Görünmeyeni Görmek: Bluetooth ve IoT Sistemlerinde Siber Tehditler

Bluetooth Teknolojisi ve Çalışma Prensibi

•Bluetooth Nedir?

- **Bluetooth**, cihazlar arasında **kısa mesafede kablosuz veri iletimi** sağlayan bir teknolojidir.
- Amaç: Kablo karmaşasını azaltmak ve düşük güçle cihazları birbirine bağlamak.
- Tipik menzili: 10 metre (class 2 cihazlar için), bazı cihazlarda 100 metreye kadar çıkabilir.

•Bluetooth Nasıl Çalışır?

- Bluetooth, **2.4 GHz ISM bandında (endüstriyel, bilimsel, medikal) çalışır**.
- Cihazlar, **master ve slave (şef ve yardımcı) ilişkisiyle** birbirine bağlanır.
- Bir master cihaz, aynı anda 7'ye kadar slave cihazı kontrol edebilir — bu yapıya **piconet** denir.
- Veri iletimi için **frekans atlamalı yayılım spektrumu (FHSS)** kullanılır; yani veri paketleri farklı frekanslarda kısa sürelerle gönderilir. Bu, parazit ve dinlemeye karşı koruma sağlar.
- Bağlantı kurulurken cihazlar eşleşir (pairing), şifreleme ve kimlik doğrulama devreye girer.

Kısa Mesafe Kablosuz İletişim Mantığı

- Bluetooth, **düşük güç tüketimiyle kısa mesafede hızlı iletişim** sağlar.
- Genelde **kulaklıklar, klavyeler, fareler, sağlık cihazları, telefonlar, araç içi sistemler** gibi cihazlarda kullanılır.
- Kısa menzil sayesinde daha az enerji harcar ve gizliliği artırır.

BLE (Bluetooth Low Energy) Farkı

- **BLE**, 2010'larda tanıtılan yeni nesil Bluetooth standardıdır.
- **Düşük güç tüketimi** odaklıdır; pil ömrünü aylar hatta yıllarca uzatabilir.
- BLE, **sensörler, giyilebilir cihazlar, IoT ürünleri** için idealdir.
- Veri iletim hızı, klasik Bluetooth'a göre daha düşüktür ama enerji verimliliği çok yüksektir.
- BLE'de bağlantı süresi çok kısadır, cihazlar hızlıca uyanıp veri gönderip tekrar uyku moduna geçer.

Klasik Bluetooth ile BLE Arasındaki Temel Farklar

Özellik	*Klasik Bluetooth*	*Bluetooth Low Energy (BLE)*
Enerji Tüketimi	Orta-yüksek	Çok düşük
Veri Hızı	Yüksek (1-3 Mbps)	Daha düşük (~1 Mbps)
Bağlantı Süresi	Uzun	Çok kısa
Kullanım Alanı	Ses, dosya transferi	Sensörler, IoT, giyilebilir
Menzil	10-100 metre	Benzer

Bluetooth Güvenlik Tehditleri

Bluejacking

- Bluetooth açık cihazlara **izinsiz mesaj gönderme saldırısıdır**.
- Mesajlar genellikle spam, reklam veya zararsız bildirimlerdir.
- Tehdit daha çok rahatsızlık verir, doğrudan veri hırsızlığı içermez.

Bluesnarfing

- Yetkisiz şekilde bir cihazın **rehber, takvim, SMS gibi kişisel verilerine erişim** sağlama saldırısıdır.
- Cihazın Bluetooth güvenlik zafiyetlerinden yararlanır.
- Ciddi gizlilik ihlalidir.

Bluebugging

- Bluetooth bağlantısını kullanarak cihaza **uzaktan komut çalıştırma saldırısıdır**.
- Saldırgan cihazın kontrolünü ele geçirip arama yapabilir, mesaj gönderebilir veya kişisel bilgilere ulaşabilir.
- En tehlikeli Bluetooth saldırılarından biridir!

Gerçek Hayattan Bluetooth Saldırı Vaka Örnekleri

1. BlueBorne Saldırısı (2017)

- Armis Labs tarafından keşfedildi.
- Android, Windows, Linux ve iOS dahil **milyonlarca cihazı etkileyen** 8 farklı açık içeriyordu.
- Cihaza **Bluetooth açıkken** ve kullanıcı hiçbir işlem yapmadan, sadece menzilde olmasıyla bile sızılabiliyordu.
- Saldırgan, hedef cihazı **uzaktan kontrol edebiliyor**, veri çalabiliyor, virüs bulaştırabiliyordu.
- **Çok kritik:** İnternet bağlantısına bile ihtiyaç yoktu!
- ⚠️ Bu olaydan sonra birçok cihaz üreticisi Bluetooth güncellemeleri yayınladı.

2. BLESA (Bluetooth Low Energy Spoofing Attack) – (2020)

- BLE protokolündeki bir açıklığı kullanan bu saldırıda, cihazlar bağlantıyı zaten tanıdığı bir cihaza yaptığını sanıyor ama saldırgana bağlanıyor.
- Özellikle IoT cihazlar ve sağlık sistemlerinde büyük risk yarattı.
- Cihaz, sahte verileri “güvenli” zannederek işliyor.

Tesla Model X – BLE Üzerinden Araç Hırsızlığı (2020)

- Güvenlik araştırmacısı Lennert Wouters, Tesla Model X'in **Bluetooth tabanlı anahtar sistemini hackledi.**
- BLE aracılığıyla anahtarı kandırarak **aracı açıp çalıştırdı**.
- Tesla hızlıca yazılım güncellemesi yayınladı.

Bluetooth Güvenliğini Sağlama Yöntemleri

- ***Pairing (Eşleştirme) Yöntemleri***
- Bluetooth cihazlar, iletişim kurmadan önce **eşleşme *(pairing)*** sürecinden geçer. Bu süreçte kullanılan yöntemler güvenliği doğrudan etkiler:
- ***Just Works:***
  - Kullanıcı onayı olmadan otomatik eşleşir.
  - En az güvenli yöntemdir.
  - IoT cihazlarda yaygın ama tehlikelidir.
- ***Passkey Entry (Şifre Girişi):***
  - Cihazlar arasında 6 haneli bir şifre girilir veya doğrulanır.
  - MITM (ortadaki adam) saldırılarına karşı dayanıklıdır.
- ***Numeric Comparison:***
  - Ekranlı cihazlarda aynı sayıyı görüp eşleştirme yapılır.
  - En güvenli yöntemlerden biridir.
- ***Out-of-Band (OOB):***
  - NFC, QR kod, USB gibi alternatif yollarla eşleştirme yapılır.
  - Gelişmiş sistemlerde tercih edilir.
  - ⚠️ ***Bluetooth 4.2 ve sonrası cihazlar, Secure Simple Pairing (SSP) desteğiyle daha güvenli eşleşme yöntemlerini kullanır.***

Şifreleme ve Kimlik Doğrulama

- Tüm veri aktarımı **AES-CCM (Counter with CBC-MAC)** gibi şifreleme algoritmalarıyla korunmalı.
- Bluetooth cihazları **her eşleşme sırasında geçici anahtarlar** üretmeli.
- **Kimlik doğrulama (authentication)**, cihazların gerçekten kim olduklarını kanıtlamasını sağlar.
- BLE'de kullanılan "bonding" (kalıcı eşleşme) yöntemleri, hem şifrelemeyi hem de kimlik doğrulamayı içerir.
- 📌 ***Not:** Şifreleme sadece bağlantı esnasında değil, eşleşme sürecinde de yapılmalı, yoksa saldırgan oraya sızabilir.*

Cihaz Görünürlüğü

- Bluetooth cihazlar genellikle "**discoverable (keşfedilebilir)**" modda bırakılıyor. Bu ciddi bir risktir!
- ***Güvenlik için:***
  - Kullanım dışında **Bluetooth kapalı olmalı**.
  - Gerekmedikçe **keşfedilebilir mod kapalı olmalı**.
  - Cihaz adı, üretici ve tür gibi bilgiler **gizlenmeli veya rastgeleleştirilmeli**.

Yazılım ve Firmware Güncellemeleri

- Bluetooth yongaları veya sürücüleri zamanla güvenlik açıkları barındırabilir (örneğin: BlueBorne).
- Üreticilerin sunduğu **firmware güncellemeleri** mutlaka düzenli yapılmalı.
- Cihazlar mümkünse **OTA (Over-the-Air)** güncelleme desteği sunmalı.
- IoT cihazlarında güncelleme mekanizması yoksa, bu büyük bir risktir!

✅ *Kural Başlığı*	💬 *Açıklama*
Bluetooth'u İhtiyacın Yoksa Kapat!	Boş yere açık bırakmak, cihazını gereksiz risklere maruz bırakır. Kullanmadığın zaman kapat!
Cihazını "Keşfedilebilir" Modda Bırakma!	Pairing bittikten sonra "discoverable" modu mutlaka kapat. Aksi takdirde herkes cihazını görebilir.
Güçlü Eşleşme Yöntemlerini Tercih Et!	"Just Works" yerine **Passkey Entry**, **Numeric Comparison** veya **OOB** yöntemlerini kullan.
Tanımadığın Cihazlarla Eşleşme!	Her bağlantı isteğine "evet" deme. Saldırgan cihazlar bu şekilde bağlantı kurmaya çalışabilir.
Cihaz ve Yazılım Güncellemelerini Yap!	Bluetooth sürücülerindeki açıklar düzenli güncellemelerle kapatılır. Firmware'leri güncel tut.
MAC Adres Randomizasyonunu Aç!	Aynı MAC adresiyle dolaşmak seni izlenebilir yapar. Yeni cihazlar bu özelliği destekler.
Ortak Alanlarda Dikkatli Ol!	Kafe, AVM gibi yerlerde Bluetooth'u kapalı tut. Kalabalık ortamlarda saldırı riski artar.

IoT(Internet of Things)Nedir?

- Nesnelerin İnterneti (IoT), günlük hayatımızdaki fiziksel nesnelerin internet ağına bağlanarak birbirleriyle veri alışverişinde bulunmalarını sağlayan yenilikçi bir teknolojidir. Bu teknoloji sayesinde, sensörler, cihazlar, araçlar ve diğer elektronik sistemler kendi aralarında iletişim kurar, çevrelerinden topladıkları bilgileri işler ve uzaktan kontrol edilebilir hale gelir. IoT, sadece cihazların internete bağlanması değil, aynı zamanda bu bağlantı üzerinden otomasyon, analiz ve daha akıllı karar mekanizmalarının oluşturulmasını da mümkün kılar. Böylece, insanların hayatını kolaylaştıran, iş süreçlerini optimize eden ve çeşitli sektörlerde verimliliği artıran geniş kapsamlı bir ekosistem ortaya çıkar.

IoT Sistemlerinin Temel Bileşenleri

- **Cihazlar (Things):** Sensörler, aktüatörler, gömülü sistemler gibi fiziksel nesneler.
- **Bağlantı:** Cihazların internete ya da yerel ağa bağlanmasını sağlayan Wi-Fi, Bluetooth, ZigBee gibi protokoller.
- **Veri İşleme:** Toplanan verilerin analiz edildiği bulut veya yerel sunucular.
- **Kullanıcı Arayüzü:** Verilerin kullanıcıya gösterildiği uygulamalar veya web portalları.

IoT Kullanım Alanları

- ***Akıllı Ev Sistemleri:*** Evlerde aydınlatma, ısıtma, güvenlik ve enerji yönetimi gibi sistemlerin otomatik ve uzaktan kontrolü.
- ***Endüstriyel Otomasyon:*** Fabrikalarda makinelerin, sensörlerin ve üretim süreçlerinin izlenmesi ve optimize edilmesi.
- ***Sağlık Hizmetleri:*** Hastaların uzaktan takibi, medikal cihazların yönetimi ve sağlık verilerinin anlık analizi.
- ***Tarım:*** Toprak, hava ve bitki sağlığı verilerinin sensörlerle izlenerek verimli ve sürdürülebilir tarım uygulamalarının desteklenmesi.
- ***Akıllı Şehirler:*** Trafik yönetimi, kamu güvenliği, atık toplama ve enerji dağıtımının akıllı sistemlerle optimize edilmesi.
- ***Lojistik ve Taşımacılık:*** Ürünlerin ve araçların konum takibi, sıcaklık kontrolü ve rota optimizasyonu.

IoT Sistemlerinde Güvenlik Neden Önemlidir?

IoT Cihazlarının Yaygınlığı

- IoT cihazları hızla yaygınlaşıyor ve hayatımızın her alanına entegre oluyor. Milyarlarca cihaz internete bağlı ve her geçen gün bu sayı artıyor. Bu yaygınlık, güvenlik açıklarının daha büyük etki yaratabileceği anlamına geliyor.

Saldırı Yüzeyinin Genişliği

- Her yeni IoT cihazı, potansiyel bir saldırı noktası oluşturuyor. Zayıf korunan cihazlar, ağlara sızma, veri hırsızlığı ve hizmet aksatma saldırıları için kapı aralıyor. Geniş cihaz ağı, saldırganlara daha fazla fırsat sunuyor.

Gerçek Hayattan Güvenlik İhlalleri Örnekleri

- IoT cihazlarına yönelik birçok yüksek profilli saldırı gerçekleşti. Örneğin, Mirai botnet saldırısı milyonlarca cihazı ele geçirip büyük çaplı DDoS saldırıları yaptı. Ayrıca ev ve endüstriyel cihazlarda yaşanan güvenlik açıkları, veri ihlallerine ve maddi kayıplara yol açtı.

IoT Güvenlik Gereksinimleri

- *Kimlik Doğrulama*
- *Yetkilendirme*
- *Veri Şifreleme*
- *Güncelleme Mekanizması*
- *Fiziksel Güvenlik*
- *Ağ Güvenliği*
- *Günlükleme ve İzleme*
- *Gizlilik*
- *Saldırı Tespiti ve Önleme*
- *Güvenli Yazılım Geliştirme*

Kimlik Doğrulama

IoT cihazları ve kullanıcıların kimlikleri, güçlü yöntemlerle doğrulanmalıdır. Bu, kötü niyetli kişilerin yetkisiz erişimini engeller ve sistemin güvenliğini sağlar.

Yetkilendirme

Doğrulama sonrası, her kullanıcının veya cihazın sadece yetkisi dahilinde kaynaklara erişmesi gerekir. Bu sınırlandırma, veri ve sistemlerin korunmasında kritik rol oynar.

Veri Şifreleme

IoT cihazları tarafından üretilen veriler, hem iletim hem de depolama aşamalarında şifrelenmelidir. Bu sayede hassas bilgiler dış müdahalelere karşı korunur.

Güncelleme Mekanizması

Cihazların yazılım güncellemeleri, güvenli ve doğrulanabilir kanallardan yapılmalıdır. Böylece bilinen güvenlik açıkları kapatılarak saldırı riskleri azaltılır.

Fiziksel Güvenlik

IoT cihazları, fiziksel müdahalelere karşı dayanıklı olmalı ve izinsiz erişimler engellenmelidir. Bu, cihazın güvenliğinin sağlanmasında ilk savunma hattıdır.

Ağ Güvenliği

Cihazların bağlı olduğu ağlar, güvenlik protokolleri ve erişim kontrolleriyle korunmalıdır. Güvenli ağ yapısı, dış saldırıları engeller ve veri bütünlüğünü sağlar.

Günlükleme ve İzleme

Cihaz faaliyetleri kaydedilmeli ve sürekli izlenmelidir. Anormal veya şüpheli aktiviteler hızlıca tespit edilip müdahale edilmelidir.

Gizlilik

Kullanıcıların kişisel verileri korunmalı, veri toplama ve işleme süreçlerinde yasal düzenlemelere uyulmalıdır. Gizlilik ihlalleri hem hukuki hem de etik sorunlara yol açar.

Saldırı Tespiti ve Önleme

IoT ağlarında ve cihazlarında kötü niyetli aktiviteler tespit edilmeli ve engellenmelidir. Bu sayede sistemin sürekliliği ve güvenliği sağlanır.

Güvenli Yazılım Geliştirme

IoT uygulamaları, güvenlik açıklarını en aza indirmek için standartlara uygun olarak geliştirilmelidir. Kodlama hataları, saldırganlar için kolay hedef oluşturur.

IoT Güvenliğini Tehdit Eden Unsurlar

Donanım Açıkları

Cihazların fiziksel bileşenlerindeki zayıflıklar, saldırganların cihaza doğrudan erişmesine veya manipülasyon yapmasına olanak tanır.

Yazılım Zafiyetleri

Eski, güncellenmemiş veya hatalı yazılımlar, kötü amaçlı yazılımlar ve saldırılar için açık kapı oluşturur.

Zayıf Parola Kullanımı

Basit veya varsayılan parolalar, cihazların kolayca ele geçirilmesine neden olur.

Varsayılan Ayarlar

Cihazların fabrika ayarları çoğunlukla güvenlik açısından zayıftır ve değiştirilmediğinde risk oluşturur.

Açık Portlar ve Servisler

Gereksiz açık portlar ve çalışan servisler, siber saldırganların sisteme sızması için fırsat yaratır.

IoT Güvenliğinde Kullanılan Savunma Yöntemleri

Savunma Yöntemi	*Açıklama*
Sertifikaya Dayalı Kimlik Doğrulama	Cihazlar, birbirlerini dijital sertifikalarla tanır. Parola yerine daha güvenli bir doğrulama sağlar.
Güvenli Boot ve Firmware Doğrulama	Cihaz sadece imzalanmış yazılımı çalıştırır. Zararlı firmware'lerin yüklenmesini engeller.
Güvenli Ağ Segmentasyonu	IoT cihazları izole edilmiş ağlarda çalışır. Saldırıların tüm sisteme yayılması önlenir.
OTA (Over-the-Air) Güncellemeleri	Cihazlar uzaktan güvenli şekilde güncellenir. Yeni güvenlik yamaları uygulanır.
IDS/IPS Sistemleri	Ağdaki tehditleri tespit eder (IDS) ve engeller (IPS). Gerçek zamanlı koruma sağlar.
Güvenlik Testleri ve Penetrasyon Testi	Sistemler düzenli olarak test edilir. Güvenlik açıkları belirlenip kapatılır.

IoT Güvenliği için Standartlar ve Rehberler

Standart / Rehber	*Açıklama*	*Uygulama Örneği*
OWASP IoT Top 10	IoT cihazlarında en sık karşılaşılan 10 güvenlik açığını listeler. Geliştiricilere risk önceliği sağlar.	Kamera üreticisi, zayıf parola kullanımını engeller ve şifreli güncelleme sistemi ekler.
NIST IoT Rehberleri	IoT güvenliği için kapsamlı çerçeveler sunar. Risk analizi, veri koruması ve erişim kontrolü içerir.	Hastane, hasta takibi yapan cihazlara veri şifreleme ve erişim kontrolü uygular.
ETSI EN 303 645	Tüketici IoT cihazları için minimum güvenlik gereksinimlerini tanımlar. AB standartlarına yön verir.	Akıllı priz firması, ilk kullanımda parola değişimini zorunlu kılar.
ISO/IEC 27030	IoT sistemlerini bilgi güvenliği yönetimiyle entegre etmeye yönelik uluslararası standarttır.	Enerji şirketi, IoT cihazlarını merkezi şekilde yönetip izler ve ISO'ya uygun hale getirir.

Sonuç ve Öneriler

•IoT teknolojileri hayatımızı kolaylaştırsa da güvenlik riskleri büyük önem taşır. Bu yüzden IoT sistemleri baştan sona güvenlik odaklı tasarlanmalı ve güçlü kimlik doğrulama, veri şifreleme, düzenli güncellemeler gibi önlemler mutlaka uygulanmalıdır.

- Fiziksel güvenlik ve ağ izleme de unutulmamalı; siber saldırılar giderek karmaşıklaşıyor ve IoT cihazları hedef alıyor. Uluslararası standartlara uyum ve düzenli güvenlik testleri, sistemlerin sağlamlığını artırır.
- Ayrıca kullanıcıların bilinçlendirilmesi ve güvenlik politikalarının etkin uygulanması, IoT güvenliğinin önemli parçalarıdır.

Kaynakça

- *Bluetooth SIG, "Bluetooth Core Specification Version 5.2," 2020.*
- *Bluetooth SIG, "Bluetooth Security Overview," https://www.bluetooth.com/specifications/bluetooth-core-specification/*
- *A. Rahman, Bluetooth Essentials for Programmers, Apress, 2015.*
- *J. Granjal, E. Monteiro, J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, 2015, pp. 1294–1312.*
- *C. Gomez, J. Oller, J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," Sensors, vol. 12, no. 9, 2012, pp. 11734-11753.*
- *M. Conti, A. Dehghantanha, K. Franke, S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, 2018, pp. 544-546.*