IoT Security and privacy challenges

Adel Abdel Moneim, MBA

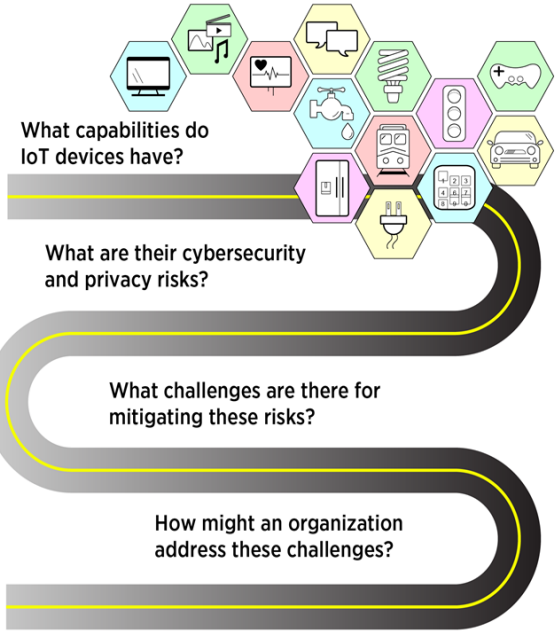
ITU-ARCC Cyber Security Expert

SCCISP ,CISSP, CISM, CRISC, CISA, CGEIT, CCISO,SABSA-SCF, CEH, CCSK,CHFI, EDRP,CSA ,ECSA, LPT,CND, ECES, CCFP-EU,PECB MS Auditor, SMSP, ECIH, Master ISO27001, ISO27005LRM , ISO31000, ISO27032 Lead Cybersecurity Manager, ISO27035 LIM, ISO38500 Lead IT Corporate Governance Manager,ISO24762 LDRM, CLSSP, ISO 29100 Lead Privacy Implementer, Lead Forensic Examiner, Certified Cyber Intelligence Professional (CCIP)

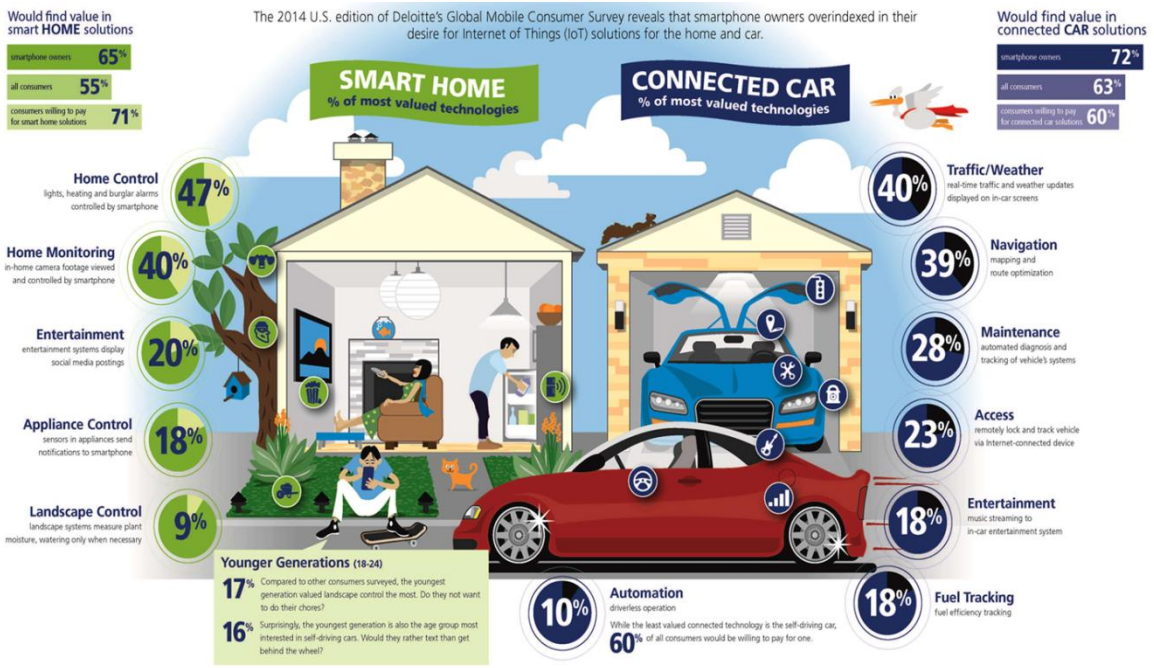
Definition of IoT

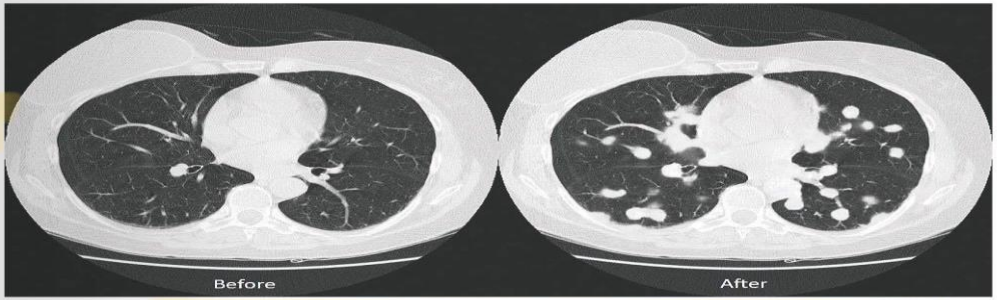
[WIKIPEDIA] The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors
and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

[OXFORD] A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.



The internet of Things moves in





IOT Attack news

THURSDAY, APRIL 4, 2019 · THE WASHINGTON POST EZ SU A19

ECONOMY & BUSINESS

DOW 26,218.13 UP 39.0 (0.2%) · NASDAQ 7,895.55 UP 46.86 (0.6%) · S&P 500 2,873.40 UP 6.16 (0.2%) · GOLD $1,295.30 DOWN $0.10 (0.01%) · CRUDE OIL $62.46 DOWN $0.12 (0.2%) · 10-YEAR TREASURY DOWN $4.20 PER $1,000; 2.5% YIELD · CURRENCIES $1=111.51 YEN; EURO=$1.124

Malware's faked malignancies in CT scans trick doctors

Researchers in Israel created program to highlight weaknesses in medical imaging equipment

BY KIM ZETTER

When Hillary Clinton stumbled and coughed through public appearances during her 2016 presidential run, she faced critics who said that she might not be well enough to perform the top job in the country. To quell rumors about her medical condition, her doctor revealed that a CT scan of her lungs showed that she just had pneumonia.

But what if the scan had shown faked cancerous nodules, placed there by malware exploiting vulnerabilities in widely used CT and MRI scanning equipment? Researchers in Israel say they have developed such malware to draw attention to serious security weaknesses in critical medical imaging equipment used for diagnosing conditions and the networks that transmit those images — vulnerabilities that could have potentially life-altering consequences if unaddressed.

The malware they created would let attackers automatically add realistic, malignant-seeming growths to CT or MRI scans before radiologists and doctors examine them. Or it could remove real cancerous nodules and lesions without detection, leading to misdiagnosis and possibly a failure to treat patients who need critical and timely care.

Yisroel Mirsky, Yuval Elovici and two others at the Ben-Gurion University Cyber Security Research Center in Israel who created the malware say that attackers could target a presidential candidate or other politicians to trick them into believing they have a serious illness and cause them to withdraw from a race to seek treatment.

The research isn't theoretical. In a blind study, the researchers conducted involving real CT lung scans, 70 of which were altered by their malware, they were able to trick three skilled radiologists into misdiagnosing conditions nearly every time. In the case of scans with fabricated cancerous

BEN-GURION UNIVERSITY

Researchers in Israel created malware that can alter CT and MRI scans to show fake, malignant-seeming growths, as in the image at right.

real 60 percent of the time, leading them to misdiagnoses involving those patients. In the case of scans where the malware removed cancerous nodules, doctors did not detect this 87 percent of the time, concluding that very sick patients were healthy.

The researchers ran their test against a lung-cancer screening software tool that radiologists often use to confirm their diagnoses and were able to trick it into misdiagnosing the scans with false tumors every time.

"I was quite shocked," said Nancy Boniel, a radiologist in Canada who participated in the study. "I felt like the carpet was pulled out from under me, and I was left without the tools necessary to move forward."

they could prevent patients who have a disease from receiving critical care or cause others who aren't ill to receive unwarranted biopsies, tests and treatment. The attackers could even alter follow-up scans after treatment begins to falsely show tumors spreading or shrinking. Or they could alter scans for patients in drug and medical research trials to sabotage the results.

The vulnerabilities that would allow someone to alter scans reside in the equipment and networks hospitals use to transmit and store CT and MRI images. These images are sent to radiology workstations and back-end databases through what's known as a picture archiving and communication system (PACS). Mir-

ords. But what happens within the [hospital] system itself, which no regular person should have access to in general, they tend to be pretty lenient [about]. It's not . . . that they don't care. It's just that their priorities are set elsewhere."

Although one hospital network they examined in Israel did try to use encryption on its PACS network, the hospital configured the encryption incorrectly and as a result the images were still not encrypted.

Fotios Chantzis, a principal information-security engineer with the Mayo Clinic in Minnesota who did not participate in the study but confirmed that the attack is possible, said that PACS networks are generally not en-

that don't have the ability to decrypt or re-encrypt images.

To develop their malware, the Israeli researchers used machine learning to train their code to rapidly assess scans passing through a PACS network and to adjust and scale fabricated tumors to conform to a patient's unique anatomy and dimensions to make them more realistic. The entire attack can be fully automated so that once the malware is installed on a hospital's PACS network, it will operate independently to find and alter scans, even searching for a specific patient's name.

To get the malware onto a PACS network, attackers would need either physical access to the network — to connect a malicious

was able to enter the radiology department after hours and connect his malicious device to the network in just 30 seconds, without anyone questioning his presence. Although the hospital had given permission for the test, staff members didn't know how or when Mirsky planned to carry it out.

To prevent someone from altering CT and MRI scans, Mirsky says, hospitals ideally would enable end-to-end encryption across their PACS network and digitally sign all images while also making sure that radiology and doctor workstations are set up to verify those signatures and flag any images that aren't properly signed.

Suzanne Schwartz, a medical doctor and the Food and Drug Administration's associate director for Science and Strategic Partnerships, who has been leading some of the FDA's efforts to secure medical devices and equipment, expressed concern about the findings of the Israeli researchers. But she said many hospitals don't have the money to invest in more-secure equipment, or they have 20-year-old infrastructure that doesn't support newer technologies.

Christian Dameff, an emergency room physician with the University of California at San Diego School of Medicine and a security researcher who has exposed vulnerabilities in the 911 emergency calling system, notes that in the case of a cancer diagnosis, some backstops would prevent a patient from receiving unwarranted treatment based only on a maliciously modified CT scan. But that doesn't mean the attack would be harmless.

"There are a couple of steps before we just take someone to surgery" or prescribe radiation and chemotherapy, Dameff said. "But there is still harm to the patient regardless. There is the emotional distress [from learning you may have cancer], and there are all sorts of insurance

IOT Attack news

Massive Botnet Attack Used More Than 400,000 IoT Devices

Researchers at Imperva Say Incident Mimicked Mirai-Style DDoS Attack

Akshaya Asokan (asokan_akshaya) · July 26, 2019

IoT cyber attacks cost the UK economy £1 billion

24TH MAY 2019 BY MEERA NARENDRA IN CYBER SECURITY, NEWS

New research from Irdeto revealed that Internet of Things (IoT) attacks cost UK businesses an average of £244,000 last year.

The Dutch Security vendor conducted research on IT security decision makers at UK organisations in sectors including health, transport and manufacturing. It was revealed IoT devices cost the UK economy over £1 billion each year.

DARKReading

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS

IoT

6/26/2019
05:30 PM

DARK Reading

Dark Reading Staff
Quick Hits

12 COMMENTS
COMMENT NOW

Login

New Linux Worm Attacks IoT Devices

Silex has 'bricked' more than 2,000 Linux-based IoT devices so far.

A new Internet of Things (IoT) bricking worm — malware designed to permanently disable the hardware it infects — is hitting Linux-based devices, and it appears the culprit responsible for the attack is 14 years old.

The new software, dubbed "Silex," is running across the Internet looking for Linux systems deployed with default admin credentials. Once it finds such a system, it overwrites all of the system's storage with random data, drops its firewall rules, removes its network configuration, and then restarts the system — effectively rendering the device useless.

https://gdpr.report/news/2019/05/24/iot-cyber-attacks-cost-the-uk-economy-1-billion/

IOT Attack news

IoT Attacks Escalating with a 217.5% Increase in Volume

By Sergiu Gatlan — March 29, 2019 — 07:00 AM — 0

Attacks against Internet of Things (IoT) devices and networks have been escalating throughout 2018 with 32.7 million IoT attacks having been detected during last year by SonicWall, while phishing saw a decrease in volume with most of the attacks being targeted.

While everyone wants to have their devices interconnected and connected to the Internet, many of the estimated 31 billion IoT devices that will be installed by 2020 according to Statista will also come with easy to abuse or no security controls.

This allows malicious actors to compromise and add them to large scale botnets they control by exploiting security flaws impacting them in great numbers or taking control of them using publicly available default credentials.

IOT Attack news

What is the Mirai Botnet?

The Mirai malware exploits security holes in IoT devices, and has the potential to harness the collective power of millions of IoT devices into botnets, and launch attacks.

Share

What is a DDoS Attack? | What is a Botnet? | Common DDoS Attacks | DDoS Attack Tools | DDoS Glossary of Terms | Famous DDoS Attacks

Mirai Botnet Learning Objectives

After reading this article you will be able to:

- Learn about the Mirai botnet
- Learn how botnets are mutating
- Learn why botnets are dangerous
- Learn how IoT devices and botnets are related

Related Content

What Is A Botnet?

What is Mirai?

Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or zombies. This network of bots, called a botnet, is often used to launch DDoS attacks.

Malware, short for malicious software, is an umbrella term that includes computer worms, viruses, Trojan horses, rootkits and spyware.

In September 2016, the authors of the Mirai malware launched a DDoS attack on the website of a well-known security expert. A week later they released the source code into the world, possibly in an attempt to hide the origins of that attack. This code was quickly replicated by other cybercriminals, and is believed to be behind the massive attack that brought down the domain registration services provider, Dyn, in October 2016.

IOT Attack news

kaspersky daily

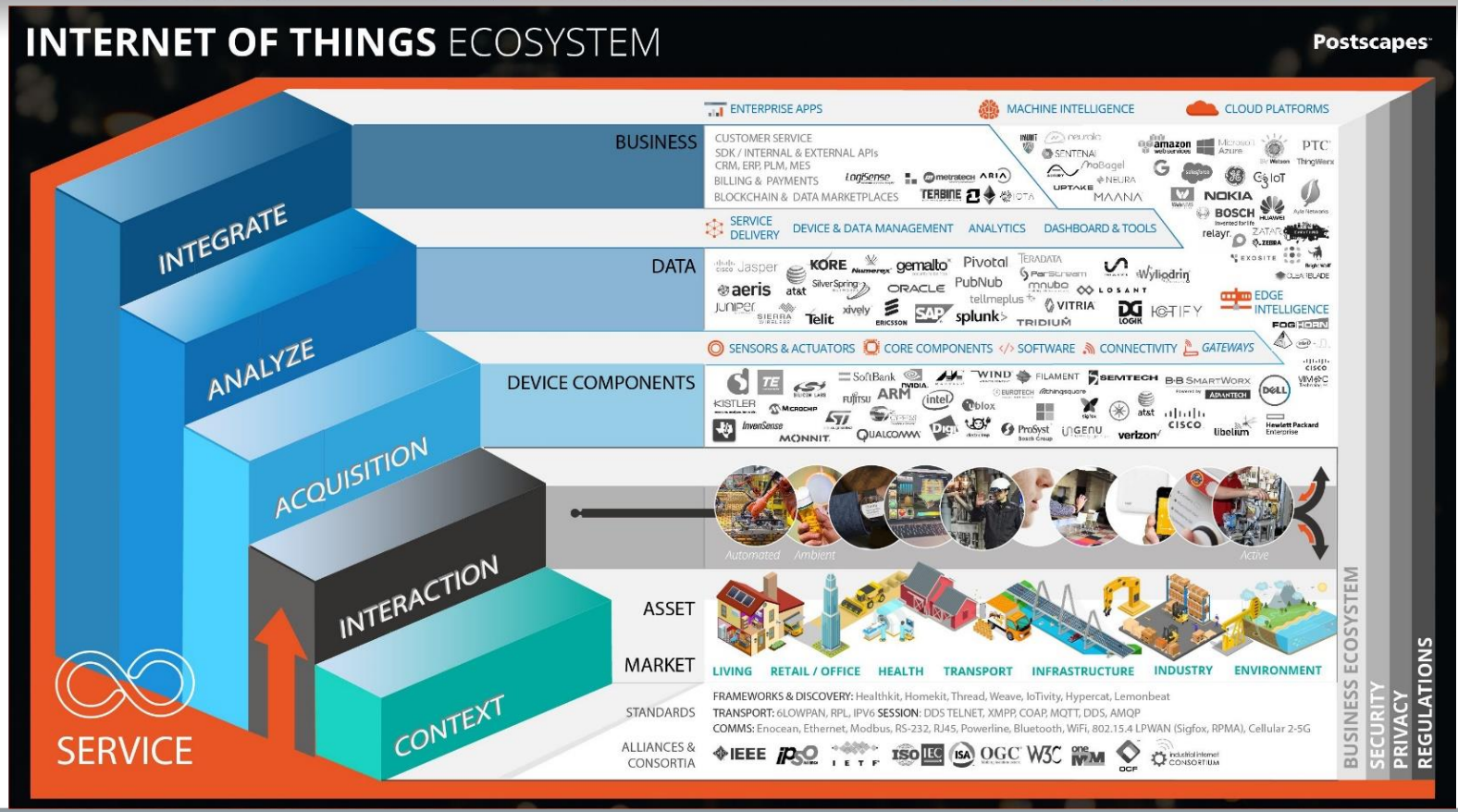
Products Renew Downloads Support Resource Center Blog

Mirai goes Enterprise

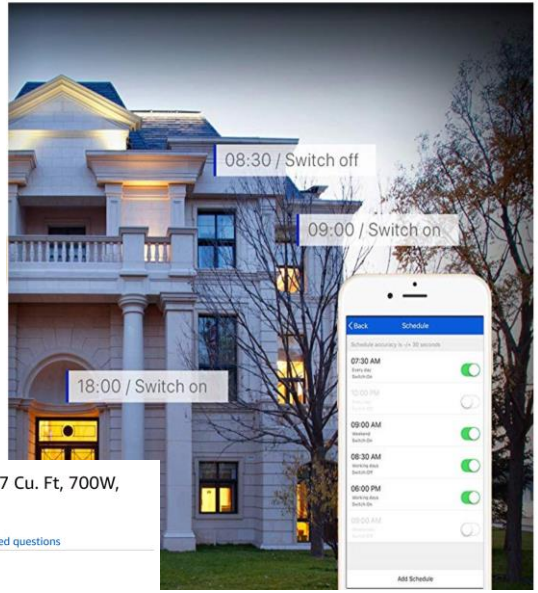
March 19, 2019

Yesterday we found a story about a new version of Mirai (a self-propagating botnet that targets IoT devices and was responsible for a massive DDoS attack on Dyn's servers back in 2016). According to the analysts, this botnet is equipped with a much wider range of exploits, which makes it even more dangerous and allows it to spread faster. More troubling is the fact that the new strain is targeting not only its usual victims — routers, IP cameras, and other "smart" things — but also enterprise IoT devices.

IOT Attack news


INTERNET OF THINGS ECOSYSTEM
Postscapes
ENTERPRISE APPS
MACHINE INTELLIGENCE
CLOUD PLATFORMS
BUSINESS
CUSTOMER SERVICE
SDK / INTERNAL & EXTERNAL APIs
CRM, ERP, PLM, MES
BILLING & PAYMENTS
BLOCKCHAIN & DATA MARKETPLACES
SERVICE DELIVERY
DEVICE & DATA MANAGEMENT
ANALYTICS
DASHBOARD & TOOLS
DATA
EDGE INTELLIGENCE
SENSORS & ACTUATORS
CORE COMPONENTS
SOFTWARE
CONNECTIVITY
GATEWAYS
DEVICE COMPONENTS
INTEGRATE
ANALYZE
ACQUISITION
INTERACTION
CONTEXT
SERVICE
Automated
Ambient
Active
ASSET
MARKET
LIVING
RETAIL / OFFICE
HEALTH
TRANSPORT
INFRASTRUCTURE
INDUSTRY
ENVIRONMENT
STANDARDS
FRAMEWORKS & DISCOVERY: Healthkit, Homekit, Thread, Weave, IoTivity, Hypercat, Lemonbeat
TRANSPORT: 6LOWPAN, RPL, IPV6 SESSION: DDS TELNET, XMPP, COAP, MQTT, DDS, AMQP
COMMS: Enocean, Ethernet, Modbus, RS-232, RJ45, Powerline, Bluetooth, WiFi, 802.15.4 LPWAN (Sigfox, RPMA), Cellular 2-5G
ALLIANCES & CONSORTIA
BUSINESS ECOSYSTEM
SECURITY
PRIVACY
REGULATIONS

Smart Home &Wearable devices



Smart WiFi Light Bulb, LED RGB Color Changing, Compatible with Amazon Alexa and Google Home Assistant, No Hub Required, A19 E26 Multicolor LUMIMAN 2 Pack

by LUMIMAN

358 customer reviews | 105 answered questions

Price: $24.99 ($12.50 / Count) prime

Get $70 off instantly: Pay $0.00 upon approval for the Amazon Prime Rewards Visa Card.

Style: **2 Pack RGBW Smart Bulb**

2 Pack RGBW Smart Bulb
$24.99 ($12.50 / Count)
prime

24FT LED Outdoor String Lights
from 1 seller

AmazonBasics Microwave, Small, 0.7 Cu. Ft, 700W, Works with Alexa

by Amazon

923 customer reviews | 345 answered questions

Price: $59.99 prime

FREE Delivery **Tuesday** Details

In Stock.

Ships from and sold by Amazon.com.

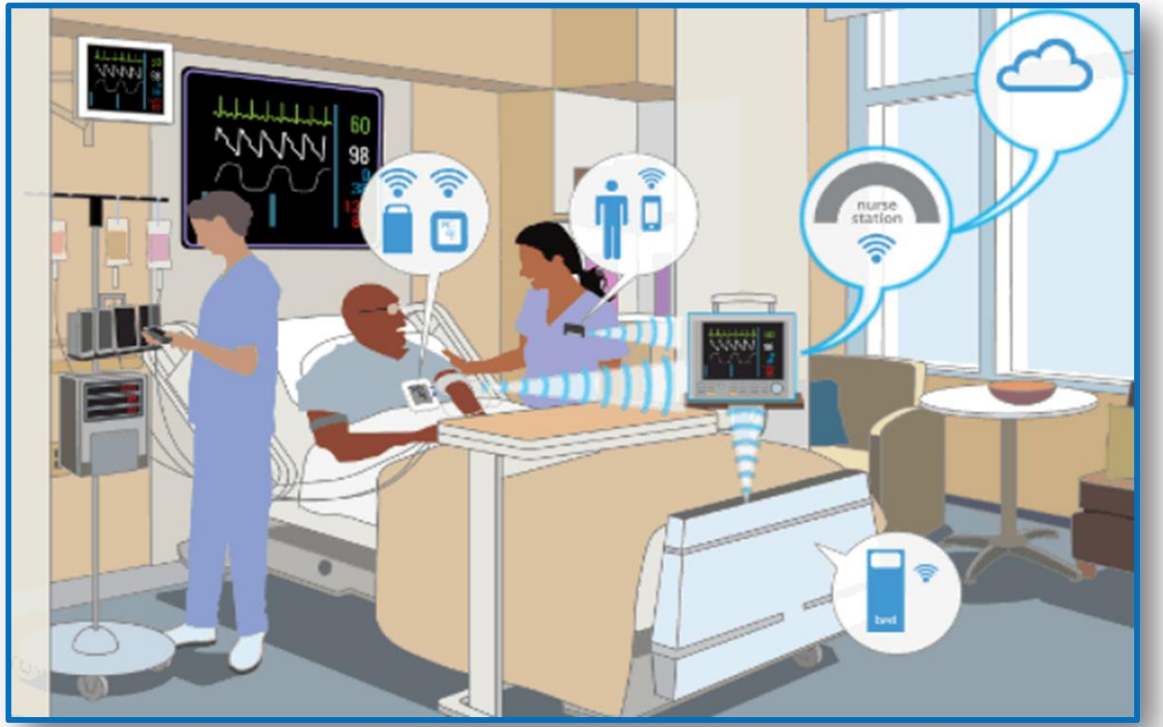
Configuration: **Microwave**

Microwave $59.99 prime

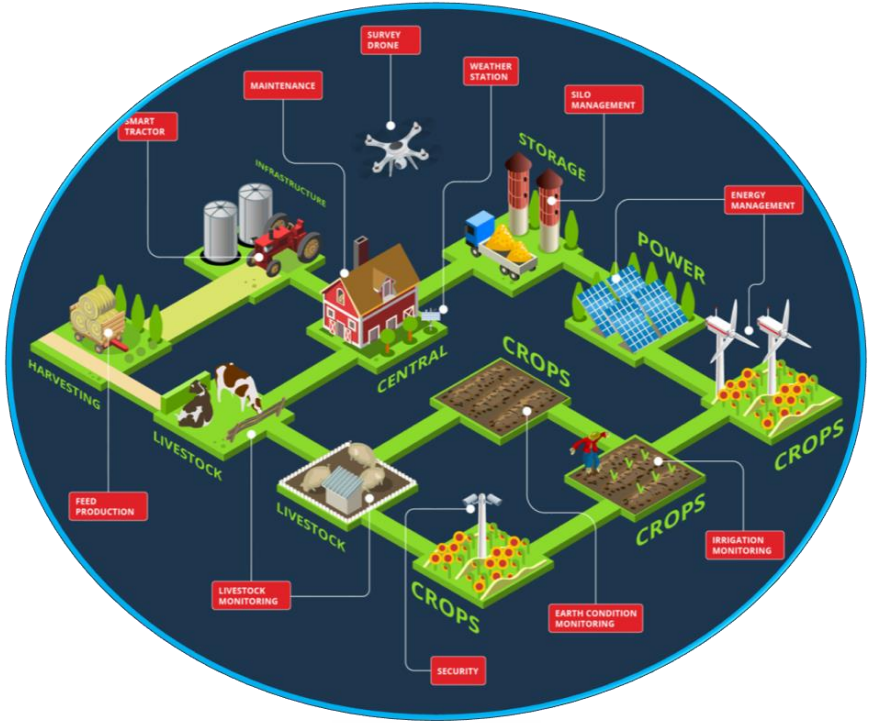
with Dot (Charcoal) $99.98 prime

with Dot (Heather Gray) $99.98 prime

IoT in Health

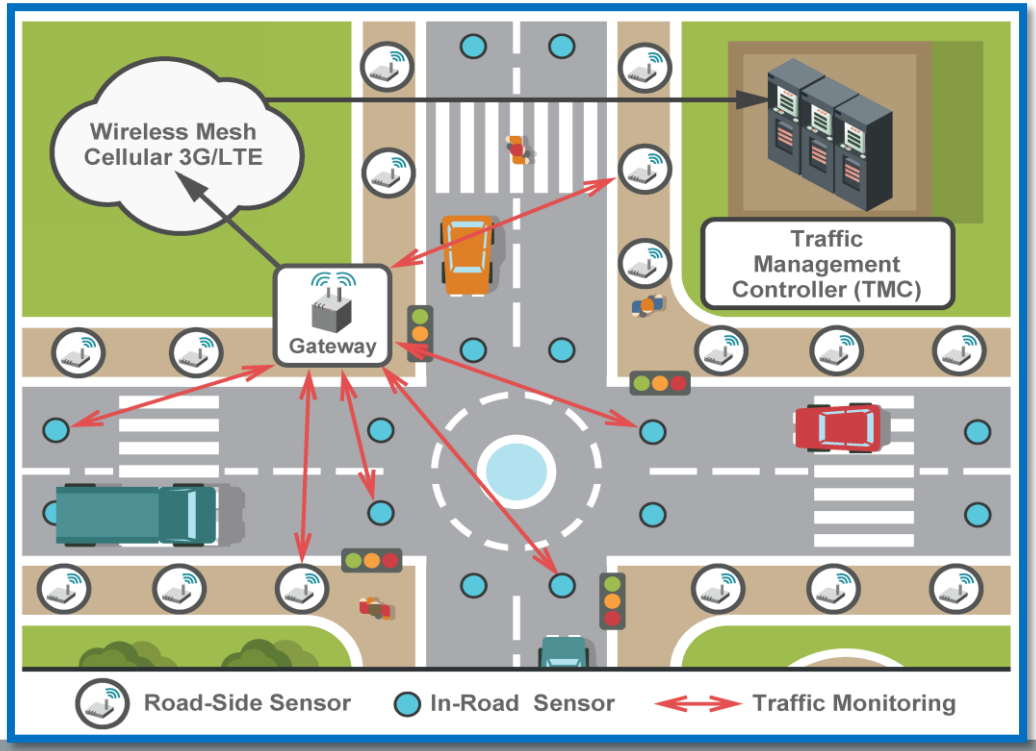


IoT in Agriculture



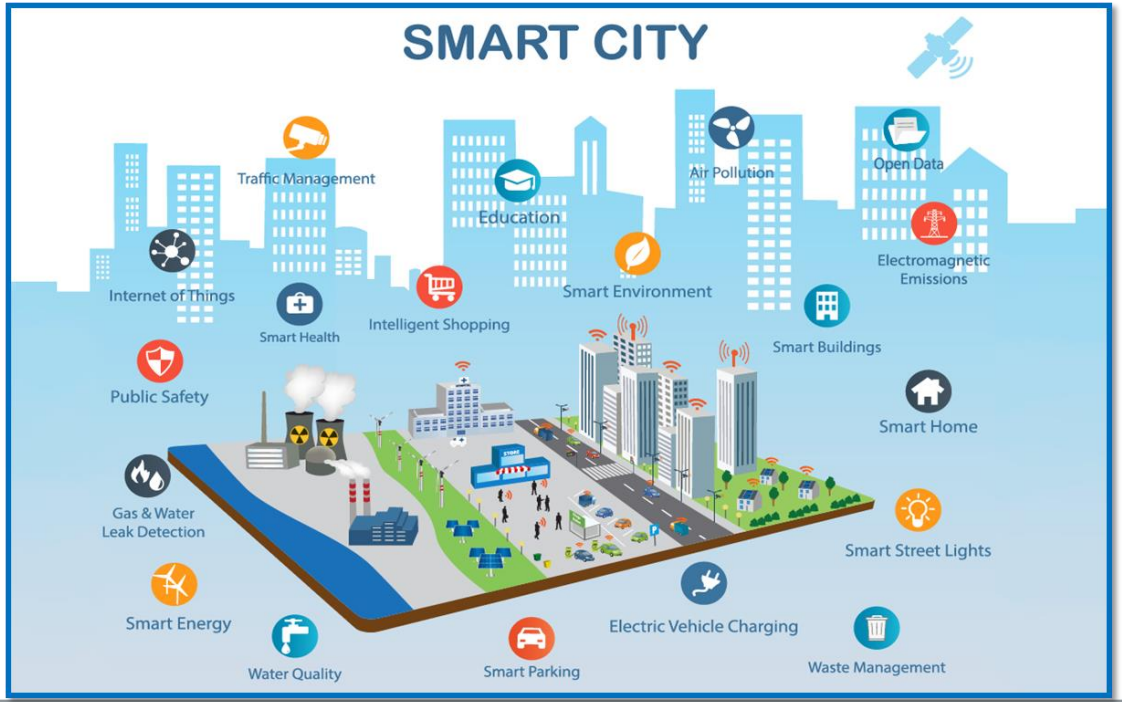
IoT in Education

IoT in Traffic

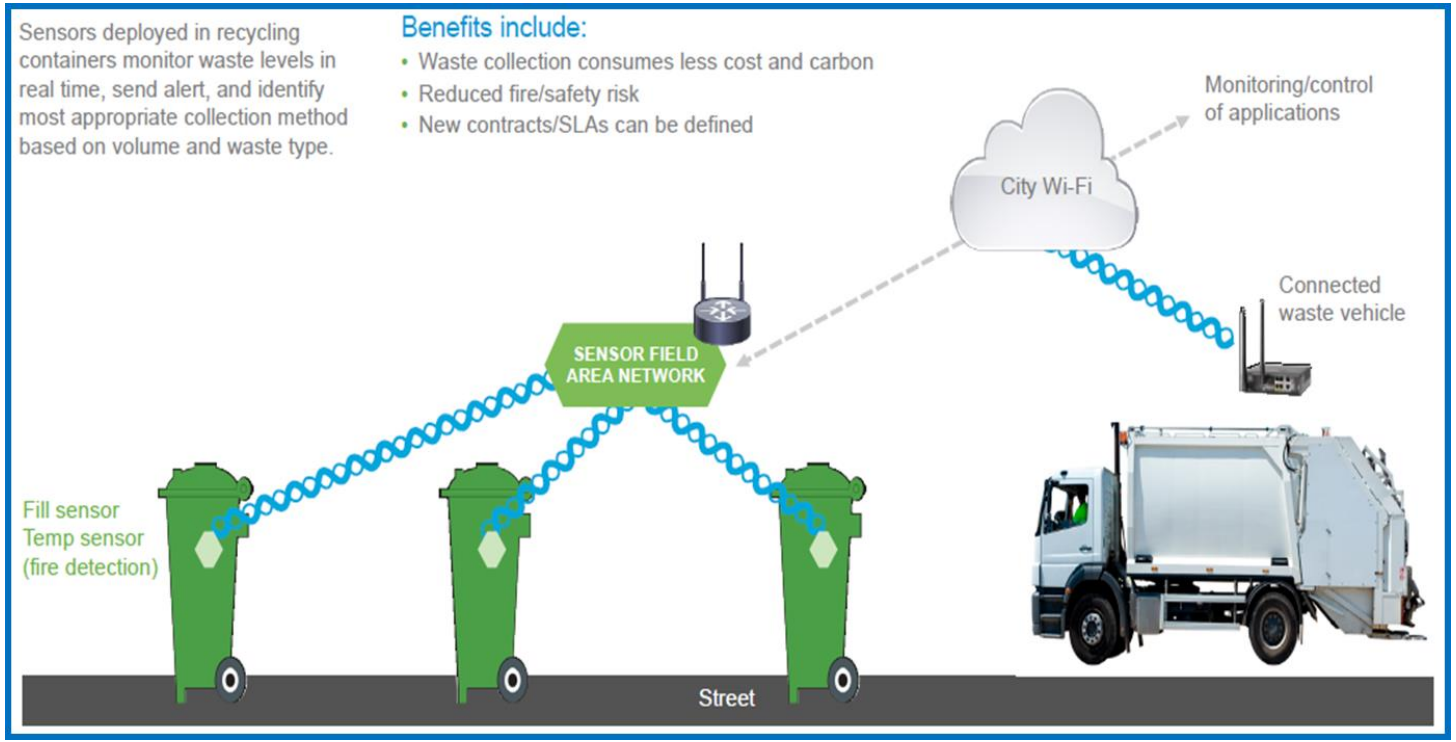


IoT in Retail

IoT in Smart City



IoT Based Waste Collection

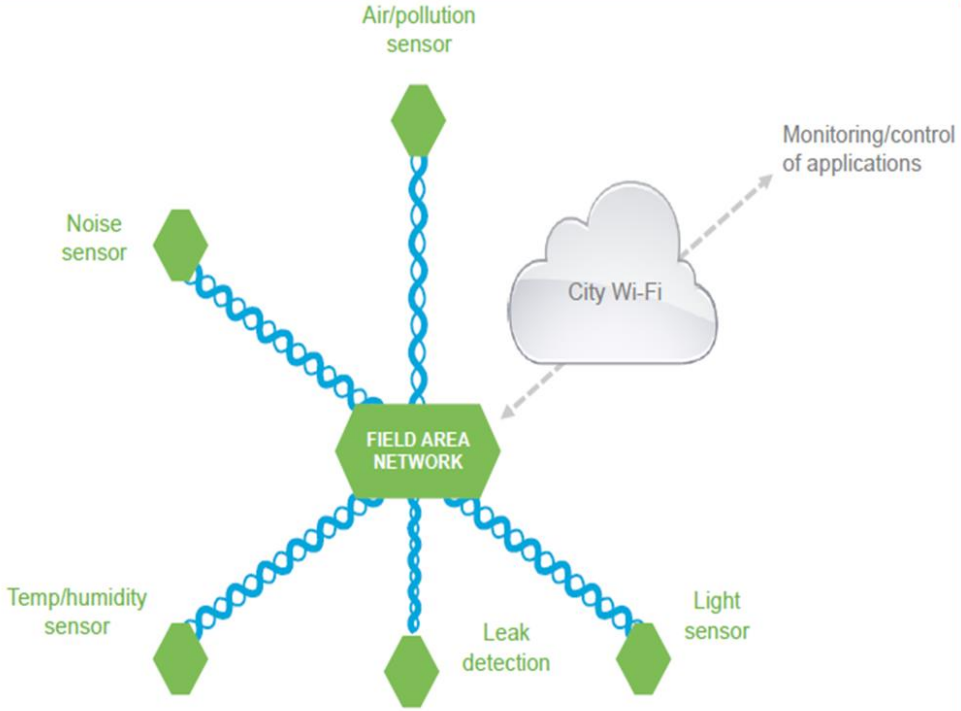


IoT Based Pollution Control

Installation of environment sensors: air, light, humidity, noise, etc.

Benefits include:

- Leverages parking sensor infrastructure
- Provides valuable data for improving analytics applications and forecasting



Smart Dust Bin in London

Smart Dust Bin in London (Cont.)

Smart Dust Bin in London (Cont.)

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	• Commercial/Institutional	• Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	• Industrial	• Process, Clean Room, Campus	
Energy	• Supply/Demand	• Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	• Alternative	• Solar Wind, Co-generation, Electrochemical	
	• Oil/Gas	• Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	• Infrastructure	• Wiring, Network Access, Energy management	Digital cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washer/ Dryers, Meters, Lights, TVs, MP3, Games Console, Alarms, etc.
	• Awareness & Safety	• Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	• Convenience & Entertainment	• HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	• Care	• Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	• In Vivo/Home	• Implants, Home, Monitoring Systems	
	• Research	• Drug Discovery, Diagnostics, Labs	
Transportation	• Non-Vehicular	• Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	• Vehicles	• Consumer, Commercial, Construction, Off-Highway	
	• Trans Systems	• Tolls, Traffic mgmt., Navigation	

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Industrial	• Resource Automation	• Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	• Fluid/Processes	• Petro-Chem, Hydro, Carbons, Food, Beverage	
	• Converting/Discrete	• Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	• Distribution	• Pipelines, Conveyance	
Retail	• Specialty	• Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	• Hospitality	• Hotels Restaurants, Bars, Cafes, Clubs	
	• Stores	• Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	• Surveillance	• Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	• Equipment	• Weapons, Vehicles, Ships, Aircraft, Gear	
	• Tracking	• Human, Animal, Postal, Food, Health, Baggage	
	• Public Infrastructure	• Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	• Emergency Service	• Ambulance, Police, fire, Homeland Security	
IT and Networks	• Public	• Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs. Routers, Switches, PBXs, etc.
	• Enterprise	• IT/Data Center Office, Privacy Nets	

OWASP TOP 10 INTERNET OF THINGS 2018

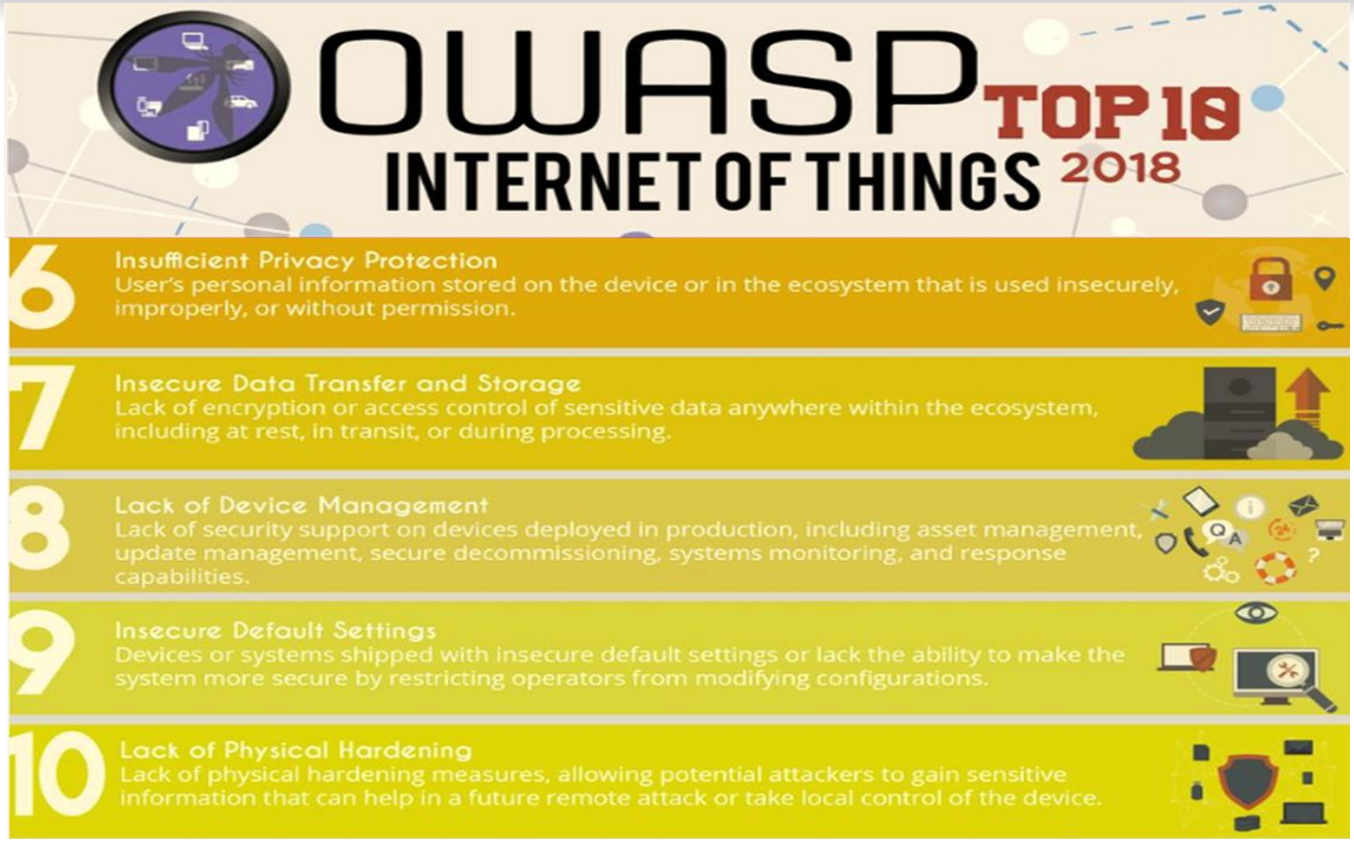
1 Weak, Guessable, or Hardcoded Passwords
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 Lack of Secure Update Mechanism
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.


OWASP TOP 10
INTERNET OF THINGS 2018
6
Insufficient Privacy Protection
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7
Insecure Data Transfer and Storage
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8
Lack of Device Management
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9
Insecure Default Settings
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
10
Lack of Physical Hardening
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

IoT Attack Surface Areas

Device Memory

- Cleartext credentials
- Third-party credentials
- Encryption keys

Ecosystem (general)

- Implicit trust between components
- Enrollment security
- Decommissioning system
- Lost access procedures

Device Physical Interfaces

- Firmware extraction
- User CLI
- Admin CLI
- Privilege escalation
- Reset to insecure state
- Removal of storage media
- Tamper resistance

Device Web Interface

- SQL injection
- Cross-site scripting
- Cross-site Request Forgery
- Username enumeration
- Weak passwords
- Account lockout
- Known default credentials

Device Firmware

- Hardcoded credentials
- Encryption keys
- Encryption (Symmetric, Asymmetric)
- Sensitive information
- Sensitive URL disclosure
- Firmware version display and/or last update date

IoT Attack Surface Areas

Device Network Services

- Information disclosure
- User CLI
- Administrative CLI
- Injection and Denial of Service
- Unencrypted Services
- Poorly implemented encryption
- UPnP
- Vulnerable UDP Services

Administrative Interface

- SQL injection
- Cross-site scripting
- Security/encryption options
- Logging options
- Two-factor authentication
- Inability to wipe device

Local Data Storage

- Unencrypted data
- Data encrypted with discovered keys
- Lack of data integrity checks

Cloud Web Interface

- SQL injection
- Cross-site scripting
- Transport encryption
- Insecure password recovery mechanism
- Two-factor authentication

Third-party Backend APIs

- Unencrypted PII sent
- Encrypted PII sent
- Device information leaked
- Location leaked

IoT Attack Surface Areas

Update Mechanism

- Update is not encrypted
- Updates not signed
- Update location writable
- Update verification & authentication
- Missing update mechanism
- No manual update mechanism

Mobile Application

- Implicitly trusted by device or cloud
- Username enumeration
- Account lockout
- Known default credentials
- Weak pass
- Transport encryption
- Insecure recovery mechanism

Vendor Backend APIs

- Inherent trust of cloud or mobile application
- Weak authentication
- Weak access controls
- Injection attacks
- Hidden services

Ecosystem Communication

- Health checks
- Heartbeats
- Ecosystem commands
- Deprovisioning
- Pushing updates

Network Traffic

- LAN
- LAN to Internet
- Short range
- Non-standard

IoT Security is the Worst-of-All-Worlds

- Network
  - services, encryption, firewall, input…
- Application
  - authN, authZ, input validation, etc.
- Mobile
  - insecure APIs, lack of encryption, etc.
- Cloud
  - AuthSessionAccess
- IoT
  - **net + app + mobile + cloud = IoT**

IoT Technologies and Protocols

Short-range Wireless Communication

- Bluetooth Low Energy (BLE)
- Light-Fidelity (Li-Fi)
- Near Field Communication (NFC)
- QR Codes and Barcodes
- Radio Frequency Identification (RFID)
- Thread
- Wi-fi
- Wi-Fi Direct
- Z-wave
- ZigBee

Medium-range Wireless Communication

- Ha-Low
- LTE-Advanced

Long-range Wireless Communication

- Low-power Wide-area Networking (LPWAN)
  - LoRaWAN
  - Sigfox
  - Neul
- Very Small Aperture Terminal (VSAT)
- Cellular

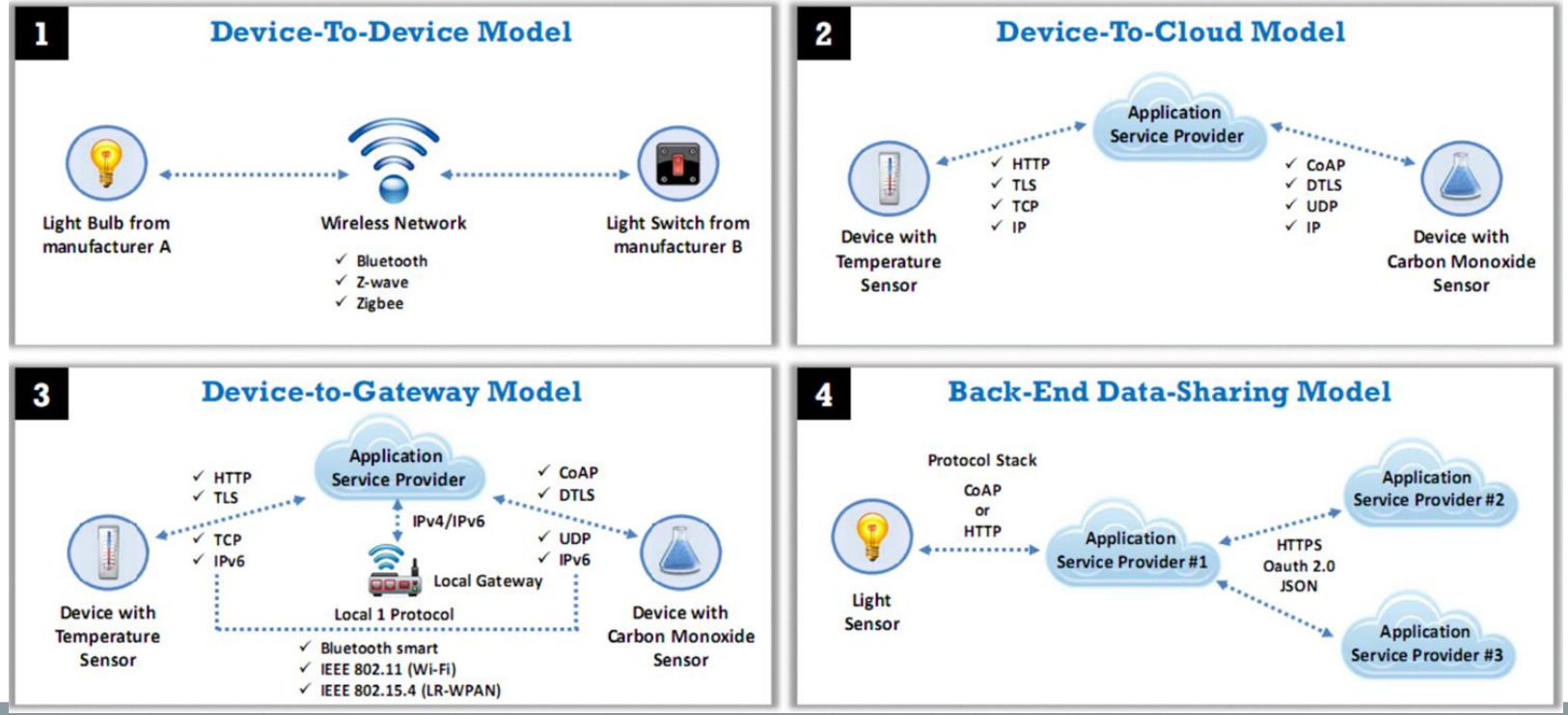
Wired Communication

- Ethernet
- Multimedia over Coax Alliance (MoCA)
- Power-line Communication (PLC)

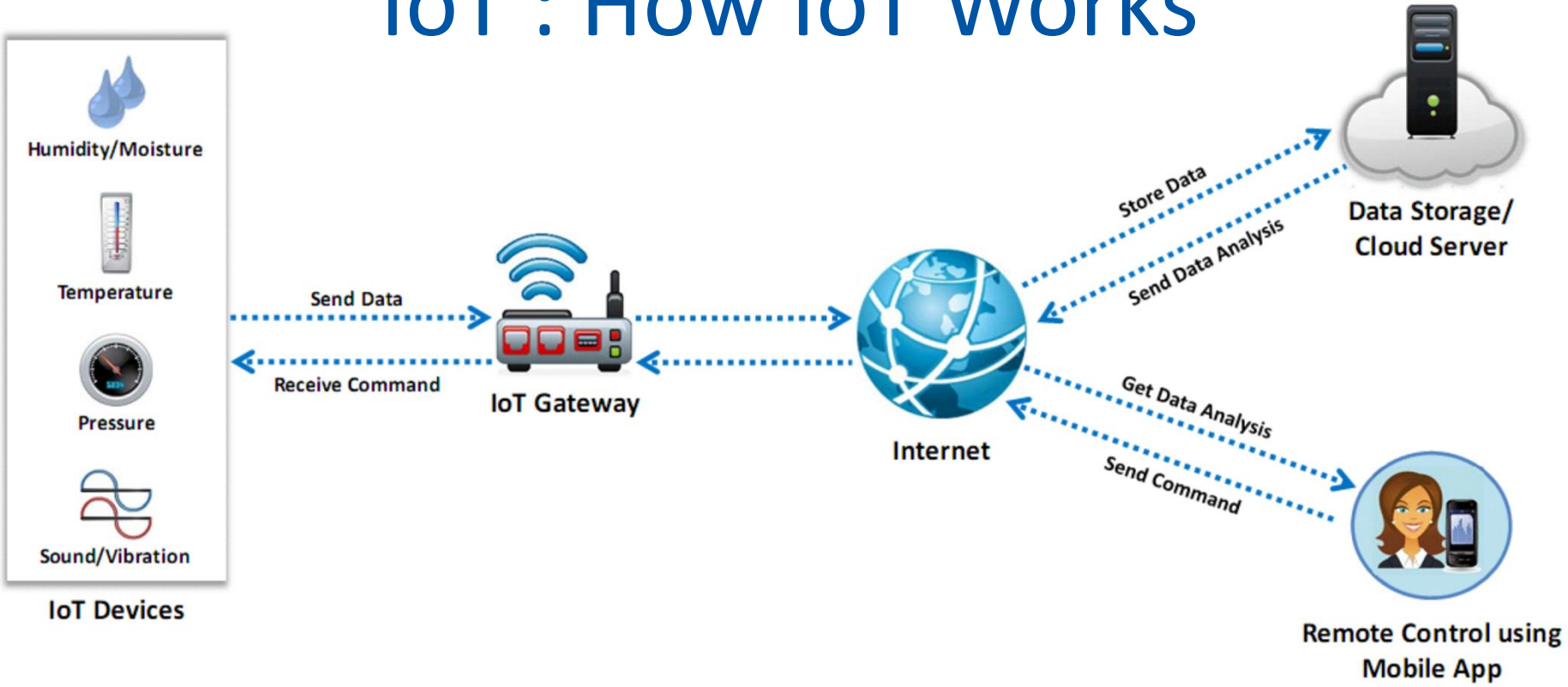
IoT Operating Systems

- RIOT OS
- ARM mbed OS
- RealSense OS X
- Nucleus RTOS
- Brillo
- Contiki
- Zephyr
- Ubuntu Core
- Integrity RTOS
- Apache Mynewt

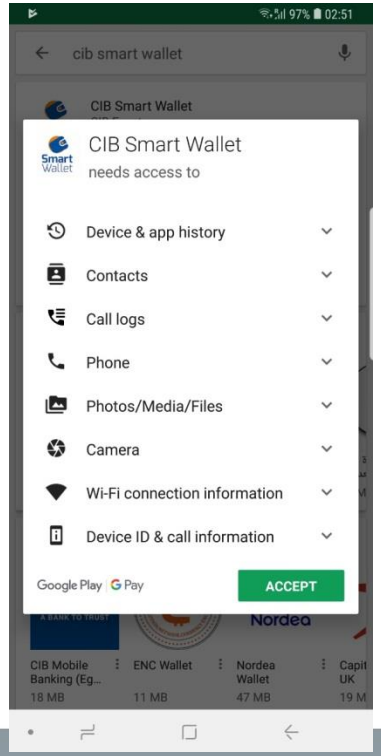
IoT Communication Models

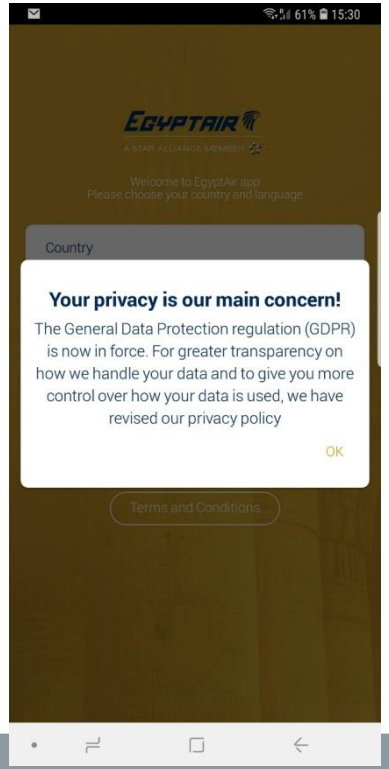


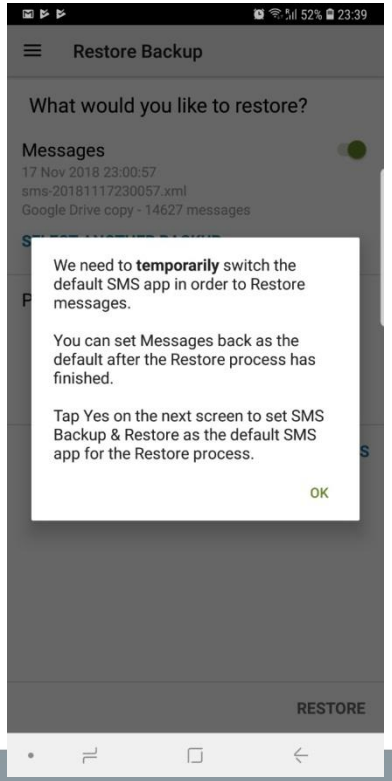
IoT : How IoT Works



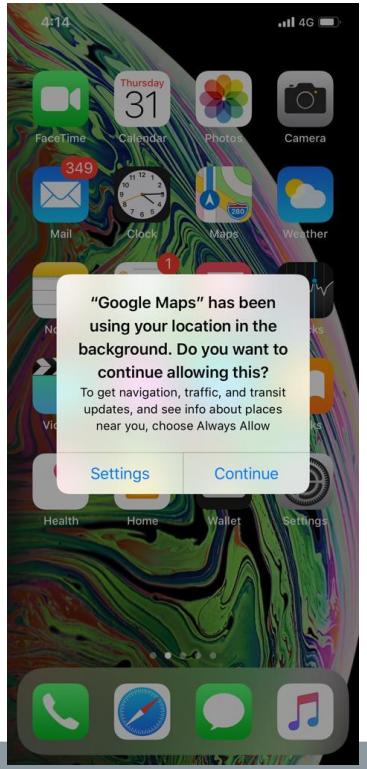
Data Leakage & Users Privacy Issues

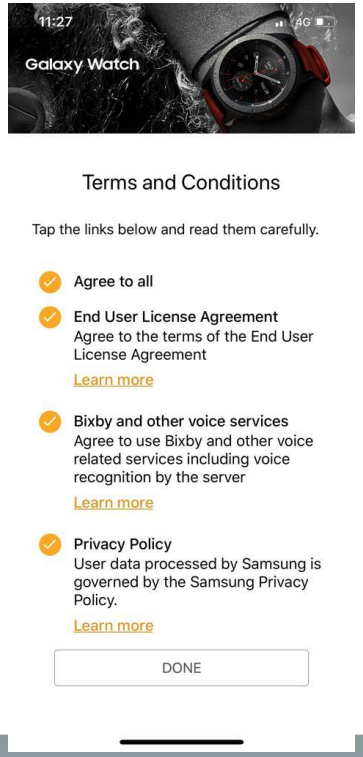


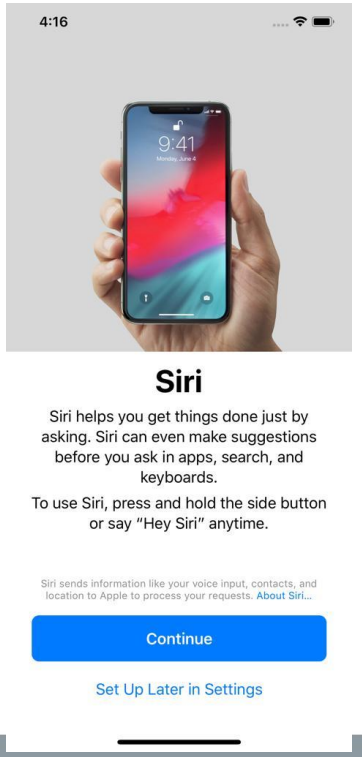




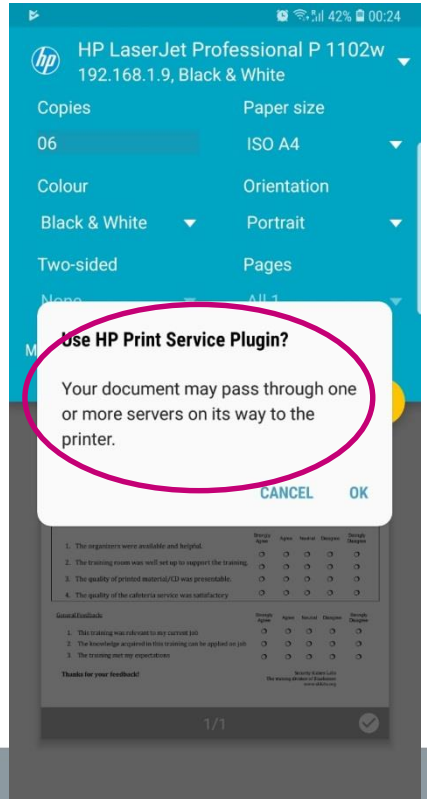
Data Leakage & Users Privacy Issues

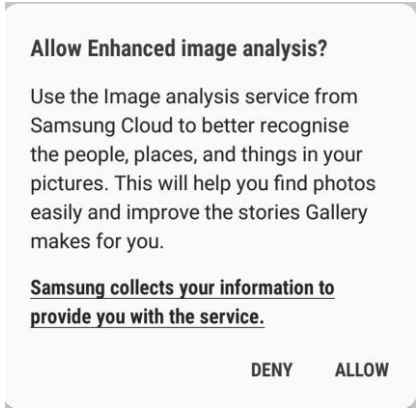


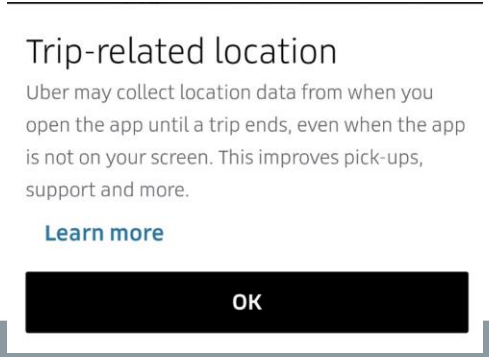


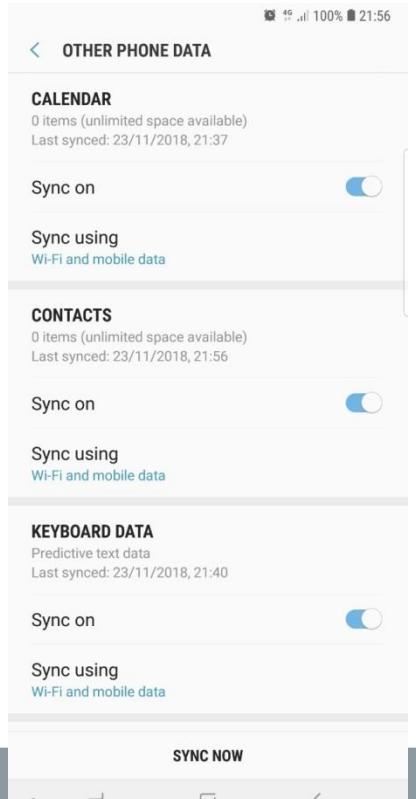


Data Leakage & Users Privacy Issues

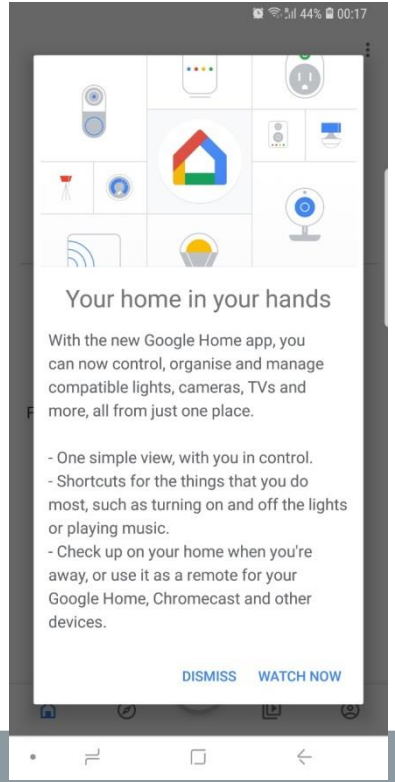


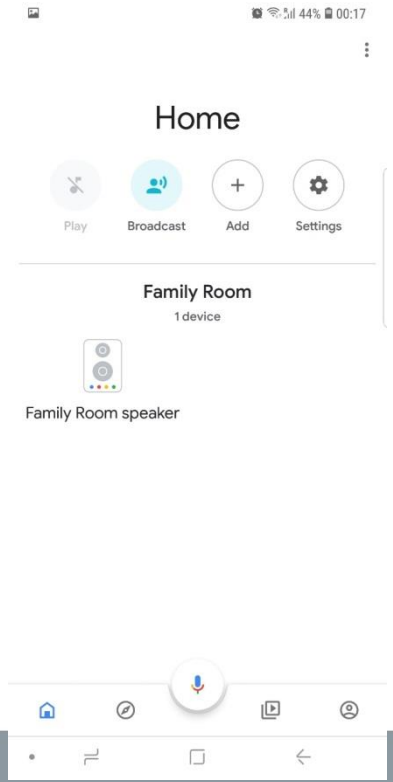


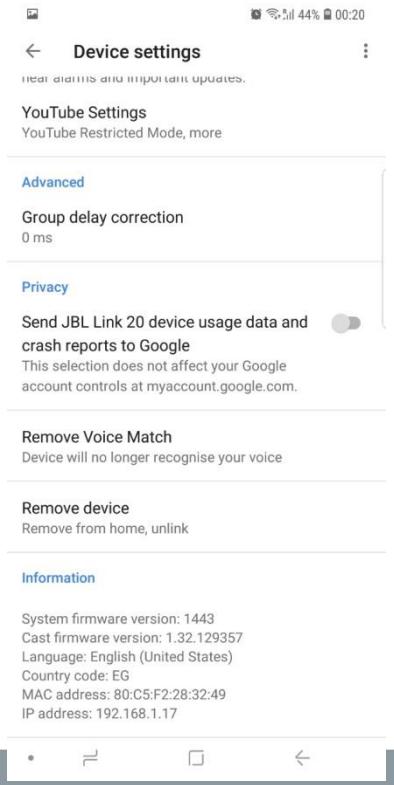




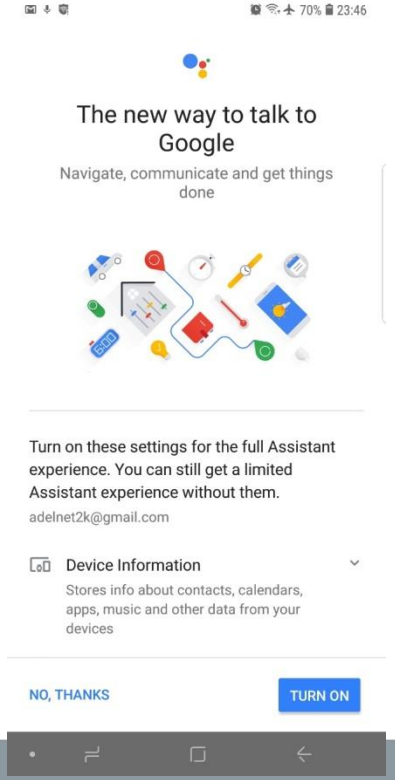
Google Services

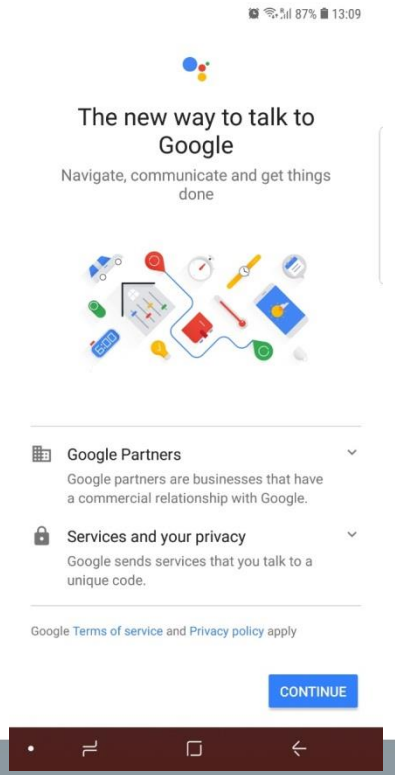




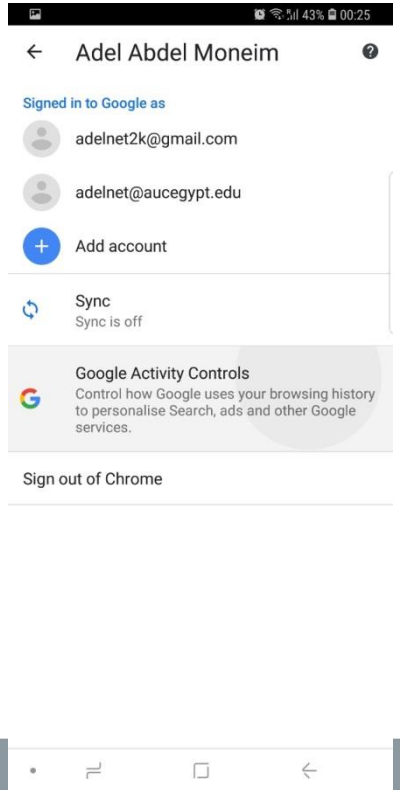


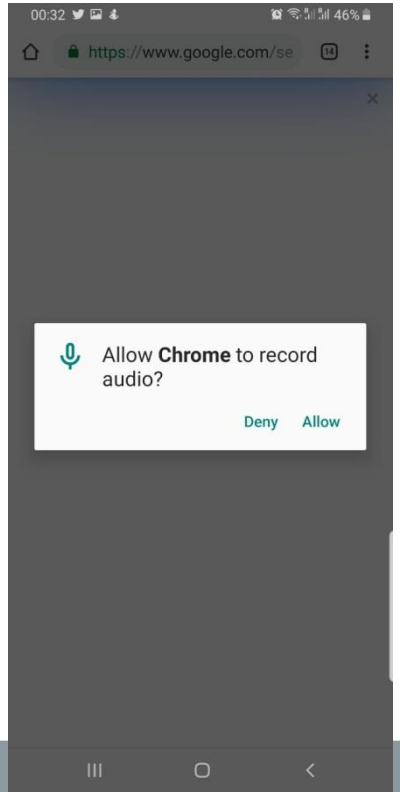
Google Services (Cont.)



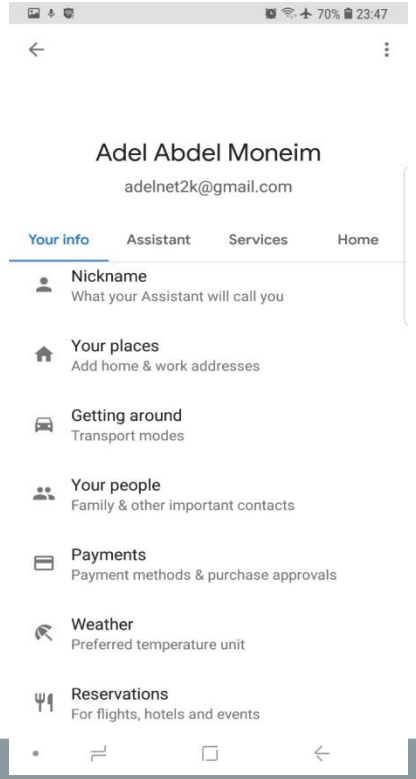


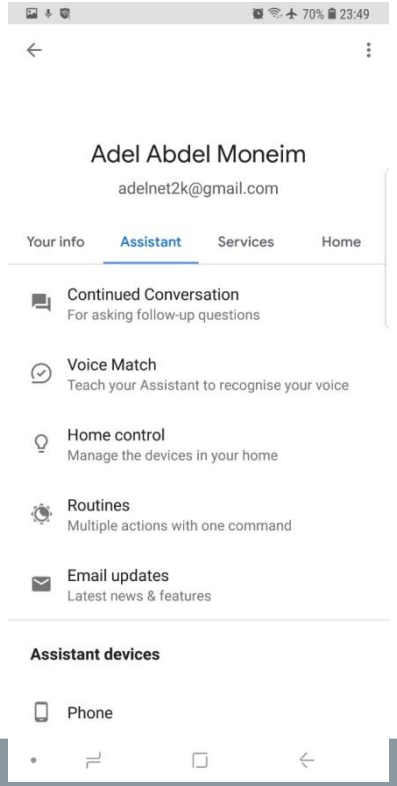
Google Services (Cont.)

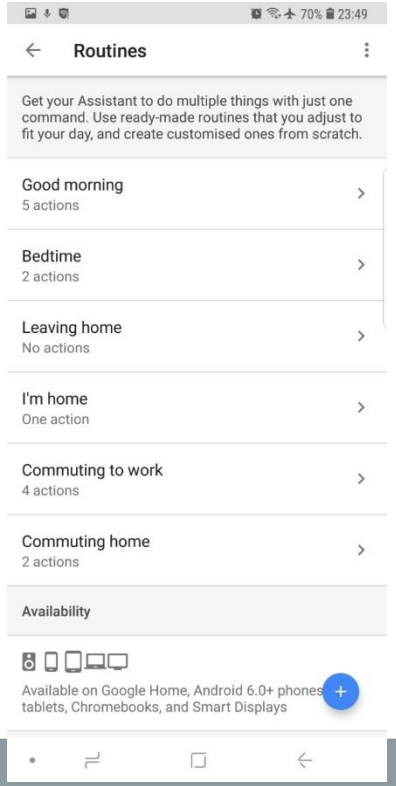




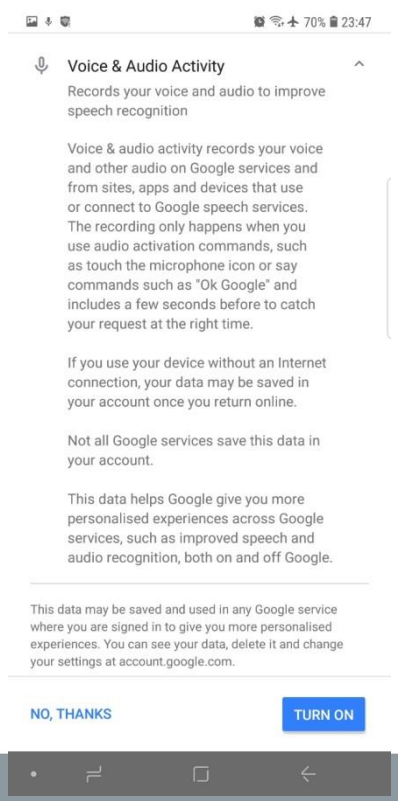
Google Services (Cont.)

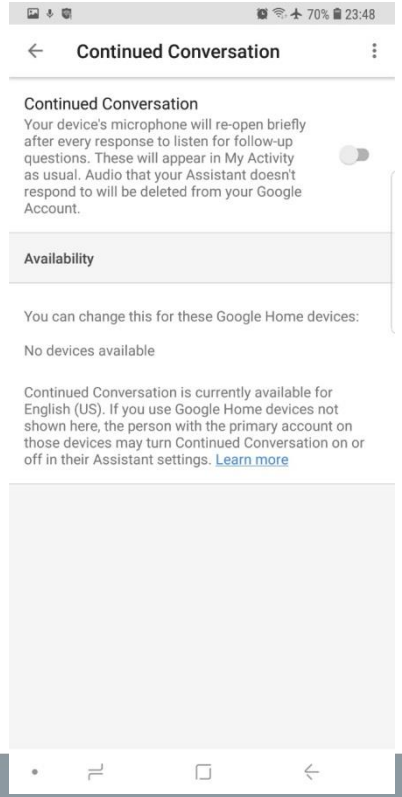


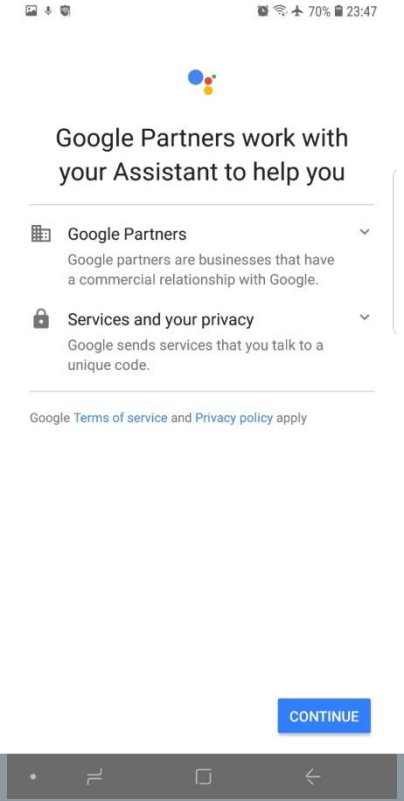




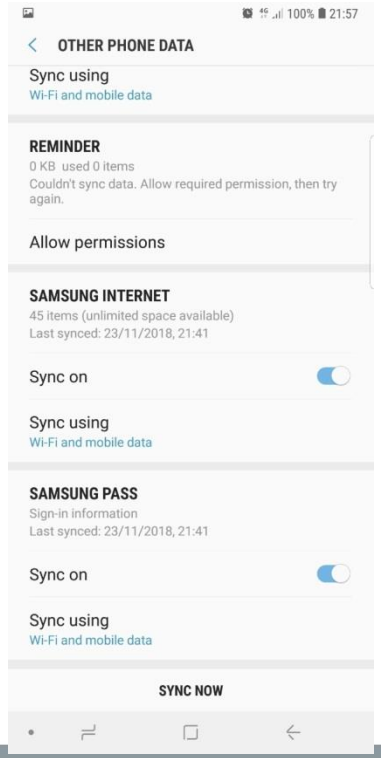
Google Services (Cont.)

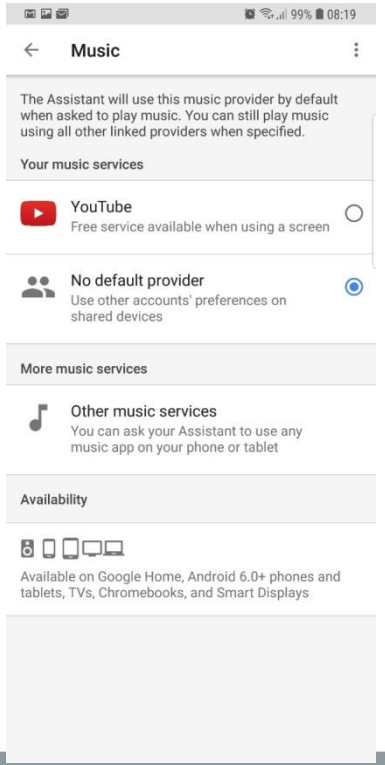




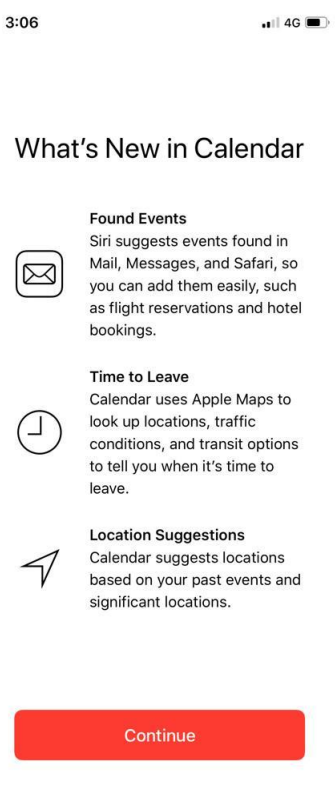


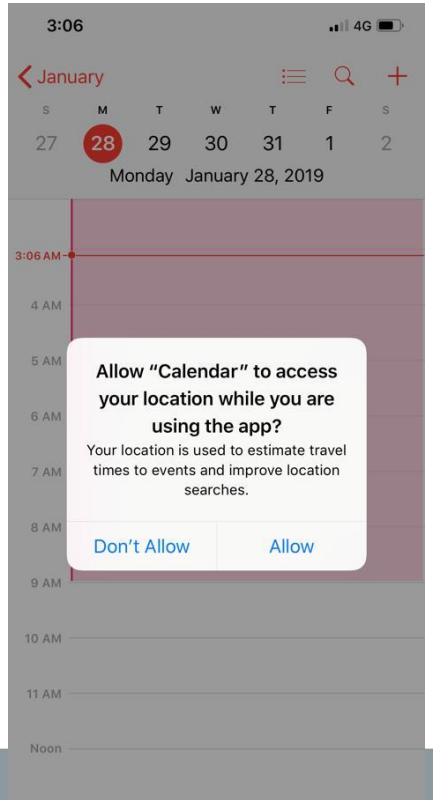
Google Services (Cont.)



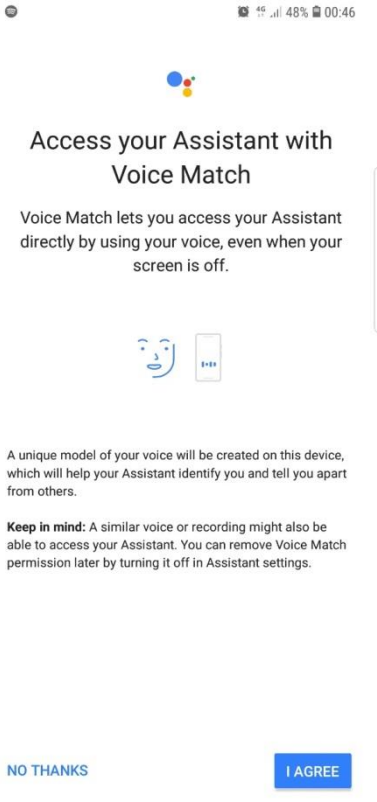


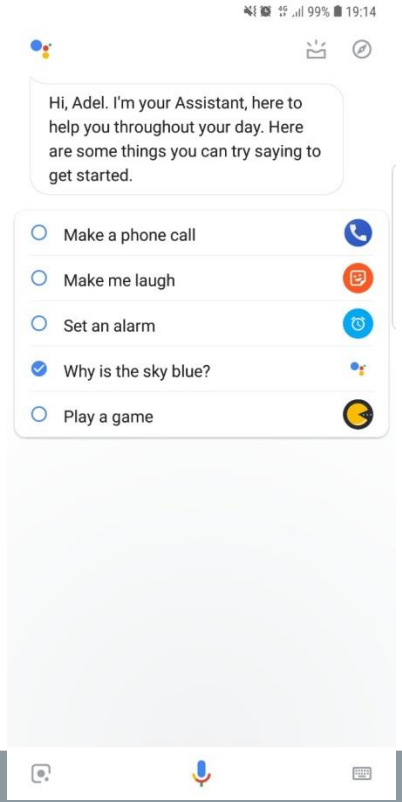
Google Services (Cont.)

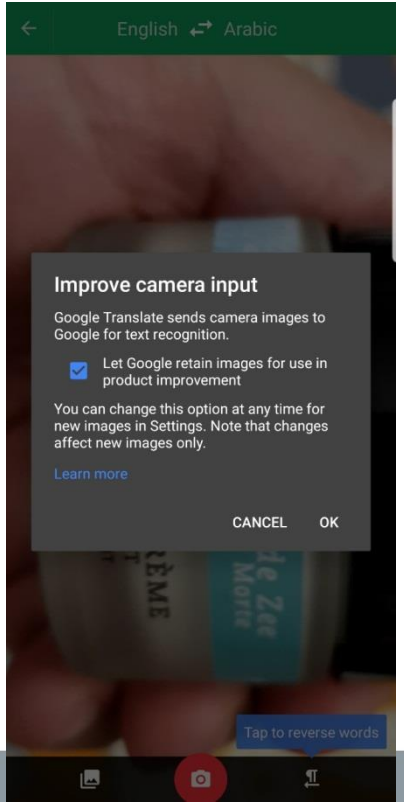




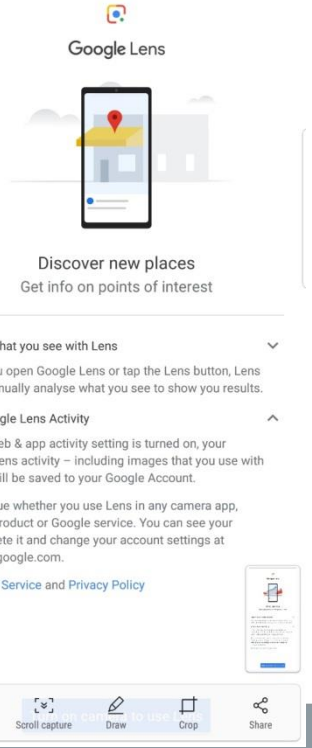
Google Services (Cont.)

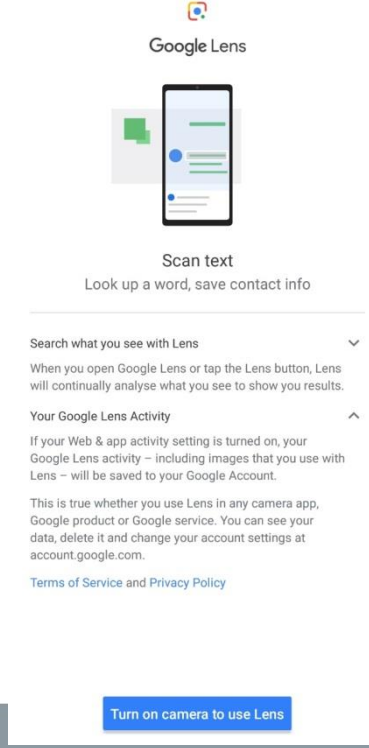


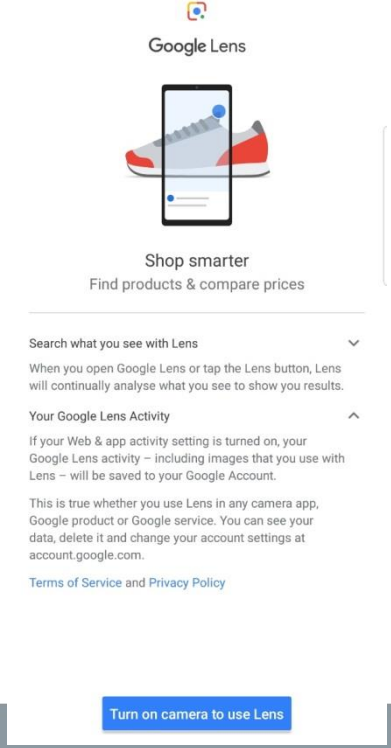


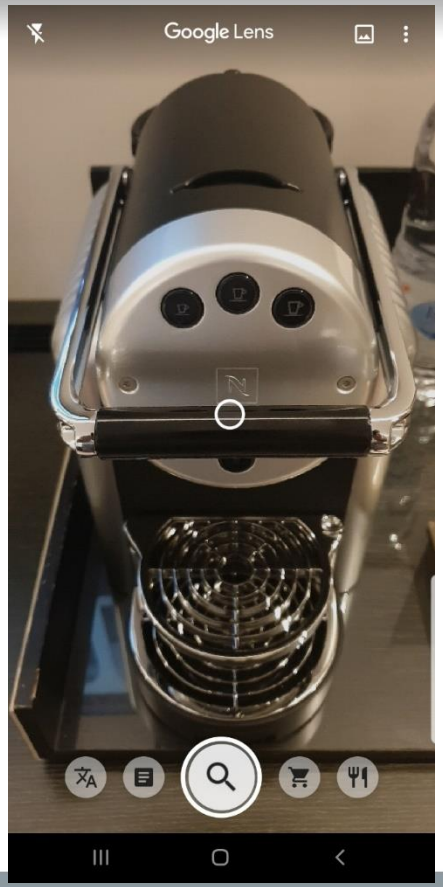


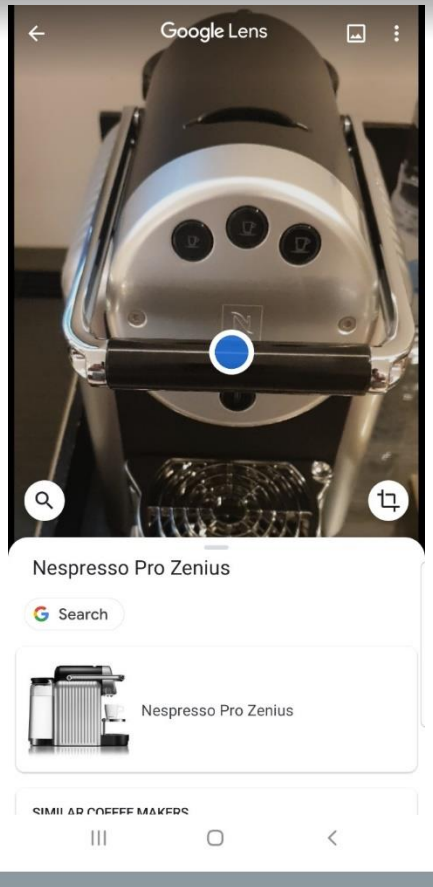
Google Services (Cont.)

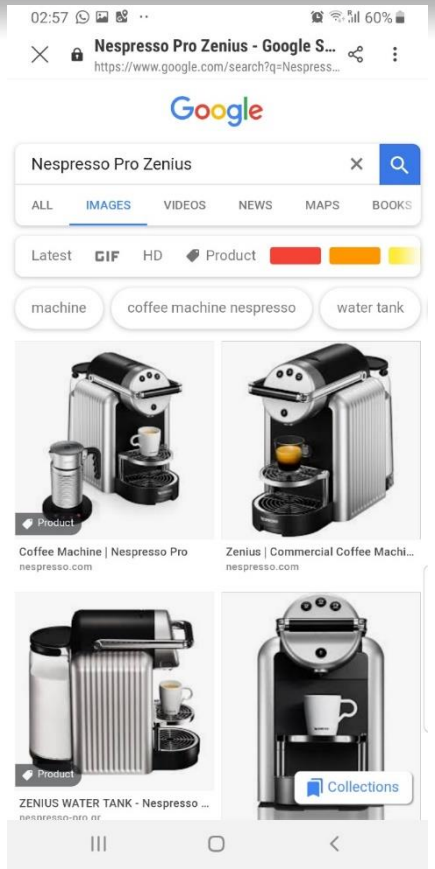







Google Lens


Google Lens
Nespresso Pro Zenius
Search
Nespresso Pro Zenius


02:57
60%
Nespresso Pro Zenius - Google S...
https://www.google.com/search?q=Nespress...
Google
Nespresso Pro Zenius
ALL
IMAGES
VIDEOS
NEWS
MAPS
BOOKS
Latest
GIF
HD
Product
machine
coffee machine nespresso
water tank
Product
Coffee Machine | Nespresso Pro
nespresso.com
Zenius | Commercial Coffee Machi...
nespresso.com
Product
ZENIUS WATER TANK - Nespresso ...
Collections

Google Services (Cont.)

Google admits it tracked user location data even when the setting was turned off

193

It did so via cell tower data

by Shannon Liao | @Shannon_Liao | Nov 21, 2017, 11:53am EST

SHARE TWEET LINKEDIN

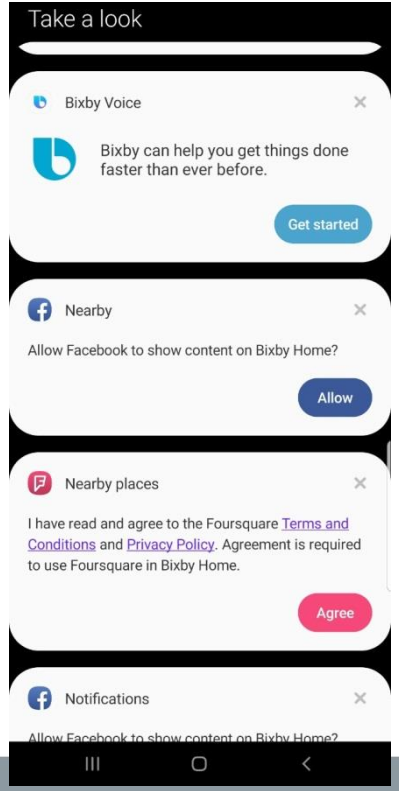
Ad closed by Google

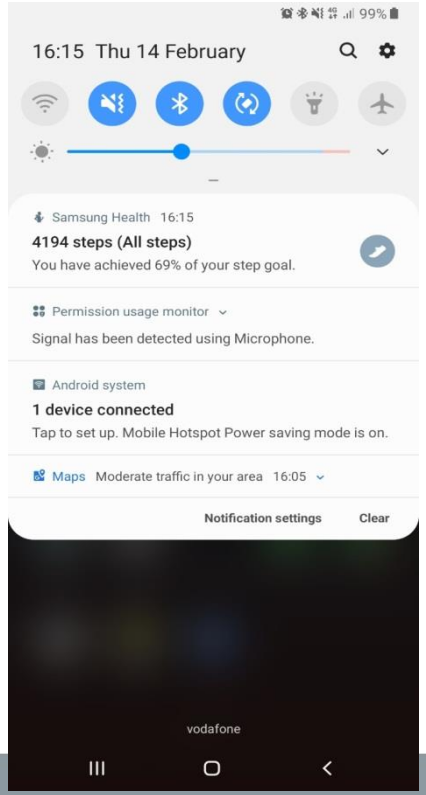
Report this ad

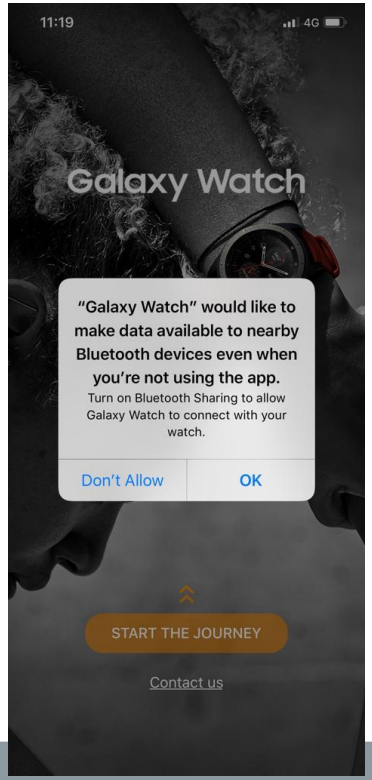
Ads by Google

Android phones gather your location data and send it to Google, even if you've turned off location services and don't have a SIM card, *Quartz* reported today.

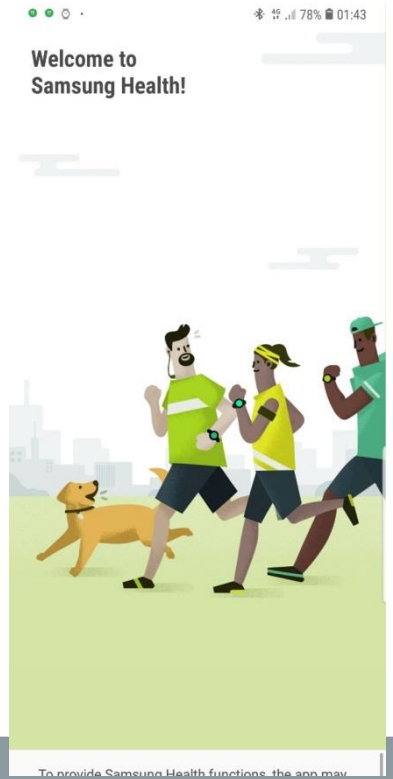
Samsung Health App

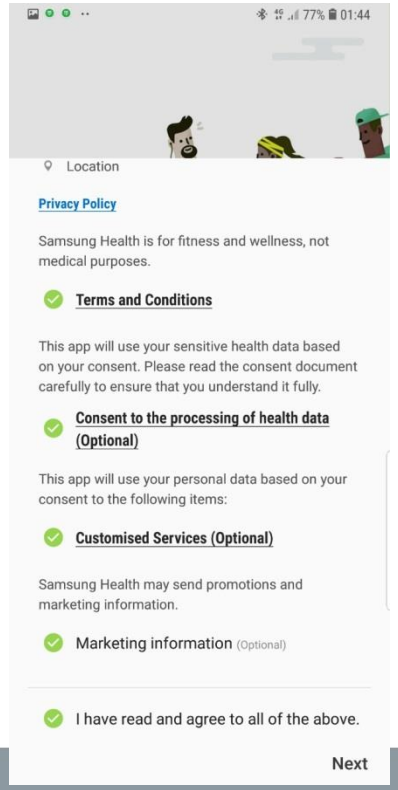


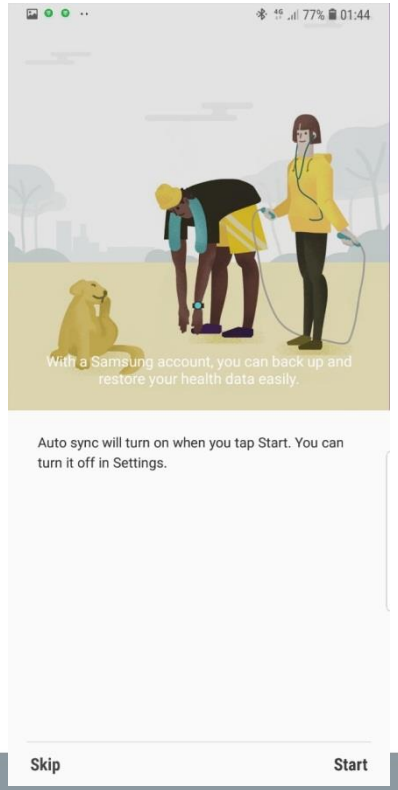




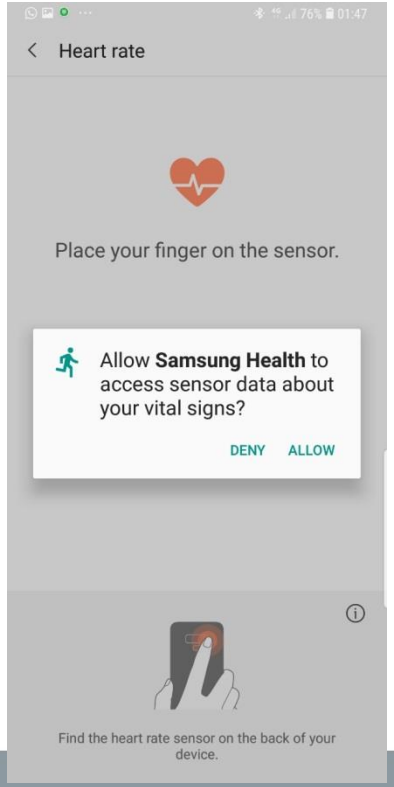
Samsung Health App

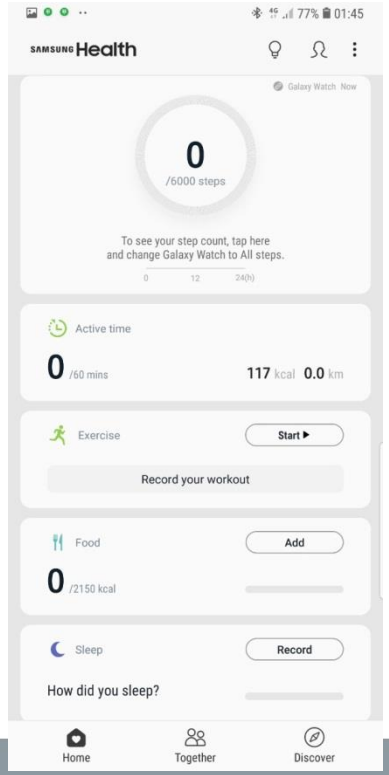


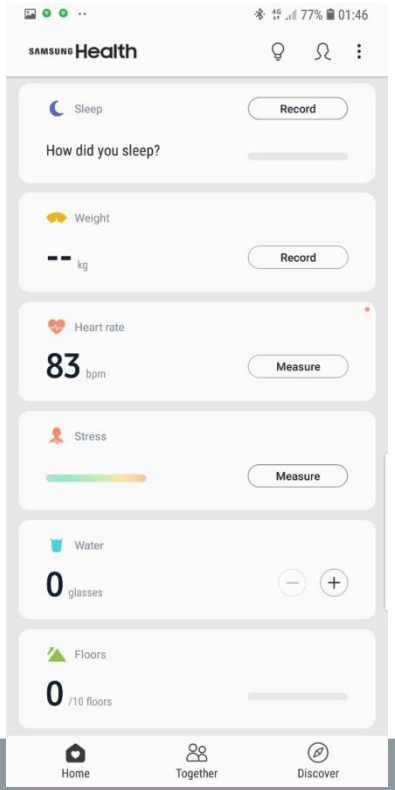




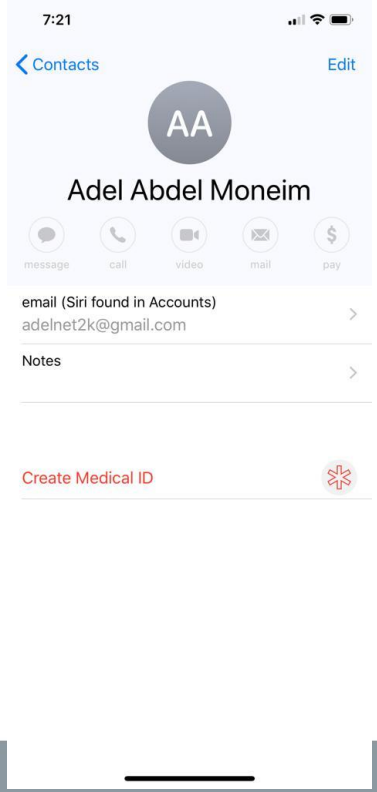
Samsung Health App (Cont.)

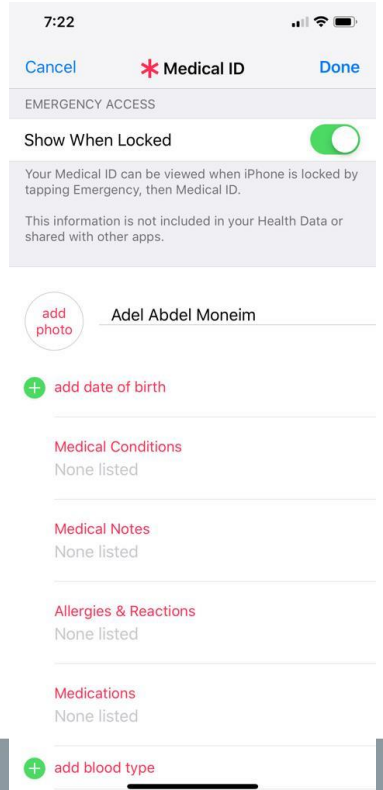


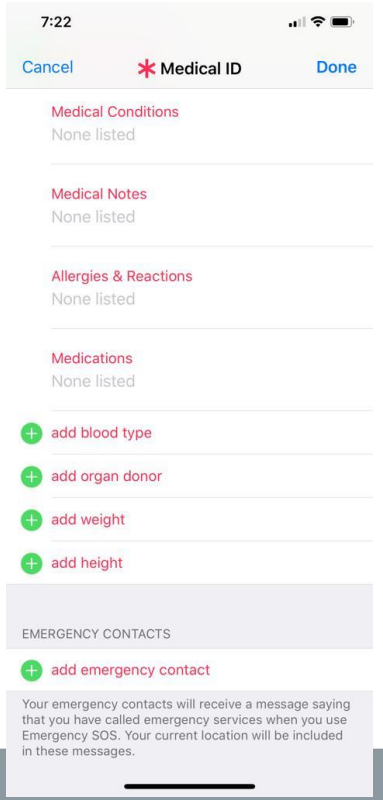




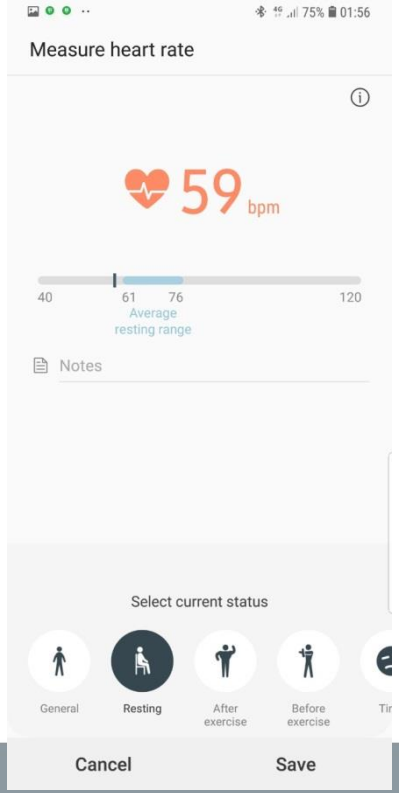
Samsung Health App (Cont.)

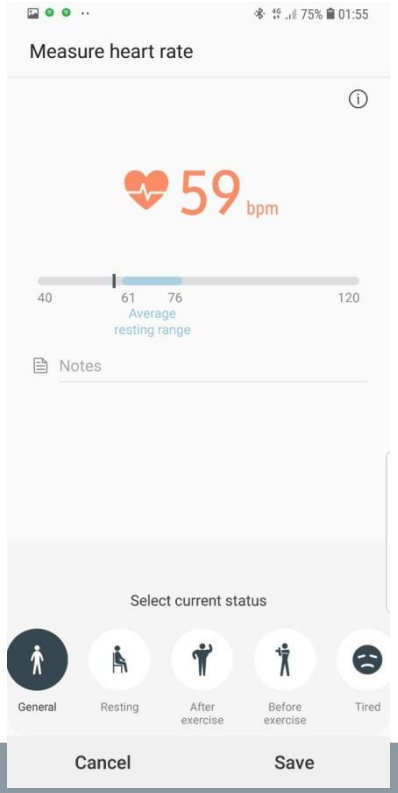


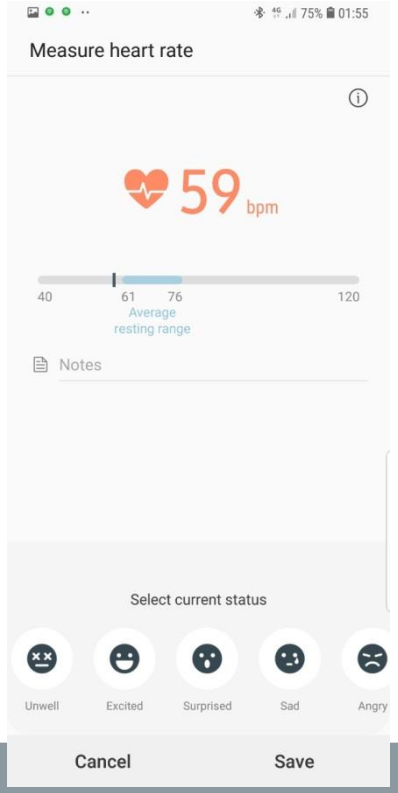


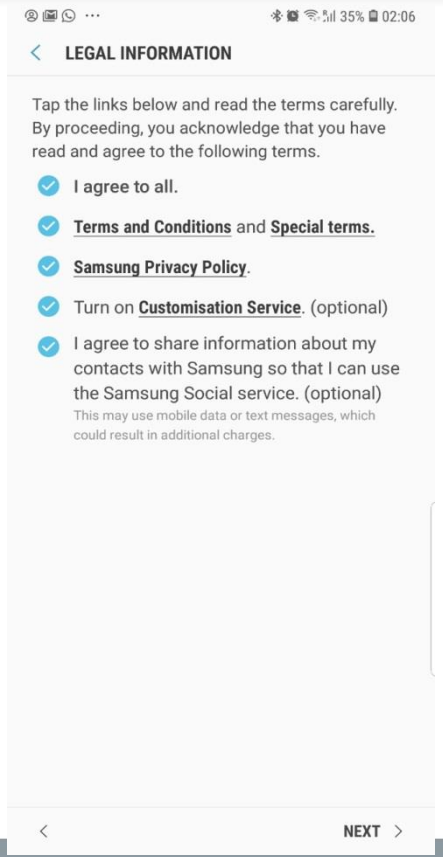


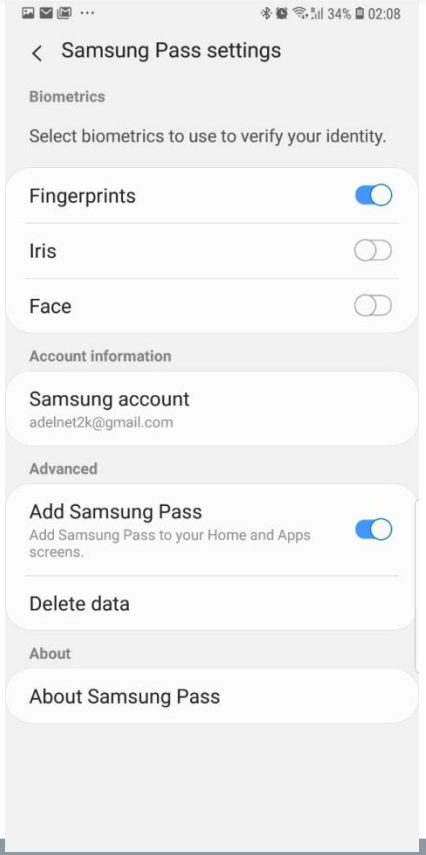
Samsung Health App (Cont.)








35% 02:06
LEGAL INFORMATION
Tap the links below and read the terms carefully. By proceeding, you acknowledge that you have read and agree to the following terms.
I agree to all.
Terms and Conditions and Special terms.
Samsung Privacy Policy.
Turn on Customisation Service. (optional)
I agree to share information about my contacts with Samsung so that I can use the Samsung Social service. (optional)
This may use mobile data or text messages, which could result in additional charges.
NEXT


34% 02:08
Samsung Pass settings
Biometrics
Select biometrics to use to verify your identity.
Fingerprints
Iris
Face
Account information
Samsung account
adelnet2k@gmail.com
Advanced
Add Samsung Pass
Add Samsung Pass to your Home and Apps screens.
Delete data
About
About Samsung Pass

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date June 25, 2019

Original Release Date September 24, 2019

Superseding Document

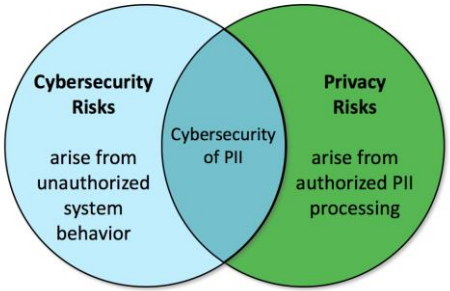
Status	Final
Series/Number	NIST Interagency or Internal Report (NISTIR) 8228
Title	Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Publication Date	June 2019
DOI	https://doi.org/10.6028/NIST.IR.8228
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8228/
Additional Information	NIST Cybersecurity for IoT Program https://www.nist.gov/programs-projects/nist-cyber program

Draft NISTIR 8259

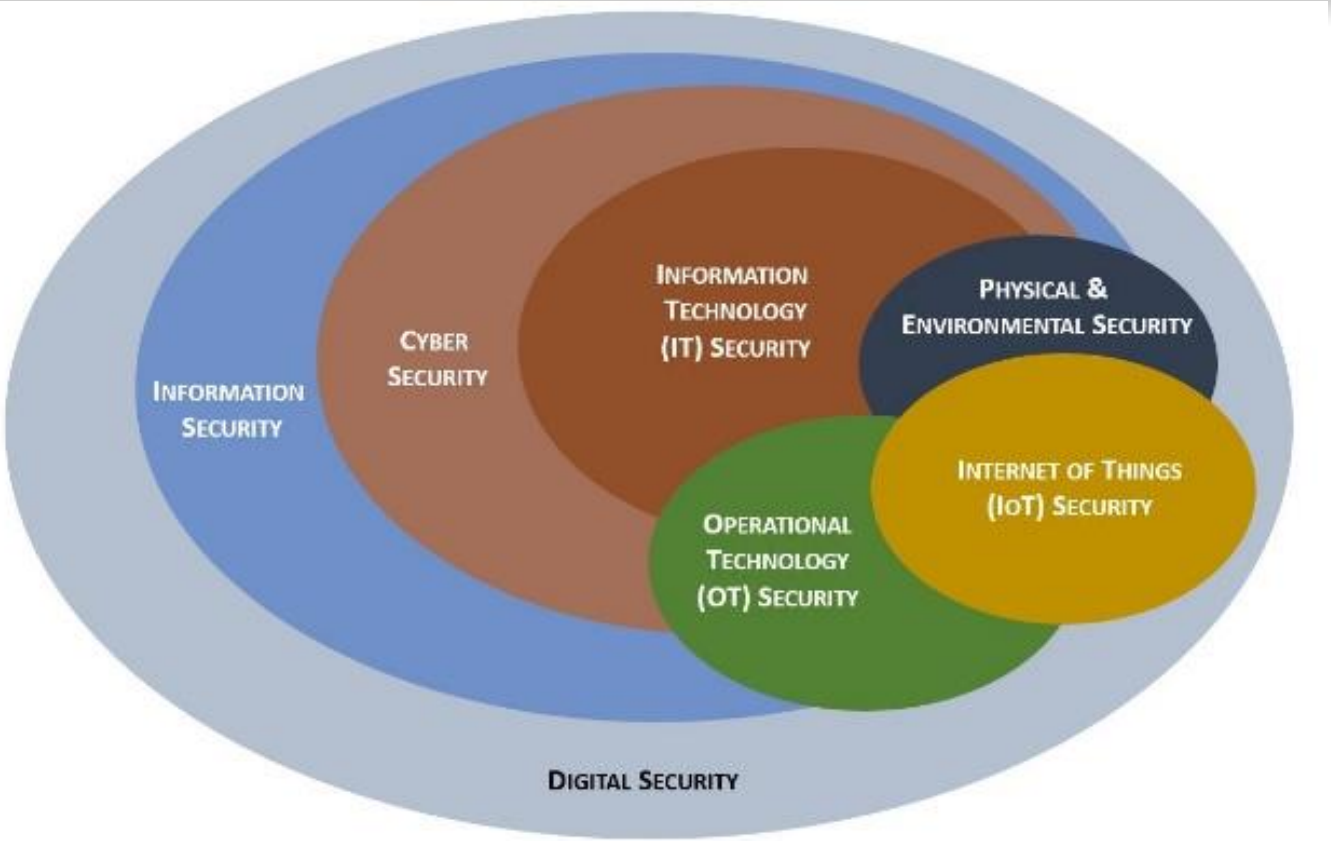
Core Cybersecurity Feature Baseline for Securable IoT Devices:

A Starting Point for IoT Device Manufacturers

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith



publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259-draft


INFORMATION SECURITY
CYBER SECURITY
INFORMATION TECHNOLOGY (IT) SECURITY
PHYSICAL & ENVIRONMENTAL SECURITY
INTERNET OF THINGS (IoT) SECURITY
OPERATIONAL TECHNOLOGY (OT) SECURITY
DIGITAL SECURITY

Contact Information

adelnet2k@gmail.com

@adelnet2k

www.facebook.com/adelnet2k

www.linkedin.com/in/Adel-Abdel-Moneim

Questions?

ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters
Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

THANK YOU