için açıklamalarda ve tavsiyelerde bulunulmuştur. Tablo 8' de incelen akademik çalışmala ve inceleme yöntemlerinden bahsedilmiştir. İncelenen araştırmalarda riskleri kümelemek ve sıralamak için değerlendirmelerde bulunulmuştur. Yapılan saldırı incelemeleri genel olarak kablosuz bağlantı vasıtası ile işlemciye ve otonom araçlar için kullanılan işletim sistemlerine yapılmaktadır. Sistem işlemcilerine sızma yapabilmek için kablolu olarak fiziksel bağlantı veya kablosuz olarak ağ bağlantıları gerekmektedir. Saldırının yapılmasından önce sistemin gereken önlemleri almış olması gerekmektedir. Sisteme sızma gerçekleşmişse, sızmanın bertaraf edilebilmesi için gereken sistemin denetlenmesi ve sisteme gönderilmiş kötü amaçlı yazılımın sistemden silinmesi gerekmektedir. Silinme işlemi gerçekleştirilemez ise sistem ve kullanıcı zarar görebilmektedir (Cerrudo et al., 2020).

6. Sonuç

Yapılan çalışmada amaç otonom hale gelen teknolojik araçların ve özellikle otomobillerin kullanımını tehdit eden siber saldırıların nasıl bertaraf edilebileceği değerlendirilmiştir. Genel olarak sistemin çalıştığı işlemcilerden doğan açıklıklar kullanılarak yapılan saldırıların sistemin kontrolünün ele geçirilmesi, durdurulması ve sistemin kapatılmasıdır.

Saldırıların yapılabilmesi için kablosuz bağlantı olmalıdır. Sistemin çalışması için kablosuz bağlantının olmaması mümkün olmadığından dolayı sistemin kullanıcı tarafından kontrollü şekilde kullanılması gerekmektedir. Sistem mimarisi temel olarak bir işlemciye ihtiyaç duymaktadır. Sistem yapısı gereği siber saldırılara müsaittir. Sistemde diğer parçalar; konum sensörü, görüş sensörü, araç parçaları sensörleri ve kablosuz iletişim modülleridir. Tüm bu sensörler kendilerinin kullanımından doğan açıklıklarla beraber kullanılmaktadır. Kullanım için gereken tedbirler alınmalı tüm sistem düzenli aralıklarla denetlenmelidir. Yapılan saldırılar genellikle otomobillerin işlemcilerine yönelik olmasından dolayı sisteme gelebilecek güncellemeler bilinen kaynaklardan gelip gelmediği kontrol edilmelidir. Bilinmeyen kaynaklardan gelen güncellemeler veya kalibrasyon güncellemeleri yapılmamalıdır. Kullanıcı dışında müdahale için izin verilmemelidir.

Sistem uzmanları, meraklıları, bu alanda kendini geliştirmek isteyenler ve kullanıcılar tarafından denetlenebilmektedir. Bunun için sistem denetimini sağlayan araçlar mevcuttur. Kablosuz bağlantı vasıtasıyla sisteme sızma yapılabilmesi için IP kullanımından dolayı sistem taramalarında çıkacak bilinmeyen IP' ler devre dışı bırakılmalıdır. Sistemlerin daima kablosuz bağlantısının olacağı düşünüldüğünden bu alanda tarama ve izinsiz girişler reddedilecek şekilde kullanılmalıdır. Sisteme müdahale olduğu düşünüldüğünde sistem dosyalarının denetimi yapılmalı ve zararlı yazılımlar tesbit edildiğinde sistemden silinmelidir. Sistem kullanımında denetleme aşaması atlanmamalıdır. Sistemde yabancı olduğu bilinen veya kimliği bilinmeyen hareketlere izin verilmemelidir.

Anti-virüs şirketleri ve bu alanda çalışma yapan uzmanların çalışmaları, yapılan siber saldırıların işlemciye yönelik olması nedeniyle işlemcinin kontroldeki payını düşürmeye yönelik olacaktır. Bu sayede işlemcinin siber saldırılarda kullanımı azalacaktır. Kontroldeki payının düşmesiyle işlemci açıklıklarında riskler azalacaktır. Bu çalışmalar saldırganların yeni saldırı metotları aramalarına sebep olacaktır. Bu sayede sistemlerde uzunca bir süre bilinen metotlarla saldırı yapılamayacaktır.

Tablo 8. Son 5 Yıl İçerisinde Otonom Araçlarla İlgili Yapılmış Çalışmalar

Çalışma İsmi	Yazar	Yıl	Yayın Yeri	İnceleme/Yöntem
Cyber Security and Resilience of smart cars	Dotan, A. Maple, C. Cleemann, L. & Friends	2016	European Union Agency For Network And Information Security (ENİSA)	Akıllı ulaşım araçlarının sahip olduğu kablolu ve kablosuz haberleşme araçlarında meydana gelebilecek siber saldırılar incelenmiştir.
Using SAE J3061 for Automotive Security Requirement Engineering	Schmittner, C. Ma, Z. Reyes, C. & Friends	2016	International Conference on Computer Safety, Reliability, and Security	Siber saldırıların otomobillerde ve insanlarda meydana getirebileceği hasarlar incelenmiştir.
Cybersecurity in Autonomous Vehicles	Morimoto, S. Wang, F & Friends	2017	Introduction to Applied Information	Otomobillerin sahip olabileceği servis saldırıları, ECU, CAN ve BUS saldırıları incelenmiştir.
İnsansız Hava Aracı Sistemlerinde Bilgi Güvenliği	Çuhadar, İ.	2017	Gazi Üniversitesi Fen Bilimleri Enstitüsü	Navigasyonla hareket eden otonom araçlarda GPS Spoofing açıklığı üzerine bir çalışmadır.
Automotive Security Best Practices	Brown, D. A. Clare, D. Wasicek, A. & Friends	2017	McAfee White Paper	Otomobillerin sahip olduğu yazılımlarda açıklıklar üzerine çalışmalardır.
A cyber-threat analytic model for autonomous detection of virtual property theft	Patterson, N. Hobbs, M. Zhu, T.	2017	Information and Computer Security	Siber tehditlerin ve hırsızlık olaylarına dair analitik model üzerine bir incelemedir.
Connected and autonomous vehicles: A cyber-risk classification framework	Sheeman, B. Murphy, F. & Friends	2019	Transportation Research Part A	Otonom otomobillerin kablosuz bağlantılarına karşı yapılabilecek saldırılar üzerine incelemeler yapılmıştır.
A taxonomy and survey of cyber-physical intrusion detection approach for vehicles	Loukas, G. Karapistoli, E. & Friends	2019	Ad Hoc Networks	Otomobil beyinlerine karşı yapılabilecek siber saldırıların incelenmesiyapılmıştır.

Siber Saldırılar ve Ülkelerin Siber Güvenlik Yöntemleri	Alioğlu, S. D.	2019	İstanbul Bilgi Üniversitesi	Ülkelerin siber saldırılara karşı alacağı tedbirler ele alınmıştır.
Autonomous Shipping & Cybersecurity	Crespo, J. P. Gomez, L.G. Areas, J.G.	2019	Ship Science & Technologies	Otonom seyehat eden gemilerde siber saldırılar için alınmış tedbirlerin incelenmiştir.
Akıllı Araçlar İçin Bulanık Mantık Temelli Siber Güvenlik Risk Modeli	Muratoğlu O.	2020	Gazi Üniversitesi Fen Bilimleri Enstitüsü	Akıllı Otomobillerdeki sensörler ve veri okuma cihazları üzerinde siber saldırı riskleri incelenmiştir.
Cybersecurity challenges in vehicular communications	Zeinab El-R. Sadatsharan, K. & Friends	2020	Vehicular Communications	Otomobiller arası iletişime karşı yapılabilecek siber saldırılar incelenmiştir.
LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them	Cerrudo, C. & Friends	2020	Securing Smart Cities White Paper	Akıllı cihazlar siber güvenlik riskleri ele alınmıştır.

Kaynakça

Agus, I. P., & Pratama, E. (2019). Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company). *International Journal of Computer Network and Information Security (IJCNIS)*, *July*, 8–12. https://doi.org/10.5815/ijcnis.2019.07.02

Ağyol, Ü. (2020). *Maltego nedir nasıl kullanılır*. https://www.unluagyol.com/2011/12/maltego-nedir-nasl-kullanlr.html

Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları. *İstanbul Bilgi Üniversitesi*, Yüksek Lisans Tezi, 2019.

Altınkaynak, M. (2020). *Siber Güvenlik ve Hacking*. Abaküs Yayınları.

Andress, J., & Winterfeld, S. (2011). Cyber Warfare Techniques, tactics, and tools. In *Cyber Warfare*. https://doi.org/http://dx.doi.org/10.1016/B978-0-12-416672-1.00001-5

Baggett, M. (2008). Effectiveness of antivirus in detecting Metasploit payloads. *SANS Institute*.

Bellu, S. (1998). *Les pionniers de la locomotion terrestre*.

Bezai, N. E., Medjdoub, B., Al-Habaibeh, A., Chalal, M. L., & Fadli, F. (2020). Future cities and autonomous vehicles: analysis of the barriers to full adoption. *Energy and Built Environment*. https://doi.org/10.1016/j.enbenv.2020.05.002

Çelik, H. (2020). *Bilgi Güvenliği Ve Sızma Testleri* (Vol. 21, Issue 1). https://doi.org/10.1155/2010/706872

ÇELİKTAŞ, B. (2016). *Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme*. 1–10.

Cerrudo, C., Martinez, E., & Sequeira, M. (2020). *LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them*. *January*, 27. https://act-on.ioactive.com/acton/attachment/34793/f-87b45f5f-f181-44fc-82a8-8e53c501dc4e/1/-/-/-/-/LoRaWAN Networks Susceptible to Hacking.pdf

Çıtak, Ö. (2020). *Offensive & Defensive Ethical Hacking*. Abaküs Yayınları.

Congress, L. of. (2018). *What is a GPS?*

Coulibaly, T. (2007). *Il ya un siècle, l'automobile*. Éd." Ouest-France.

Çuhadar, İ. (2017). İnsansız Hava Aracı Sistemlerinde Bilgi Güvenliği Ve Risk Tabanlı Çok Kriterli Karar Verme Modeli İle Değerlendirilmesi [Gazi Üniversitesi]. In *Gazi Üniversitesi Fen Bilimleri Enstitüsü* (Vol. 11, Issue 3). https://www.m-culture.go.th/mculture_th/download/king9/Glossary_about_HM_King_Bhumibol_Adulyadej's_Funeral.pdf

Devichnick. (2017). *Самокатка Кулибина*. https://web.archive.org/web/20170127231326/http://www.devichnick.ru/031kulibin.htm

Duan, Z., Yuan, X., & Chandrashekar, J. (2006). Constructing inter-domain packet filters to control IP spoofing based on BGP updates. *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFOCOM.2006.128

Eckermann, E. (2001). *World history of the automobile*. SAE.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, *23*, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

Elif Tuğba KILIÇ. (2015). Siber Saldırıları İzleme Yöntemleri Ve Zararlı Yazılım Analizi. In *Journal of Visual Languages & Computing*. Gazi Üniversitesi.

Esteban, B. (2019). *Vehículos Autónomos*.

European Union Agency for Network and Information Security (ENISA). (2017). Cyber security and resilience of smart cars. Good practices and recommendations. In *2017-02-1* (Issue December). https://doi.org/10.2824/87614

Feng, S. (2019). *Cognitive Dynamic System for Connected and Autonomous Vehicles*.

Forshaw, J. (2018). *Attacking Network Protocols*.

Gps.gov. (2020). *what is GPS?* https://www.gps.gov/systems/gps/

Green, H. (1925). Radio Controlled Automobile. *Radio News*, *592*, 656.

Gridin, A. (2017). *Трехколесное чудо механика КулибинаTitle*. https://web.archive.org/web/20170715203308/http://www.carseller.ru/articles/10-01-2008.1350.html

Hai-Jew, S. (2014). *Using Maltego Tungsten™ To Explore the Cyber-Physical Confluence in Geolocation*. *2014*, 236–385. https://scholarspace.jccc.edu/cgi/viewcontent.cgi?referer=https://scholar.google.es/&httpsredir=1&article=1082&context=c2c_sidlit

Haider, Z., & Khalid, S. (2017). Survey on effective GPS spoofing countermeasures. *2016 6th International Conference on Innovative Computing Technology, INTECH 2016*, 573–577. https://doi.org/10.1109/INTECH.2016.7845038

Han, K., Weimerskirch, A., & Shin, K. (2014). Automotive Cybersecurity for In-Vehicle Communication. *IQT Quarterly*, *6*(1), 22–25. https://kabru.eecs.umich.edu/papers/publications/2014/IQT Quarterly_Summer 2014_Han et al.pdf

İSPİR, M. T. (2019). Endüstriye Amaçlı Bir Otonom Robotun Tasarımı ve Gerçekleştirilmesi [Fırat Üniversitesi]. In *Fırat Üniversitesi*. https://doi.org/10.1145/1390630.1390641

Jadoon, A. K., Wang, L., Li, T., & Zia, M. A. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wireless Communications and Mobile Computing*, *2018*. https://doi.org/10.1155/2018/1640167

Kendi, A. (2017). *Sürücüsüz Araçlar ve Türkiye*. https://thinktech.stm.com.tr/uploads/raporlar/pdf/14122017157 32202_stm_surucusuzaraclar_.pdf

Kennedy, D., Gorman, J. O., Kearns, D., Aharoni, M., & Moore, H. D. (n.d.). *Metasploit*.

Luo, Q., Cao, Y., Liu, J., & Benslimane, A. (2019). Localization and Navigation in Autonomous Driving: Threats and Countermeasures. *IEEE Wireless Communications*, *26*(4), 38–45. https://doi.org/10.1109/MWC.2019.1800533

Maltego.com. (2020). *Maltego*. https://www.maltego.com

Marquez, C. J. (2010). An Analysis of the IDS Penetration Tool : Metasploit. *The InfoSec Writers Text Library*, *9*. http://www.infosecwriters.com/text_resources/pdf/jmarquez_M etasploit.pdf

McAfee. (2016). Automotive Cyber Security Best Practices. *Auto Tech Review*, *5*(8), 20–25. https://doi.org/10.1365/s40112-016-1180-1

Milev, G., Hastings, A., & Al-Habaibeh, A. (2019). *Investigating The Effect of Expanding The Use of Electric Cars On The Environment: A Case Study From Scotland*.

Miller, O. (2014). *Robotic Cars and Their New Crime Paradigms*. https://www.linkedin.com/pulse/20140903073835-260074537-robotic-cars-and-their-new-crime-paradigms

Molla, T., & Electronik, T. M. (2018). *Self-Driving car*. *December*. https://doi.org/10.13140/RG.2.2.36042.82885

Morimoto, S., Wang, F., Zhang, R., & Zhu, J. (2018). Cybersecurity in Autonomous Vehicles. *Researchgate.Net*, *May 2017*. https://doi.org/10.13140/RG.2.2.31503.23207

Muratoğlu, O. (2020). Akıllı Araçlar İçin Bulanık Mantık Temelli Siber Güvenlik Risk Modeli. *Journal of Visual Languages & Computing*, *11*(3), 55. https://www.m-culture.go.th/mculture_th/download/king9/Glossary_about_HM _King_Bhumibol_Adulyadej's_Funeral.pdf

Naranjo, J. E., Bouraoui, L., García, R., Parent, M., & Sotelo, M. Á. (2009). Interoperable control architecture for cybercars and dual-mode cars. *IEEE Transactions on Intelligent Transportation Systems*, *10*(1), 146–154. https://doi.org/10.1109/TITS.2008.2011716

OWASP. (2015). *Man in the Middle Attack*. https://www.owasp.org/index.php/Man-in-the-middle_attack

Pancorbo Crespo, J., Guerrero Gomez, L., & Gonzalo Arias, J. (2019). Autonomous Shipping and Cybersecurity. *Ciencia y Tecnología de Buques*, *13*(25), 19–26. https://doi.org/10.25043/19098642.185

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*(11), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968

Patterson, N., Hobbs, M., & Zhu, T. (2017). A cyber-threat analytic model for autonomous detection of virtual property theft. *Information and Computer Security*, *25*(4), 358–381. https://doi.org/10.1108/ICS-11-2016-0087

Polat, Ç. (2016). Penetration tests and security solutions for corporate networks. In *Master of Science Thesis, Dokuz Eylül University {\.I}zmir*.

Puiboube, D. (2000). *Un siècle d'automobile en France*.

Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., & Puschner, P. (2016). *Using SAE J3061 for Automotive Security Requirement Engineering*. *1*(November 2018), 286–297. https://doi.org/10.1007/978-3-319-45480-1

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, *124*(November 2018), 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Şimşek, H. F. (2020). *ARP Spoofing*. https://includekarabuk.com/kategoriler/cesitliSizmaTeknikleri/Arp-Spoofing-Saldirisi-Nedir-ve-Nasil-Yapilir.php

Sinai, M. Ben, Partush, N., Yadid, S., & Yahav, E. (2014). *Exploiting Social Navigation*. http://arxiv.org/abs/1410.0151

Singh, A. (2013). Metasploit Penetration Testing Cookbook. In *Network Security* (Vol. 2013, Issue 11). https://doi.org/10.1016/s1353-4858(13)70125-9

Sweshsec. (2020). *vulnerability explaitation*. https://sweshsec.wordpress.com/2015/07/31/vsftpd-vulnerability-exploitation-with-manual-approach/

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, *39*(1), 103–128. https://doi.org/10.1080/01441647.2018.1494640

Taymans, A., Taymans, A., & De, G. (2020). *Gestion de trafic par les assistances coopératives To cite this version : HAL Id : tel-02903323 Docteur De l ' Universitê De Bordeaux École doctorale des Sciences Physiques et de l ' Ingénieur Spécialité : Automatique , Productique , Signal et Image Alexa*.

Technical, F. O. F., & Str, U. (2019). *Implementation Of The Web Based Platforms For Collecting And Footprinting IP Information Of Hosts In The Computer Network And Systems Petar Kr. Boyanov*. *16*, 42–50.

THT. (2020). *Nmap Kullanımı*. https://www.turkhackteam.org/network/1744147-detayli-nmap-kullanimi.html

TÜİK. (2018). *Trafik Kaza ve Denetim İstatistikleri*. https://www.pa.edu.tr/Upload/editor/files/Trafik_Kaza_ve_Den etim_İstatistikleri.pdf

Tunalı, M. M. (2019). *Otonom Araçların Tarihçesi*. https://www.tekyolbilim.com/otonom-araclarin-tarihcesi/

Ünver, M. (n.d.). *Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri*.

Ünver vd. (2009). Siber Güvenliğin Sağlanması: Türkiye'de ki Mevcut Durum ve Alanması Gereken Tedbirler. In *Bilgi Teknolojileri ve İletişim Kurumu*.

Ustam, B. (2020). *Otonom araçlar nedir*. https://www.bilgiustam.com/surucusuz-otonom-araclar/

uzmanim.com. (2018). *Malware Nedir?* https://uzmanim.net/soru/emsisoft-anti-malware-nedir-nasil-kullanilir/3908

Uzmanim.com. (2018). *malware ve türleri nelerdir?* https://uzmanim.net/soru/malware-nedir-turleri-nelerdir/25343

Vers, J. B., Hydractive, C., Doctorale, É., Sciences, D. E. S., & Et, P. (2019). *Vers une version alternative à la suspension CRONE Hydractive To cite this version : HAL Id : tel-02119390 Jean-Louis BOUVIN Spécialité : Automatique Vers une version alternative à la suspension CRONE Hydractive*.

Vinnem, J. E., & Utne, I. B. (2018). Risk from cyberattacks on autonomous ships. *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*, 1485–1492. https://doi.org/10.1201/9781351174664-188

Yaşar, H., & Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *3*, 488–507.

Yüksek, H. Y. (2014). Kurumsal Siber Güvenliğe Yönelik Tehditler Ve Mücadele Yöntemleri: Eylem Planı Örneği [Gazi Üniversite]. In *Journal of Visual Languages & Computing* (Vol. 11, Issue 3). https://www.m-culture.go.th/mculture_th/download/king9/Glossary_about_HM _King_Bhumibol_Adulyadej's_Funeral.pdf