Internet of Things :

What are the **Privacy and Security** Risks involved ?

are they listening to what the shouldn't 🤔

Nandulal Krishna
S5 Computer Engineering

Seminar Contents

മലപ്പുറം-ഗൺ മുതൽ
മെഷീൻ-കത്തി വരെ

Agenda

01. **Introduction.**
    - 01.a. What is Internet of Things?
    - 01.b. 5-Layer IoT Architecture.
    - 01.c. Why IoT Security is more Important than Traditional Security.
02. **Real World Applications of IoT.**
03. **IoT Security Threats - The Threat Landscape.**
    - 03.a. Communication Standards.
    - 03.b. Communication Protocols.
    - 03.c. Hardware Vulnerabilities.
    - 03.d. Software Vulnerabilities.

Agenda

04. **Privacy Threat Landscape.**
    - 04.a. Data Collection.
    - 04.b. Illegal/Mass Surveillance.
    - 04.c. Data Dumps from Security Breaches.
05. **Real World Incidents.**
06. **How to Implement a Secure IoT Network.**
    - 06.a. Hardware Security.
    - 06.b. Software/Firmware Security.
    - 06.c. Network Security.
    - 06.d. Client/User Side Policies and Incident Response.
07. **Conclusion**

0.1. Introduction

What is Internet of Things ?

IoT is the Physical Devices that are **Connected to the Internet** , Sir.

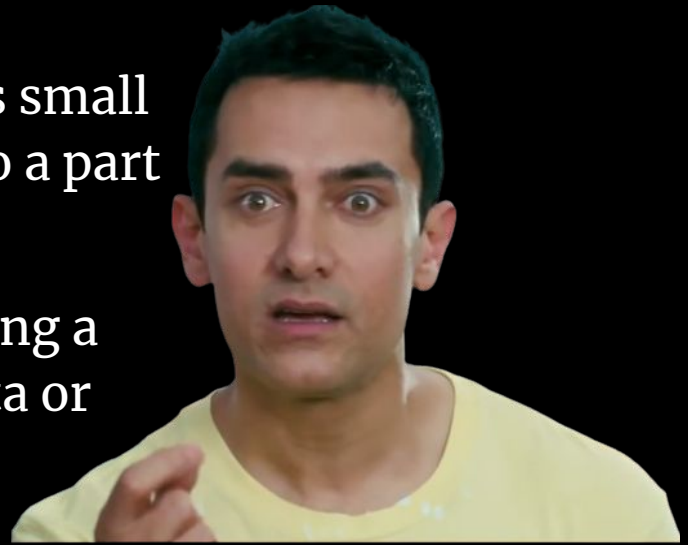
They **Collect Data and eXchange** them to do specific tasks

And the makes our lives **Easier**

Will You Please Elaborate ?

it's possible to turn anything, from something as small as a Pill to something as big as an Aeroplane, into a part of the IoT.

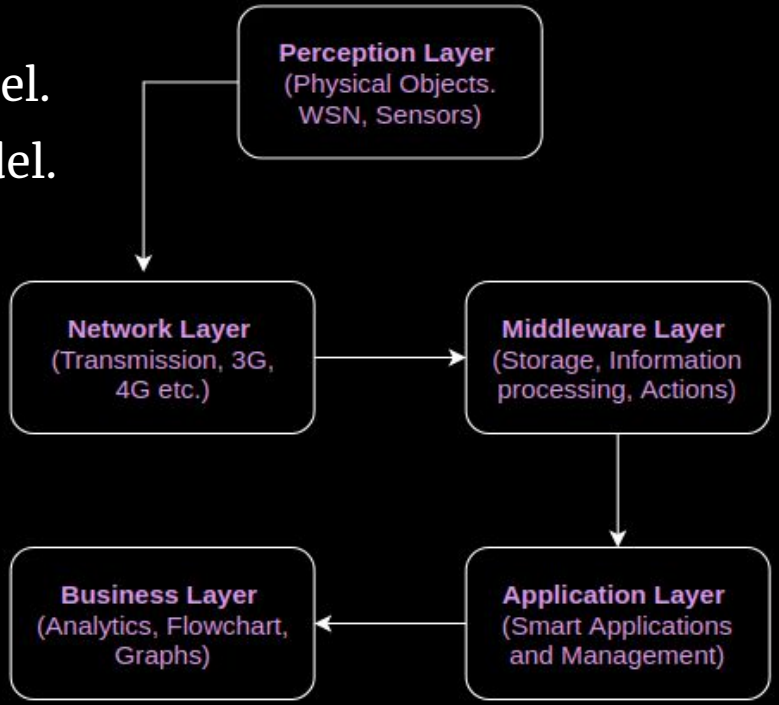
They **Collect data** using sensors , **Processes** it using a microcontroller and **Communicate** real-time data or results without involving a human being.



5-Layer IoT Architecture.

- 5 layer architecture is considered as best.
- It is the extension to the basic 3 layer model.
- Has two additional layers to the basic model.
- The 5 layers are

1. **Perception Layer**
2. **Network Layer**
3. **Processing Layer**
4. **Application Layer**
5. **Business Layer**



Perception Layer :

- first layer of IoT architecture.
- sensors and actuators are used to gather useful information like temperature, moisture content, intruder detection, sounds, etc.
- main function is to get information from surroundings and to pass data to another layer

Network Layer :

- Responsible for communication b/w perception and middleware layer.
- Uses Network technologies like 3G, 4G, Ethernet, WiFi, Bluetooth, ZigBee, Z-Wave .etc
- Uses Messaging Protocols like DDS, AMQP, CoAP, MQTT, .etc
- also called communication layer.

Middleware Layer :

- Has features like storage, computation, processing, action taking capabilities.
- It stores all data-set and based on the device address and name it. gives appropriate data to that device. It can also take decisions based on calculations done on data-set obtained from sensors.
- Manage and provide a diverse set of services to the lower layers

Application Layer :

- Manages all application process based on information obtained from middleware layer.
- Involves sending emails, activating alarm, security system, turn on or off a device, smartwatch, smart agriculture, etc.
- also known as an Abstraction Layer.

Business Layer :

- Decides how processed information is delivered to its consumers.
- Acts like a manager of a whole system.
- Manage and control applications, business and profits models of IoT.
- Also responsible for user’s privacy.

Why IoT Security is more Important than Traditional Security ?

Why IoT Security is more Important than Traditional Security ?

Why IoT Security is more Important than Traditional Security ?

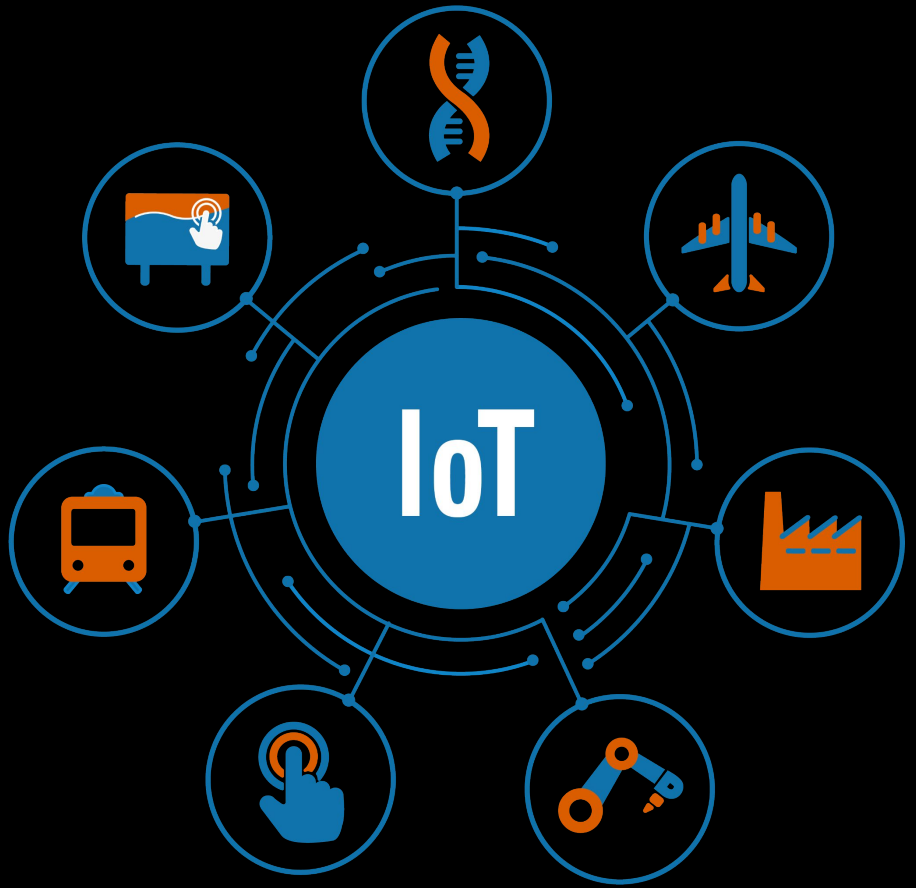
- IoT security failures might cause;
    - Direct Loss of Life/Lives.
    - Financial Loss.
    - Bankruptcy of an Organisation.
    - Compromise Privacy.
- IoT devices are a **Low-hanging fruits** in a network.

Why IoT Security is more Important than Traditional Security ?

- IoT devices have **Non-Typical Constraints** like;
  - Size.
  - Power Consumption.
  - Computation.
  - Price.
- User aren't always Educated.
- IoT Environments takes time to adopt new technologies.

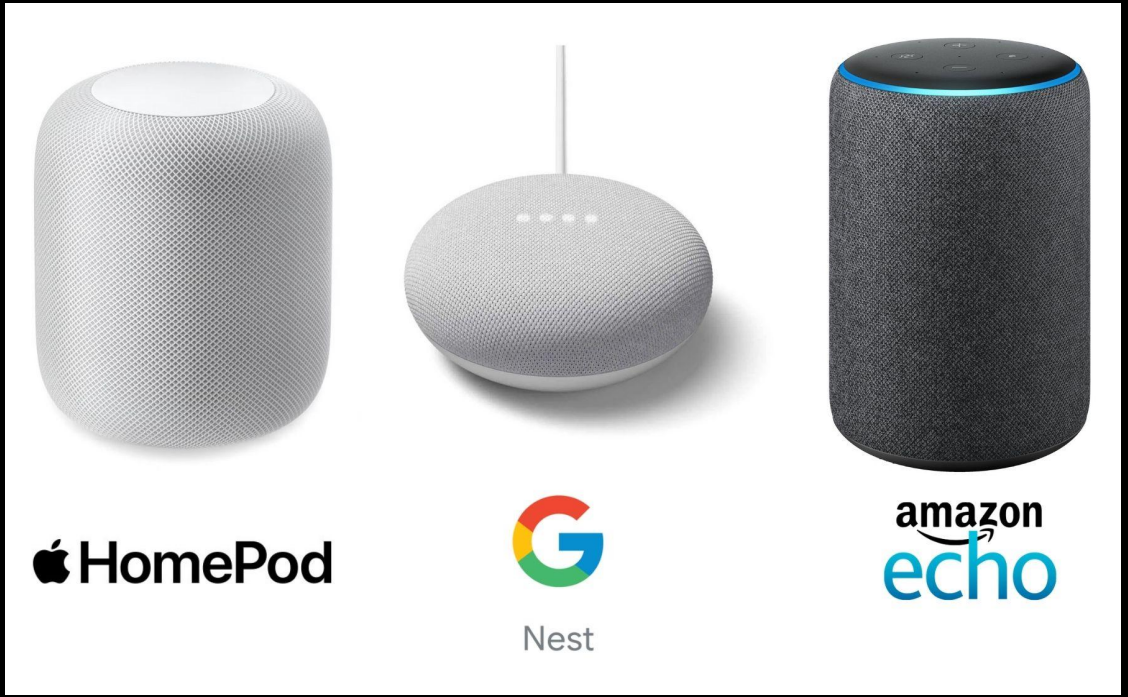
Real World Applications of IoT.

- Smart <Everything>.
- Home Automation.
- Industrial Automation.
- Healthcare.
- Agriculture.
- Logistics.



Smart Voice Assistants / Speakers

- “Ok Google”
- “Alexa”
- “Hey Siri”



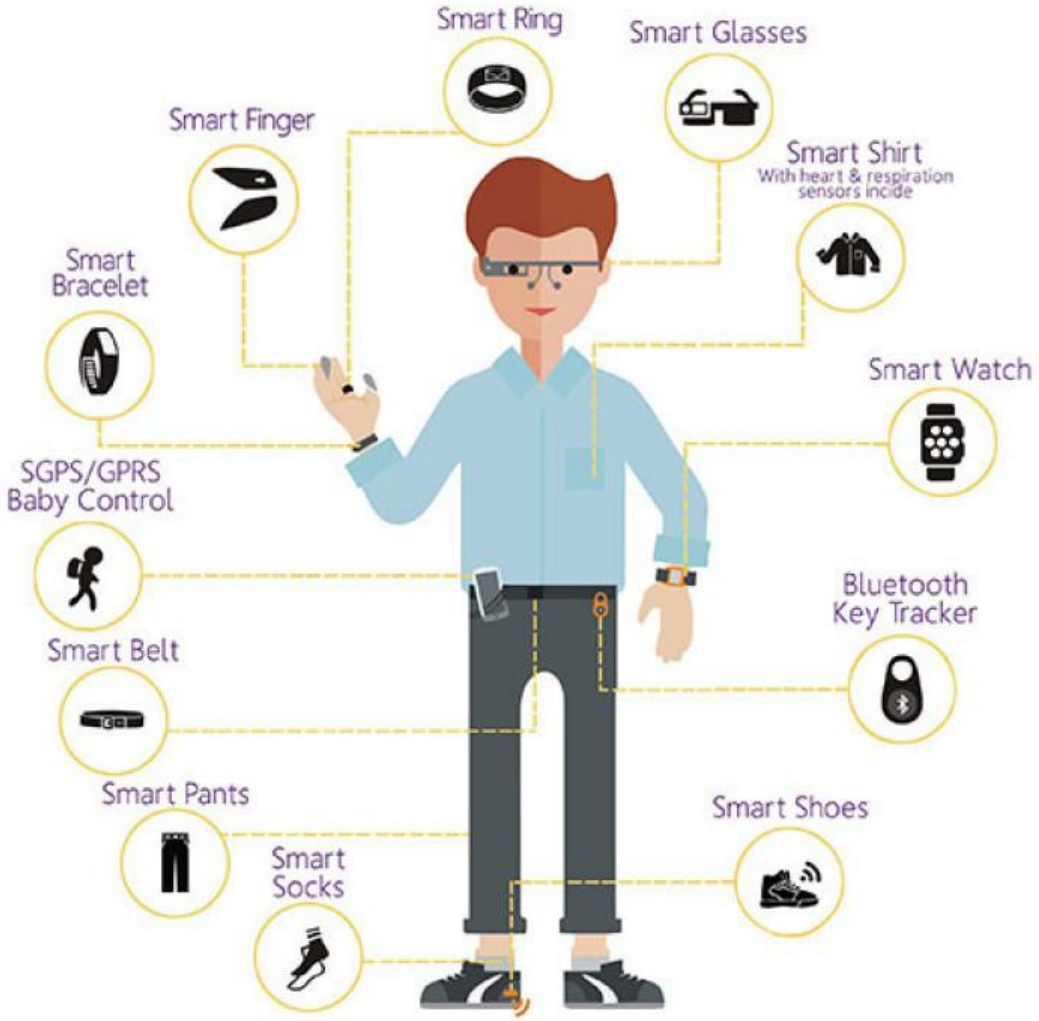
- Voice Commands.
- Integration.
- Ecosystem.
- Cloud Storage and Processing.
- Scheduled tasks.

Smart illumination

- Intelligent lighting.
- Wireless control.
- Autonomous control.
- Voice Commanding.
- Energy efficient.
- Seamless integration.

Smart Wearables

- Health Tracking.
- Keyless entry.
- RFID tags.
- Notifications.
- Connected Devices.
- Location Based Services.
- Cashless Payments.
- Remote Control


Smart Ring
Smart Glasses
Smart Finger
Smart Shirt
With heart & respiration sensors incide
Smart Bracelet
Smart Watch
SGPS/GPRS Baby Control
Bluetooth Key Tracker
Smart Belt
Smart Pants
Smart Shoes
Smart Socks

Apple Watch Saves 61-year-old Indian Man's Life, Tim Cook Wishes Him Speedy Recovery


IANS photo.

R. Rajhans, a retired pharma professional who uses an Apple Watch Series 5, decided to check his ECG on the Apple Watch after he felt unwell in March this year.

- IANS
- LAST UPDATED: OCTOBER 21, 2020, 13:08 IST
- FOLLOW US ON: Facebook Twitter Instagram Telegram Google News

Apple Watch saves another man's life after he falls from electric bike

The watch informed the Hermosa Beach Police in California that the watch owner fell and based on the location, the department ordered emergency services to the spot.

By: **Trends Desk** | New Delhi |
Updated: February 7, 2022 11:27:43 am

• LIVE BLOG

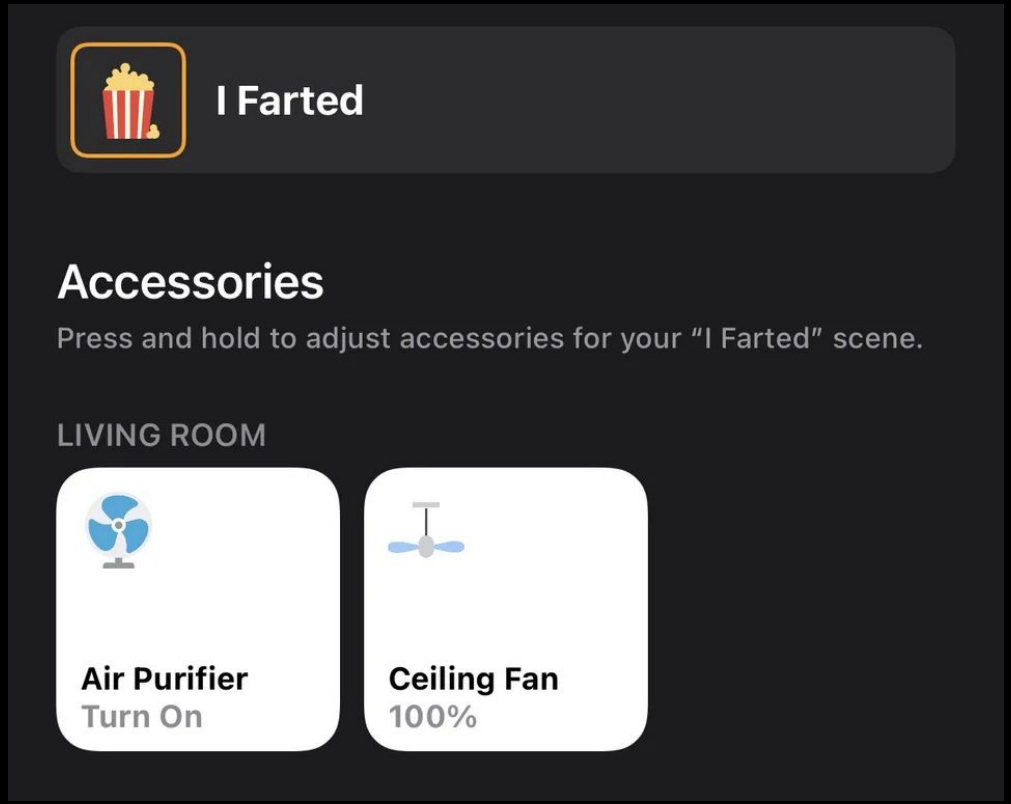
Karnataka hijab controversy Live Updates: Karnataka govt orders closure of educational institutions for 3 days
51 mins ago

Assembly Elections 2022 Live Updates: Opposition parties daydreaming about division of votes in western UP, says PM Modi
1 hour ago

Home Automation

Home Automation

Some Automations are created for Convenience, others… for Necessity.



Some Automations are created for Convenience, others… for Necessity.

Posted by u/allanparsons1 9 months ago 8 2 5 2

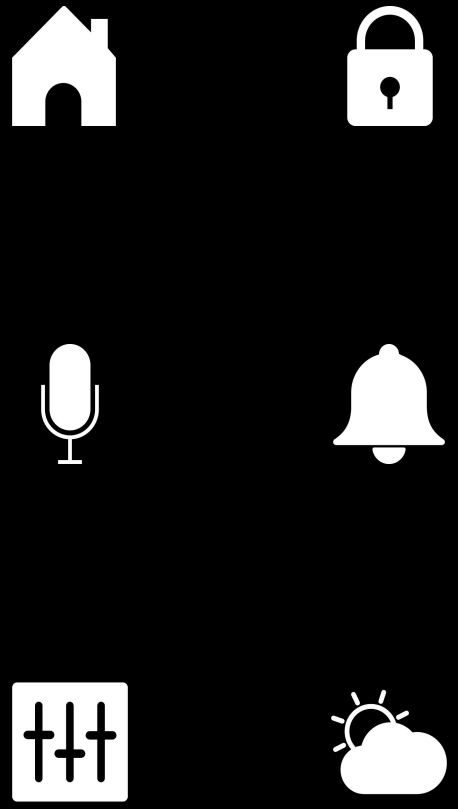
1920

I got sick of people pissing behind my garage. So I added a motion-activated sprinkler (using drip irrigation lines).

HOME ASSISTANT

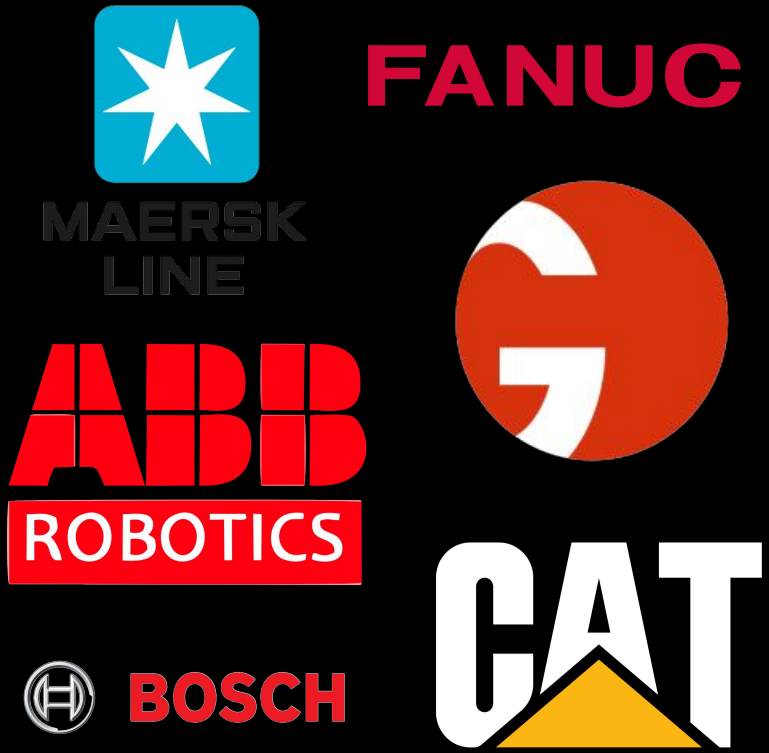
Home Automation

- Efficient power Consumption.
- Better Integration using Voice Assistants.
- Better Security and Surveillance.
- Effective Maintenance.
- Remote Access.
- Keyless Entry.
- Motion Sensing Doors , Taps , LIghts .etc
- Presence/Motion Detection.
- Air Quality Monitoring.



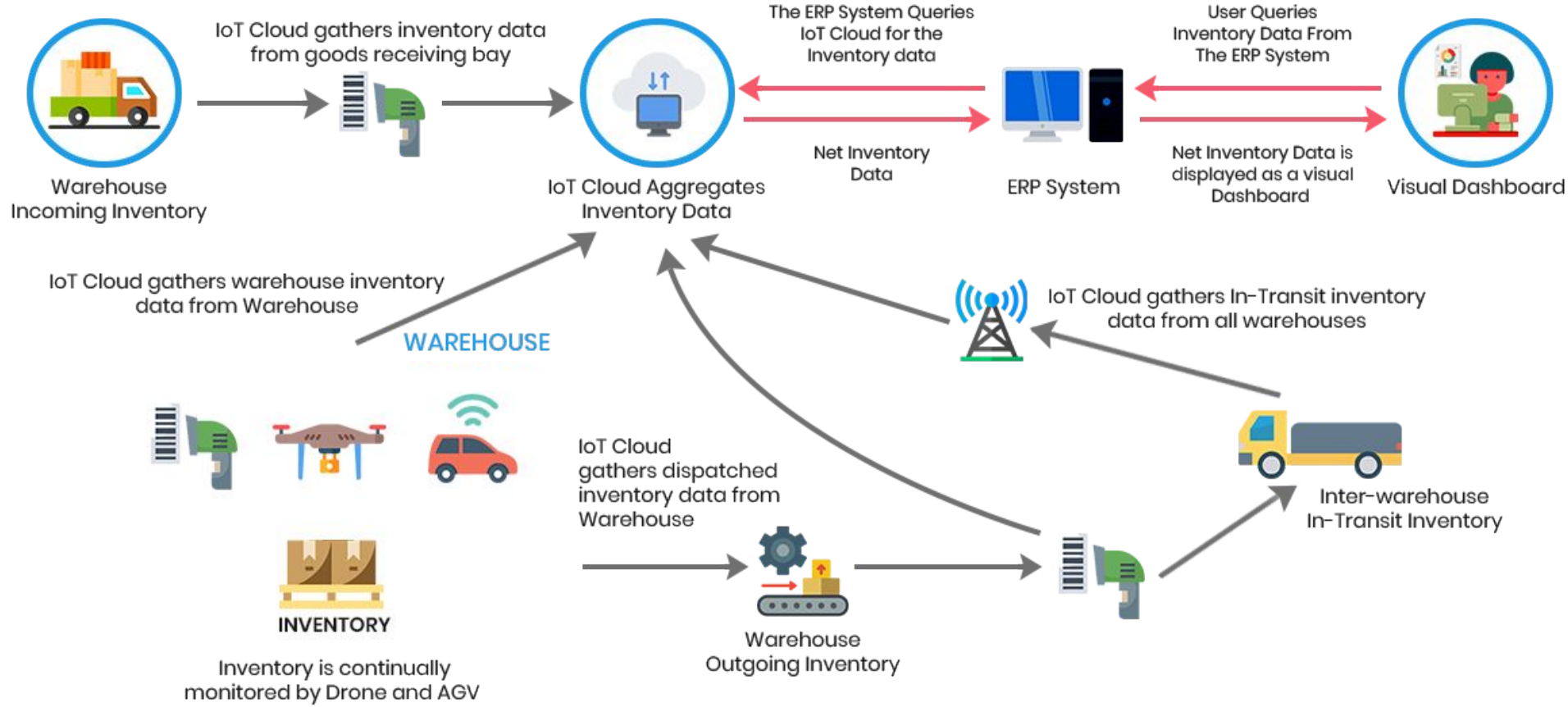
Industrial Automation - IIoT.

Industrial Automation - IIoT.



- Process Automation.
- Product flow Monitoring.
- Inventory Management.
- Predictive Maintenance.
- Efficient Quality Control.
- Packaging optimization.
- Logistics and Supply Chain Optimization.

IoT Enabled Warehouse Management



Healthcare

- RFID Implants.
- Connected Pacemaker/ICD.
- Connected Insulin Pump.
- Remote Patient Monitoring.
- Heart rate Monitoring.
- Glucose Monitoring.

IOT in Agriculture

DreamzTech Solutions

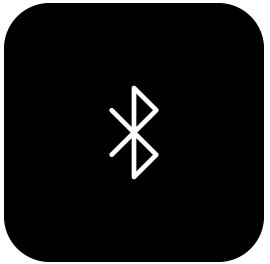
IoT Security Threats

-

The Threat Landscape.

03.a. Communication Standards.

- **Short-Range Radio**
  - RFID.
  - NFC.
  - Bluetooth.
  - Bluetooth Low Energy.



03.a. Communication Standards.

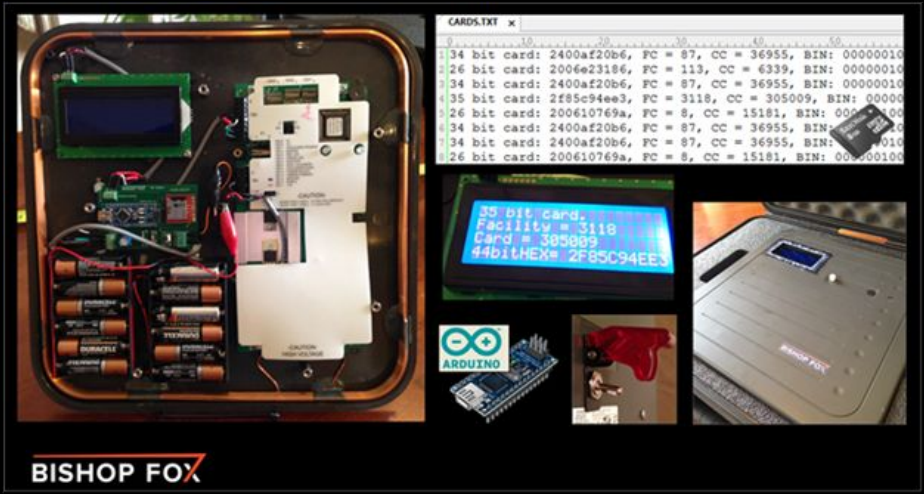
- **Medium-Range Radio**
  - WiFi.
  - Zigbee.
  - Z-Wave.
  - Thread.

03.a. Communication Standards.

- **Long-Range Radio**
  - LPWAN.
  - LoRa.
  - LoRaWAN.
  - SigFox.
  - Ingenu.
  - Satellite.

RFID/NFC Vulnerabilities

- RFID Cards and Tags can be Cloned or Spoofed.
- Denial of Service through Signal Jamming.
- Man in the Middle Attacks or Sniffing.
- Gain Access through Brute Forcing RFID.



Bluetooth/BLE Vulnerabilities

- MAC Spoofing Attack.
- PIN Cracking Attack.
- Man-in-the-Middle Attack.
- Fuzzing Attack.
- Denial of Service Attacks.
- Bluecasing/War Nibbling Attack.

Bluetooth/BLE Vulnerabilities

- BlueJacking Attack.
- BlueBugging Attack.
- BlueBump Attack.
- BlueDump Attack.
- BluePrinting Attack.
- BlueOver Attack.
- BlueBorne Attack.
- BlueSmack Attack.
- MultiBlue Attack.
- HeloMotto Attack.
- Bluecasing Attack.

Wifi Vulnerabilities

- WPS Vulnerability.
- WPA2 / WPA Vulnerability.
- MAC Address Spoofing.
- Packet Sniffing.
- Evil Twin Attacks.
- Denial of Service.

Wi-Fi security vulnerabilities allow attackers to flip smart switches

Some attack scenarios include intercepting users' authentication credentials and flipping a smart power socket. Attackers could also exploit the vulnerabilities as a "stepping stone to launch advanced attacks."

When exploited, they could allow hackers to execute malicious code, intercept information, hijack the affected devices, or become launchpads for more sophisticated attacks.

Zigbee Vulnerabilities

- Insecure Key Storage.
- Battery Depletion Attacks.
- DOS by Radio and Link layer Jamming.
- Default and Un-Encrypted Link-Keys.
- Node Hijacking.
- ACK Spoofing and Dropping

Z-Wave Vulnerabilities

- Steal Encryption Keys by Downgrade Attack.
- Packet Sniffing.
- Packet Injection.
- Man In The Middle Attacks.

Forbes

May 24, 2018, 07:10am EDT

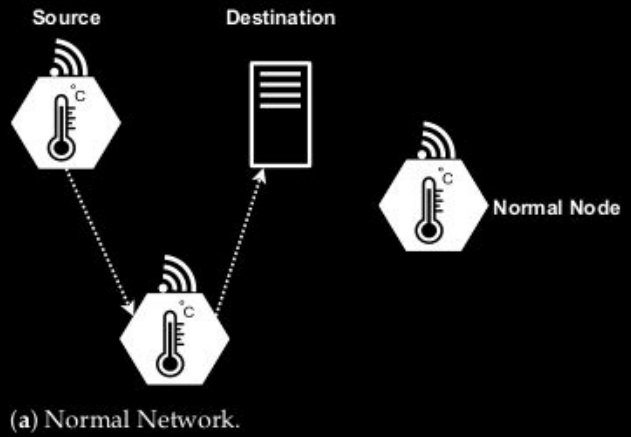
A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices

Forbes

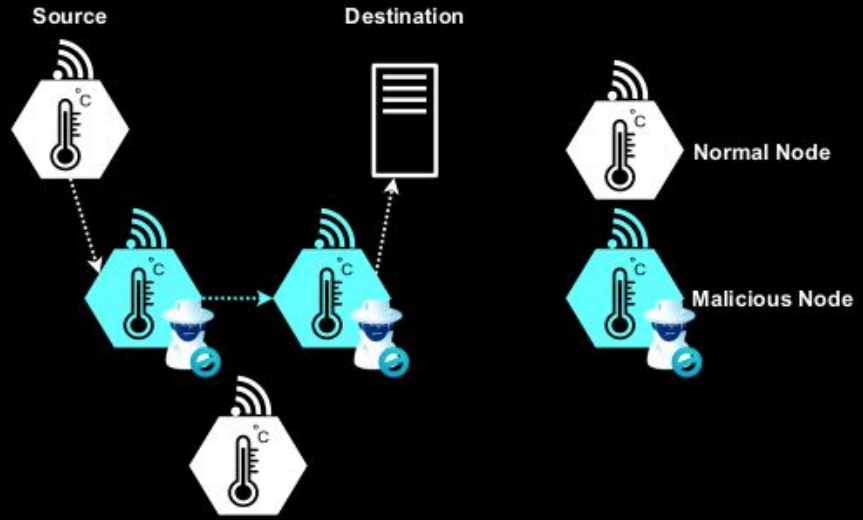
May 24, 2018, 07:10am EDT

A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices

Z-Shave Attack Could Impact Over 100 Million IoT Devices



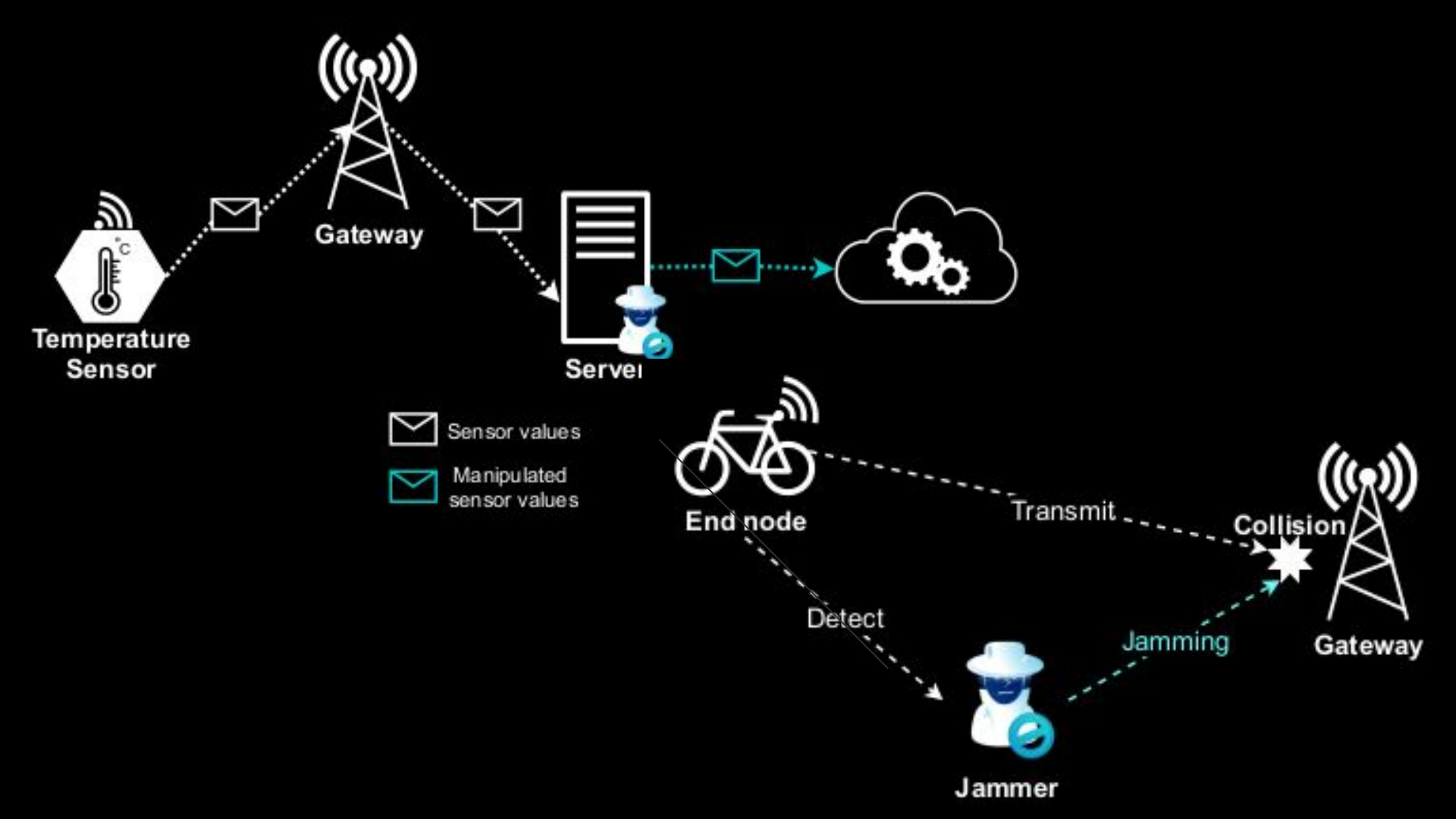
(a) Normal Network.



(b) Network with wormholes.

LoRa/LoRaWAN Vulnerabilities

- DOS Attack.
- ACK Spoofing.
- Bit Flipping.
- Replay Attack.
- Wormhole Attack.
- Jamming Attack.


Gateway
Temperature Sensor
Server
Sensor values
Manipulated sensor values
End node
Transmit
Collision
Gateway
Detect
Jamming
Jammer

5G/4G Vulnerabilities

Several open-source projects are available to enumerate and exploit vulnerabilities that affect LTE:

- SigPloit (https://github.com/SigPloiter/SigPloit): This tool abuses vulnerabilities within the GTP protocol. It can also exploit SS7 vulnerabilities that affect 2G and 3G networks
- gtp_scan (https://insinuator.net/2011/03/gtp_scan-released/): This tool was designed to enumerate and scan GTP services in a network
- apnbf (https://insinuator.net/tag/apnbf/): This script can be used to brute-force access-point names (APNs) that can be used to establish sessions in a network.
- s1ap_enum (https://insinuator.net/2014/06/new-tool-s1ap_enum/): This tool is used to attempt to brute-force parameters for a host (such as an MME) and establish an s1ap session
- diameter_enum (https://github.com/ernw/diameter_enum): This tool implements the Diameter protocol and can be used to scan related services
- pytackle (https://insinuator.net/2012/10/pytacle-alpha1-released/): This tool was designed to sniff GSM packets out of the air
- dizzy (https://github.com/ernw/dizzy): This framework is capable of both stateful and stateless network protocol fuzzing. The project was built in parallel with scripts (https://github.com/ernw/dizzfiles) to assist with the fuzzing of various protocols like GTP and SIP.

03.b. Communication Protocols.

- MQTT - The Message Queue Telemetry Transport.
- M2M - Machine to Machine.
- WS-Discovery
- UPnP - Universal Plug n Play.
- CoAP.
- DICOM.
- C-ECHO.
- HTTP.

CVE-2020-12695: CallStranger Vulnerability in Universal Plug and Play (UPnP) Puts Billions of Devices At Risk

Universal Plug and Play (UPnP), a ubiquitous protocol used by "billions of devices," may be vulnerable to data exfiltration and reflected amplified TCP distributed denial of service (DDoS) attacks.

> Because UPnP doesn't need authorization or authentication in most cases, an enabled router will automatically assume that all devices attempting to make a connection are safe. This is not always the case. This functionality could theoretically allow a hacker into your network with ease and allow them remote access to other devices on the network, proxy their traffic with your router, utilize your network in DDoS attacks, and much more.

Vulnerabilities with M2M communication protocols slowing smart city innovation

As IoT comes into focus, the goal of fully integrated smart cities becomes more plausible, though significant challenges lie ahead for the

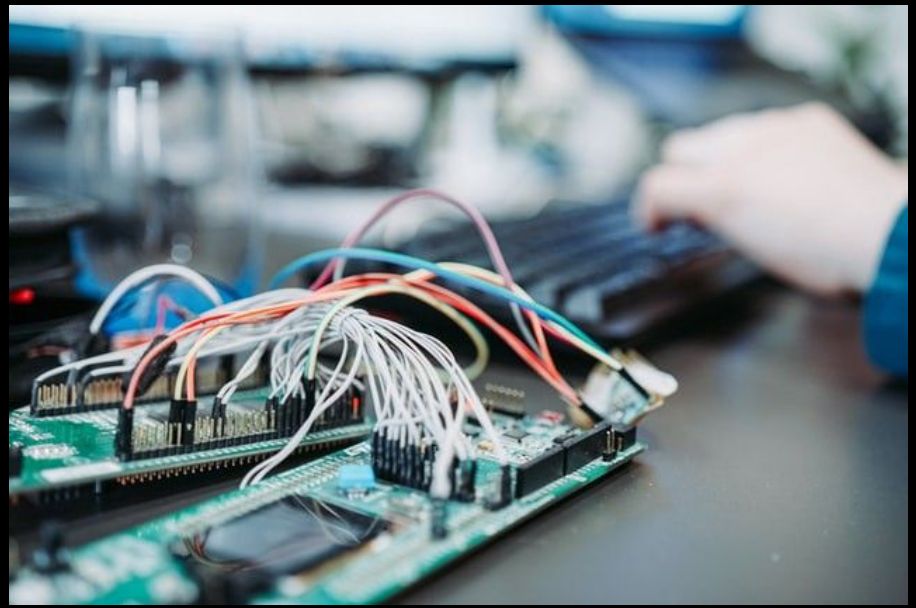
IoT devices using CoAP increasingly used in DDoS attacks

More devices affected by Ripple20 vulnerabilities

Researchers from JSOF and Tenable **discovered** more devices affected by the vulnerabilities dubbed **Ripple20**. Ripple20 is the name given to 19 security holes affecting the Treck TCP/IP stack, which is used by millions of IoT devices.

Hardware Attack Vectors

- Exposed Debug Ports.
  - UART.
  - JTAG.
- Outdated Hardware.
- Chip level Vulnerabilities.
- Cryptographic Vulnerabilities.
- Power Related Bugs.



Variants of the Kr00k attack impact Wi-Fi chips from Qualcomm and MediaTek

The Kr00k vulnerability, which allows attackers to decrypt wireless communications, only affects Wi-Fi chips from Broadcom and Cypress, but ESET researchers discovered recently that **similar vulnerabilities** also exist in chips made by MedaTek and Qualcomm.

Plundervolt: using CPU voltage modifications to steal data

Researchers from various universities have described **Plundervolt**, an attack method disclosed last year that leverages CPU voltage modifications to expose data stored using Intel Software Guard Extensions (SGX).

IoT Inspector GmbH

Critical security vulnerabilities in Realtek chips affect more than 65 hardware manufacturers

Software Attack Vectors

- Weak Admin Passwords.
- Hardcoded Passwords.
- Insecure API.
- Buggy Firmwares.
- Lack of Updates.
- Update Mechanisms.
- Main OS Vulnerabilities.

Software Attack Vectors

- Logic Attacks.
- Malwares.
- Remote Exposure.
- Proprietary Softwares.
- Timing Attacks.
- Lack of Encryption.
- Weak Authentication.

Zero-Day Vulnerability Timeline

Software Is Developed

Software is developed, but unknown to the developers, it contains a security vulnerability.

Hacker Detects Vulnerability

A threat actor finds the vulnerability either before the developer or exploits it before the developer has the opportunity to release a patch.

Malware Is Released

Attackers release malware to exploit software while the vulnerability is still open and unpatched.

Detection and Patching

After hackers release the exploit, either the public detects identity or data theft, or the developer uncovers and creates a patch.

Privacy Threat Landscape

- Data Collection without Consent.
- Location Tracking.
- Illegal/Mass Surveillance.
- Data Dumps from Security Breaches.
- Home Invasions.
- Industrial Sabotage.
- Espionage.

WILL GPS AND THE IOT ENABLE A NEW LEVEL OF MASS-SURVEILLANCE?

IOT MASS-SURVEILLANCE

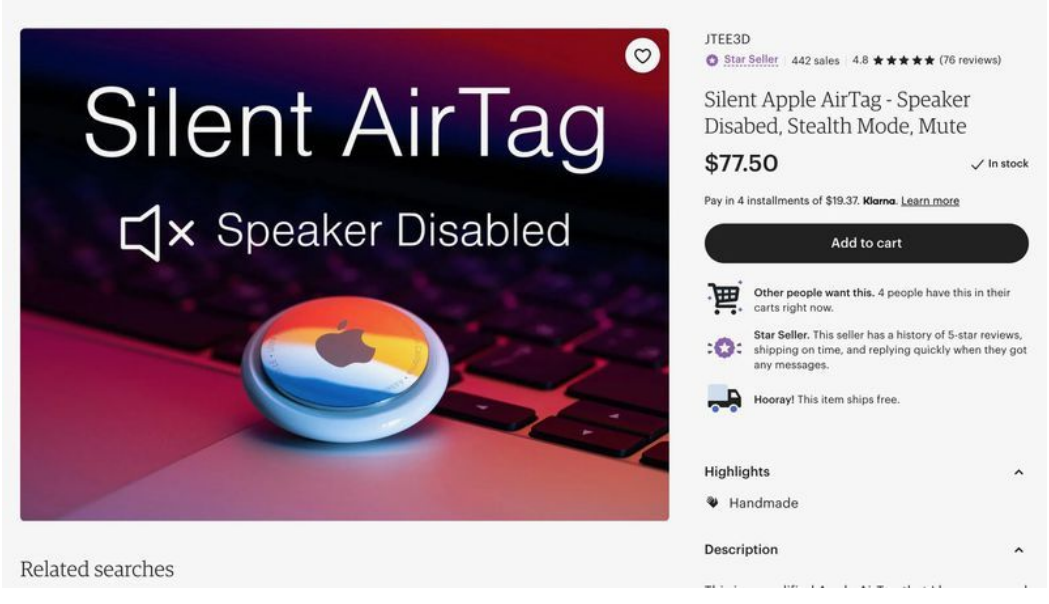
There's a dark cloud hanging over the cloud. Recently, US security chief James Clapper blithely revealed that the government "could" use the Internet of Things for civilian **surveillance**.

Internet of things: the greatest mass surveillance infrastructure ever?

Does the expanding network of connected devices herald a brave new compact for our digital lives – or the end of politics?

'Stealth AirTags' Are Real And A Privacy Nightmare

An Etsy seller specializing in modified AirTags briefly released a 'Stealth AirTag,' which has a hardware-disconnected speaker and warnings disabled.



Little did she know, Alexa was recording every word she said

An Oregon woman discovered that her Amazon device was sending her private chats by email to her husband's employee when he called and warned her, "You're being hacked."

Real World incidents where IoT was compromised

- Medical Devices Compromised

MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks

Attackers are infecting medical devices with malware and then moving laterally through hospital networks to steal confidential data, according to TrapX's MEDJACK report.

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

Drug regulator warns of hacking risk in Medtronic insulin pumps

A 19-year-old security researcher describes how he remotely hacked into over 25 Teslas

GRACE KAY | JAN 25, 2022, 21:31 IST

TECHNOLOGY

Tesla Model X's keyless system can be hacked, and car stolen in minutes

How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed

IoT security: Now dark web hackers are targeting internet-connected gas pumps

As more and more devices get connected to the Internet of Things, researchers say compromising pumps has become a hot topic on cyber criminal forums.

A hi-tech padlock secured with a fingerprint can be opened by anyone with a smartphone, security researchers have found.

Smart Locks can be Hacked remotely

Devin Coldewey @techcrunch / 4:46 AM GMT+5:30 • August 9, 2021

Comment

How a fish tank helped hack a casino

Nest's Smart Thermostat is Easily Hacked for Mods… or Evil

Hackers leave Finnish residents cold after DDoS attack knocks out heating systems

Hacker terrorizes family by hijacking baby monitor

Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more

A massive security breach for the Silicon Valley startup

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

- **Major cyber attack using IoT devices disrupts internet service across Europe and US**

Smart Refrigerators Hacked to Send out Spam: Report

A new report shows cyberattacks aren't relegated to laptops anymore: Now, even a fridge or a TV can send malicious emails.

Russian government hackers are targeting IoT devices

That Toy You Got for Christmas Could Be Spying on You

Security flaws in the recently released Fisher-Price Chatter Bluetooth telephone can allow nearby attackers to spy on calls or communicate with children using the device.

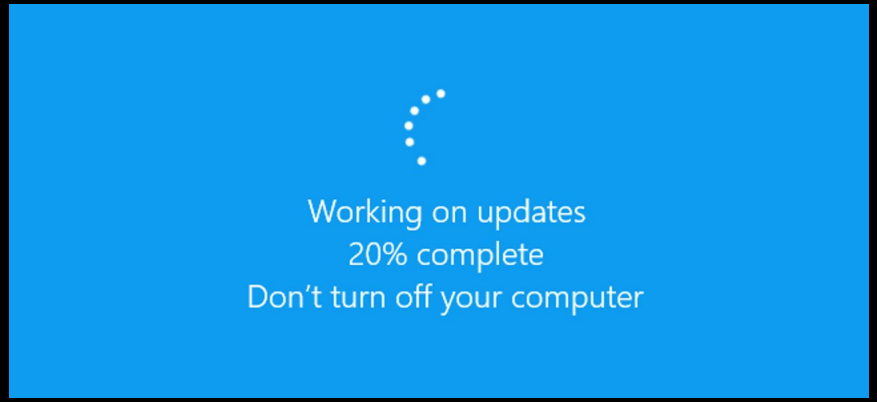
How to Secure a IoT Network

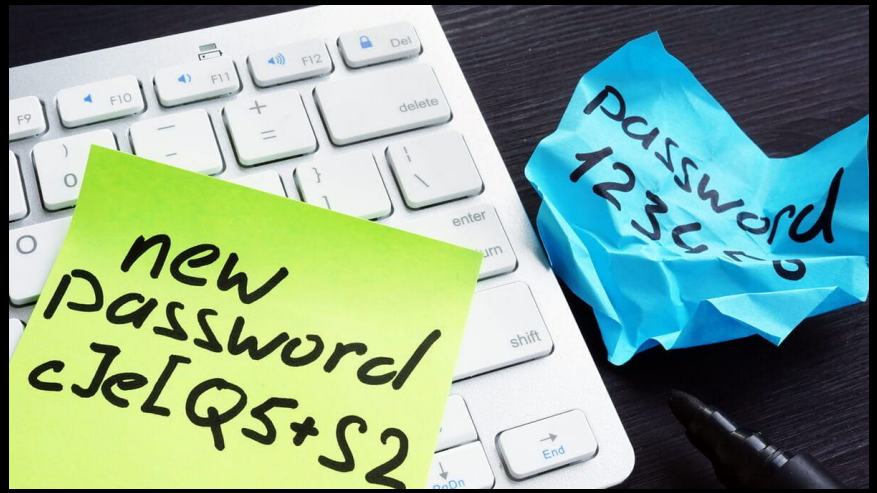
Hardware Security

- Physical Hardening.
- Implement Security in Chip level Design.
- Remove Prototype debug ports from production model.
- Hardware Encryption.
- Advanced Tamper Protection.
- Secure Boot Environment.
- Open Source Hardware.

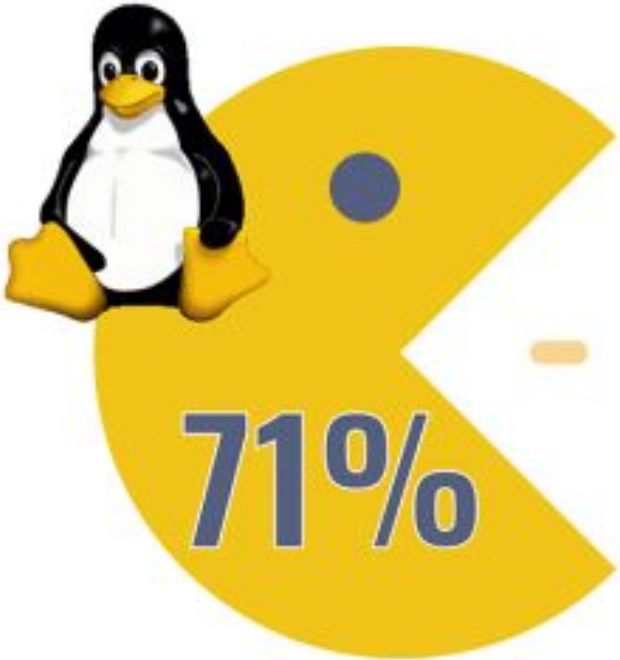
Software Security

- Security Patches and Updates.
- Secure Update Mechanisms.
- API Security.
- Strong Passwords.
- Randomized Default Passwords.
- Software level Encryption.
- Open Source Software.





Top IoT Operating Systems & Distros



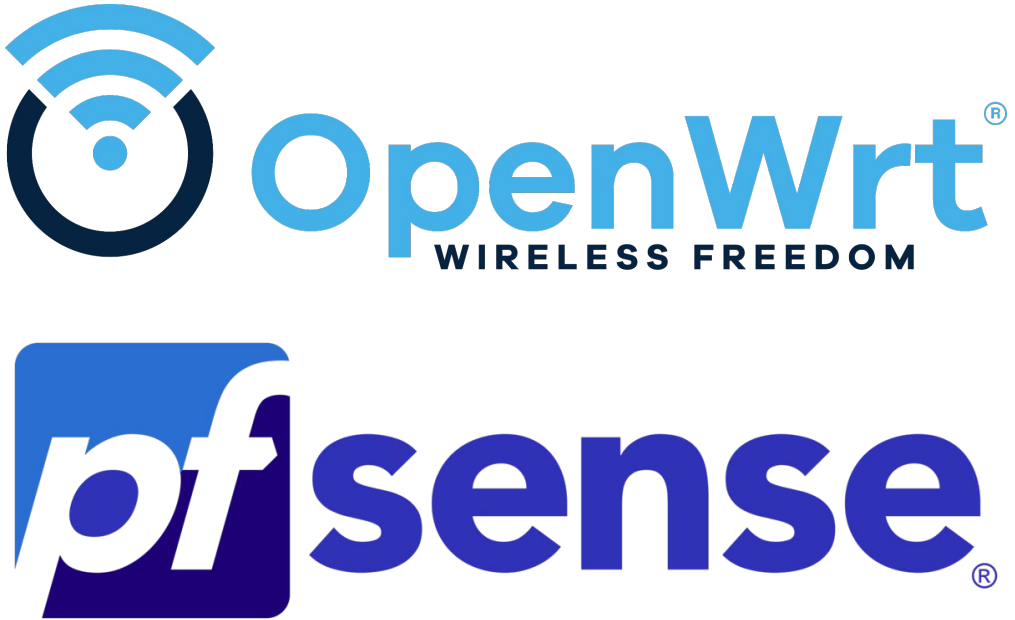
Raspbian

ubuntu

debian

Network Security

- Network Segmentation.
- Open Source Firmwares.
- Intrusion Detection.
- Honeypots.
- Regular Security Audits.
- Network Authentication.



Client/User Side Policies and Incident Response

- Educate Users.
- More Security Awareness.
- Incident response protocols.
- Efficient backup plans.

Network Security

- Network Segmentation.
- Open Source Firmwares.
- Intrusion Detection.
- Honeypots.
- Regular Security Audits.
- Network Authentication.

TRENDING

The Logical Indian Crew

Kerala: Kochi Smart Mission To Install 26,000 Smart Meters For Electricity Board, No Change In Power Tariff Rates

KSEB കേരളത്തിന്റെ ഊർജ്ജം

സ്മാർട്ട് മീറ്റർ

എന്താണ്?

സ്മാർട്ട് മീറ്റർ

നമ്മൾ അറിയേണ്ടതെല്ലാം..

Conclusion

- IoT Security is very different and little bit more important than traditional Security.
- Manufacturers must consider security in R&D stages.
- They need to provide appropriate security updates and patches.
- Provide better awareness for end users about Security.
- Follow better security practices overall