Araştırma Makalesi

ÇOCUKLARA YÖNELİK AKILLI SAATLERİN SİBER GÜVENLİK VE MAHREMİYET AÇISINDAN İNCELENMESİ

Cafer ULUÇ[†], Can EYÜPOĞLU[††]

[†] Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye

[††] Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye

cafer@tutanota.com, caneyupoglu@gmail.com

0000-0003-4756-5757, 0000-0002-6133-8617

Atıf/Citation: ULUÇ, C, EYÜPOĞLU, C., (2024), Çocuklara Yönelik Akıllı Saatlerin Siber Güvenlik Ve Mahremiyet Açısından İncelenmesi, Journal of Technology and Applied Sciences 7(1) s.77-87, DOI: 10.56809/icujtas.1419510

ÖZET

Akıllı saat, içerisinde bulunan bileşen ve servislerle kullanıcının bileğine taktığı küçük bir bilgisayardır. Cep telefonuyla bağlantılı hareket eden bu cihaz, telefonun tüm kabiliyetleriyle donanabilmektedir. Akıllı saatler metropol kentlerinin dinamik yaşamında güvenilir bir yardımcı mı yoksa iyi niyetli görünen ve gönüllü olarak eşlik edilmesine izin verilen casus cihazlar mıdır? Bu çalışmada, özellikle akıllı çocuk saatlerinin gerek ekonomik erişilebilirlik gerek ürüne ulaşımdaki kolaylığın her geçen gün artması ile orantılı olarak yaygınlaşmasıyla yaşanan ve yaşanabilecek kişisel verilerin ve mahremiyetin ihlali üzerinde durulmaktadır. Ayrıca akıllı saatler üzerinde yapılan teknik incelemeler ile endişe verici sonuçlara ulaşılmıştır. Çalışma kapsamında teknik incelemelere ayrıntılı olarak yer verilmekle birlikte olası güvenlik ve mahremiyet riskleri incelenmekte, önleyici unsurlar aktarılmakta ve konuya Türkiye perspektifinden yaklaşılarak güvenlik önerilerinde bulunulmaktadır. Bu çalışma aracılığıyla toplumsal siber güvenlik direncinin artırılması ve araştırmacılara IoT (Internet of Things-Nesnelerin İnterneti) cihazlarında tersine mühendislik çalışmaları için fikir verilmesi amaçlanmaktadır.

Anahtar Kelimeler: Akıllı Saat, Tersine Mühendislik, IoT Güvenliği, Mahremiyet, Veri Güvenliği

EXAMINING SMARTWATCHES FOR KIDS IN TERMS OF CYBER SECURITY AND PRIVACY

ABSTRACT

A smart watch is a small computer with components and services that the user wears on their wrist. This device, which is connected to a mobile phone, can be equipped with all the capabilities of the phone. Are smart watches a reliable assistant in the dynamic life of metropolitan cities or are they spy devices that look well-intentioned and are allowed to be accompanied voluntarily? In this study, the focus is on the violation of personal data and privacy that has been and may be experienced, especially with the widespread use of smartwatches for kids in proportion to the increasing economic accessibility and ease of access to the product day by day. In addition, technical studies on smart watches have yielded worrying results. Within the scope of the study, technical investigations are included in detail, possible security and privacy risks are examined, preventive elements are explained and security recommendations are made by approaching the issue from the perspective of Turkey. Through this study, it is aimed to increase social cyber security resilience and give researchers ideas for reverse engineering studies on IoT (Internet of Things) devices.

Keywords: Smartwatch, Reverse Engineering, IoT Security, Privacy, Data Security

Geliş/Received	**:**	**14.01.2024**
Gözden Geçirme/Revised	**:**	**1.02.2024**
Kabul/Accepted	**:**	**8.02.2024**

1. GİRİŞ

Gelişen teknoloji ile kişilerin mahremiyetine yönelik tehditler artarken gözetim mekanizmaları da güçlenmektedir (Bundesnetzagentur, 2017). Bu çalışmada odaklanılan akıllı çocuk saatleri, özellikle 5-12 yaş aralığını hedef pazar olarak görmektedir. GPS (Global Positioning System-Küresel Konumlama Sistemi) modülü ile yüklü gelen bu cihazlar en iyi ihtimalle ebeveyne çocuğunun nerede olduğuna yönelik bilgi vermektedir. Bütünleşik mikrofon ile çocuğun dinlenmesi, bütünleşik kamera ile çocuğun fotoğrafının çekilmesi uzaktan erişimle mümkün olmaktadır. Üstelik tüm bunlar olurken çocuğun haberi olmayacak biçimde ayarlanmaktadır. Bu endişe verici konu, hukuk açısından II. bölümde ayrıca ele alınacaktır.

Çocuklara yönelik akıllı saatlerin maddi açıdan ekonomik olması, satın almada ve kullanmada onları oldukça yaygın hale getirmektedir. Yurt dışı pazaryerlerinde 7$'a satılan akıllı saatler de bulunmaktadır. Bir yazılımda güvenlik zafiyetinin ana unsurlarından birisi de ekip yetersizliğidir. Böylesine düşük fiyatla satılan bu teknolojinin olası güvenlik risklerini de barındırabileceği ifade edilebilir.

Konuyla ilgili yapılan akademik literatür taramasında doğrudan akıllı çocuk saatlerinin siber güvenliğini ele alan Türkçe bir çalışma bulunamamıştır. Diğer dillerdeki çalışmalar ise yok denecek kadar azdır. Bununla birlikte bu çalışmanın ele alınmasında dolaylı olarak gerek akademik gerek teknik çalışmalardan yararlanılmıştır. Konuyla ilgili çalışmalar ağırlıkla blog yazıları ve raporlardan oluşmaktadır. En kapsamlı çalışma ise Norveç Tüketici Konseyi (Forbrukerrådet) tarafından yapılmıştır. Konsey (Norwegian Consumer Council, 2017) dört farklı akıllı çocuk saatini teknik olarak incelemiş ve kişisel verilere yönelik tehditleri ayrıntılı olarak ele almıştır. Buna rağmen ilgili çalışmada tekniz analizin nasıl yapıldığı ile ilgili ayrıntı verilmemiştir. Al-Sharrah ve ark. (Al-Sharrah, Salman, & Ahmad, 2018) Apple Watch üzerinden bir adli bilişim analizi yapmıştır. Saatjohann ve ark. (Saatjohann, Ising, Krings, & Schinzel, 2020) tarafından yapılan çalışmada ise akıllı saatler üzerine bilgi verilmiş ve mobil uygulamalar incelenmiştir.

Bu çalışmada ise konuya Türkiye perspektifinden yaklaşılacaktır. Nitekim yasal çerçeve ve satılan ürünler farklılık göstermekle birlikte yapı olarak aynıdır. Özellikle çocukların ve yaşlıların mahremiyetinin göz ardı edildiği görülmektedir. Çalışmada ele alınan iki farklı cihaz, donanım ve yazılım analizlerine tabi tutularak incelenecektir. Kötü niyetli kişilerin neler yapabileceği uygulamalı olarak okura ve karar vericilere sunularak bireysel ve kamusal önlemlerin alınmasına dikkat çekilecektir.

Çalışmanın geri kalanı şu şekilde organize edilmiştir: 2. bölümde kişilerin mahremiyetine yönelik kapsayıcı yasal düzenlemelerden söz edilmektedir. Araştırma ve uygulamalı analiz ise 3. bölümde yapılmaktadır. Bu bölümde yapılan çalışmalara yer verilmekle birlikte iki farklı cihazın teknik analizi ayrıntılı olarak ele alınmaktadır. 4. bölümde sonuç olarak varılan yargılara ve önerilere yer verilmektedir. 5. bölümde ise yararlanılan kaynaklar bulunmaktadır.

2. YASAL DÜZENLEMELER

Akıllı saatler, özellikle çocuklar ve bakıma muhtaç yaşlı bireylerin güvenliklerine yönelik iyi niyetlerle tercih ediliyor olsa da kişilerin mahremiyetinde ciddi ihlallere neden olabilmektedir. Nitekim bu cihazlarda genel olarak GPS, bütünleşik olarak mikrofon ve kamera bulunmaktadır. Böylelikle kişinin nerede olduğu konum bazlı bilinebilmekte, ortam dinlenebilmekte ve anlık görüntü alınabilmektedir.

Bu çalışmanın gerçekleştirildiği tarih itibariyle Türkiye'de bu cihazların satışı ve kullanımı serbesttir. Cihazların kabiliyetleri ve kötüye kullanımdaki kolaylıklardan dolayı kötü niyetli kişi ve kişilere kapı aralanmaktadır. Buna rağmen kamuoyunun ve teknik bireylerin konuya olan ilgisi oldukça sınırlıdır.

Konuya yasal olarak bakıldığında ise temelde Türk Ceza Kanununun dokuzuncu bölümünde (Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar) yer alan 133. ve 134. maddelerde (Türk Ceza Kanunu, 2023) kişinin rızası olmadan yapılan dinlemenin suç sayıldığı ve yaptırımla cezalandırılacağı belirtilmektedir: "Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. (3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur. Madde 134- (1) Kişilerin özel hayatının

gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.”.

Çocuklara yönelik akıllı saatler, özellikle anaokulu ve ilkokul yaşlarındaki çocuklarının güvenliğinden emin olmak isteyen ebeveynler tarafından tercih edilmektedir. Milli Eğitim Bakanlığınca bu saatlerin okullarda kullanılmamasına yönelik (doğrudan olmasa da) kapsayıcı bir düzenleme bulunmaktadır. Milli Eğitim Bakanlığı Ortaöğretim Kurumları Yönetmeliği 164. maddede (Disiplin cezasını gerektiren davranış ve fiiller) “Ders saatleri içinde öğretmenin bilgisi ve kontrolü dışında bilişim araçlarını açık tutarak dersin akışını bozmak.” ibaresi yer almaktadır (MEB). Tüm bunlara rağmen söz konusu çocuk saatlerinin okullarda kullanıldığı ve bu durumdan dolayı öğretmen-veli arasında sorunlar yaşandığı bilinmektedir (Annelere Sor, 2023). Üstelik bu durum diğer ülkelerde de geçerlidir. Velilerin, öğretmenleri gizlice dinlemek niyetiyle bu saatleri çocuklarına taktırdıkları ilgili referans metninde yer almaktadır (Bundesnetzagentur, 2017).

Almanya Federal Ağ Ajansı (Bundesnetzagentur) Başkanı Jochen Homann, çocuklar için tasarlanan bu akıllı saatlerle çocuğun bulunduğu ortamdaki diğer kişilerin de konuşmalarının dinlenebileceğine dikkat çekmektedir. Akıllı saatlerin bu özelliğinden dolayı ilgili cihazların casusluk endişeleri nedeniyle satışı ve kullanımı Almanya’da yasaklanmıştır. Elinde bu cihazdan olanlar için ise bir an önce imha edilmesi gerektiği ifade edilmektedir (Bundesnetzagentur, 2017).

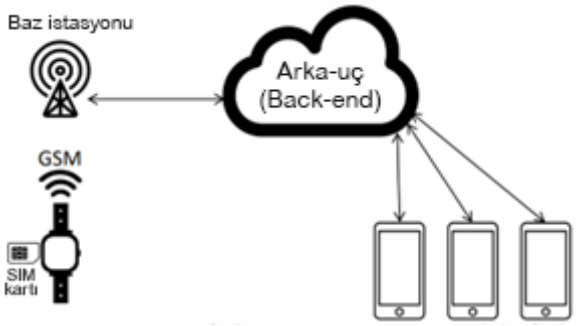
Ortam dinlemesiyle ilgili olarak Kişisel Verileri Koruma Kanununun 5. maddesinin 1. fıkrasında şu ifade geçmektedir: “Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.” (Kişisel Verilerin Korunması Kanunu, 2016).

Avrupa Komisyonu (European Commission) ise yayınladığı ürün bazlı inceleme raporunda doğrudan incelemeye aldığı “Enox Safe-Kid-One” adlı akıllı çocuk saatinin hackerlar tarafından kolayca ele geçirilebileceğini, dolayısıyla ebeveynin uzaktan erişebildiği (mikrofon, kamera, konum vb.) tüm olanakların istismara açık olduğunu ifade ederek ilgili cihazın satışını ve kullanımını Avrupa Birliği’nde yasaklamıştır. Komisyon, örnek olarak GPS’nin kolayca hacklenebileceği ve hackerların çocukları izlemesine ya da kullanıcının gerçek konumunu ebeveynlerinden gizlemesine olanak sağlayabileceğini vermektedir (European Commission, 2020).

3. ARAŞTIRMA VE BULGULER

IoT (Internet of Things-Nesnelerin İnterneti) için kullanılan 2G ve 3G gibi teknolojiler güvenlik açıkları barındırmaktadır. Güncel olarak kullanılan LTE’ye (Long-Term Evolution-Uzun Vadeli Evrim) yönelik güvenlik açığı oluşturabilecek atakların olduğu da ifade edilmektedir (Saatjohann, Ising, Krings, & Schinzel, 2020).

Akıllı çocuk saatleri, yetişkinlere yönelik geliştirilen saatlerden farklı olarak SIM kartı barındırmaktadır. Yetişkin saatlerinde telefon ile yapılan haberleşme bluetooth ile sağlanır. Bu da telefon ve saati fiziksel olarak birbirlerine yakın olmasını zorunlu kılmaktadır. Çocuk saatlerinde ise amaç uzaktan gözetim olduğu için İnternet altyapısı olan donanımlar kullanılmaktadır (Şekil 1). İnternet ağı ile birbirine bağlı her cihaz da bilgisayar korsanları tarafından kötüye kullanılabilir. Bu ağ, potansiyel olarak MITM’ye (Man in the Middle-Ortadaki Adam Saldırısı) açık olabilir. Verilerin iletişiminde SSL (Secure Sockets Layer-Güvenli Soket Katmanı)/TLS (Transport Layer Security-Taşıma Katmanı Güvenliği) olmaksızın doğrudan HTTP’nin (Hyper-Text Transfer Protocol-Hiper-Metin Transfer Protokolü) kullanıldığı görülmektedir. Bu çalışmanın ilerleyen aşamalarında bu konuya uygulamalı olarak değinilecektir.



Şekil 1. Akıllı çocuk saatlerinin iletişim modeline genel bakış.

Mobil cihazlarda tersine mühendislik saldırıları oldukça yaygındır. OWASP'nin (Open Web Application Security Project-Açık Web Uygulama Güvenliği Projesi) "Mobile Top 10" (OWASP, 2023) listesinde (M9: Reverse Engineering) yer alan bu yöntem ile bir mobil uygulamaya yönelik gerçekleştirilecek kaynak kod analiziyle olası güvenlik açıklıklarına zemin hazırlanabilmektedir. Saldırgan, bu uygulamanın kaynak kodunda değişiklikler yaparak uygulamanın haberleştiği cihazı ya da kullanıcıyı manipüle edebilmektedir.

Bir başka durumda ise saldırgan, manipüle ettiği uygulamayı hedefte çalıştırdığı takdirde tüm iletişimi kolayca dinleyebilmektedir. Bu çalışmada ele alınan akıllı saatler çerçevesinde konuya yaklaşıldığında, çocuğuna "eve gelmesine" yönelik SMS atabilen anne-baba yerine saldırgan, doğrudan amacına yönelik kısa mesaj gönderebilir. Bir diğer durumda ise hafızası zayıflayan ve ilaç alımında yönlendirilmeye ihtiyaç duyan demans hastalığı bulunan bir yaşlıya yanlış bilgiler (fazla doz alımı gibi) (Stykas, 2020) gönderilebilir. Nitekim çocuklar için geliştirilen bu cihazların tasarım olarak farklı sürümleri hasta bireyler arasında oldukça yaygındır. Bu gibi güvenlik zafiyeti barındıran saatler manipüle edilmeye açıktır.

CVE'de (Common Vulnerabilities and Exposures-Yaygın Güvenlik Açıkları ve Etkilenmeleri) yapılan sorguda CVE-2019-20468 ID numarasıyla bir kayıt bulunmuştur (MITRE Corporation, 2023). Akıllı çocuk saatlerinde yaygın olarak kullanılan SeTracker2 mobil uygulaması, ihtiyacı olmadığı halde "Read_External_Storage", "Write_External_Storage" ve "Read_Contacts" gibi alanlara eriştiği kaydedilmiştir. Yapılan analiz sırasında uygulamanın rehbere erişmeden de işlemleri yapabildiği görülmüştür.

Yukarıda adı geçen erişim izinleri hakkında kısa açıklamalar ise şöyledir (Android Developers, 2023):

- READ_EXTERNAL_STORAGE: Uygulamanın harici depolamadan veri okumasına izin verir.
- WRITE_EXTERNAL_STORAGE: Uygulamanın harici depolamaya veri yazmasına izin verir.
- READ_CONTACTS: Uygulamanın kullanıcının rehberindeki kişi verilerini okumasına izin verir.

Norveç Tüketici Konseyinin 2017 yılında dört farklı akıllı çocuk saati üzerinde gerçekleştirdiği karşılaştırma Tablo 1'de görülmektedir.

Tablo 1. Farklı akıllı çocuk saatlerinin karşılaştırılması (Norwegian Consumer Council, 2017).

Cihaz / Gizlilik isterleri	**Gator**	**Tinitell**	**Viksfjord**	**Xplora**
Kayıt sırasında onay istenir.	✗	✓	✗	✗
Şartlar değiştirilirse bilgilendirileceğim.	✗	✗	✗	✗
Kişisel verilerim pazarlama amacıyla kullanılmayacaktır.	✗	?	?	✗
Uygulamadaki verileri silebilirim.	✗	✗	?	?
Konum verileri belirli bir süre sonra otomatik olarak silinir.	✗	✗	✗	✗

Kullanıcı hesabımı silebilirim.	✕	✕	✕	✕
Makul güvenlik standartlarını uygulama sözü verir.	✕	✓	✕	✕
Kişisel verilerin nereye aktarıldığı ve depolandığı açıkça belirtilir.	✕	✕	✕	✕

3.1. İncelenen Cihazlar ve Mobil Uygulamalar

Bu çalışmada iki ayrı markanın akıllı saati incelenmektedir (İki çocuk saati temin edilmiştir. Ancak gelen ürünlerden birisi olan Hangarex Kallow cihazı bozuk çıkmış olup yerine başka bir cihaz sipariş edilmiştir.). Cihazlar inceleme için temin edildiğinde, Türkiye'de popüler olan bir alışveriş sitesinde giyilebilir teknolojilerin alt kategorilerinde (akıllı çocuk saati ve akıllı saat) en çok satılan ilk konumunda idiler. Toplam değerlendirme sayısı ise 15.557 idi. Her satın alan kişinin değerlendirme yapmadığı göz önüne alındığında söz konusu iki cihazın on binlerce kişinin kolunda olduğu sonucuna varılabilir. Nitekim ürünlerin toplam favorilere eklenme sayısı ise 250.757'dir. Saatin telefon ile haberleşmesinde kullanılan uygulamanın ise (FitPro) 50+ milyondan fazla indirmesi bulunmaktadır. Aşağıdaki tabloda cihazlara yönelik genel anlamda bilgiler yer almaktadır. Ayrıntılar ise ilerleyen sayfalarda uygulamalı olarak irdelenecektir.

Tablo 2. İncelenen ürünlere genel bir bakış.

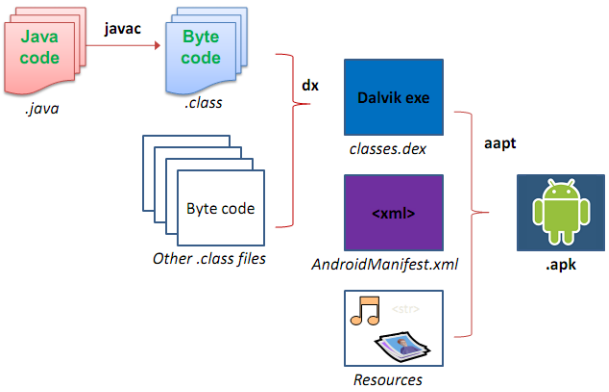
Ürün	Odak	Fiyat	Üretim	Kullanılan Uygulama
Smart Berry	Çocuk	22$	Çin	SeTracker2
Supen T500	Yetişkin	16$	Çin	FitPro

2023 yılında yaklaşık 224 milyon akıllı saatin kullanımda olduğu belirtilmektedir (Demand Sage, 2023). Statista'nın raporuna göre dünya genelinde kullanıcı sayısının 2027 yılında yaklaşık 229 milyona ulaşacağı tahmin edilmektedir (Statista, 2023). Yapılan teknik araştırmalar sonucunda akıllı çocuk saatlerindeki bu zafiyet hemen hemen tüm markalarda görülmektedir (Ken, 2018).

Saat üreticisi ile telefonda kullanılan uygulama aynı firmaya ait değildir. Saat üreticileri çoğunlukla dış kaynaktaki bir uygulamayı saatleri için tercih etmektedirler. Akıllı çocuk saatlerini savunmasız ve güvensiz kılan ana unsur temelde bu durumdan kaynaklanmaktadır.

3.2. Teknik Analiz

Bu bölümde, akıllı saatlere uzaktan erişim için kullanılan mobil uygulamaların (FitPro ve SeTracker2) APK dosyaları yüklü olan telefondan edinilmiştir. Ardından, yazılımın kaynak kodlarına erişilmiştir. Bir APK (Android Package Kit) dosyası, yapı olarak Şekil 2'deki şemada gösterilmektedir.

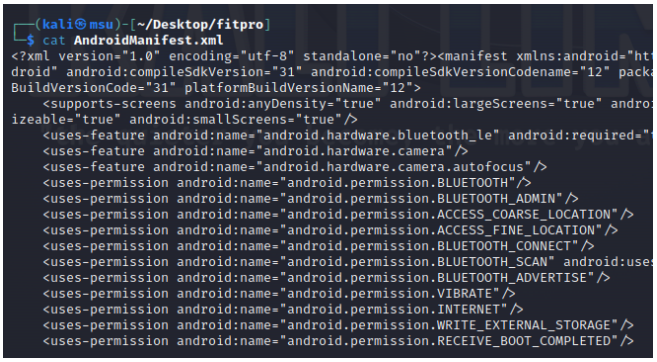


Şekil 2. Bir APK'nin mimarisi (Shehata, El Fiky, Torky, Farag, & Abbas, 2020).

İnceleme sırasında tersine mühendislik yöntemleri kullanılmıştır. Aşağıdaki iki alt bölümde ise sırasıyla cihazlar ve mobil uygulamalar ele alınmıştır.

Supen T500 & FitPro

FitPro'nun üyelik oluşturma ve giriş yapmada ciddi zayıflıkları tespit edilmiştir. Uygulamada hesap oluşturulurken parola olarak "123456789" girdisi kabul edilmektedir. Giriş yapılırken ise 2FA (Two Factor Authentication – İki Adımlı Doğrulama) önlemi bulunmamaktadır. Bu da (ilerleyen aşamalarda gösterileceği üzere) MITM saldırısından elde edilecek giriş bilgileriyle oturum açılabilmesine neden olmaktadır. Şekil 3'te FitPro uygulamasının AndroidManifest.xml dosyasında, uygulamanın yüklendiğinde telefonda eriştiği alanlar görünmektedir.



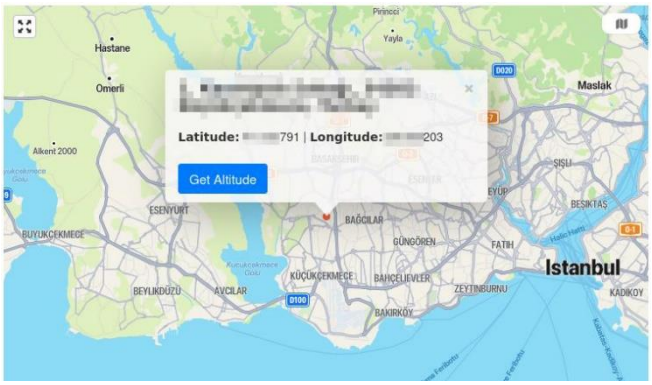
Şekil 3. FitPro uygulamasının AndroidManifest.xml dosyasında, uygulamanın yüklendiğinde telefonda eriştiği alanlar.

Supen T500 akıllı saati, telefonla bağlantısını FitPro uygulamasıyla bluetooth ağı üzerinden sağlamaktadır. Telefonun bluetooth'u kapatılmasına rağmen akıllı saat üzerinden (bluetooth bağlıyken) alınan SMS görüntülenebilmektedir. Yapılan denemelerde yalnızca son gönderilen SMS'nin varlığına ulaşılmıştır. Cihaz, kapatılıp açıldığında ise yine son SMS görüntülenmektedir. Buradan ise cihazın kendi üzerinde ayrıca veri tuttuğu bir depolama alanı olduğu sonucuna varılabilmektedir. Şekil 4'te akıllı saate gelen son SMS'nin, saatin hafızasında tutulduğu ve yeni gelen SMS'nin ise bir öncekinin üzerine yazıldığı görülmektedir. Nitekim donanımsal olarak cihazın hafıza yongasında veri saklanabilmektedir ve daha fazla bilgi edinmek chip-off teknikleriyle mümkün olabilmektedir.

Şekil 4. Akıllı saate gelen SMS görüntüsü.

Uygulamanın, cihazdan aldığı konum bilgisi ile oldukça isabetli yer tespiti yapabildiği uygulamalı olarak görülmüştür. Şekil 5'te görüldüğü üzere koordinatlar, FitPro uygulamasının Android içinde tuttuğu veri tabanından manuel olarak SQLite Browser ile edinilmiştir. Şekil 6'da görüldüğü üzere, haritaya yaklaşıldığında uygulamanın, yüklü olduğu cihazın konumundaki bina bilgisine kadar doğru tespit ettiği sonucuna varılmıştır.

Şekil 5. Akıllı telefon koordinatları.



Şekil 6. Uygulamanın yüklü olduğu cihazın konumu.

Bu bilgilerin yanı sıra veri tabanında kullanıcının temel bilgileri de bulunmaktadır. Temel bilgiler, adli bilişim sürecinde cihaza el koyulduğunda dijital kanıt olarak değerlendirilebilir. Her dijital kanıtta olduğu gibi manipüle edilme olasılığı da göz önünde bulundurulmalıdır.

İncelenen bu modeldeki akıllı saatte yer alan sensörler, doğrudan kullanıcının derisi ile temas ettiğinden kişinin sağlığına yönelik hassas verileri de doğrudan toplayabilmektedir.

Önceki bölümlerde MITM saldırısı ile giriş bilgilerinin alınabileceğinden söz edilmişti. Akıllı saatin kullandığı mobil tarafta FitPro'nun, bu açıdan değerlendirmeye alındığında uygulama katmanı üzerinden HTTP protokolünü kullandığı görülmektedir. HTTP, kullanıcı ile sunucu arasındaki veri iletimini şifresiz olarak gerçekleştirmektedir. Böylece saldırgan, ağı dinleyerek (Şekil 7'de görüldüğü üzere) oturum bilgilerini ele geçirebilmektedir. Güvenli iletişimin sağlanması için SSL/TLS sertifikası kullanılmalıdır.

Şekil 7. Ağın dinlenmesiyle (packet sniffing) kişinin kullanıcı adı ve parolasının elde edilmesi.

"Password" alanında parola bilgisi açıkça görünmektedir. Ek olarak, bir parolanın birçok yerde kullanıldığı bir gerçektir. Siyahla üstü kapatılan yerde kullanıcının e-posta adresi yer almaktadır. E-posta ve sosyal medya hesaplarının parolaları da aynı olabilir.

SmartBerry & SeTracker2

SeTracker2 uygulaması, çoğunlukla çocuk saatlerinde tercih edilen bir mobil uygulamadır. Daha önceki teknik incelemelerde de bu uygulamayla sıklıkla karşılaşılmıştır. Dolayısıyla söz konusu şirket bazı açıkları zamanla giderse de bu durum genel zararı kapatmamakta, potansiyel güvenlik ve mahremiyet sorunlarını halen kullanıcısına

yaşatmaktadır. Şekil 8'de SeTracker2 uygulamasının AndroidManifest.xml dosyasında, uygulamanın yüklendiğinde telefonda eriştiği alanlar görünmektedir.

```
┌──(kali㉿msu)-[~/Desktop/SeTracker2]
└─$ cat AndroidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="h
droid" android:compileSdkVersion="29" android:compileSdkVersionCodename="10" pac
BuildVersionCode="29" platformBuildVersionName="10">
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="com.tgelec.setracker"/>
    <permission android:name="com.tgelec.setracker" android:protectionLevel="sig
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_CONFIGURATION"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.CAMERA"/>
```

Şekil 8. SeTracker2 uygulamasının AndroidManifest.xml dosyasında, uygulamanın yüklendiğinde telefonda eriştiği alanlar.

Bu bölümde bir önceki incelemeye ek olacak bilgiler aktarılacaktır. Özellikle saatin yapısı ve kabiliyetleri gereği mahremiyet konusuna odaklanılacaktır. Saati kullanan çocuk, tuvalete gittiğinde her zaman dikkatli olmayabilir. Bazı saatlerin su geçirmezlik özelliği dolayısıyla banyoda kolundan çıkarmayabilir. Ailesi tarafından bu konuda gerekli bilgilendirmeler titizlikle yapılsa dahi göz ardı edilme olasılığı oldukça yüksektir. Daha dikkatli ebeveyn ve çocukların yüksek olduğu varsayıldığı durumda bile, bir kişinin dahi bu durumdan olumsuz etkilenmesine ortam bırakılmamalıdır. Öz savunması ve bilinci yeteri kadar bulunmayan çocukları korumak bizlerin sorumluluğundadır. Nitekim böylesi mahrem görüntülerle çocuklara yönelik yapılan siber zorbalık ve şantajlar yaşandığı bilinmektedir. Şekil 9'da uygulama üzerinden verilen komut ile doğrudan saatin üzerindeki kameradan çekilen fotoğraflar görülmektedir.

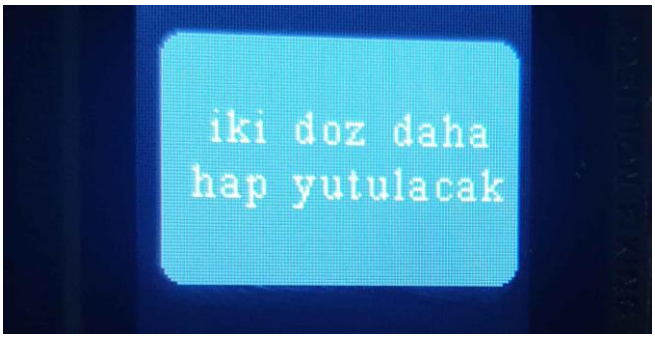
Şekil 9. Uygulama üzerinden verilen komut ile doğrudan saatin üzerindeki kameradan çekilen fotoğraflar.

Saatin kaybolması ya da çalınması durumunda ise içindeki bilgiler can sıkıcı sonuçlar doğurabilir. Bu durum bir adli bilişim sürecinde yararlı görünmektedir. Buna rağmen kötü niyetli kişilerin eline geçme olasılığı her zaman daha yüksektir. Fotoğrafların metadata verileri incelendiğinde ise EXIF (Exchangeable Image File Format-Değişebilir Görüntü Dosyası Biçimi) verilerinin tutulmadığı görülmüştür.

Yapılan denemelerde konum bilgisinin 15-20 dakika arasında gecikmeli olarak ekrana yansıdığı tespit edilmiştir.

Önceki bölümde MITM ile oturum bilgisinin ele geçirilebildiği gösterilmişti. Uygulamaya erişildikten sonra telefona mesaj gönderilebilmektedir. Akıllı saatler yalnızca çocukların izlenmesinde değil aynı zamanda hasta bireylerin sağlığıyla ilgili yardımcı olunması için de tercih edilmektedir.

Peki, kötü niyetli birisi uygulamaya eriştiğinde neler olabilir? Aşağıdaki görseldeki gibi doz artırımında bulunabilir. Şekil 10'da görüldüğü üzere SeTracker2 uygulaması üzerinden akıllı saate mesaj gönderildiğinde, bu mesaj ekrana sesli uyarıyla birlikte otomatik olarak düşmektedir.



Şekil 10. SeTracker2 uygulaması üzerinden akıllı saate mesaj gönderilmesi.

4. SONUÇLAR

Bu çalışmanın tamamı incelendiğinde, çocukların ve bakım gereksinimi duyan kişilerin güvenliği için yazılım güvenliği konusunu göz ardı eden cihazların tercih edilmemesi gerektiği sonucuna varılmaktadır. Elbette bu sonucun son kullanıcı için geçerli olduğu söylenebilir. Kamu otoritesinin ise konuyla ilgili denetim mekanizması oluşturması yönünde yaptırım gücü yüksek yapı oluşturması gerekmektedir. Nitekim üreticilerin birçoğu, sürümden maddi kazanç elde etmek uğruna kişisel mahremiyeti göz ardı etmekte, güvenliğe gerektiği önemi vermemektedir. Statista'nın yaptığı araştırmada, dünya genelinde akıllı saatten elde edilecek gelirin, yıllık %8,26 büyüme oranı göstermesi ve bunun sonucunda 2027 yılına kadar 61,69 milyar dolarlık bir pazar hacmine ulaşması beklenmektedir (Statista, 2023). 7$'a dahi satın alınabilen bu akıllı çocuk saatleri, güvenlik amacıyla alındığı halde, ters etkiyle kullanıcısına geri dönülemez zararlar verebilecek bir araca dönüşmektedir.

Yasal düzenlemelerin kapsayıcılığının olmasına ve güvenlik ile mahremiyet ihlallerinin yaşanmasına rağmen bu konuda kamuoyu ve araştırmaların azlığı ise dikkat çekicidir.

Ebeveynlerin ve hasta yakınlarının güvenlik ihtiyacını giderecek yeni bir çözüm üzerinde çalışılmasında yarar görülmektedir. Bu doğrultuda uygulanabilecek dört öneri bulunmaktadır:

1. *"Akıllı çocuk saati" adı altında satılan saatlerin satışının yasaklanması:* Türkiye'de gözetim ve denetim amacıyla kullanılan akıllı çocuk saatleri, hassas düzeydeki kişisel verilerin güvenliği ve kişi mahremiyetindeki ihlallere zemin hazırladığı gerekçesiyle satışı ve kullanımı (Almanya örneğinde olduğu gibi) yasaklanabilir. Buradan hareketle de bu çalışmanın ardılı olarak çocuklar ve bakım gereksinimi gereken hasta ve yaşlılar için güvenli bir iletişim modeli üzerine çalışılabilir.
2. *IoT cihazlarının tabi tutulacağı bir güvenlik sisteminin geliştirilmesi:* IoT cihazlarının yaygınlaşmasıyla birlikte ülkemize giren bu cihazların siber güvenlik testlerinden geçtikten sonra satışa sunulmasına yönelik bir yol izlenebilir. Böylece bir kalite standardı etiketi üzerinde çalışma yapılabilir. Nitekim özellikle sağlık sektöründe, giyilebilir teknolojiler oldukça fayda sağlamaktadır. Ayrıca sağlık verileri, oldukça hassas verileri içermektedir.
3. *Kamu bünyesinde siber güvenlik test merkezinin kurulması:* Bu konuda faaliyet gösteren kamu kurumlarının bünyesinde ekip kurulabilir. Türkiye'de siber güvenlik kapsamındaki görev ve sorumluklar T.C. Ulaştırma ve Altyapı Bakanlığındadır (T.C. Ulaştırma ve Altyapı Bakanlığı). 2018 yılında Cumhurbaşkanlığına bağlı olarak kurulan Dijital Dönüşüm Ofisi ise ülkemizde siber güvenlik faaliyetinde etkin konumdadır. İlaçların denetimden geçtikten sonra satışa sunulması çerçeve olarak örnek teşkil edebilir. Sağlık Bakanlığı bünyesindeki "İlaç Ruhsatlandırma Dairesi" (T.C. Sağlık Bakanlığı, 2023) bu aşamada yapı olarak ilişkilidir.
4. *Bireysel çalışmaların artırılması:* Bu öneri, alanla ilgili her bireyi ilgilendirmektedir. Özellikle ülkemizde siber güvenlik alanında lise ve yükseköğrenim düzeyinde eğitim gören kişiler bu konuya eğilebilir. Örneğin, Türkiye'nin ilk siber güvenlik lisesi olan Teknopark İstanbul MTAL öğrencileri, çevrelerinde satılan (zincir marketlerde satılanlar gibi) bu cihazları gönüllü olarak inceleyerek teknik rapor haline getirebilir ve yaygın platformlarda hem literatüre katkı sağlayabilir hem de toplumsal siber güvenlik direncinin artmasına katkıda bulunabilirler.

KAYNAKLAR

Al-Sharrah, M., Salman, A., & Ahmad, I. (2018). Watch Your Smartwatch. International Conference on Computing Cciences and Engineering (ICCSE). Kuwait City.

Saatjohann, C., Ising, F., Krings, L., & Schinzel, S. (2020). STALK: Security Analysis of Smartwatches for Kids. Proceedings of the 15th International Conference on Availability, Reliability and Security, (s. 1-10). Virtual Event, Ireland.

Shehata, S. M., El Fiky, A. H., Torky, M. S., Farag, T. H., & Abbas, N. A. (2020). Android Malware Prevention on Permission Based. International Journal of Applied Engineering Research, 15(1), s. 5-11.

İNTERNET KAYNAKLARI

Android Developers. Manifest Permission. 10 26, 2023 tarihinde https://developer.android.com/reference/android/Manifest.permission adresinden alındı.

Annelere Sor. 10 25, 2023 tarihinde https://anneleresor.com/qa/1-sinifa-giden-cocugumun-ogretmeni-okulda-akilli-saat-istemiyor-8468 adresinden alındı.

Bundesnetzagentur. (2017, 11 17). Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor. 10 29, 2023 tarihinde https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/17112017_Verbraucherschutz.html adresinden alındı.

Demand Sage. (2023). Smartwatch Statistics 2023: How Many People Use Smartwatches? 10 26, 2023 tarihinde https://www.demandsage.com/smartwatch-statistics/ adresinden alındı.

European Commission. (2020). Product-based Case Studies: Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment. 5 6, 2023 tarihinde https://ec.europa.eu/docsroom/documents/40763/attachments/6/translations/en/renditions/pdf adresinden alındı.

Ken, M. (2018, 11 15). Consumer Advice: Kids GPS tracker watch security. (Pen Test Partners) 5 6, 2023 tarihinde https://www.pentestpartners.com/security-blog/consumer-advice-kids-gps-tracker-watch-security/ adresinden alındı.

Kişisel Verilerin Korunması Kanunu. (2016, 4 7). 10 26, 2023 tarihinde https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 adresinden alındı.

MEB. Milli Eğitim Bakanlığı Ortaöğretim Kurumları Yönetmeliği. 10 24, 2023 tarihinde https://ogm.meb.gov.tr/meb_iys_dosyalar/2017_09/20161748_MYLLY_EYYTYM_BAKANLIYI_ORTAYYRETYM_KURUMLARI_YYNETMELYYY.pdf adresinden alındı.

MITRE Corporation. CVE-2019-20468. 10 25, 2023 tarihinde https://www.cve.org/CVERecord?id=CVE-2019-20468 adresinden alındı.

Norwegian Consumer Council. (2017). Analysis of Smartwatches for Children. 5 5, 2023 tarihinde https://storage02.forbrukerradet.no/media/2017/10/watchout-rapport-october-2017.pdf adresinden alındı.

OWASP. OWASP Mobile Top 10. 10 22, 2023 tarihinde https://owasp.org/www-project-mobile-top-10/ adresinden alındı.

Statista. (2023). Number of users of smartwatches worldwide from 2018 to 2027. 10 26, 2023 tarihinde https://www.statista.com/forecasts/1314339/worldwide-users-of-smartwatches adresinden alındı.

Statista. Smartwatches - Worldwide | Statista Market Forecast. 10 28, 2023 tarihinde alındı.

Stykas, V. (2020, 7 9). Hacking smart devices to convince dementia sufferers to overdose. (Pen Test Partners) 5 6, 2023 tarihinde https://www.pentestpartners.com/security-blog/hacking-smart-devices-to-convince-dementia-sufferers-to-overdose/ adresinden alındı.

T.C. Sağlık Bakanlığı. İlaç Ruhsatlandırma. 10 30, 2023 tarihinde https://www.titck.gov.tr/faaliyetalanlari/ilac/ilac-ruhsatlandirma adresinden alındı.

T.C. Ulaştırma ve Altyapı Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. 5 8, 2023 tarihinde http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf adresinden alındı.

Türk Ceza Kanunu. 10 24, 2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf adresinden alındı.

TEŞEKKÜR ve BEYANLAR

Yazarlar çalışmaya eşit oranda katkı sağlamıştır. Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır. Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.