Nesnelerin İnterneti ve Güvenlik

PELIN ANGIN

METU WIRELESS SYSTEMS, NETWORKS AND CYBERSECURITY LAB,

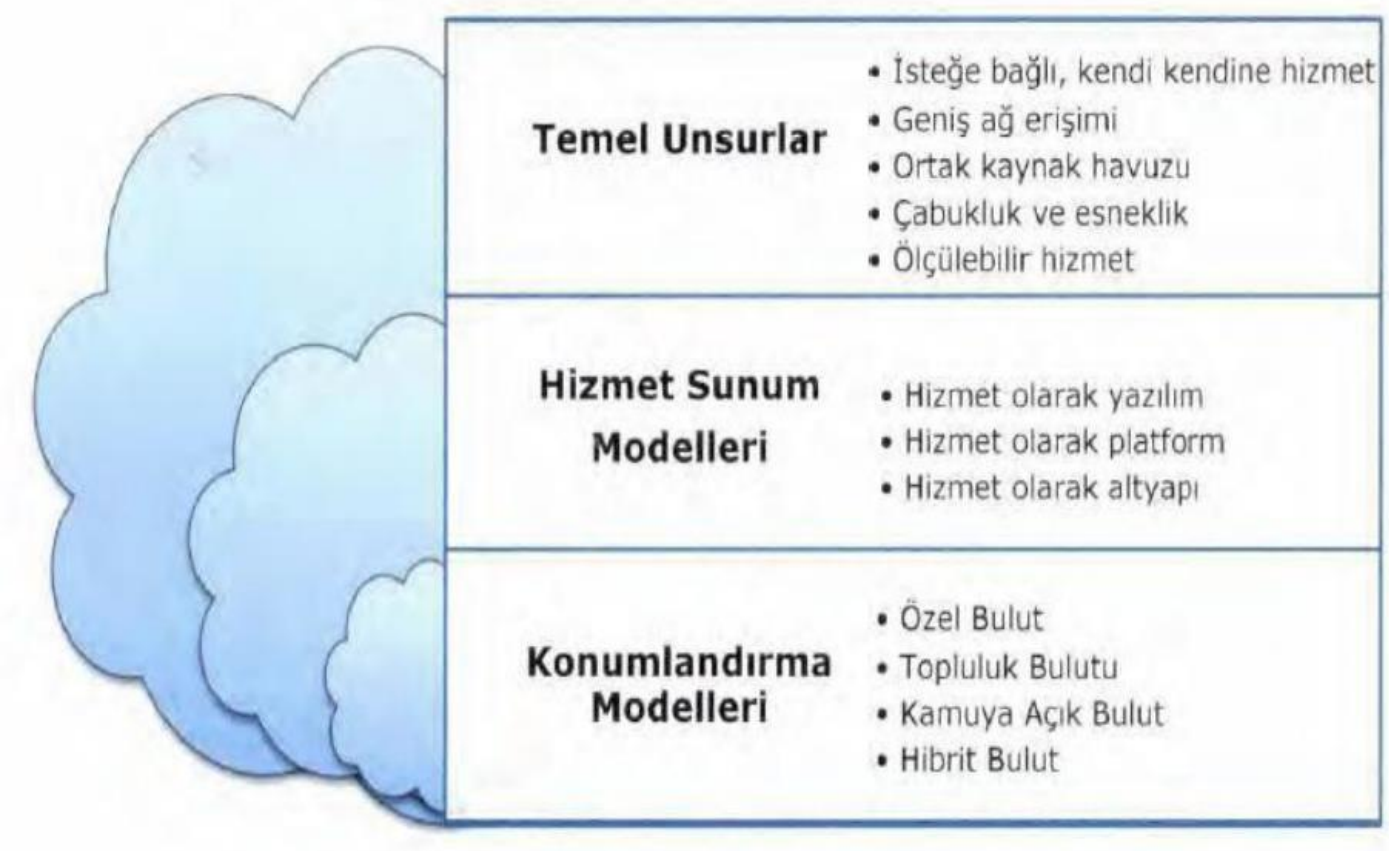
METU SYSTEMS SECURITY RESEARCH LAB

24.11.2018

BULUT BİLİŞİM NEDİR?

“Bulut bilişim, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza, uygun koşullarda ve isteğe bağlı olarak her zaman, her yerden erişime imkân veren bir modeldir. Söz konusu kaynaklar (bilgisayar ağları, sunucular, veri tabanları, uygulamalar, hizmetler vb.) asgari düzeyde yönetimsel çaba ve hizmet alıcı-hizmet sağlayıcı etkileşimi gerektirecek kolaylıkta tedarik edilebilmekte ve elden çıkarılabilmektedir. Bu model erişilebilirliği desteklemekte ve gösterilen, beş temel unsur, üç hizmet sunum modeli ve dört konumlandırma (deployment) modelini kapsamaktadır.” (NIST, 2009)

BULUT BİLİŞİM BİLEŞENLERİ



Kaynak: NIST, 2009

BULUT BİLİŞİM TEMEL ÖZELLİKLERİ

- Hızlı esneklik
- Talebe bağlı self-servis
- Geniş ağdan erişim
- Kaynak paylaşımı
- Ölçülebilir hizmet

TEMEL HİZMET MODELLERİ

- SaaS (Software as a Service) – Hizmet olarak yazılım: Servis sağlayıcı tarafından sunucu üzerinde bulundurulan yazılım uygulamasının birden fazla kişi ve kuruluşa kullanıma sunulmasıdır.
- PaaS (Platform as a Service) – Hizmet olarak platform: Servis sağlayıcı tarafından müşteriye kendi uygulamasını geliştirip, çalıştırabileceği bir platform ile tamamlayıcı servislerin ve gerekli teknolojik altyapının sunulmasıdır.
- IaaS (Infrastructure as a Service) – Hizmet olarak altyapı: Müşterinin ihtiyaç duyduğu temel bilişim kaynaklarını kendisinin yapılandırabilmesi ve bunların üzerine ihtiyacı olan işletim sistemi ve uygulamaları kurabilmesidir.

Kaynak: https://www.btk.gov.tr/uploads/pages/slug/bulut-bilisim.pdf

BULUT BİLİŞİM AVANTAJLARI

- Düşük donanım maliyeti
- Gelişmiş performans
- Düşük yazılım maliyeti
- Anında güncelleme
- Sınırsız depolama kapasitesi
- Grup çalışması
- Kaynakların etkin kullanımı

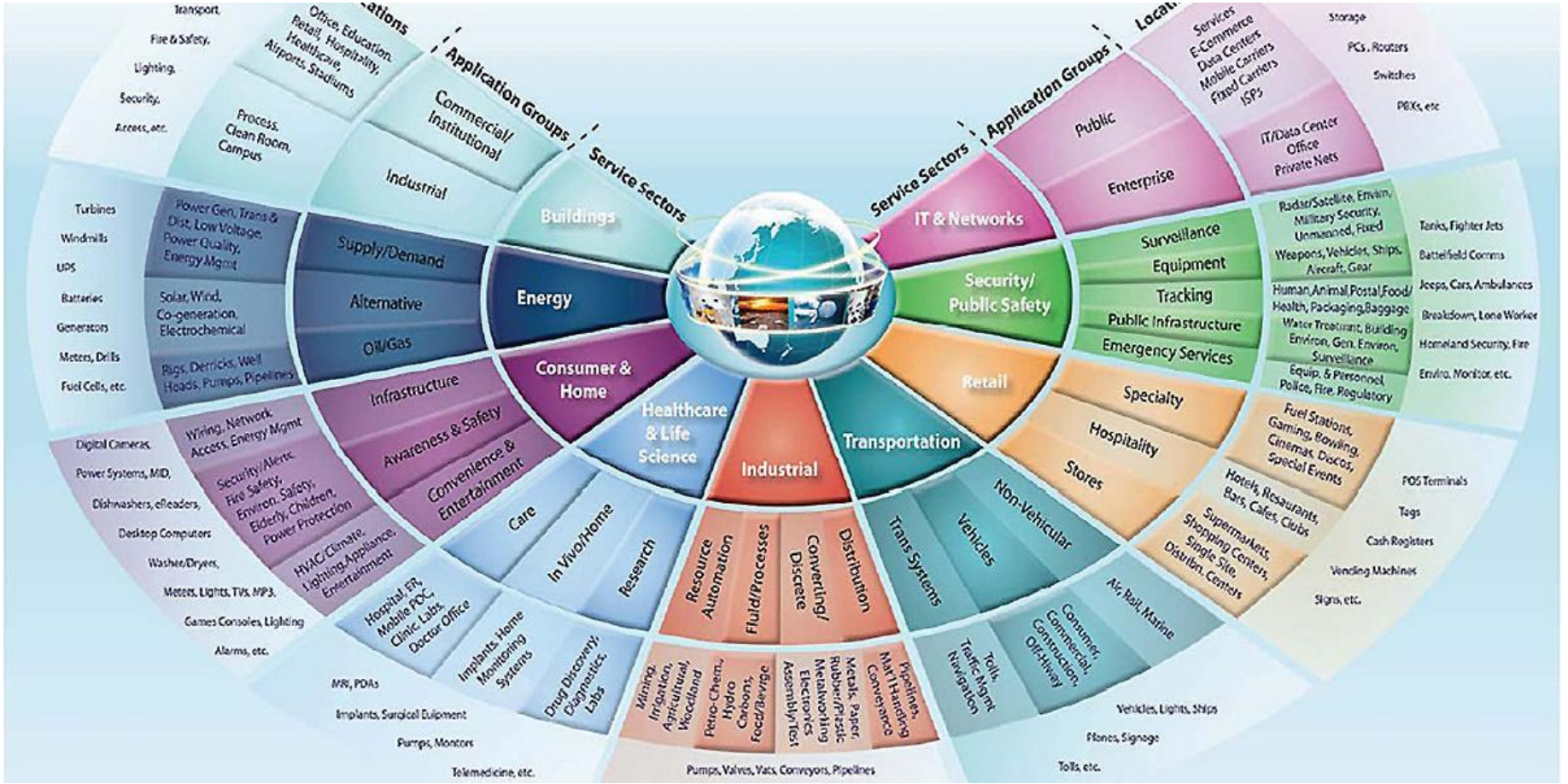
NESNELERİN İNTERNETİ (IoT)

Kaynak: https://www.jigsawacademy.com/iot/

NESNELERİN İNTERNETİ (IoT)

- Kevin Ashton tarafından 1999 yılında ortaya atılan bir kavram - başta RFID etiketleri sayesinde radyo frekansı üzerinden birbirleriyle haberleşen cihazları kapsıyordu
- Bugün çok daha geniş bir alana sahip
- IoT evimizdeki eşyaları, yoldaki trafik ışıklarını, fabrikalarda üretim yapan makinaları, sağlık cihazlarını... kapsıyor
- Nesneler düşünüyor ve karar veriyor

IoT Sektörleri

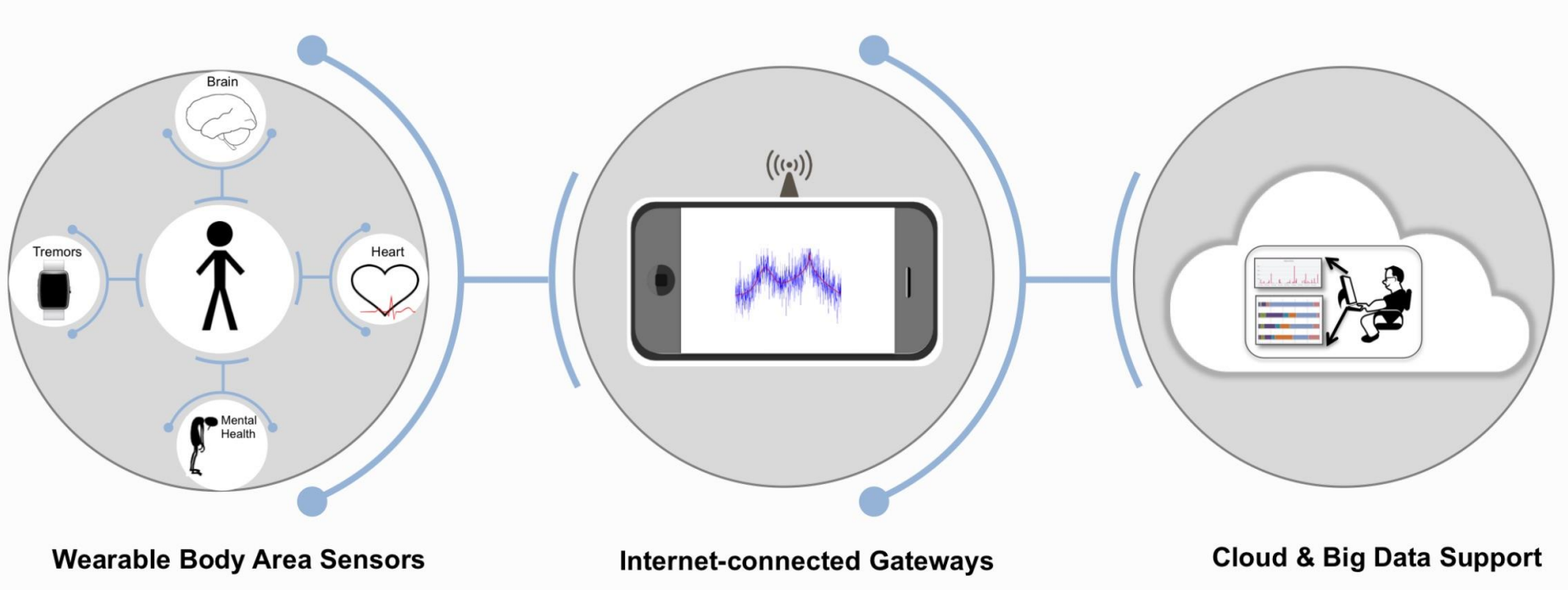


https://gernotkapteina.com/2015/08/31/iot-internet-of-things/

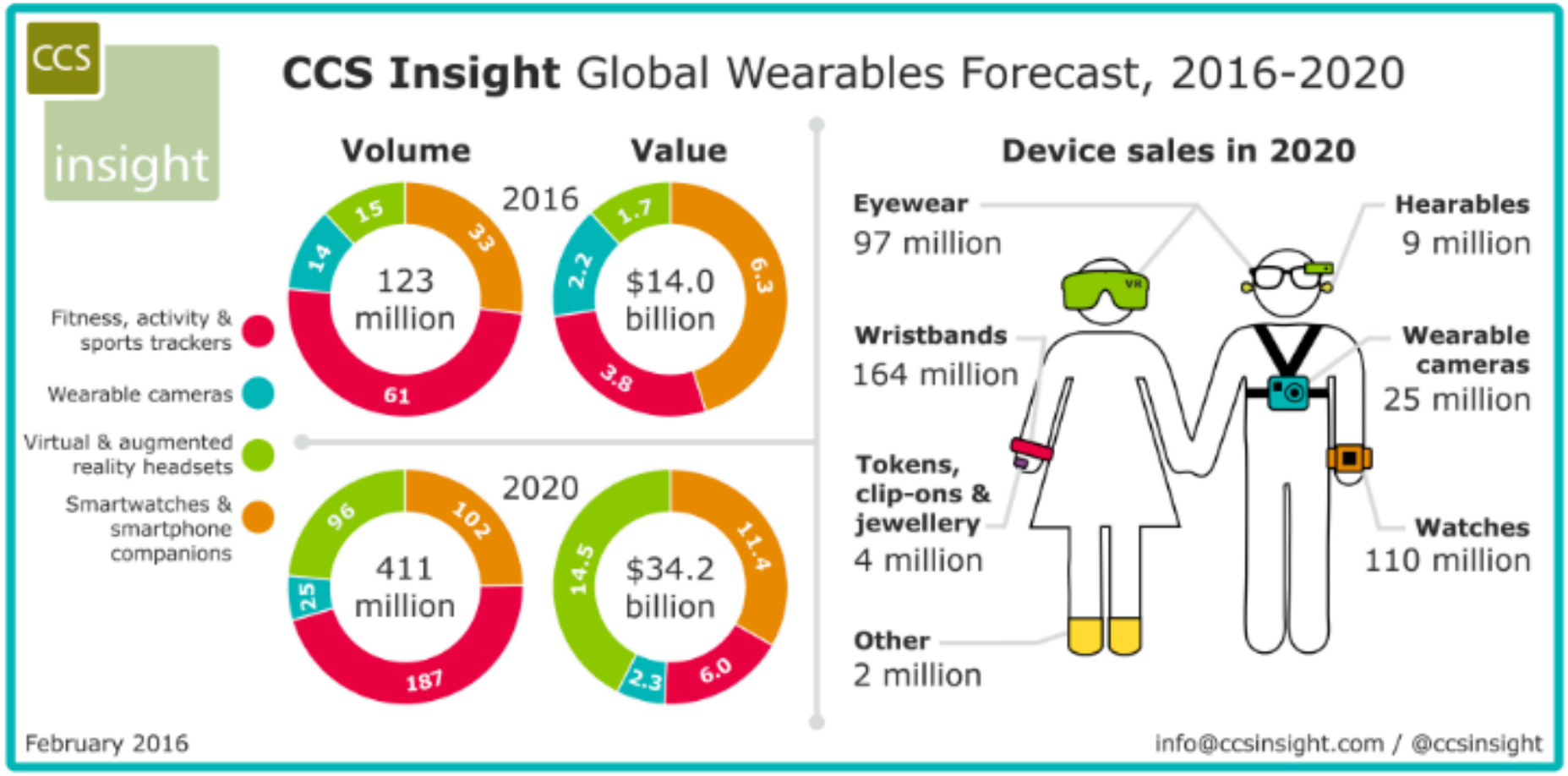
Örnek IoT Senaryoları

- İnsanları mobil cihazlarından uyaran deprem tespit sistemleri
- Barajlardaki su seviyesini takip sistemleri
- Gerçek zamanlı yol yönlendirmesi yapan akıllı trafik sistemleri
- Anlık nesne takibi yapabilen tedarik zinciri sistemleri
- Akıllı enerji kullanım takibi, güvenlik alarmı, uzaktan sıcaklık ayarlama, kahve ve tost makinesi çalıştırma özellikli ev sistemleri
- Evde hasta takip sistemleri
- …

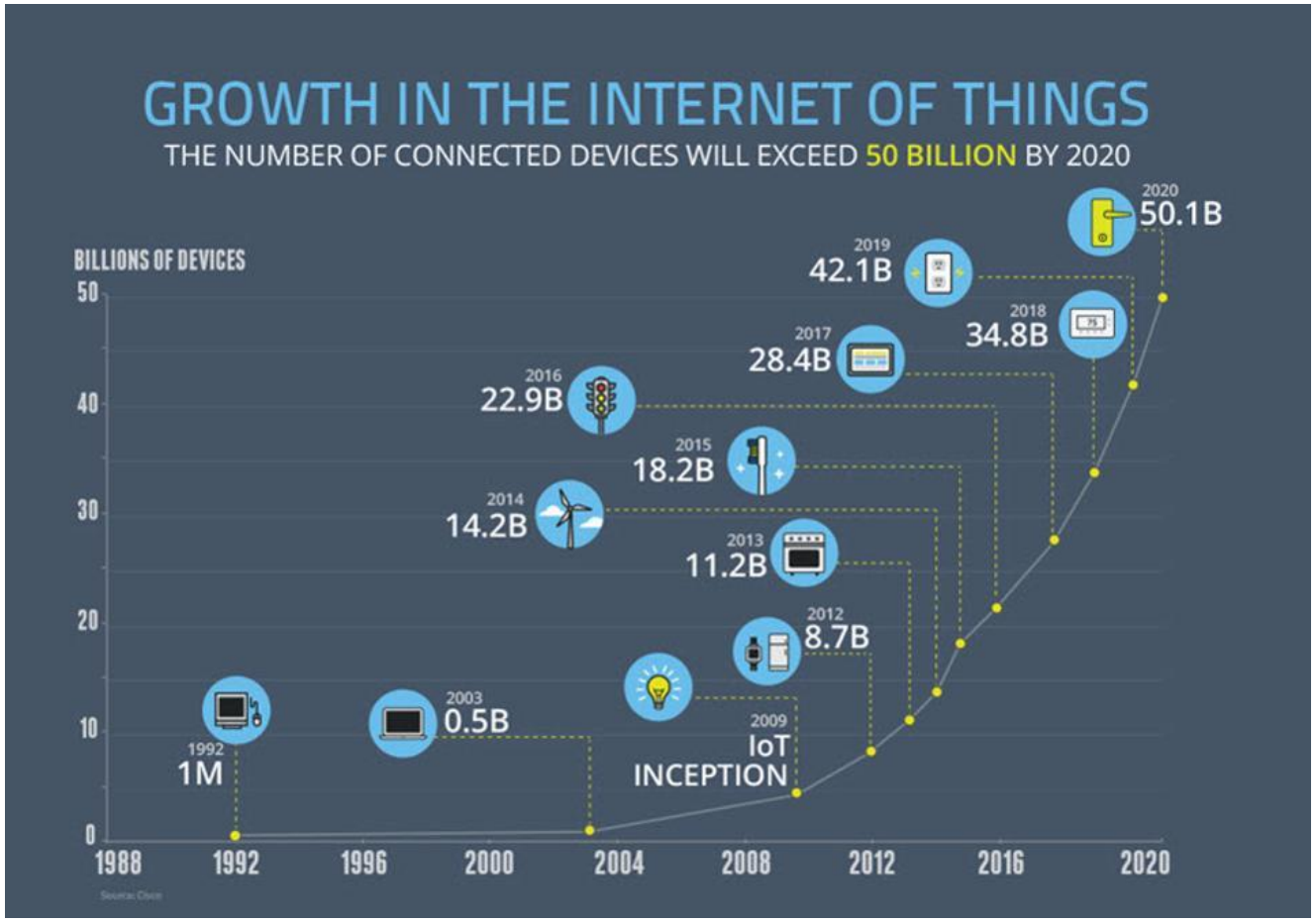
Giyilebilir IOT



Giyilebilir IoT Pazarı



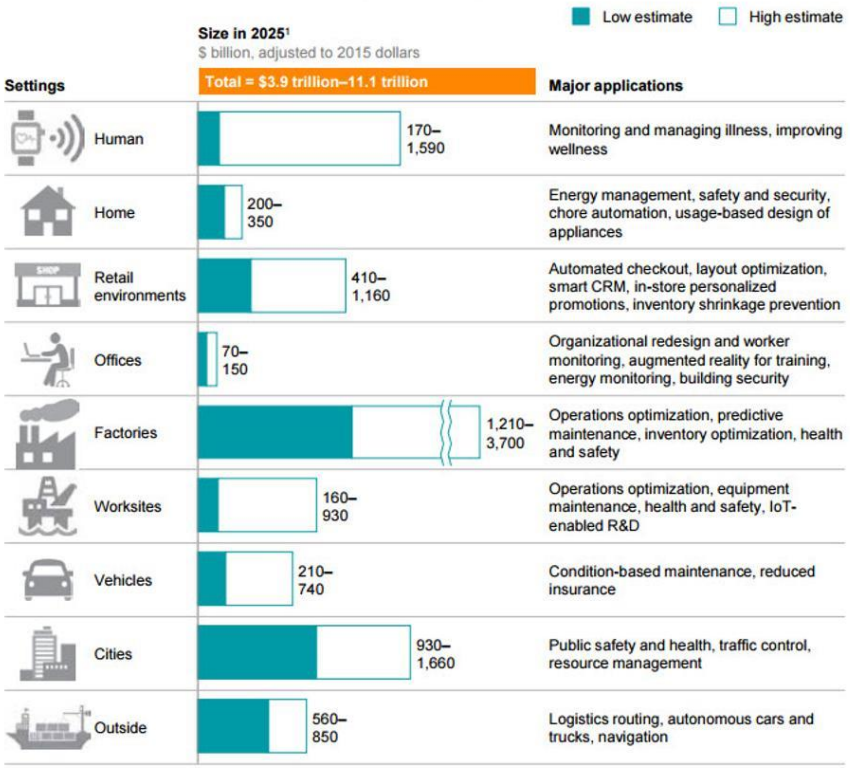
IoT - BÜYÜME HIZI



Kaynak: https://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/2/#2b677f9f5fa7

IoT – EKONOMİK ETKİ

Potential economic impact of IoT in 2025, including consumer surplus, is $3.9 trillion to $11.1 trillion



1 Includes sized applications only.
NOTE: Numbers may not sum due to rounding.

SOURCE: McKinsey Global Institute analysis

M2M (Machine-to-Machine)

- 1960’larda telekomünikasyon endüstrisinde ortaya çıktı
- Makineler arası direk iletişimin, insan müdahalesi olmadan kablolu ya da kablosuz ağlarla sağlandığı bir mimari
- Genelde uçtan-uca iletişim için gömülü donanım modülleri ve kablolu ya da mobil operatör tabanlı ağlar kullanır
- Sürekli bağlıdırlar, yüksek güç ve enerji gerektirebilirler
- Uzaktaki makinenin verisine genelde kapalı/özel protokollerle erişim sağlar; örneğin uzaktan sistem kontrolü, hata denetimi, güncelleme gibi amaçlarla kullanılabilir

M2M – IoT Farkları

M2M	IoT
Point-to-point communication usually embedded within hardware at the customer site	Devices communicate using IP Networks, incorporating with varying communication protocols
Many devices use cellular or wired networks	Data delivery is relayed through a middle layer hosted in the cloud
Devices do not necessarily rely on an Internet connection	In the majority of cases, devices require an active Internet connection
Limited integration options, as devices must have corresponding communication standards	Unlimited integration options, but requires a solution that can manage all of the communications

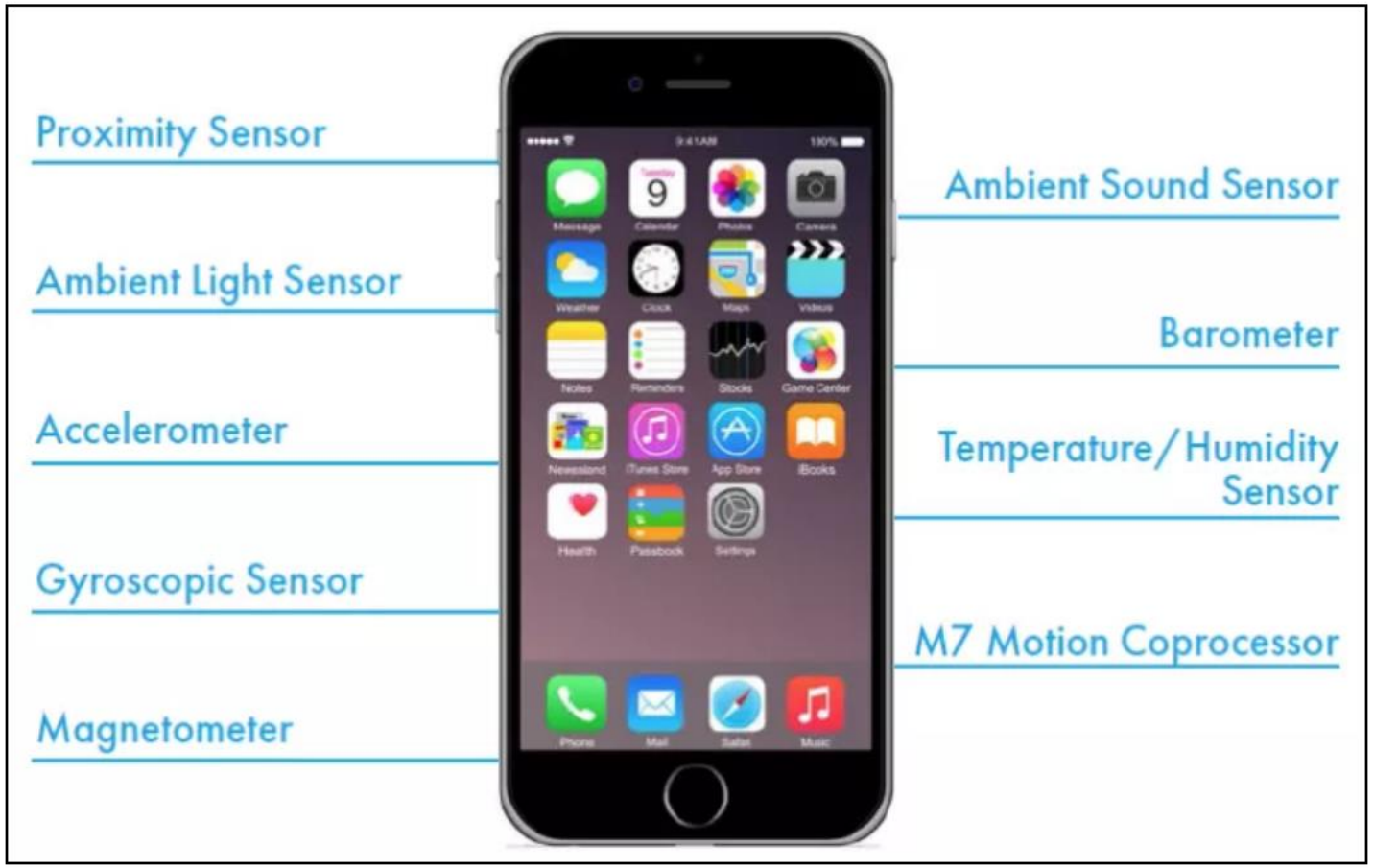
https://www.incognito.com/iot-and-m2m-whats-the-difference/

M2M- IoT Farkları

M2M	IoT
Machines	Sensors
Hardware-based	Software-based
Vertical applications	Horizontal applications
Deployed in a closed system	Connects to a larger network
Machines communicating with machines	Machines communicating with machines, humans with machines, machines with humans
Uses non-IP protocol	Uses IP protocols
Can use the cloud, but not required to	Uses the cloud
Machines use point-to-point communication, usually embedded in hardware	Devices use IP networks to communicate
Often one-way communication	Back and forth communication
Main purpose is to monitor and control	Multiple applications; multilevel communications
Operates via triggered responses based on an action	Can, but does not have to, operate on triggered responses
Limited integration options, devices must have complementary communication standards	Unlimited integration options, but requires software that manages communications/protocols
Structured data	Structured and unstructured data

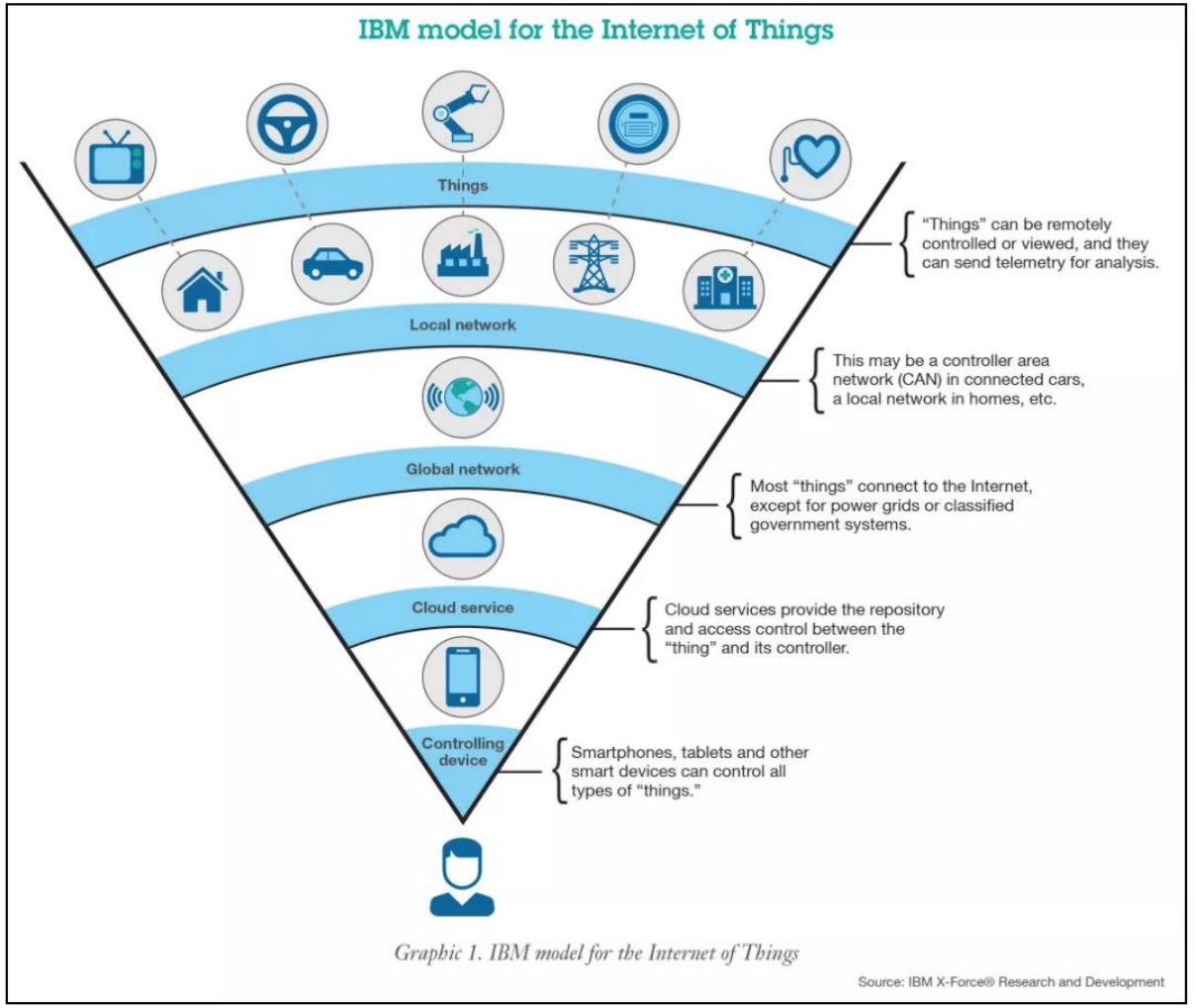
https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M

Bir IoT Cihazı olarak iPhone



https://gernotkapteina.com/2015/08/31/iot-internet-of-things/

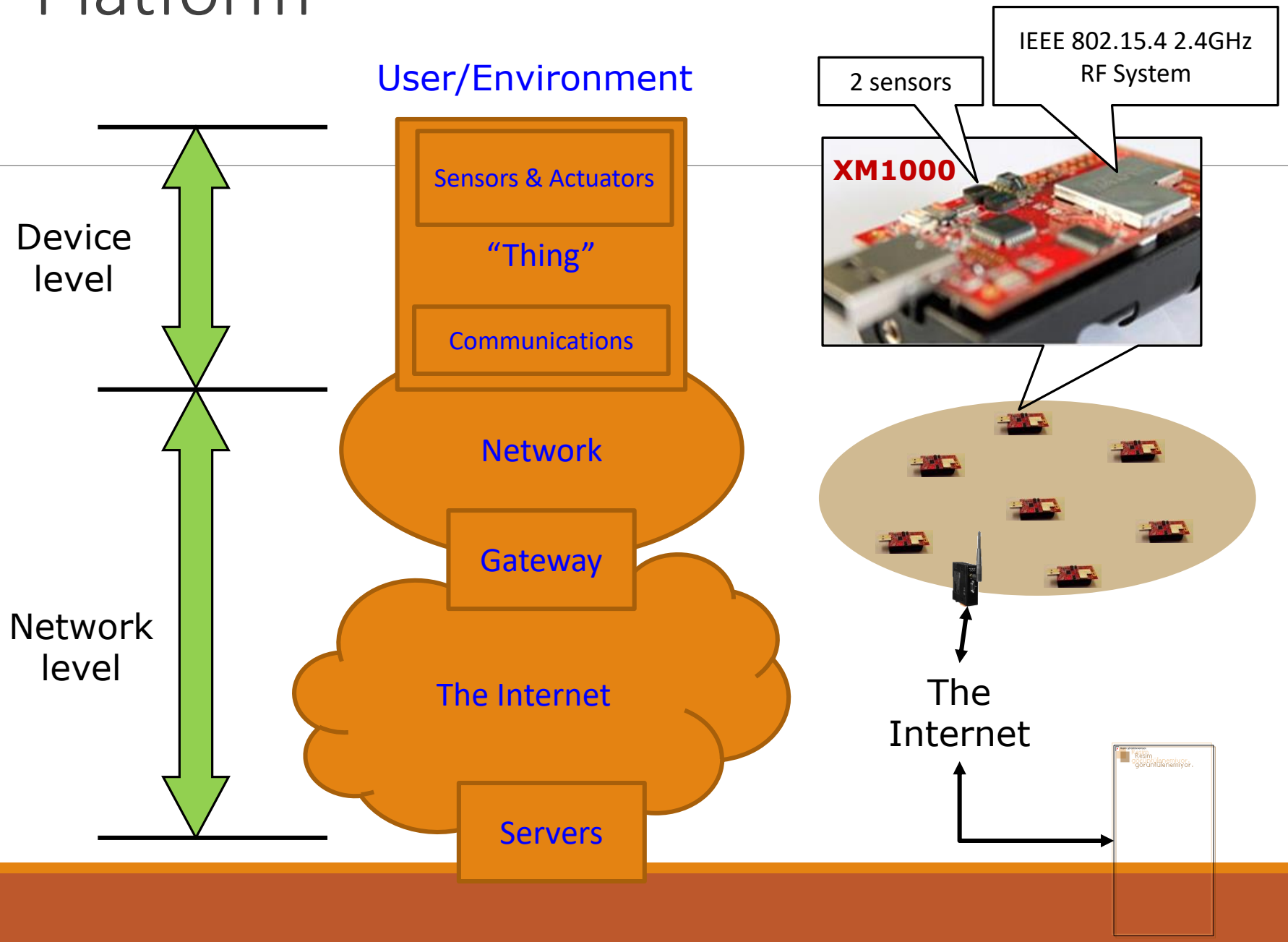
IoT Modelleri



IoT Çözüm Bileşenleri

- İletişim: WiFi, Bluetooth, GSM/GPRS/xG, LAN; WAN, RFID, NFC…
- Omurga: IP, UDP, TCP…
- Donanım: Cihaz ve sensörler, SoC (Wireless systems on chips)
- Yazılım: Gömülü işletim sistemleri (TinyOS, LiteOS vb), açık kaynak yazılımlar (RIOT vb), middleware …
- Protokoller
- Veri Aracısı ve Bulut Platformları

Platform


User/Environment
Device level
Network level
Sensors & Actuators
"Thing"
Communications
Network
Gateway
The Internet
Servers
2 sensors
IEEE 802.15.4 2.4GHz RF System
XM1000
The Internet

Sensors & Actuators

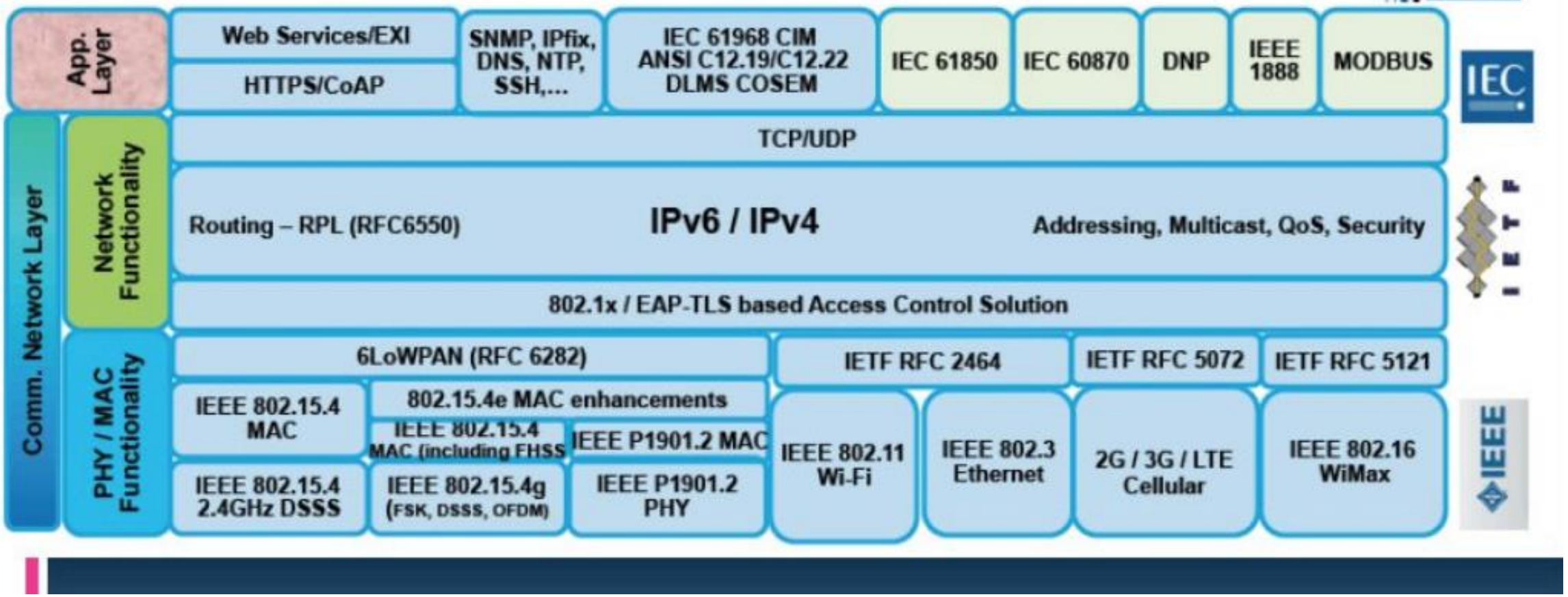
Sensors:

- «Veri Giriş» bileşenleridir
- Çevrelerinden veri algılar ve toplarlar.
- Temel olarak 3 gruptur:
  - Passive, omnidirectional (e.g. mic)
  - Passive, narrow-beam sensor (e.g. PIR)
  - Active sensors (e.g. sonar, radar, etc.)

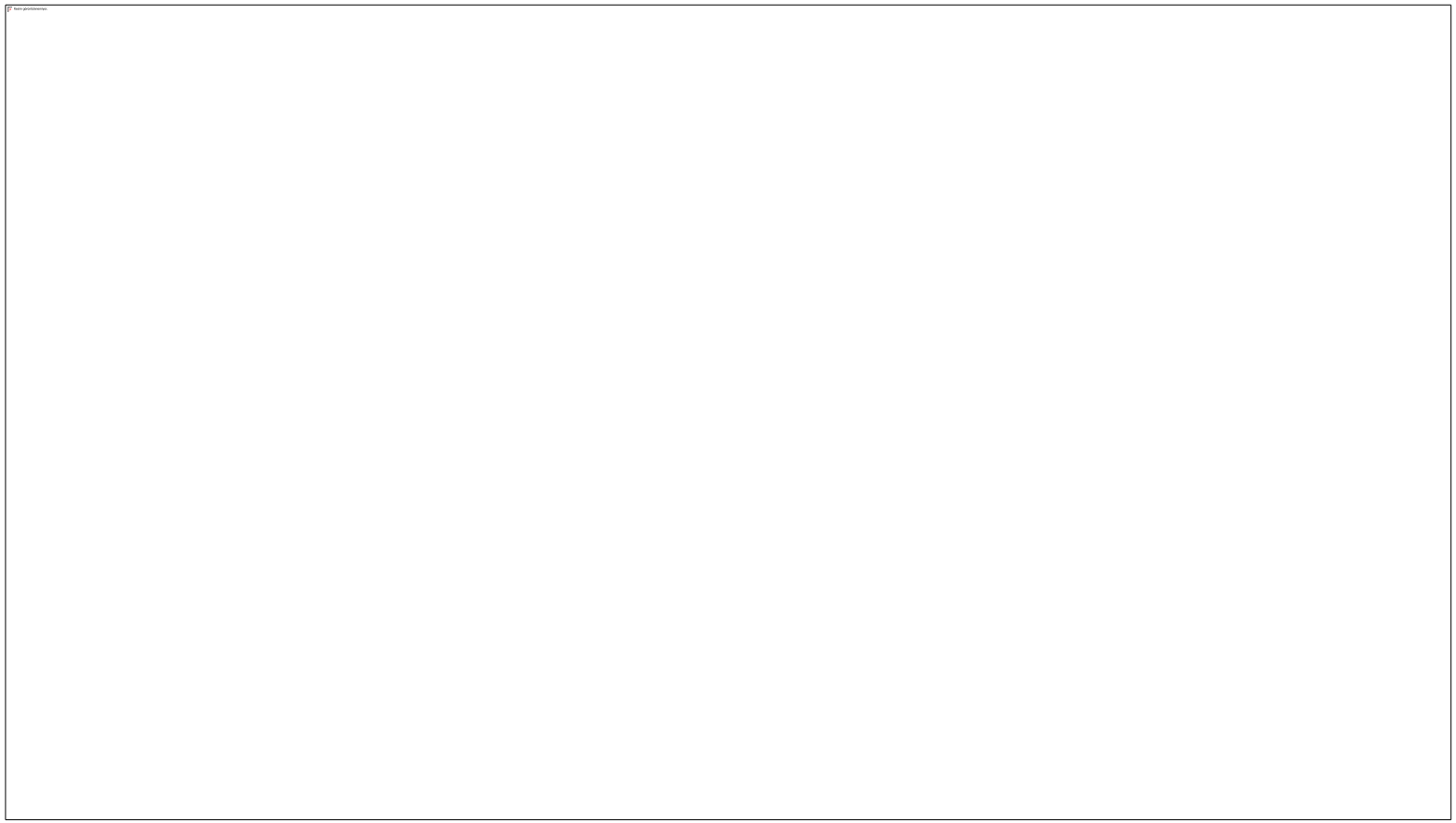
Actuators:

- «Veri çıkış» bileşenleridir
- Çevremizdeki şeyleri değiştirirler. Örneğin:
  - Işık, sıcaklık, ses vb değiştirmek.
  - Motor ve hareketli objeleri kontrol etmek
  - Mesaj göstermek
  - …

Open Standards Reference Model



Protokol Yığını Karşılaştırması



https://www.postscapes.com/internet-of-things-protocols/

Altyapı Protokolleri

- IPv6
- 6LoWPAN: IPv6'nın düşük enerjili, IEEE802.15.4 linkleri için adaptasyonu
- UDP
- DTLS: Datagram protokolleri için güvenli iletişim protokolü (TLS tabanlı)
- NanoIP: Gömülü ve sensör cihazlarına İnternet-benzeri iletişim sağlama
- Content-centric networking (CNN): Efektif içerik dağıtımı için uygulamadan bağımsız caching

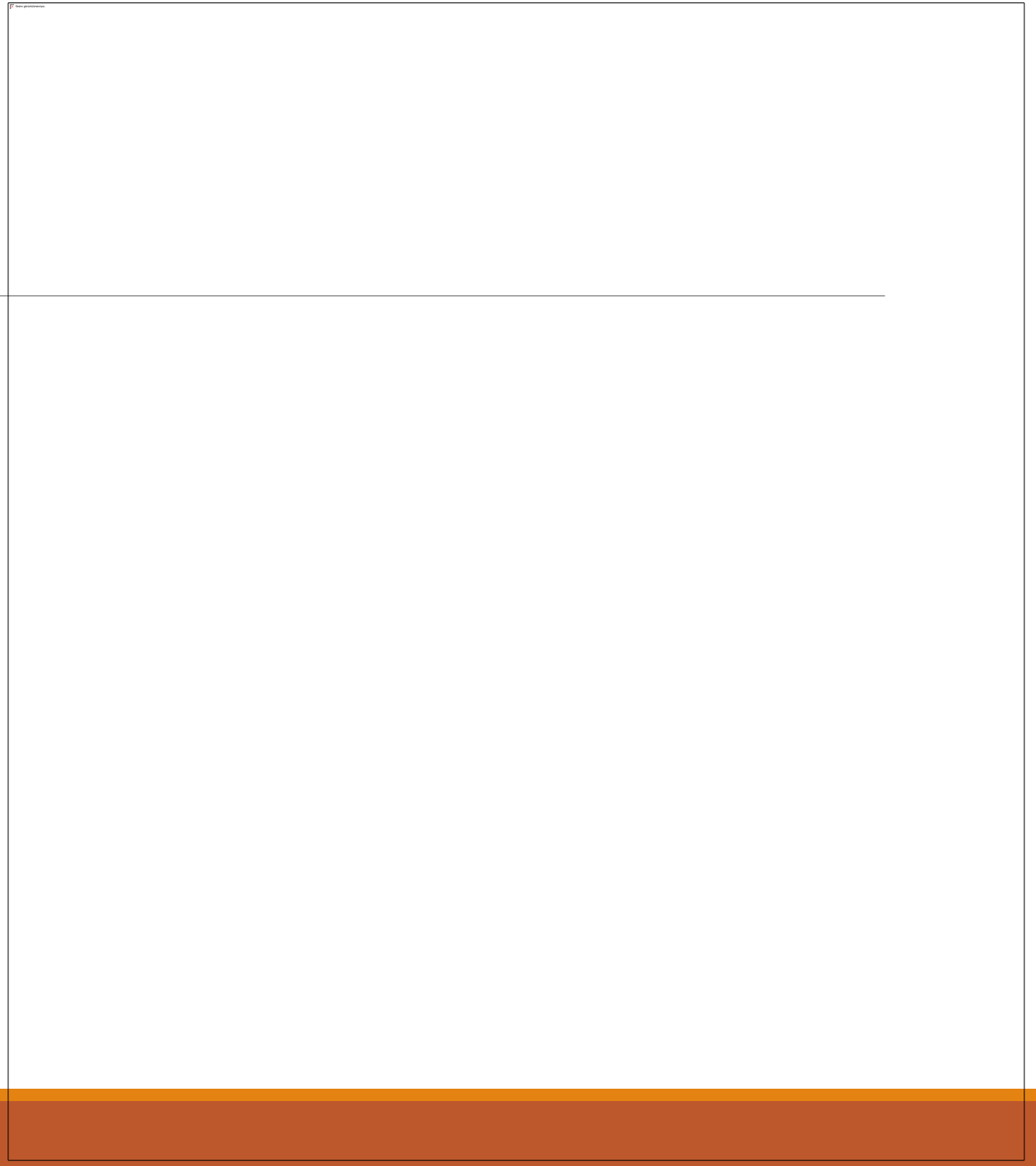
Keşif Protokolleri

- mDNS: Lokal bir isim sunucusu olmayan küçük ağlarda Host-IP çözümü
- Physical Web: Etraftaki nesneler tarafından BLE kullanarak yayınlanan URL'lerin listesini görmeye yarar
- UPnP (Universal Plug and Play): Ağdaki cihazların birbirini keşfetmesini sağlayan protokol kümesi

Veri Protokolleri

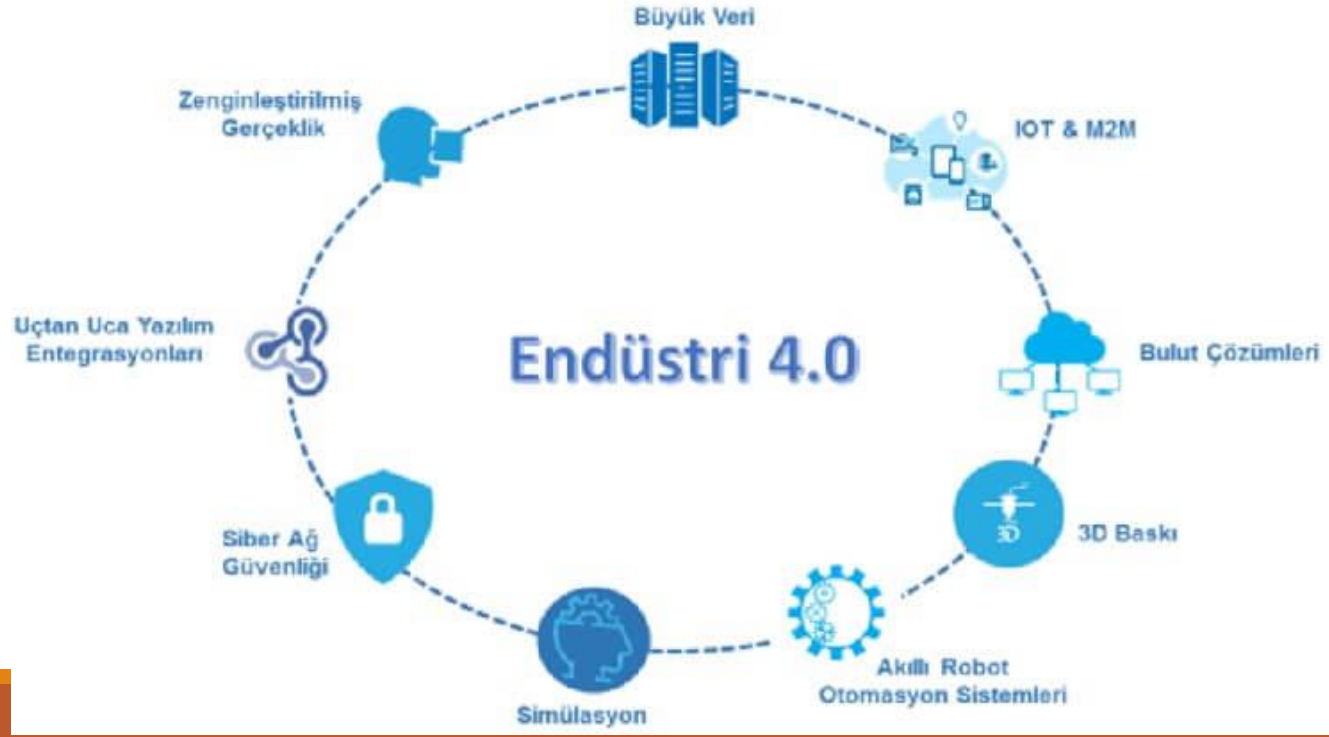
- MQTT (Message Queueing Telemetry Transport): Publish-subscribe mesaj modelini çok hafif bir şekilde sağlayan protokol
- MQTT-SN: Kablosuz sensör ağları için MQTT
- CoAP (Constrained Application Protocol): Düşük kaynaklı İnternet cihazları için bir uygulama katmanı protokolü, Web entegrasyonu için HTTP'ye kolayca çevrilebiliyor
- XMPP: Gerçek zamanlı iletişim için kullanılan IM, ses ve videolu görüşme, XML datasının yönlendirilmesi gibi birçok uygulamayı destekleyen bir protokol
- REST
- SOAP

Transport Katmanı



Endüstri 4.0

Endüstri 4.0'ın en büyük amacı, birbirleriyle haberleşen, sensörlerle ortamı algılayabilen ve veri analizi yaparak ihtiyaçları fark edebilen robotların üretimi devralıp; daha kaliteli, daha ucuz, daha hızlı ve daha az israf yapan bir üretim yapmaktır.



Endüstri 4.0 prensipleri

1) Karşılıklı Çalışabilirlik: Siber fiziksel sistemlerin yeteneği ile (örn. iş parçası taşıyıcıları, montaj istasyonları ve ürünleri) nesnelerin interneti ve hizmetlerin interneti üzerinden insanların ve akıllı fabrikaların birbirleriyle iletişim kurmasını içerir.

2) Sanallaştırma: Bu yapı akıllı fabrikaların sanal bir kopyasıdır. Sistem, sensör verilerinin sanal tesis ve simülasyon modelleri ile bağlanmasıyla oluşur.

3) Özerk Yönetim: Siber-Fiziksel sistemlerin akıllı fabrikalar içinde kendi kararlarını kendi verme yeteneğidir.

4) Gerçek-Zamanlılık Yeteneği: Verileri hızlı toplama ve analiz etme yeteneğidir.

5) Hizmet Oryantasyonu: Hizmetlerin interneti üzerinden siber-fiziksel sistemler, insanlar ve akıllı fabrika servisleri sunulmaktadır.

6) Modülerlik: Bireysel modüllerin değişen gereklilikleri için akıllı fabrikalara esnek adaptasyon sistemi sağlar.

Endüstri 4.0

http://kisi.deu.edu.tr/userweb/asli.ergun/Nesnelerin%20Interneti(IOT)%20(1).ppt

IOT GÜVENLİK PROBLEMLERİ

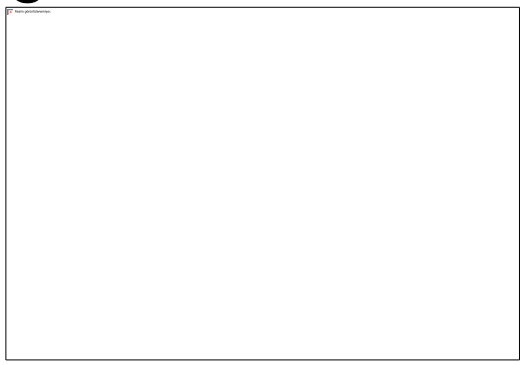
- Gizlilik
- Kimlik denetleme
- Büyüyen saldırı yüzeyi
- Veri bütünlüğü
- Dağıtılmış hizmet reddi (DDoS)
- Sorumluluk
- Cihaz kapasite problemleri
- Yeni ağ protokollerinin açıkları

YAŞANMIŞ VAKALAR

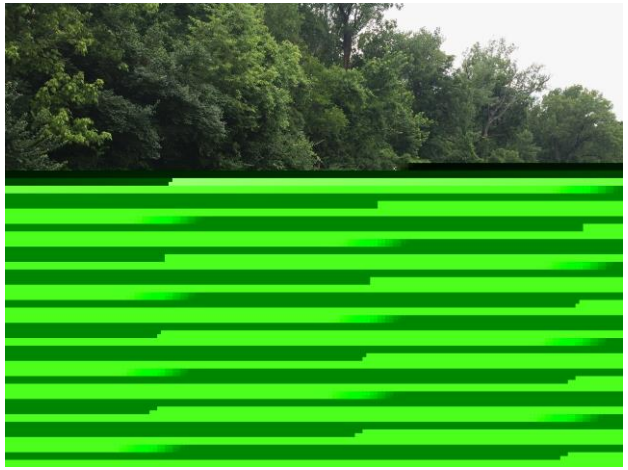
1

2

3



4



5

Kaynaklar:
1. https://ahmedbanafa.blogspot.com.tr/2016/10/a-wake-up-call-for-iot.html
2. https://thehacktoday.com/hackers-can-easily-hijack-popular-baby-monitors-to-watch-your-kids
3. https://thehackernews.com/2015/02/smart-tv-spying.html
4. https://www.thedailybeast.com/the-terrifying-us-israeli-computer-worm-that-could-cause-world-war-iii
5. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

MİRAİ BOTNET

- Linux çalıştıran ağa bağlı aygıtları uzaktan kontrol edilen “bot”lar haline getiren kötücül yazılım
- Özellikle IP kamerası, evlerdeki routerlar gibi aygıtlara 60’dan fazla sık kullanılan varsayılan şifreyi kullanarak giriş yapıp, Mirai yazılımıyla enfekte ediyor
- İlk Ağustos 2016’da keşfedildi
- Dağıtılmış hizmet reddi (DDoS) saldırılarında kullanıldı:
  - 21 Ekim 2016’daki DNS hizmetleri (Dyn) saldırısı
  - Kasım 2016’da Liberya’nın İnternet altyapısına saldırı
- Kaynak kodu hacker forumlarında paylaşıldı

MİRAİ'DEN ÖĞRENDİKLERİMİZ

- Varsayılan kullanıcı adı ve şifreler kullanılmamalı
- Mümkünse İnternet tarafında konfigürasyon arayüzüne izin verilmemeli
- IoT aygıtları sadece kurumun içinde kullanılıyorsa İnternete açılmamalı
- İnternet kullanımı gerekiyorsa sadece gerekli portlar açık tutulmalı

TİPİK IOT ALTYAPISI

Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

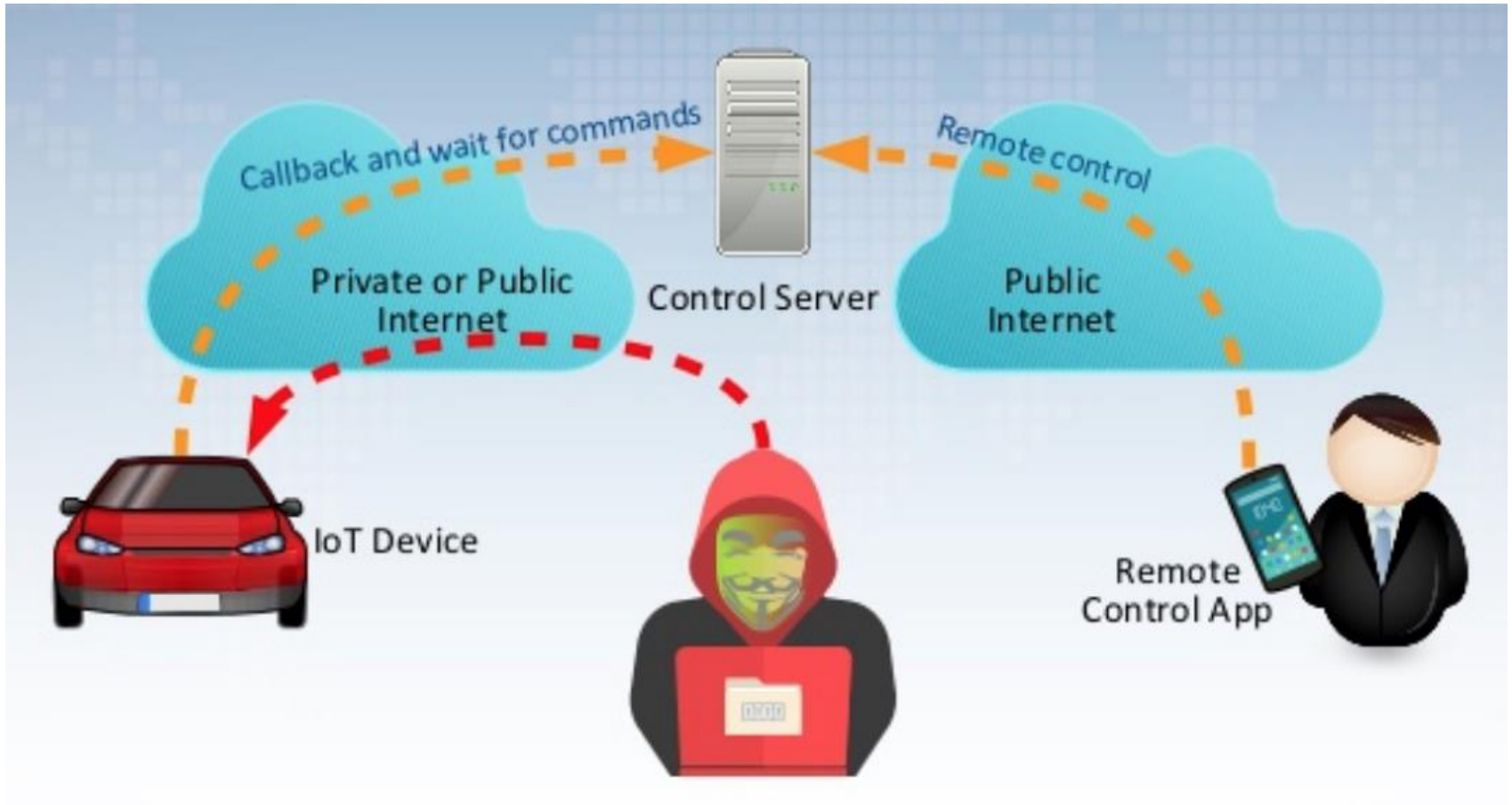
IOT SALDIRI YÜZEYLERİ

- Aygıt hafızası
- Aygıtın fiziksel arayüzü
- Aygıtın Web arayüzü
- Aygıt yazılımı
- Aygıtın ağ servisleri
- Admin arayüzü
- Lokal veri deposu
- Bulut arayüzü
- Dışarıdan sağlanan arka-uç APIleri
- Güncelleme mekanizması
- Mobil uygulama
- Satıcının arka-uç APIleri
- Ekosistem iletişimi
- Ağ trafiği
- Kimlik denetimi
- Gizlilik
- Donanım (sensörler)

TİPİK IOT SALDIRILARI
1. SAHTE KONTROL SUNUCUSU

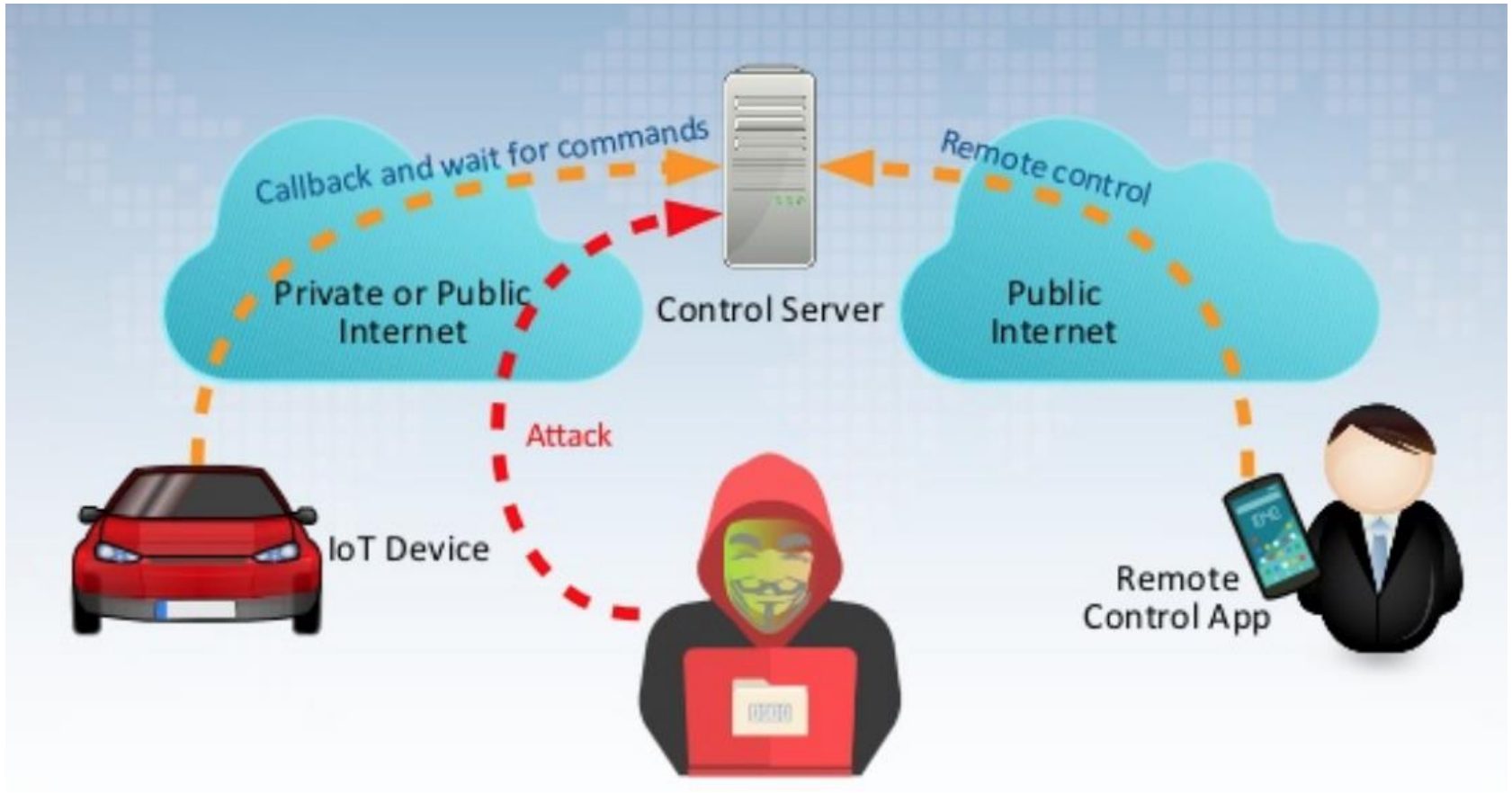
Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

TİPİK IOT SALDIRILARI
2. AYGIT PORTLARINA SALDIRI



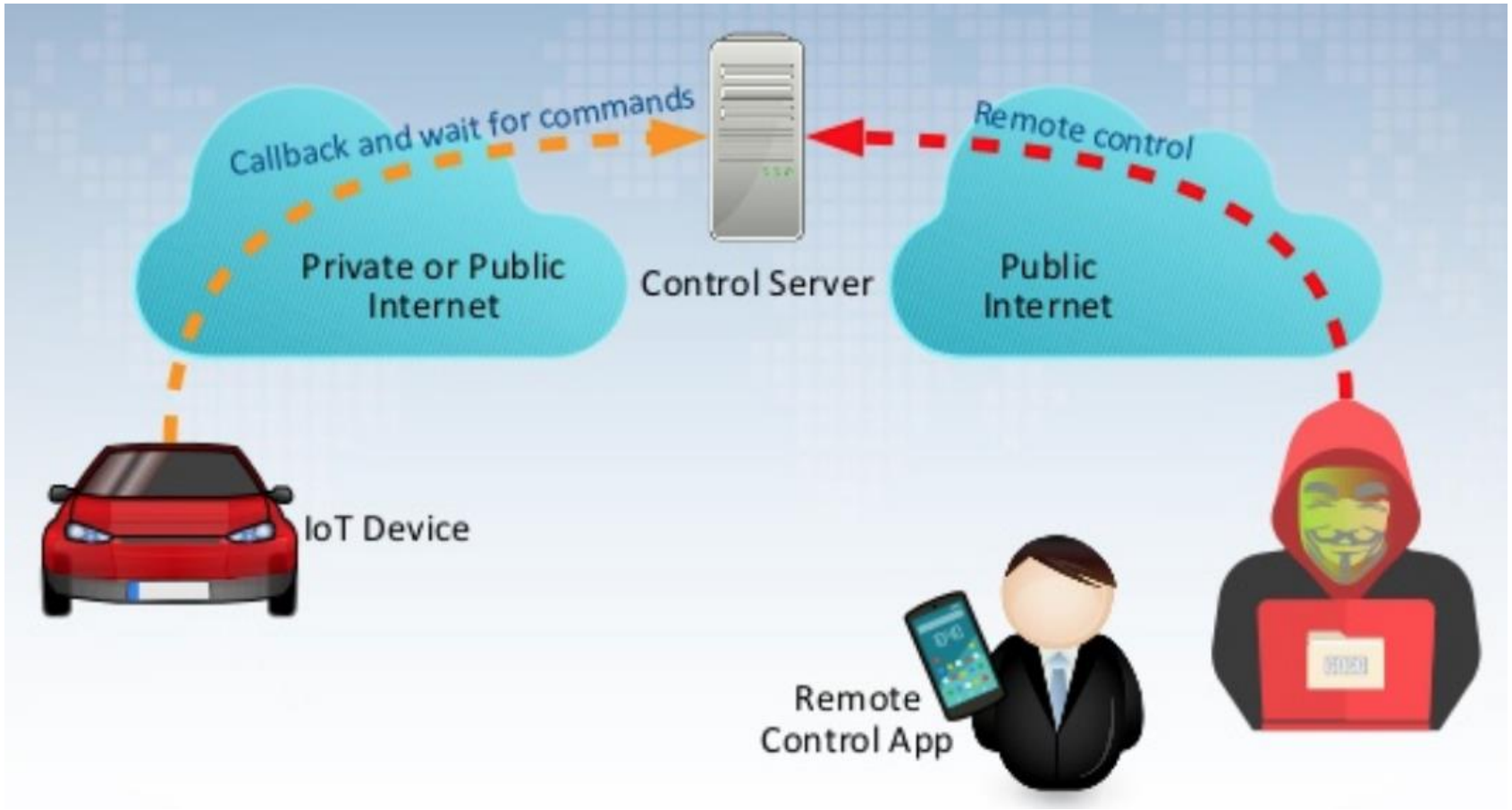
Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

TİPİK IOT SALDIRILARI
3. SUNUCU PORTLARINA SALDIRI



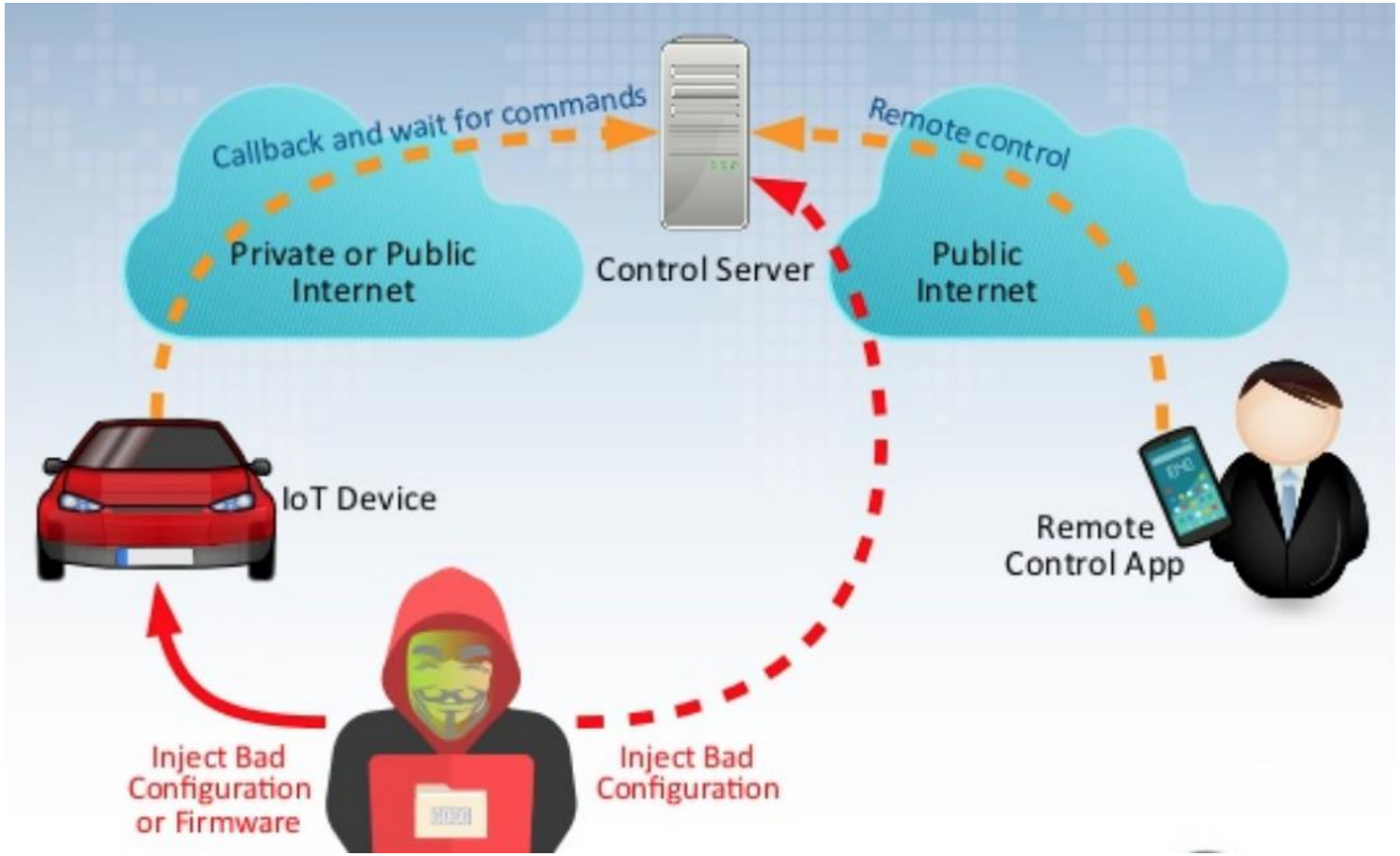
Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

TİPİK IOT SALDIRILARI
4. KULLANICI BİLGİLERİNİ ÇALMA



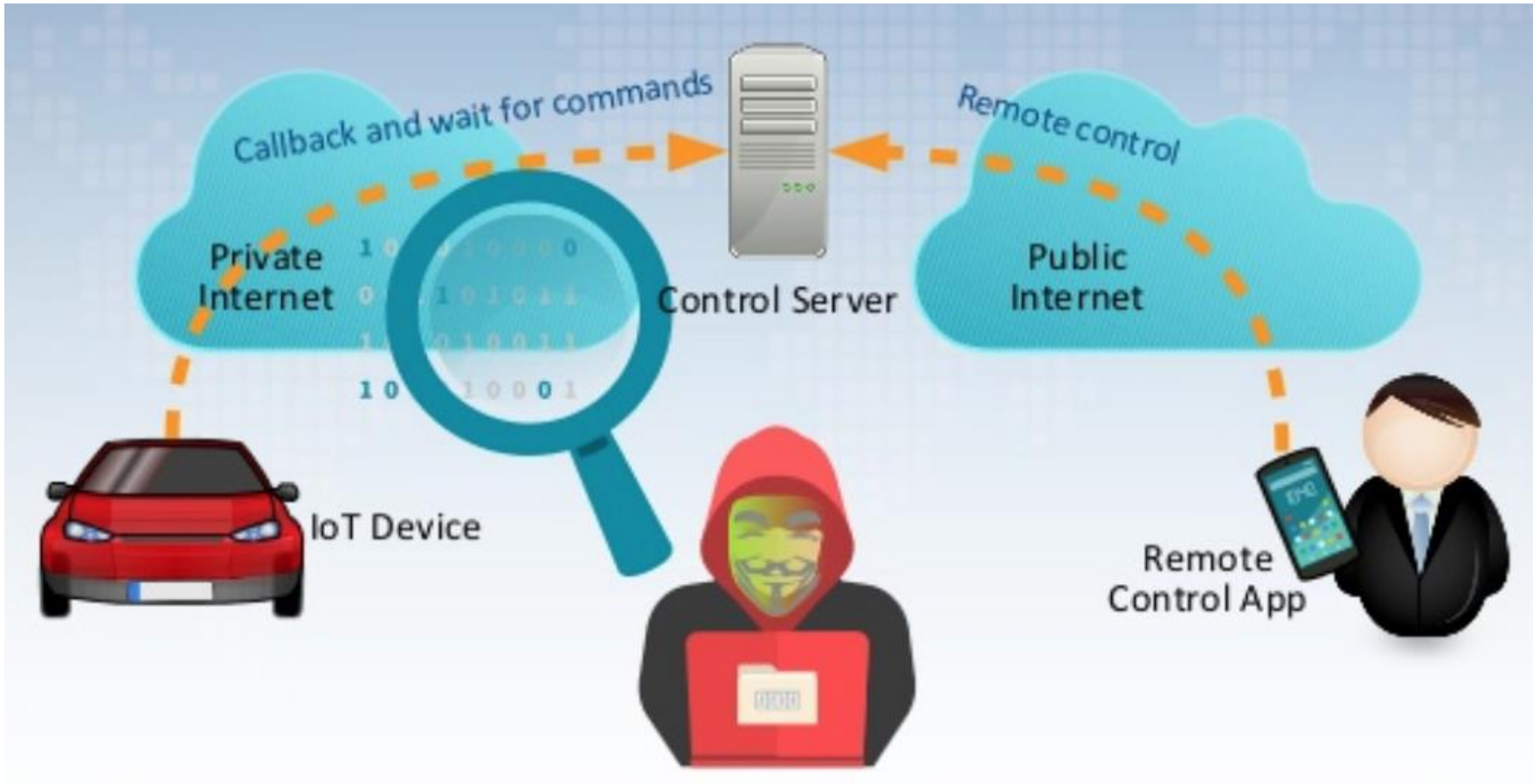
Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

TİPİK IOT SALDIRILARI
5. KÖTÜCÜL KONFİGÜRASYON ENJEKSİYONU



Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

TİPİK IOT SALDIRILARI
6. AĞ TRAFİĞİNİ İZLEME



Kaynak: https://www.slideshare.net/narudomr/iot-security-81762130

OWASP TARAFINDAN BELİRLENEN EN ÖNEMLİ 10 IOT GÜVENLİK AÇIĞI

1. Güvensiz Web arayüzü
2. Yetersiz kimlik/izin doğrulama
3. Güvensiz ağ hizmetleri
4. Taşımada şifreleme/bütünlük doğrulama eksikliği
5. Gizlilik sorunları
6. Güvensiz bulut arayüzü
7. Güvensiz mobil arayüz
8. Yetersiz güvenlik konfigürasyonu
9. Güvensiz yazılım/aygıt yazılımı (firmware)
10. Yetersiz fiziksel güvenlik

GÜVENSİZ WEB ARAYÜZÜ

- IoT aygıtlarının admin arayüzlerini etkiler
- Sorunlar:
  - Varsayılan şifre ve kullanıcı adı kullanımı
  - Hesap kilitlenmesi olmaması (birden fazla şifre hatasında)
  - XSS, CSRF, SQLi açıklıkları
- Çözümler:
  - Varsayılan kullanıcı adı/şifre değiştirilmeli
  - Web uygulaması güvenlik değerlendirmesi yapılmalı
  - Hesabın kilitlenmesine izin verilmeli

YETERSİZ KİMLİK/İZİN DOĞRULAMA

- Bütün aygıt arayüzlerini ve servisleri etkiler
- Sorunlar:
  - Güçsüz şifreler
  - Şifreyi yeniden öğrenme/sıfırlama mekanizmalarının güvensizliği
  - İki-faktörlü doğrulama yapılmaması
- Çözümler:
  - Güçlü, karmaşık şifre gerektirmek
  - Şifre öğrenme mekanizmalarının güvenliğini değerlendirmek
  - İki-faktörlü kimlik doğrulama

GÜVENSİZ AĞ HİZMETLERİ

- Bütün ağ hizmetlerini (aygıt, bulut, web, mobil) etkiler
- Sorunlar:
  - Gereksiz portların açık olması
  - Portların İnternet'e UPnP yoluyla açık olması
  - Ağ hizmetlerinin hizmet reddi saldırısına açık olması
- Çözümler:
  - Açık portların minimum tutulması
  - UPnP kullanmamak
  - Ağ hizmetlerini açıklıklar için taramak

İLETİMDE ŞİFRELEME/BÜTÜNLÜK DOĞRULAMA EKSİKLİĞİ

- Bütün ağ hizmetlerini (aygıt, bulut, web, mobil) etkiler
- Sorunlar:
  - Hassas verinin şifrelenmeden gönderilmesi
  - SSL/TLS'in kullanılamaz olması ya da konfigürasyon hatası
  - Özel şifreleme protokollerinin kullanılması
- Çözümler:
  - Sistem bileşenleri arasında iletişimin şifrelenmesi
  - SSL/TLS konfigürasyonuna dikkat edilmesi

GİZLİLİK SORUNLARI

- IoT'nin bütün bileşenlerini etkiler
- Sorunlar:
  - Çok fazla kişisel veri toplanması
  - Toplanan veri güvenliğinin sağlanmaması
- Çözümler:
  - Toplanan verinin sınırlanması
  - Toplanan verinin anonimleştirilmesi
  - Son kullanıcılara toplanan veri konusunda seçim şansı verilmesi

GÜVENSİZ BULUT ARAYÜZÜ

- Bulut-tabanlı web arayüzleri ve bulut APIlerini etkiler
- Sorunlar:
  - Arayüzlerin güvenlik açıklıkları için taranmaması
  - Güçsüz şifre kullanımı
  - İki-faktörlü kimlik denetimi kullanılmaması
- Çözümler:
  - Bütün bulut arayüzlerinin güvenlik testinin yapılması
  - İki-faktörlü erişim denetimi
  - Güçlü şifre gerektirme

GÜVENSİZ MOBİL ARAYÜZ

- Sorunlar:
  - Zayıf şifreler
  - İki-faktörlü kimlik denetimi olmaması
  - Hesap kilitleme mekanizması olmaması

YETERSİZ GÜVENLİK KONFİGÜRASYONU

- IoT aygıtını etkiler
- Sorunlar:
  - Şifre güvenliği opsiyonlarının olmaması
  - Değişik şifreleme opsiyonlarının olmaması
  - Güvenlik loglarının olmaması

GÜVENSİZ YAZILIM/AYGIT YAZILIMI (FIRMWARE)

- IoT cihazını etkiler
- Sorunlar:
  - Güncelleme sunucularının güvenliğinin sağlanmaması
  - Aygıt güncellemelerinin şifrelenmeden iletilmesi
  - Güncellemelerin imzalı olmaması

YETERSİZ FİZİKSEL GÜVENLİK

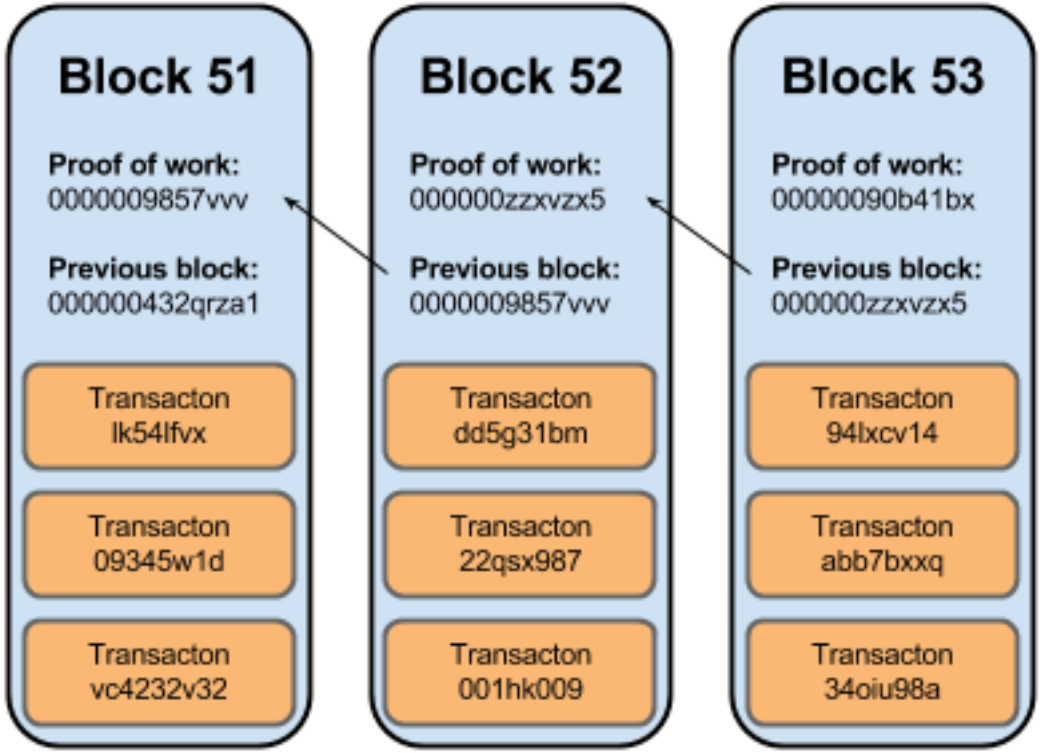
Sorunlar:

- USB gibi gereksiz dış portlar
- İşletim sistemine dışarıdan takılabilir aygıtlarla erişim
- Admin özelliklerinin sınırlanamaması

MEVCUT GÜVENLİK ARAÇLARININ SORUNLARI

- Merkezi olmaları
- Yüksek kapasite gerektirmeleri
- Yüksek enerji sarfiyatı
- Standart yoksunluğu
- Ölçeklenebilirlik problemleri
- Platformlar-arası uyuşmazlık

BLOK ZİNCİRİYLE (BLOCKCHAIN) MERKEZİ OLMAYAN GÜVENLİK



- Dağıtılmış
- Değiştirilemez
- Güvenilir (uzlaşma yöntemli)
- İnkar edilemez
- Tüm tarihçeyi saklayan
- Herkesçe doğrulanabilen
- Anonim

Kaynak: http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/

IOT BLOKZİNCİRİ

Sorunlar:

- Enerji sarfiyatı
- Cihazların işlem ve saklama kapasiteleri
- Değiştirilemezlik
- Uzlaşma protokolünün süresi

Çözüm önerileri:

- Hafif sıklet şifreleme/çözme algoritmaları
- Katılan sayısı azaltılmış, bağlama duyarlı uzlaşma algoritmaları
- Hiyerarşik veri saklama ve kriptografik işlem yapısı