SİBER TEHDİT DURUM RAPORU

TEMMUZ-EYLÜL 2022

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

2022 yılının üçüncü çeyreğinde hazırladığımız raporda her zaman olduğu gibi birçok güncel ve ilginç konuyla karşınızdayız.

Bunlar arasında teknolojik gelişmeler, siber saldırı metotları, güncel siber güvenlik haberleri ve honeypot verileri gibi başlıklar bulunuyor. Bulut depolama servisi olan Mega'da bulunan anahtar hiyerarşisiyle başlayan bölümü popüler bir oltalama saldırısı olan smishing saldırısı takip ediyor.

Dokunmatik ekranlı cihazların sayısı hayatımızda gün geçtikçe artıyor. Bunun neticesinde ekranlarda güvenlik açıkları da oluşuyor. Bu sebeple sıradaki yazımızda dokunmatik ekranlı cihazların güvenliğinden ve saldırı türlerinden bahsediyoruz.

Bunun devamında, özellikle pandemi dolayısıyla daha da popüler hâle gelen uzaktan çalışma bağlamında iş arayışındaki çalışanlara yönelik kimlik avı saldırı yöntemlerini ve bu kimlik avcılığına karşı alınabilecek önlemleri inceliyoruz.

Ardından, artırılmış gerçeklik, endüstriyel IoT cihazları iletişimi, otonom sürüşlerde araçlar arası iletişim gibi düşük gecikme süresi ve yüksek verim sağlayan "mmWave (Milimetre Dalga)" iletişim teknolojisi aracılığıyla telefon konuşmalarının dinlenmesi konusunu ele alıyoruz.

Daha sonra, anahtarsız araba kilitlerinin işleyiş yapısı ve bu yapıya yönelik saldırılar arasında olan "RollBack" ile "RollJam" saldırılarının teknik analizini ele alıyoruz.

Raporumuzda daha sonra honeypot sensörlerimizden topladığımız veriler ışığında saldırılan yerler, denenen portlar veya parolalar gibi bilgileri sunuyoruz.

Son olarak bu çeyrekte dönem konusu olarak seçtiğimiz platform siber güvenliği hakkında genel bilgiler ile birlikte tehditleri ve tehdit aktörlerini inceleyerek raporumuzu tamamlıyoruz.

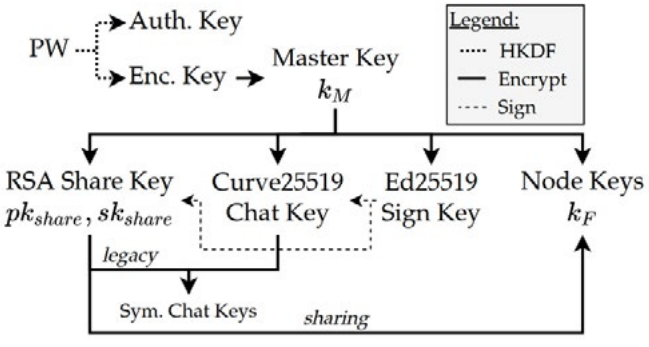
TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. MEGA Anahtar Hiyerarşisi Zafiyeti

MEGA, 250 milyondan fazla kullanıcısı olan bir dosya paylaşım, bulut ve mesajlaşma platformu sağlayıcısıdır. Tüm servislerinde uçtan uça şifreleme bulunmaktadır. ETH Zürich'ten araştırmacılar, MEGA'nın kriptografik mimarisinde beş zafiyet saptamıştır. Bu zafiyetlerin dördü pratik olarak uygulanabilmektedir[1].

1.1. Tehdit Modeli

Bu saldırının modelinde, servis sağlayıcısının kullanıcı için bir tehdit aktörü olduğu varsayılmaktadır. Sunucunun, kullanıcıyla olan etkileşiminde MEGA ya da kontrole sahip üçüncü bir parti tarafından art niyetli faaliyetlerde bulunması beklenmektedir. İstemci programının açık kaynak olmasından dolayı, bir güncellemeyle kullanıcı tarafında bir arka kapı oluşturulması ele alınmamıştır.



Şekil 1: MEGA kullanıcı anahtar hiyerarşisi.

1.2. MEGA Anahtar Hiyerarşisi

MEGA, birden fazla cihazda sadece parola aracılığıyla uçtan uça şifreleme sağlamak için her kullanıcıya anahtar hiyerarşi sahiplendirir. Kullanıcının şifresi, parola bazlı bir özetleme algoritma (PBKDF2-HMAC-SHA512) aracılığıyla genişletilir. Genişletilmiş anahtar, doğrulama ve şifreleme amaçlı iki parçada kullanılır.

Doğrulama parçası, yeni bir cihazda giriş yapan kullanıcının MEGA sunucularında kimliğini doğrulamasında kullanılır. Şifreleme parçası, hesabın kaydına oluşturulan, rasgele üretilmiş kullanıcı kök anahtarını şifreler.

Kök anahtar, MEGA servislerinde kullanılan diğer anahtarları şifreler. Bu anahtarlar, kullanım ve algoritmasına göre dört kategoriye ayrılır:

- Dosya paylaşımı için RSA anahtarı
- Mesajlaşma uygulaması için Curve25519 anahtarı
- Paylaşım ve mesajlaşma açık anahtarlarının imzalanması için Ed25519 anahtarı
- Dosya ve klasör başına oluşturulan AES-CCM anahtarı

1.3. Tasarım Hatası 1 – Mesaj Doğrulama Kodu Eksikliği

MEGA, anahtarların şifrelenmesi için, MAC (Mesaj Doğrulama Kodu) olmadan AES-ECB kullanır. Mesajın bütünlüğünün kontrol edilmemesi durumunda, şifrelenmiş mesajlar saldırgan tarafından deşifre edilmeden manipüle edilerek değiştirilebilir (Malleability).

Araştırmacılar, şifrelenmiş dosya paylaşım anahtarında padding öncesi en son bloğu manipüle ederek RSA-CRT'in davranışı gözlemlemiştir. Paylaşılan dosyaların modifiye edilmiş anahtarla başarılı olup olmaması ölçülerek anahtar uzayı, deneme başına yarıya düşmektedir. Arama optimizasyonları sonrasında, araştırmacılar, hedef kullanıcının 512 adet giriş yapması sonrasında sunucu tarafında şifrelenmiş dosya paylaşım anahtarını elde etmiştir.

1.4. Tasarım Hatası 2 – Anahtar Hijyeni İhlali

Kriptografik sistemlerin tasarım sürecinde en önemli prensiplerinden biri anahtar hijyenidir. Kullanım alanlarına göre farklı anahtarların kullanımı, çeşitli sistemlerin etkileşiminden oluşan zafiyetlerin ve sürüm indirgeme saldırılarının önüne geçmektedir.

MEGA'nın mesajlaşma uygulaması, bir kullanıcının Curve25519 anahtarı olmaması durumunda dosya paylaşım anahtarını kullanır. RSA anahtarının hijyeni sağlanmadığında iki zafiyet ortaya çıkmaktadır:

- Kullanıcılar arası anahtar dağıtımı MEGA sunucuların üzerinden olması, sunucuya konuşmaların hangi anahtar üzerinden yapılacağını belirleme hakkını kazandırır. Hedef kullanıcının dosya paylaşım anahtarını elde eden sunucu, Curve25519 anahtarını diğer kullanıcılardan gizleyerek pasif olarak hedefle olan mesajlaşmaları dinler.
- Gelen mesajın deşifre edilip edilmediği RSA ile mesajlaşmada ölçülebildiği için araştırmada Bleichenbacher Padding Oracle saldırısının[2] uygulanabildiğini keşfetmiştir. Padding Oracle saldırısı sonucunda RSA anahtarının elde edilebildiği yeni bir saldırı vektörü oluşmuştur.

1.5. Kısa ve Uzun Dönemli Müdahaleler

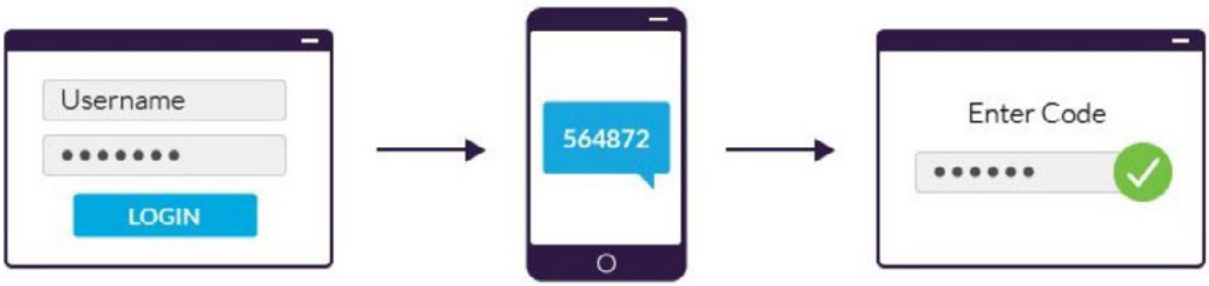
Malleabilility için kısa dönemde AES-ECB'nin yanında HMAC kullanılması planlanmıştır. Araştırmacılar uzun dönem için farklı alanlarda kullanılan farklı simetrik şifreleme algoritmalarının AES-GCM ile değiştirilmesini önermiştir. MEGA sistemlerinde sadece AEAD (ilişkili verilerle kimliği doğrulanmış şifreleme) kullanımıyla şifrelenmiş verilerde değiştirilebilirliğin gelecek projelerde tekrardan yaşanmaması hedeflenmiştir.

Anahtar hijyeninin sağlanması için kısa dönemde mesajlaşma için farklı RSA anahtarların kullanılması planlanmıştır. Uzun dönemli çözüm olarak, RSA şifrelemenin mesajlaşmada yedek çözüm statüsünden kaldırılması tavsiye edilmiştir. Parola bazlı özetleme algoritmayla açılan anahtar ile doğrulama aşamasından çıkartılarak OPAQUE kullanılması önerilmiştir[3].

2. Smishing Saldırıları ile Verilerimiz Tehlikede

1990'lı yıllarda geliştirilen SMS (Short Message Service), cep telefonları aracılığıyla karşılıklı mesajlaşma yöntemidir. Günlük hayatta çok kullandığımız mesajlaşma yöntemlerinden biri değildir. Çoğunlukla alışveriş siteleri, web siteleri, banka hesapları gibi kişisel bilgilerimizin kayıtlı bulunduğu yerlerde onaylanan işlemlerden sonra doğrulama kodu SMS olarak gönderilmektedir. Parola ile giriş yaptığımız güvenlik sistemleri tek faktörlü koruma olarak bilinmektedir. Tek faktörlü doğrulama sisteminde parola ne kadar tahmin edilemez veya güçlü olursa olsun, saldırganlar tarafından geliştirilen virüs, worm, trojan gibi yazılımlarla bilgilerimiz elde edilebilmektedir. Sosyal medya platformları ve bankalar parolanın yeterli koruma yöntemi olmadığını ve bu yüzden iki faktörlü kimlik doğrulama yöntemi kullanmak gerektiğini düşünmektedir. İki faktörlü kimlik doğrulamayla hesabınıza bir güvenlik katmanı sağlanmaktadır.

Yakın zamanda yapılan araştırmalarda iki faktörlü kimlik doğrulama kodu göndermenin güvenli olmadığına dair sonuçlar elde edilmiştir. İki faktörlü kimlik doğrulamaya çift parola da diyebiliriz. Kullanıcı kimliğini onaylamak için kullanılan güvenlik önlemi çeşidi sayılmaktadır. Banka, sosyal medya hesabı gibi hesaplarda parola dışında cep telefonuna sistem tarafından bir parola gönderilir. Söz konusu parola tek kullanımlıktır. Saldırganlar bu tek kullanımlık mesajda verilen parolayla verilerinize erişim sağlamaya çalışmaktadır. Bu erişimi genellikle phishing'in bir çeşidi olan smishing ile gerçekleştirdikleri görülmektedir. Smishing, SMS yoluyla yapılan bir saldırı çeşidir. Saldırganlar, smishing yöntemi kullanarak



Şekil 2: İki faktörlü doğrulama.

kurbana ilişkin ödenmemiş bir fatura veya bloke edilmiş bir hesap mevcutmuş gibi mesajlar göndererek karşı tarafın kişisel bilgilerine rahatlıkla ulaşabilmektedir. Saldırganların smishing yöntemini seçmesi farklı bir bakış açısı oluşturmaktadır. Çünkü e-posta saldırıları son zamanlarda arttığı için çoğumuz bilinçlenmekteyiz. Gelen postaların phishing saldırısı olup olmadığını anlayabilmekteyiz. E-posta saldırısına karşı nasıl önlem alacağımızı veya ne gibi durumlarla az çok karşılaşacağımızı tahmin edebilmekteyiz.

Smishing saldırısının ayrıca tercih edilmesinin sebeplerinden biri de günümüzde e-posta hizmetlerinde akıllı spam filtresi bulunmasıdır. Saldırganın akıllı spam filtresini aşması daha zordur. SMS'lerin akıllı spam filtresi ise yetersiz ve güvensizdir. Bu koruma yetersizliğinden dolayı da saldırganlar smishing saldırılarına yönelmeye başlamaktadır. Saldırgan amacına ulaşabilmek için gerçekçi bir mesajla link göndermektedir. Burada amaç kurbanın linke tıklamasıdır, bunu yaparsa bilgilerine ulaşılması mümkün hâle gelir. SMS saldırılarıyla ilgili araştırma yapan İsveçli bir araştırma ekibi saldırılara karşı kullanılabilecek bazı yöntemler üzerine çalışmaktadır[4]. Araştırmacılar SMS iletişimine güvenilmemesi gerektiğini düşünmektedir. Genel sonuç SMS tabanlı kimlik doğrulamanın çok tercih edilmemesi yönündedir.

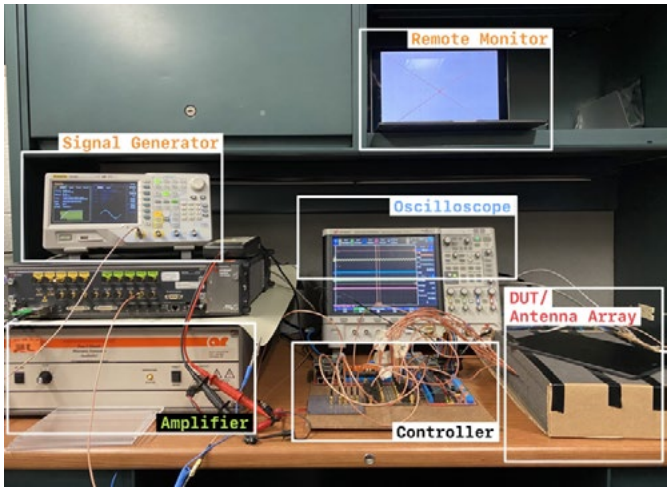
Şekil 3: Smishing mesajı.

3. "Görünmez Dokunuş" ile Dokunmatik Ekranların Ele Geçirilmesi

Dokunmatik ekranlı cihazların sayısı hayatımızda gün geçtikçe artıyor. Bununla birlikte bu cihazlardaki güvenlik açıkları, dolayısıyla güvenlik uzmanlarının bu alandaki çalışmaları da artıyor. Araştırmacılar[5] Black Hat 2022 konferansında dokunmatik ekranlı cihazların kasıtlı elektromanyetik müdahalelere açık olduğunu yayınlamışlardır. Bu cihazların belli bir alan içinde ele geçirebildiğini gözlemlemiştir.

3.1. Saldırı için Sistemin Kurulması

Saldırıda iki anten dizisi kullanılır. Biri hedeflenen dokunmatik cihazın yerini tam olarak belirlemek için kullanılır, diğeri hedef cihazın ekranındaki sensörlere voltaj sinyalleri göndermek için elektromanyetik bir alan oluşturmak üzere kullanılır. Hedef cihazın işlemcisi bu işlemler sonucu oluşan sinyalleri bir dokunma türü olarak algılar.



Şekil 4: Dokunma türü oluşturmak için kullanılan sistem.

Araştırmacılar, yapılan çalışmada iPad, OnePlus, Google Pixel, Nexus ve Surface dahil olmak üzere birden fazla cihazda herhangi bir yöne dokunma, uzun basma ve kaydırma işlemlerini simüle edebilmiştir[6]. Araştırmacılardan, Black Hat konferansının baş sunucusu Haoqi Shan, denemiş oldukları cihazlar için şöyle diyor: "Parmağınız ekrana tıklıyormuş gibi algılıyor. iPad ve Surface üzerinde çok yönlü bir kaydırma bile oluşturabiliriz ve bunu bir ekran kilidi açmak için kullanabiliriz."

3.2. Araştırmacıların Gerçekleştirdiği Saldırılar

- **Android cihazlara kötü amaçlı uygulamalar yükleme:**
  Saldırgan kötü amaçlı uygulamayı yüklemek için hedef cihaza uygulamanın indirme linkini yollamaktadır. Yollanan linke de anten dizisi yardımıyla saldırganlar (Oneplus 7 Pro cihazında denenmiştir) beş tane ardışık ekrana dokunuşlar gerçekleştirmiş ve kötü amaçlı uygulama hedef cihaza yüklenmiştir.
- **Mesaj Gönderme:**
  Kısa dokunuşlarla mesajlar gönderilebilir. Özellikle bankalardan gelen onay mesajları için kullanılabilen bir tekniktir. Araştırmacılar bu senaryoyu test ederken bankadan gelen mesaja onay vermek için "Y, E, S" mesajını yazmışlar ve bu testi 10 saniyenin altında gerçekleştirmişlerdir.
- **Para Gönderme:**
  iOS cihazlarda PayPal uygulamasının üzerine uzun süreli basılı tutarak para gönderilebildiğini tespit

etmişlerdir. Hedef cihazdan parayı beş saniyenin altında göndermişlerdir.

- **Ekran Kilidini Açma:**

  Anten dizisi sayesinde gerçekleştirilen kaydırmalı işlemlerde, birçok dokunmatik cihazdaki ekran kilidinin açıldığını tespit etmişlerdir. Hedef cihazların şifrelerini bulup yaklaşık beş saniyede hedef cihazın ana ekranına giriş yapmışlardır.

3.3. Alınabilecek Önlemler

- **Kuvvet Algılama:**

  Elektromanyetik dalgalarla uzaktan cihaz kontrolünü engellemek için kuvvet algılayan sensörler kullanılarak gerçekleştirilebilir. Kimi cihazlarda bu teknoloji hâlihazırda kullanılmaktadır. Kullanıcı tarafından uygulanan kuvvet gerçek bir parmağın dokunuşu gibi algılanabilir ve uzaktan kontrol saldırısının farkına varılabilir.

- **Cihazlara Aksesuar Takma:**

  Hedef cihazlara metal bir kılıf veya aksesuar takılarak, saldırılar veya elektromanyetik dalgayla gelen herhangi bir işlem kesilir. Araştırmacılar 0,28 mm olan bir ürünün bile saldırıyı başarılı bir şekilde engellediğini gözlemlemiştir.

4. İş Ararken Bilgilerinizi Çaldırmayın

Günümüzde giderek yaygınlaşan uzaktan çalışma, saldırganlar için de cazip bir alan oluşturuyor. Çoğunlukla bir siber saldırı çeşidi olan phishing'in kullanıldığı bu saldırıları araştıran "Black Hat" konferansındaki siber güvenlik uzmanları saldırıların nasıl yapıldığını, nereden geldiğini, nasıl başarılı olduğunu açıkladılar ve kimlik avı saldırıları konusunda uyarıda bulundular.

PwC'nin küresel tehdit istihbarat ekibi, İran ve Kuzey Kore'deki devlet destekli tehdit aktörlerini phishing olarak belirlemiştir. PwC'nin önde gelen siber tehdit istihbarat analisti Sveva Vittoria Scenarelli ve siber tehdit istihbarat direktörü Allion Wikoff'a göre, kötü niyetli gruplar büyük şirketlerdeki çalışanların bilgilerini ele geçirmek için genellikle e-posta, sosyal medya ve mesajlaşma uygulamalarını kullanmaktadır [7].

Bu phishing saldırılarında iş arayışındaki insanlara iş teklifi sunulmaktadır. Black hat hacker'lar bu amaçla genellikle Indeed.com ve LinkedIn.com gibi popüler iş sitelerini kullanarak uzaktan çalışan kişilere iş fırsatları sunan mesajlar atmaktadır. Aslında tüm sosyal medya platformları dolandırıcılık için elverişli bir zemin oluşturmaktadır. Ama LinkedIn'i özel kılan şeylerden biri insanlara güven arz etmesidir. Saldırganlar genellikle iş teklifi sundukları mesajlarında sahte web sitelerini kullanmaktadır. Kurbanların bu bağlantılara tıklamaları için saldırganlar sosyal mühendislik yöntemlerini kullanırlar. Sahte iş teklifleri sizin o anki ihtiyaç veya ilgi alanınıza göre ayarlanmış olabilir ve siz de hazırlıksız yakalanarak cevap verebilir, bağlantıya tıklayabilir ya da Google formu aracılığıyla kişisel bilgilerinizi doğrulayabilirsiniz. Bazen de LinkedIn'deki dolandırıcılık örneklerinde görüldüğü gibi, "Bu hafta 25 aramada çıktınız" gibi sahte bildirimlerle ilginizi çekerek hesabınıza giriş yapmanızı isteyebilirler [8], [9].

Peki hacker grupları ne istiyor? Bazı gruplar maddi amaçla saldırırken, bazıları ticari sırları elde etmek ister, bazıları da kimlik hırsızlığı yapmaya çalışır. Birkaç örnek verirsek; Kuzey Koreli tehdit aktörü Black Alicanto, kripto alanındaki büyük oyuncuları hedef almasıyla bilinmektedir. İran merkezli bir tehdit aktörü olan Charming Kitten, e-postalarda kimlik avı bağlantılarıyla gazetecileri hedef almaktadır. "Yellow Dev 13" diye bilinen tehdit aktörü, sosyal medya sitesi çalışanı kimliğine bürünerek ayrıntılı profiller yayınlamakta ve işveren gibi göründüğü bu sahte profillerle iletişime geçtiği insanları kandırmaktadır [7].

Şekil 5: Uzaktan çalışma.

Şekil 6: Phishing saldırısı.

4.1. Kimlik Avcılığından Korunmak için Nelere Dikkat Etmeliyiz?

Kimlik avı saldırılarında en yaygın olarak kullanılan yol e-posta ve mesajlaşmadır. Bu yollarla hedeflenen kişiye kötü amaçlı bağlantılar ve ekler gönderilir. E-posta ile gelen bir web adresinin sahte olup olmadığını anlamak için imlecinizi e-postadaki bağlantının üzerine getirmeniz gerekir. Tanımadığınız kişilerden gelen bağlantılara tıklamamak gerekir.

Örneğin LinkedIn'den size önemli bir iş teklifi geldi. Bu durumda ne yapmanız ve hangi önemli noktalara dikkat etmeniz gerektiği aşağıda yer almaktadır.

- LinkedIn profilinde dil bilgisi ve yazım hataları olup olmadığına dikkat edilmelidir. Garip konuşma dilleri ve yazım hatalarıyla dolu bir iş ilanı dikkate alınmamalıdır.
- Sözde işe alım görevlisinin mesleki geçmişi incelenmelidir.
- Görüşmecinin konuşma tarzı dikkate alınmalıdır. Gerçek bir alım müdürü muhtemelen size sadece "Hey" yazan bir doğrudan mesaj göndermeyecektir.
- Kısa sürede yanıt verme baskısı varsa veya mesajlaştığınız kişi birkaç dakika içinde size gönderdikleri bağlantıya tıklamanız gerektiğini, yoksa fırsatı kaçıracağınızı söylüyorsa yanıt verilmemelidir.

Yukarıdaki maddelerden herhangi biriyle karşılaşılırsa, söz konusu profil engellenmelidir[10].

5. mmSpy: mmWave Radarlarıyla Telefon Konuşmalarının Dinlenmesi

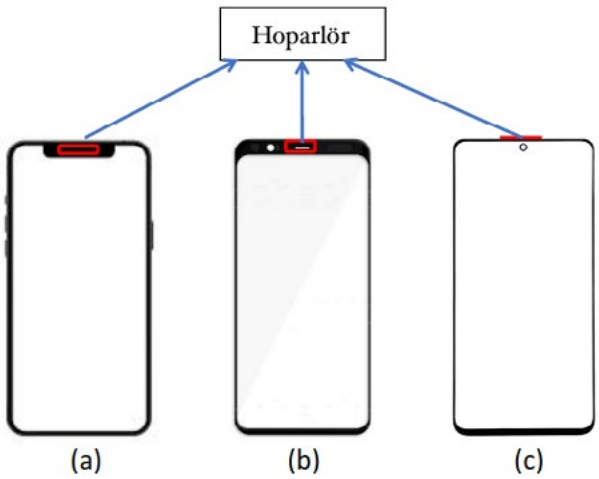
Milimetre dalga (mmWave) iletişim teknolojisi, artırılmış gerçeklik[11], endüstriyel IoT'de makine iletişimi[12], [13], otonom sürüşlerde araçtan araca (V2V) veya araçtan altyapıya (V2L) gibi düşük gecikme süresi ve yüksek verim gerektiren yeni nesil ağ uygulamalarında giderek daha fazla benimseniyor. Ağ oluşturmaya ek olarak mmWave teknolojisi, malzeme algılama, endüstrilerde titreşim algılama, robotik, hassas tarım alanlarında ve bir dizi uzaktan algılama uygulamasında da giderek daha popüler hâle geliyor. 5G ve diğer ağ teknolojilerine dahil edilmesiyle mmWave teknolojisinin IoT uygulamalarındaki kullanımı da hızlı bir şekilde yaygınlaşmaktadır. mmWave'nin bu kullanımlarını inceleyen araştırmacılar, bir saldırganın mevcut teknolojiyi kullanarak pasif olarak telefon görüşmelerini nasıl dinleyebileceğini gösteren bir çalışma ortaya koyuyorlar.

Bu çalışmada belirli mesafelerden telefon hattının diğer ucunda olan kişinin sesini dinlemek için piyasada satılan mmWave radarlarını kullanan mmSpy adı verilen bir yöntem geliştirilmiştir. mmSpy telefonun gövdesinden yansıyan mmWave sinyallerinin fazlarındaki değişiklikleri algılar. Geliştirilen yöntemde kulaklıktan çıkan ses çevredeki insanlar veya mikrofonlar tarafından algılanamayacak kadar alçak seviyede dahi olsa başarılı şekilde çalışmaktadır. Ek olarak ses direkt titreşim kaynağından alındığından ortamdaki kirlilikten etkilenmemektedir. Bu sayede saldırgan konferans, parti gibi sosyal ortamlarda dahi belirli mesafelerden başarılı saldırılar gerçekleştirebilmektedir.

5.1. Mikrofon Titreşimleri

Şekil 7'de iPhone-12, Google Pixel 4a ve Samsung Galaxy S4 gibi popüler telefon modellerindeki hoparlörlerin yerleri gösterilmektedir. Normal kullanımda hoparlörden yayılan titreşim, sesin dışarıya verilmesine kıyasla daha küçüktür. Bu nedenle, kullanıcıların sesi net bir şekilde duyabilmeleri için kulaklarını doğrudan telefona temas edecek şekilde yerleştirmeleri gerekir. Doğrudan fiziksel temas nedeniyle ses dalgaları doğrudan bir katı yüzeyden başka bir katı yüzeye yayılır, böylece telefonla fiziksel temasın olmadığı duruma kıyasla insan kulağında yüksek kaliteli bir ses alımı sağlar. Sonuç olarak hoparlör titreşimlerinin hava üzerinden yayılması da sesin dışa verilmesine kıyasla çok daha zayıftır.

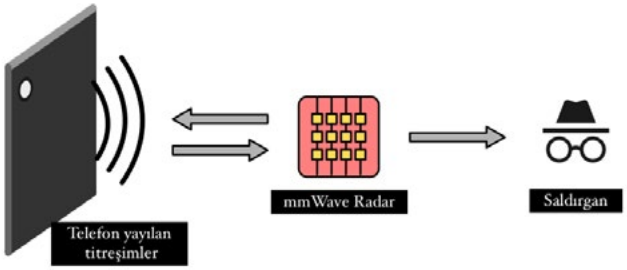
Ancak mmSpy hoparlör tarafından üretilen titreşimleri doğrudan izlemek için mmWave sinyallerinin yansımalarını kullanır. Hoparlör titreşimleri de telefonun gövdesinde titreşimlere neden olur. mmSpy telefonun arka yüzeyinden yayılan titreşimleri algılar, bu sızıntı zayıf olsa bile hoparlör titreşimlerinin gizlice dinlenmesini sağlar.



Şekil 7: Popüler telefonlardaki hoparlör yerleri.

Şekil 8'de mmSpy tehdit modeli gösterilmektedir. mmWave radarına sahip bir saldırgan yakındaki kurban tarafından yapılan telefon görüşmesinin sesli içeriğini gözetlemeye çalışır. Bu amaçla saldırgan kurbanın telefonuna mmWave sinyallerini gönderir ve yansımaları yakalar. Yansımanın fazları analiz edilerek telefon hoparlörünün titreşimi tespit edilebilir. Bu saldırının gerçekleştirilmesi için gerçek konuşmalardan alınan eğitim

verilerine sahip olunmasına gerek yoktur. Saldırgan ML konuşma tanıma modellerini geliştirmek için bu tür eğitim verilerini kendi telefonundan üretebilir. Araştırmacılar mmSpy'ın ML modellerinin ortamdan kaynaklanan gürültülü titreşimlerden etkilenmeyecek şekilde tasarlandığına dikkat çekmektedir.



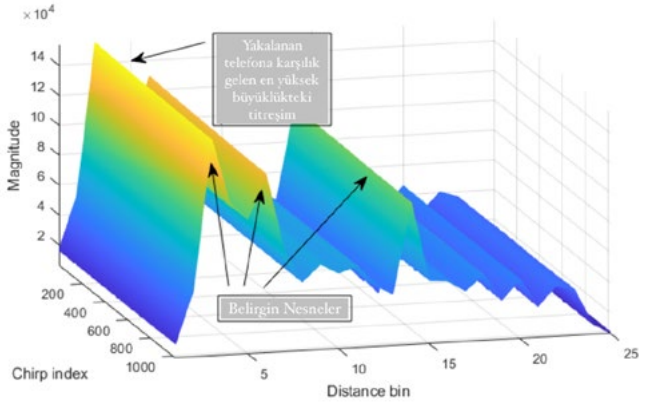
Şekil 8: mmSpy saldırı modeli.

Gerçekleştirilen saldırı sırasında şüphesiz telefondaki yansımaların yanı sıra ortamdaki diğer nesnelerden de etrafa çok yönlü titreşimler yayılacaktır. Bu noktada araştırmacılar telefon yansımalarını izole etmekte iki ana zorlukla karşılaşmaktadır:

1. Telefondan yansıması beklenmeyen birkaç gürültü tepe noktasının da algılanması,
2. Gürültü tepe noktalarına ek olarak, ortamdaki statik yansıtıcılara karşılık gelen tepe noktalarının da yakalanması.

Bu bahsedilen kaynaklardan ilgili sinyalin daha iyi yalıtılması için yapılan çalışmada gözlem boyunca tutarlı olan zirveler dikkate alınmaktadır. Gürültülü tepe noktaları belirli bir mesafede tutarlı bir şekilde görünmediği için ortadan kaldırılır. Şekil 9'da belirli bir ortamda mmSpy ile yapılan titreşim yansımalarının dinlenmesi gösterilmektedir. Burada telefondan kaynaklanan yansımaların yanı sıra ortamdaki diğer nesnelerden kaynaklanan yansımalar da görülebilmektedir. Fakat telefon yansımalarındaki faz bir salınım gösterirken diğer nesnelerden gelen yansımaların fazlarında böyle bir salınım yoktur. Bu özellikten yararlanan mmSpy, ilk olarak ses titreşimlerinden kaynaklanan yansımaları ve duvarlar gibi statik reflektörlerden gelen yansımaları sınıflandırmak için Evreşimsel Sinir Ağları tabanlı yüzde 99,4 doğruluk oranına sahip bir model tanımlamaktadır. Böylece duvar, mobilya gibi statik reflektörleri eleyebilmektedir. Ayrıca arka plan gürültüsünü kaldırmak için ses işlemede sıklıkla kullanılan spektral çıkarma tekniklerinden faydalanılmıştır[13], [14].

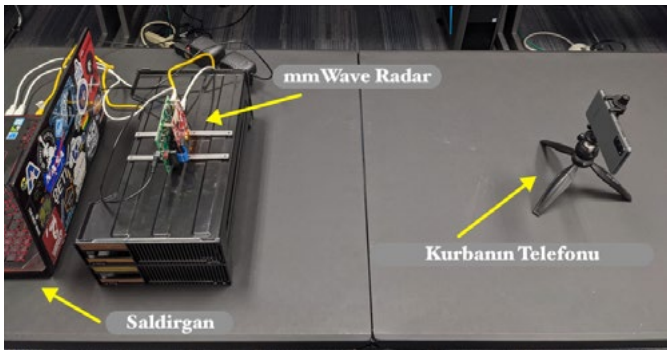
Ses işleme algoritmaları lehçe, cinsiyet, konuşma şekli gibi farklılıklardan etkilenmeyecek şekilde geliştirilmelidir.



Şekil 9: mmWave ile yapılan dinlemeler.

Ancak bu derece kararlı algoritmalar geliştirmek yıllar boyunca biriken oldukça büyük veri kümelerine ihtiyaç duyar. Görüntü ve ses işleme alanları için oldukça büyük veri kümeleri mevcut olmakla birlikte, mmSpy kullanılan mWave radarları için bunun söz konusu olmaması kararlı algoritmalar geliştirilmesini zorlaştırmaktadır. Bu noktada araştırmacılar AudioMNIST[14] ve Speech Commands[15] veri kümelerini temel alarak kendi sentetik veri kümelerini oluşturmuşlardır.

Deneysel kurulum Şekil 10'da gösterilmektedir. mmSpy'ın sisteminin ön ucunda sırasıyla 77 GHz ve 60 GHz spektrumunda çalışan Texas Instruments marka ve 1798.92 GHz bandında çalışan AWR1843BOOST ve IWR6843ISK mmWave radarları kullanılmaktadır. Yapılan deneylerde kurbanların kullandığı telefon modelleri Samsung Galaxy S20 (S20) ve Google Pixel 4a (Pixel)'dir. Yakalanan yansımalar telefonun arka yüzünden yayılan yansımalardır. Yapılan ölçümlerde telefon ve frekans fark etmeksizin yaklaşık 2 m'den sonra (6 ft) sonra yakalanan yansımaların ortam gürültüsüyle eş değerde olduğu fark edilmiştir ve mevcut kurulumla bu mesafenin üzerinde etkili bir saldırı mümkün olmamaktadır. Tablo 1'de mesafe arttıkça gerçekleşen başarım oranlarının telefonlara ve frekanslara göre nasıl olduğu gösterilmektedir.



Şekil 10: mmSpy saldırı modelinin bir örneği.

Ayarlar	Mesafe					
	1 ft	2 ft	3 ft	4 ft	5 ft	6 ft
S20 (77 GHz)	83.33	73.10	65.09	60.66	50.14	47.99
S20 (60 GHz)	78.35	70.05	62.37	60.11	50.91	49.92
Pixel (77 GHz)	80.11	70.94	66.30	58.33	49.09	46.60
S20 (Sp, 77 GHz)	69.37	63.81	60.74	56.70	48.62	44.56

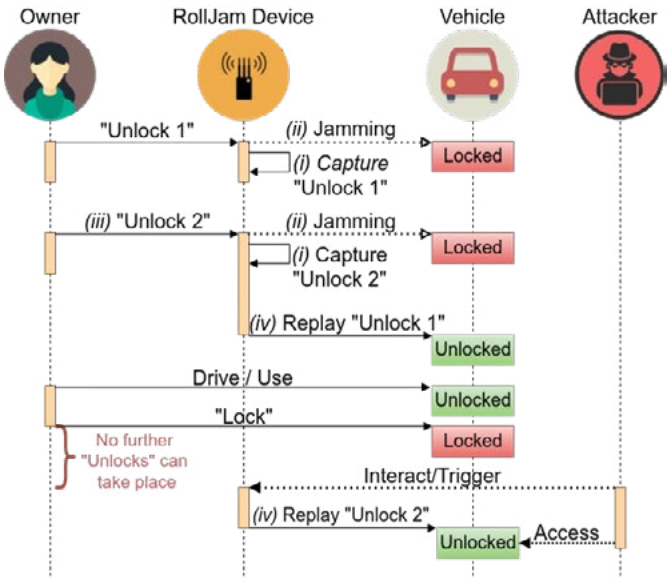
Tablo 1: Farklı mesafe ve ayarlara göre doğruluk oranları.

Sonuç olarak mmWave radar kullanan mmSpy tekniği ile telefon konuşmalarını kalabalık ortamlarda dahi belirli mesafelerden yüksek hassasiyetle ve efektif bir şekilde dinlemenin mümkün olduğu ispatlanmaktadır. Araştırmacılar ayrıca mmWave radarlarda ve 5G teknolojilerindeki olası ilerlemelerle mmSpy saldırı tekniğinin daha güçlü uygulanabileceğini öngörmektedir.

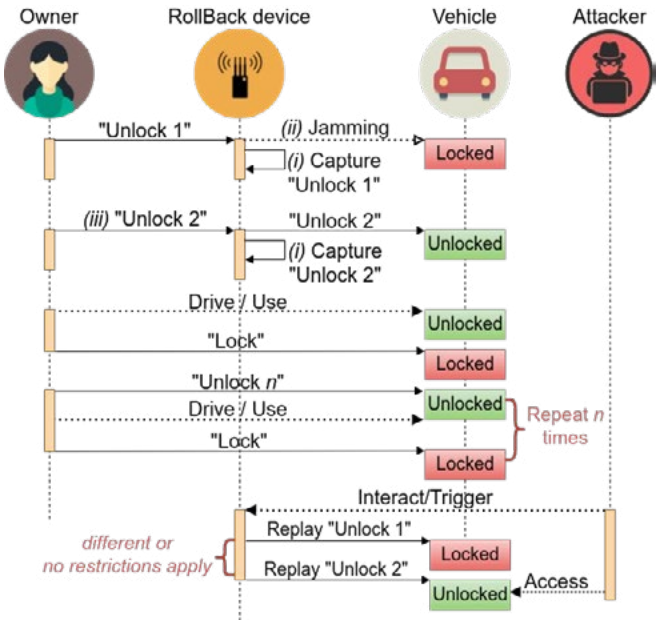
6. Anahtarsız Araba Kilidi Nasıl Açılır?

Araba kilitleri, kumanda aletlerinin açma/kapama sinyalleri araba spesifik olduğu için güvenlidir. Aynı model iki ayrı arabanın anahtarları birbirlerini açamaz, her anahtar ancak ait olduğu arabayı açar/kilitler. Ama bir aracın kumandasının tek bir sinyal yayması da güvenli değildir, saldırgan bu sinyali bir defa yakalarsa bununla arabanın kilidini açma şansını elde eder. Bu sebeple araç ile anahtarı arasında n adet sinyal belirlenmiştir ve her kilit açma/kapamada ikisi de sayaçlarını artırır ve araç bir sonraki kilit açma için belirli yeni bir sinyali bekler. Bu sistemin adı uzaktan anahtarsız giriştir (Remote Keyless Entry)[16]. Fakat bu sefer de anahtarda tuşa basıldığında ve bu sinyal arabaya ulaşmadığında anahtarın sayacı bir artarken arabanınki sabit kalacaktır. Bu durumun kullanıcı için problem oluşturmaması için kilit aç tuşuna basıldığında araç anahtarın sayacının ilerlediğini fark eder ve kendininkini de artırarak sayaçları eşitler, böylece normal kullanıma dönülmüş olur. Ama bu durum aynı zamanda bir güvenlik açığı oluşturmaktadır. Bu açıktan yararlanabilen iki saldırı türü vardır: RollBack [17] ve RollJam saldırıları. Önce RollJam adı verilen sinyal yakalayıcı/bozucu alet ile yapılan 2015 yılında bulunmuş bir anahtarsız araba kilidi açma saldırısından bahsedelim [18].

RollJam ucuza temin edilebilen bir sinyal yakalayıcı ve bozucusudur. RollJam kullanılarak dinleme yapılır ve araç sahibi ilk kilit aç tuşuna bastığında bu sinyal RollJam tarafından yakalanır ve sinyal boğucu (jammer) özelliği kullanılarak araca ulaşması engellenir. Aracın kilidi açılmaz. Kullanıcı ikinci defa kilit açma tuşuna bastığında yine aynı adımlar uygulanır ve sinyal araca ulaşmaz. Ardından saldırgan ilk kilit açma sinyalini RollJam ile yayar ve aracın kilidi açılır. Kullanıcı aracını kullanır ve işi bittiğinde kilitler. Saldırgan ikinci kilit aç sinyalini ele geçirdiği için sahibi yokken aracın kilidini rahatlıkla açabilir.

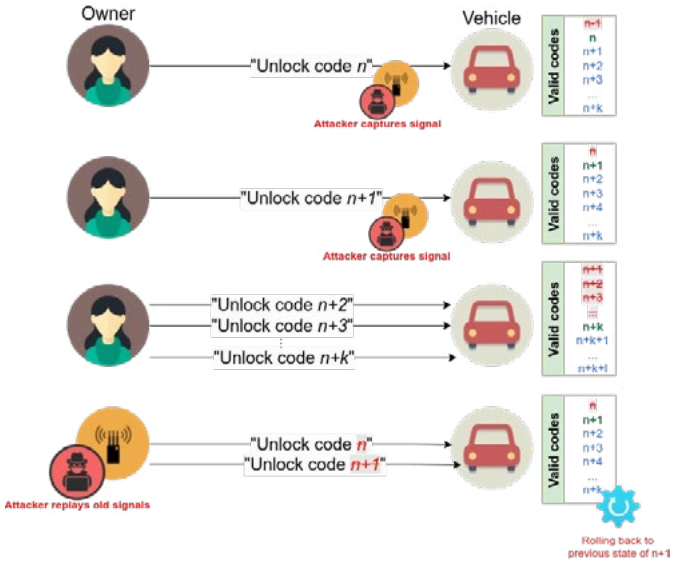


Şekil 11: RollJam cihazı kullanılarak iki kilit aç sinyalinin manipüle edilmesi ve saldırının yapılması.



Şekil 12: HackRF cihazı kullanılarak sadece (i) kilit aç sinyalinin ele geçirilmesi.

Konumuz olan RollBack saldırılarına gelecek olursak, 2022 yılında bulunmuş güncel bir saldırı türünden üretim yılı 2009-2020 arasında olan Nissan, Hyundai, Mazda ve KIA gibi markaların etkilendiği gözlemlenmiştir. Bu türün uygulaması RollJam saldırısından daha kolaydır ve zaman kısıtlaması da yoktur. Saldırının ilk adımı RollJam ile bire bir aynıdır: Araç sahibi tarafından iki defa kilit aç tuşuna basılır ve saldırgan sinyallerden birini daha sonra kullanmak üzere kaydeder. Burada RollJam saldırısından farklı olarak arabanın kilidini açmak için hangi sinyalin gönderildiği önemli değildir ve anahtardan çıkan sinyalin bozulmasına da gerek yoktur, HackRF, yani sinyali yakalayan/yayan aygıtın sinyali yakalaması yeterlidir. Telsiz frekansını yakalayan aygıt sayesinde aracın n ve n+1'inci kilit açma sinyalleri yakalanır. Bundan sonra araç sahibi aracını herhangi bir k sayısı kadar kilitleyip açabilir. Araç n+k+1'inci kilit açma sinyalini beklerken saldırgan n ve n+1 sinyallerini cihaz ile yayar. Araç ve anahtar belirli sayıda sinyali sırasıyla kabul ettiği için ve anahtarın sinyal sayacında öne geçmesi, aracın kilidinin açılmasına engel olmayacağı için saldırganın n sinyalini yayınlaması aracın sayacını sözde anahtar ile eşitlemek için artırmasına (aslında başa dönmesi gerektiği için düşürüyor) neden olur ve araç bu adımdan sonra n+1'inci sinyali bekler. Saldırganın önceden kaydettiği ikinci sinyal olan n+1'inci sinyali yayınlamasıyla aracın kilidi açılır.

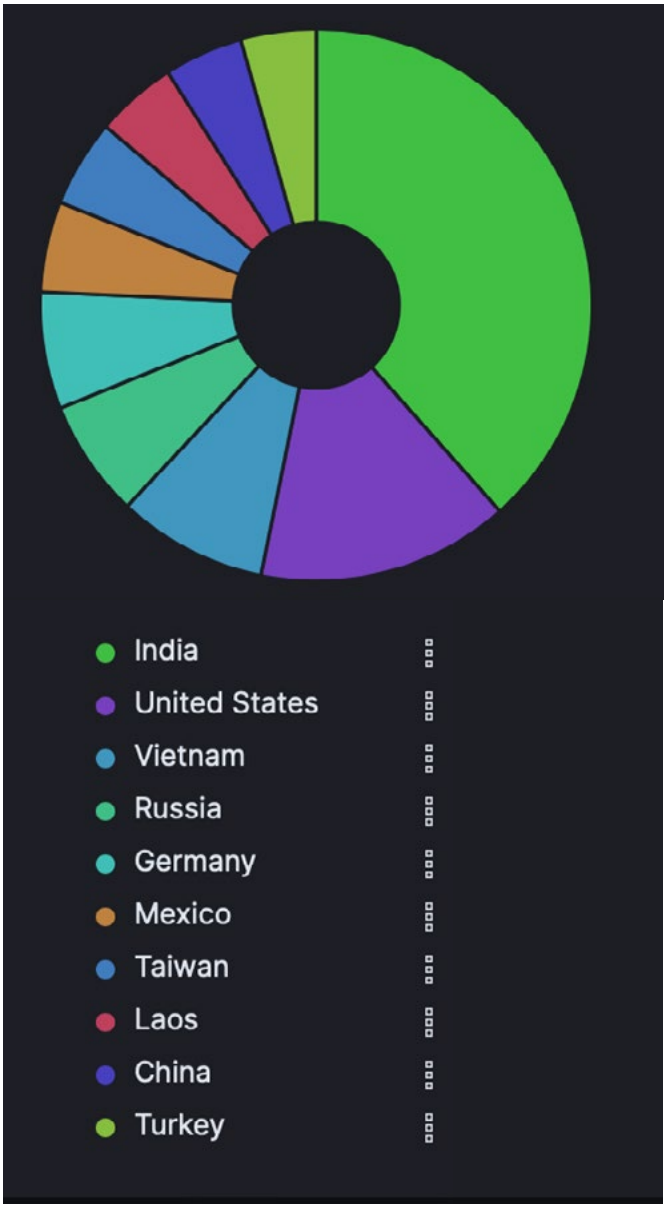


Şekil 13: HackRF cihazı kullanılarak saldırganın kilit açma kodlarını nasıl geriye sardığı.

HONEYPOT VERİLERİ

Bu rapor son üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen parolalar ve kullanıcı isimleri gibi veriler azalan sırada listelenerek incelemeye için sunulmuştur.

Temmuz, Ağustos ve Eylül ayları boyunca Honeypot sensörlerimize toplam 6.137.330 saldırı gelmiştir.



Şekil 14: Gelen saldırıların ülkelere göre dağılımı.

Saldıran Ülke	Saldırı Sayısı
Hindistan	1.046.654
ABD	403.354
Vietnam	239.607
Rusya	187.866
Almanya	186.719
Meksika	144.543
Tayvan	139.613
Laos	130.007
Çin	125.880
Türkiye	120.273

Tablo 2: En çok saldırı gelen ülkeler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Hindistan olduğu; ABD, Vietnam, Rusya ve Almanya'nın onu takip ettiği görülmektedir.

Saldırılan Port	Saldırı Sayısı
445 - SMB	2.947.211
3389 - RDP	449.754
22 - SSH	81.343
25 - SMTP	90.222
8080 - HTTP-ALT	9.869
14333 - MSSQL	18.196
23 – TELNET	140.420
443 - HTTPS	3.662
3182 - bmcpatrolrnvu	10.078
20046 - tmophl7mts	9.095

Tablo 3: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Yukarıdaki tablo incelendiğinde, en çok saldırının SMB servisinin kullandığı port 445'e geldiği görülmektedir. SMB servisi, sunucuların paylaşılan dosyalar ve yazıcılar için kullandığı servis olduğundan, bu servisin diğer servislere kıyasla çok daha fazla saldırı alması beklenen bir durum olarak değerlendirilmektedir. SMB'yi sırasıyla RDP, SMTP ve SSH servisleri takip etmektedir. Son iki en çok saldırı alan port dikkat çekmektedir. "bmcpatrolrnvu" servisi, "BMC Petrol Ajansı" tarafından 3182 portu üzerinden kullanılan bir servistir. "tmophl7mts" servisi ise sağlık alanında elektronik veri aktarımı için kullanılan bir standart olan HL7 ile oluşturulmuş mesajları transfer eden ve 20046 portu üzerinden kullanılan bir servistir. Bu iki porta gelen saldırıların sayılarının beklenenin çok üzerinde olmasından dolayı petrol ajansları ve sağlık sektörüne karşı planlanan saldırıların sayılarında artış olabileceği öngörülmektedir.

Denenen Parola	Denenme Sayısı
admin	7,846
123456	3,566
(boş)	2.475
nproc	2.437
password	1.470
12345	1.048
123	964
1234	950
0	720
root	647

Tablo 4: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan admin, root, password gibi kelimeler gözlemlenmektedir. Bu parolaların test süreci tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir.

Denenen Kullanıcı Adı	Denenme Sayısı
root	24.152
admin	9.607
sh	6.148
nproc	2.437
support	2.259
user	2.064
(boş)	1.918
test	1.804
guest	1.487
default	1.307

Tablo 5: SSH ve RDP honeypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, ftp) tavsiye edilmektedir.

DÖNEM KONUSU

7. Platform Siber Güvenliği

Günümüz savaşlarının önemli bir kısmı artık siber dünyada gerçekleşmektedir. Ülkelerin savunma yeteneklerinin zayıflatılması için sıklıkla siber saldırılar düzenlenmektedir. Askeri casusluk ve bilgilerin ifşa edilmesi ile sonuçlanan siber saldırılar devletlerin silahlı kuvvetleri için büyük tehdit oluşturmaktadır. Müttefik olmayan devletlerin savaş stratejilerinin, askeri birliklerinin görev bilgilerinin, silah ve platform tasarımlarının ifşa edilmesi ilerleyen yıllarda yaşanabilecek saldırılardandır. Daha da artacak siber güvenlik tehditleri ile ülkelerin sanayilerinde geliştirilen platformlar kadar bu platformların siber güvenliğinin sağlanması da oldukça önemli hâle gelmiştir.

Platformlar kara, hava, deniz ve uzay olarak sınıflandırılmak üzere; ağ destekli sistemler, uygulamalar ve ilişkili fiziksel altyapılar aracılığıyla bilgilerin saklanması, işlenmesi, iletilmesi, değiştirilmesi, depolanmasının sağlanması ve bunun yanı sıra muhabere, algılayıcı sistemler, komuta kontrol, istihbarat, keşif gözetleme sistemleri ile tüm operasyonel uzayı kapsayan bütünleşik sistemlerdir.

Ülkemizde geliştirilen platformlar arasında yer alan araçların siber güvenlik risklerinin göz önünde bulundurularak geliştirilmesi çok önemlidir.

Türkiye'de geliştirilen önemli platformları İHA ve SİHA sistemleri (TOGAN, KARGU ve ALPAGU), suüstü ve denizaltı platformları, Muharip İnsansız Uçak Sistemi (MİUS), Milli Muharip Uçak (MMU), MİLGEM, TOGG yerli otomobil olarak listeleyebiliriz.

Dünyada geliştirilen önemli platformları da Predator C Avenger (ABD), Heron TP (İsrail), CH-5 (Çin), Yabhon United 40 (Birleşik Arap Emirlikleri), TESLA (ABD) şeklinde listeleyebiliriz.

Devletlerin savunma stratejilerinin önemine bağlı olarak platformlara yönelik siber güvenlik saldırılarının arttığını izlemekteyiz. Platformlara yönelik gerçekleştirilen saldırılara bakacak olursak, dünyada arabalara yapılan siber saldırıların sıklığının 2018'den 2021'e yüzde 225 arttığını görebiliriz[20].

Devletlerin savunma stratejilerinde önemli yer tutar hâle gelen platformlara yönelik siber güvenlik tehditleri önümüzdeki yıllarda daha da fazla gündemimize girecektir. Örneğin, savaş uçakları görevlerini yerine getirmek için hem bilgi teknolojilerine hem de ilişkili fiziksel altyapılara ihtiyaç duymaktadır. Uçağın mühimmatı hedefe göndermesi için gereken basıncın nasıl düzenleneceği, uçak ekipmanlarının tahmini kullanım ve bakım periyodu, pilota iletilmesi gereken bilgilerin anlaşılabilir ve düzenli şekilde kokpitte nasıl gösterileceği gibi fonksiyonların yerine getirilmesi için hem bilgi teknolojilerine (yazılım, ağ sistemleri vb.) hem de ilişkili fiziksel altyapılara ihtiyaç vardır. Sistemlerin karmaşıklığı göz önüne alındığında gerekli güvenlik önlemleri alınmazsa platformlar siber saldırılara açık durumda kalabilir. Örneğin hafife alınan sosyal mühendislik saldırısı sonucu bir USB ile zararlı yazılım platformlara bulaşabilir, DDOS saldırısı ya da bilgilerin ifşası gerçekleşebilir veya injection saldırıları ile verilerin bütünlüğü bozulabilir. Bu ve benzer saldırıların sonucunda mühimmatın hedefe gönderilmesi engellenebilir, radar sistemlerinin kapatılmasına neden olabilir veya daha kötüsü müttefik unsurların düşman gibi gösterilerek imha edilmesine neden olunabilir.

Platformlarda bulunan sistemlerin her birinin farklı siber güvenlik gereksinimleri vardır. Bu sistemlerin geliştirilmesinde güvenli sistem geliştirme süreçlerinin takibi,

Şekil 15: Kara, hava, deniz ve uzay platformları[19].

Şekil 16: Kara, hava, deniz ve uzay platformları.

düzenli olarak sistemler üzerindeki zafiyetlerin tespiti, kayıtların ve alarm sistemlerinin düzenli olarak gözden geçirilmesi son derece önemlidir. Ayrıca platformlar üzerindeki sensörlerin ve diğer fiziksel ekipmanların bakımı, yazılımların güncellenmesi, erişimlerin düzenli gözden geçirilmesi, tedarik zincirindeki risklerin ve tehditlerin göz önünde bulundurulması son derece önemlidir.

Bu sebeple güvenlik ekipleri, platformlarda siber güvenliğin sağlanması için en son tehditleri ve zafiyetleri takip etmeli, bütüncül bir yaklaşımla ele almalı ve yeni güvenlik stratejileri geliştirmelidir. Askeri otoriteler; uçakları, platformları ve donanımları izledikleri gibi platformu kullanan kişileri de izlemeli, güvenlik risklerini değerlendirmelidir.

7.1. Platform Siber Güvenlik Tehditleri

- **Truva Atı**

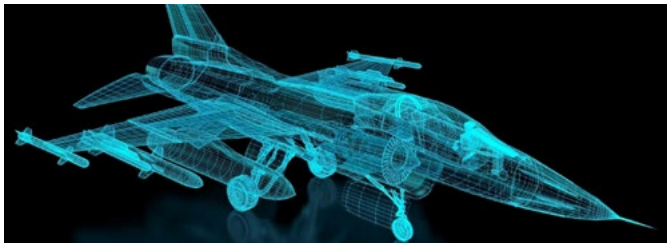
  Truva atı, savunma platformları için oldukça ciddi bir güvenlik açığıdır. Platformlar içisinde tümleşik devrelerde truva atlarının tasarlanmasının zor olması, günümüzde bu truva atlarının seyrek görülmesine ve ciddi bir tehdit olarak değerlendirilmemesine yol açmaktadır. Farklı küresel güç merkezleri, birbirleri üzerinde güvenlik açığı oluşturmak isteyebileceği gibi kendilerini de bu tip zafiyetlerden korumak zorundadırlar. Dolayısıyla bu konu gizli bir şekilde pek çok devlet tarafından ciddiyetle yürütülmesi beklenen bir konudur[21].

- **DDoS Saldırıları**

  Çoğu zaman kullanıcıların bilgisi dahi olmadan başkalarınca ele geçirilmiş sistemler olan robot/bot ve bunların oluşturduğu botnet ile yapılan DDoS saldırıları da platform altyapılarının çalışamamasına neden olabilmektedir. Sistemlerin cevaplayabileceğinden çok daha fazla çoklu isteğin iletilmesiyle çalışan DDoS, veri akışının kilitlenmesine ve platformların kullanılmaz hâle gelmesine neden olmaktadır.

- **Zararlı Yazılımlar**

  Platformlara yönelik önemli tehditlerden biri de zararlı yazılımlardır. Yakın geçmişte en önemli zararlı yazılım olarak akılda kalan STUXNET, ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı solucan yazılımdır[22]. STUXNET, endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin de hedef olabileceğini göstermesi açısından siber güvenlik konusunda önemli bir yere sahiptir. Yakın gelecekte de STUXNET solucanı gibi birçok zararlı yazılımın, platformları donanım ve yazılım seviyesinde ciddi şekilde tehdit edeceği öngörülmektedir. Bu tür zararlı yazılımları platforma zarar vermeden önce tespit edebilme yeteneğinin yerli ve milli olarak geliştirilmesi gerektiği aşikârdır.



Şekil 17: Uçak siber güvenliği[23].

7.2. Tedarik Zinciri

Platformların geliştirilmesi süreçlerinde bazı sistemler, yazılımlar ve fiziksel altyapılar farklı ülkelerden tedarik edilebilir. Çok sayıda farklı tedarikçiden satın alınan ürünlerin entegre edilerek kullanılması avantajların yanı sıra bazı siber güvenlik tehditlerini de beraberinde getirmektedir. Bu tedarik zinciri platformların seri üretilmesi sırasında dışa bağımlılığa sebep olmaktadır. Ayrıca tedarik edilen ürüne bağlı devletler ile savaş stratejilerinin değişmesi durumunda hem dış bağımlılık oluşturur hem de tedarik edilen ürüne kasten zafiyet yerleştirilebilir. Ülkemizde de ana yüklenici rolüne sahip savunma sanayi şirketlerimiz yurtiçi ve yurtdışından çok sayıda alt yükleniciden donanım/yazılım bileşeni tedarik edip sistem bütünleştirmesi yapmaktadır. Tedarik zincirinden kaynaklanan en büyük risk, donanım ve yazılımların içinde bulunma ihtimali yüksek olan arka kapı veya truva atlarının varlığıdır. Tümleşik devre üretme tesislerinin kurulması, sadece sanayileşmiş ve güçlü ekonomiye sahip ülkelerin tekelinde kalmaya devam etmektedir. Uzakdoğu ekonomisinin, özellikle Çin ekonomisinin son 20 sene içinde gösterdiği büyüme ve sundukları düşük maliyetli üretim fırsatları, birçok sektörde olduğu gibi tümleşik devre sektöründe de üretiminin yaygın olarak bu bölgeye taşınmasına yol açmıştır. Bu durum üretilen tümleşik devrelerin güvenliğini tartışmalı hâle sokmuş, üretim aşamasında tümleşik devrelere zararlı bileşenler eklenebileceği şüphesi uyanmaya başlamıştır[24].

7.3. Tehdit Aktörleri

Platform güvenliğini tehdit eden aktörler başta devlet destekli tehdit aktörleri olmak üzere organize suç ekipleri, hacktivistler, fırsatçı kişiler, memnuniyetsiz çalışanlar ve casuslar olarak listelenebilir.

- **Devlet Destekli Tehdit Aktörleri:** Bu saldırı grupları çok iyi finanse edilmektedir ve genellikle hedefli karmaşık saldırılar gerçekleştirir. Genellikle politik, ekonomik, teknik veya askeri motivasyon ile hareket ederler.
- **Organize Suç Ekipleri:** Bu saldırı grupları en çok finansal kazanç sağlayacak eylemleri gerçekleştirmeyi tercih ederler. Genelde sistemler üzerinde gizli bilgileri ele geçirip bunlar üzerinden fidye almaya çalışırlar.
- **Hacktivistler:** Bu saldırganların genelde politik amaçları bulunur. Amaçları propagandalarını yaymaya yardımcı olan yüksek profilli saldırılar düzenlemek veya karşı oldukları kuruluşlara zarar vermektir. Temel amaçları bir konuya dikkat çekmektir.
- **Fırsatçı Kişiler:** Bu saldırganlar genelde amatör suçlulardır ve tanınma, ünlü olma arzusu peşindedirler. Ancak sadece zarar vermek amacıyla hareket etmezler. Sistemlerde buldukları güvenlik açıklıklarını bildirip, bununla isim duyurmaya da çalışabilirler.
- **İşinden Memnun Olmayan Mutsuz Çalışanlar:** Sistemlerinize karşı kötü niyetli faaliyet gösteren kişilerin tamamı dışarıdan gelmek zorunda değildir. İşinden memnun olmayan, mutsuz çalışanlar daha fazla maddi kazanç elde etmek veya iş hayatında karşılaşılan tatsız olaylardan dolayı intikam almak için karşı firmalarla işbirliği yapabilirler.
- **Casuslar:** Siber casuslar, kişilerden, rakiplerden, gruplardan, hükümetlerden sahip oldukları kişisel, ekonomik, politik ve askeri avantajlar hakkında bilgi edinmeye çalışırlar ve edindikleri bilgileri düşmana aktarırlar. Sistemlere kötü amaçlı yazılım bulaştırma ve yetkilerini kullanarak eriştikleri bilgileri dışarı çıkarma/sızdırmaya çalışmak siber casusların yaptıkları işlemlere örnek gösterilebilir.

KAYNAKÇA

[1] M. Backendal, M. Haller ve K. G. Paterson, «MEGA: Malleable Encryption Goes Awry,» 28 07 2022. [Çevrimiçi]. Available: https://eprint.iacr.org/2022/959.

[2] D. Bleichenbacher, « Annual International Cryptology Conference CRYPTO 1998: Advances in Cryptology — CRYPTO '98 pp 1–12Cite as Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1,» %1 içinde *Annual International Cryptology Conference*, 1998.

[3] S. Jarecki, H. Krawczyk ve J. Xu, «OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-computation Attacks,» %1 içinde *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2018.

[4] N. J. Rubenking, «SMS-Based Multi-Factor Authentication: What Could Go Wrong? Plenty,» August 11, 2022.

[5] B. Z. Z. Z. D. S. S. W. Y. J. Haoqi Shan, «Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Electronic Devices,» 2022.

[6] N. J. Rubenking, «This 'Invisible Finger' Can Take Over Your Touch Screen,» PCMag, 11 Ağustos 2022. [Çevrimiçi]. Available: https://www.pcmag.com/news/this-invisible-finger-can-take-over-your-touch-screen.

[7] B. K. Key, «Global Threat Actors Use the 'Great Resignation' to Target Job Seekers,» 12 August 2022.

[8] BY, «Global Threat Actors Use the 'Great Resignation' to Target Job Seekers,» 12 AUGUST 2022.

[9] A. Lameiras, «Common LinkedIn scams: Beware of phishing attacks and fake job offers,» 9 May 2022.

[10] B. K. Key, «Global Threat Actors Use the 'Great Resignation' to Target Job Seekers,» 12 August 2022.

[11] ELBAMBY, M. S., ET AL., «Edge computing meets millimeter-wave enabled vr: Paving the way to cutting the cord.,» %1 içinde *IEEE Wireless Communications and Networking Conference (WCNC)*, 2018.

[12] [Çevrimiçi]. Available: Boosting smart manufacturing with 5g wireless connectivity. https:// www.ericsson.com/en/reports-and-papers/ericsson-technology-review/ articles/boosting-smart-manufacturing-with-5g-wireless-connectivity.

[13] S. BOLL, «Suppression of acoustic noise in speech using spectral subtraction.,» *IEEE Transactions on acoustics, speech, and signal processing 27*.

[14] S. E. A. BECKER, « Interpreting and explaining deep neural networks for classification of audio signals.,» 2018.

[15] P. WARDEN, «Speech Commands: A Dataset for Limited-Vocabulary Speech Recognition.,» 2018.

[16] T. Chetvorno, «Wikipedia,» 2022. [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Remote_keyless_system.

[17] L. Csikor, «blackhat,» 6 August 2022. [Çevrimiçi]. Available: https://www.blackhat.com/us-22/briefings/schedule/#rollback---a-new-time-agnostic-replay-attack-against-the-automotive-remote-keyless-entry-systems-27185.

[18] C. Coward, «Hacking a Car's Key Fob with a Rolljam Attack,» 2019. [Çevrimiçi]. Available: https://www.hackster.io/news/hacking-a-car-s-key-fob-with-a-rolljam-attack-7f863c10c8da.

[19] «aselsan.com,» 12 9 2022. [Çevrimiçi]. Available: https://www.aselsan.com.tr/tr/cozumlerimiz/gudum-ve-insansiz-sistemler.

[20] «Israel21c.org,» 12 9 2022. [Çevrimiçi]. Available: https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/.

[21] «wikipedia.org/wiki/Back_door,» 12 9 2022. [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Back_door.

[22] «wikipedia.org/wiki/Stuxnet,» 12 9 2022. [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Stuxnet.

[23] «swri.org/aircraft-cybersecurity,» 12 9 2022. [Çevrimiçi]. Available: https://www.swri.org/aircraft-cybersecurity.

[24] «enisa.europa.eu,» 12 9 2022. [Çevrimiçi]. Available: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech