# The research Article Hacking Internet of Things (IoT)

## Introduction:

The Internet of Things (IoT) is the network of physical objects devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity that enable these objects to collect and exchange data.

The IoT extends internet connectivity other than traditional devices such as desktops and laptop computers, and smart mobile phone devices to a diverse range of real world devices such as a refrigerator, air conditioner, television, washing machine, water purifier, door locks, cars, DTH set top box, and many more which are connected to the internet and become part of IoT.

**IoT (Internet of Things)** and embedded devices present a new challenge to ethical hackers hoping to understand the security vulnerabilities these devices contain. To hack IoT interfaces as well as the integrated applications, a person requires knowledge of Python, Swift and PHP, among others.

As IoT grows, the attack surface also grows and all the loopholes/vulnerabilities present in the digital world will flow into our real world. Before IoT, attackers used vulnerabilities for data theft or to make money or sometimes just for fun, but with IoT, the attack surface has grown to such extent that attacker can use vulnerabilities or loopholes in the car, smart sniper rifle etc., to kill a person remotely with a few strokes of the keyboard.

Attackers are constantly finding the vulnerabilities to break into IoT and use those vulnerabilities for many illegal purposes.

In this Article, we will learn how easy it is to hack IoT devices with few real scary attacks And the 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History.

## A few real existing scary attacks are mentioned below,

- **Hacking Car:**

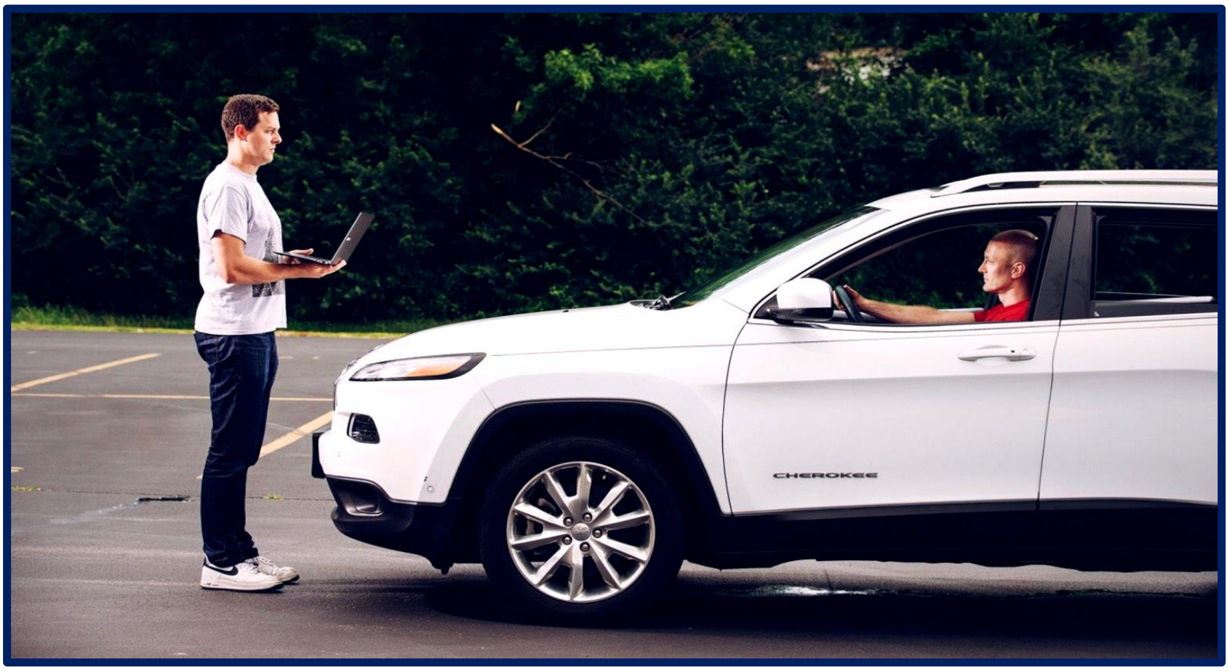


**Figure 1 - Hackers Remotely Kill a Jeep on the Highway**

Cars are part of IoT now; attackers find vulnerabilities in the car. Once they find it, it can be used to hijack the car controls completely, and they will be able to apply the brakes, accelerator, steering, open the doors etc. Two security researchers Charlie Miller and Chris Valasek showed a demo on how they kill a Jeep on the highway and Jeep vendor recalled 1.4M vehicles for security fix. What if the attackers find these vulnerabilities and use it for dangerous purposes like killing people by crashing their cars or damaging their properties?

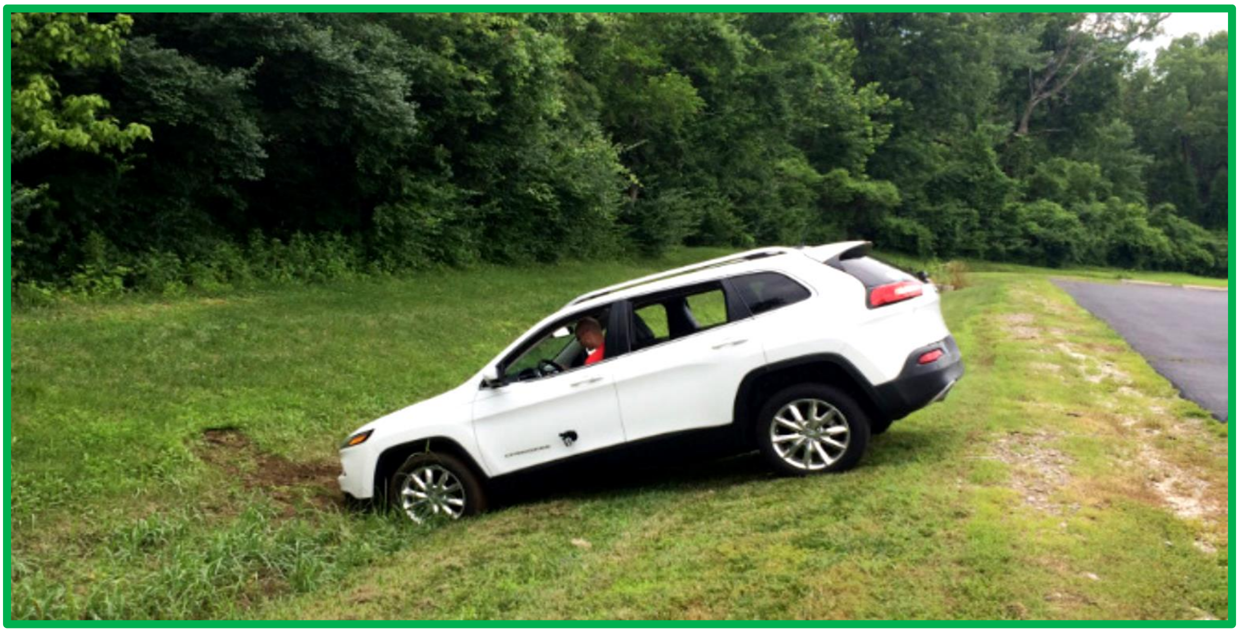


**Figure 2 - Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch.**

- ## Hacking Hospitals:

Figure 3 - Hospitals Hacked

Attackers can break into hospitals in many different ways and they can use medical records for different purposes. They can sell the medical records for money which can be used for some dangerous purposes or attackers can hit the hospital with ransomware and encrypt patient's record and threaten the hospital to pay ransom to get the data back by putting the patient's life at risk. Hospitals have no other option but to pay the ransom to get the data back as the patient's data will be critical for the patient's operation or recovery. In April 2016, two hospitals were hit by ransomware in California and Indiana. Hospitals are a soft and perfect target for ransomware attacks.

- ## Hacking Smart Sniper Rifle:

Figure 4 - Security Researcher Hacking TP750 Smart Sniper Rifle

Smart weapons can save people's lives if used properly. With smart rifle, the accuracy, and efficiency can be increased. At the same time, it's vulnerable to attacks. Attacker can find vulnerabilities and compromise the rifle via its wireless connection. Exploiting those vulnerabilities to jam the rifle and more deadly, attacker can change the scope of the target system, literally changing the target leading to an innocent person's death. Security researchers Runa Sandvik and Michael Auger showed how smart sniper rifle can be hijacked.

Figure 5 - Security Researcher Aiming Target with TP750 Smart Sniper Rifle.

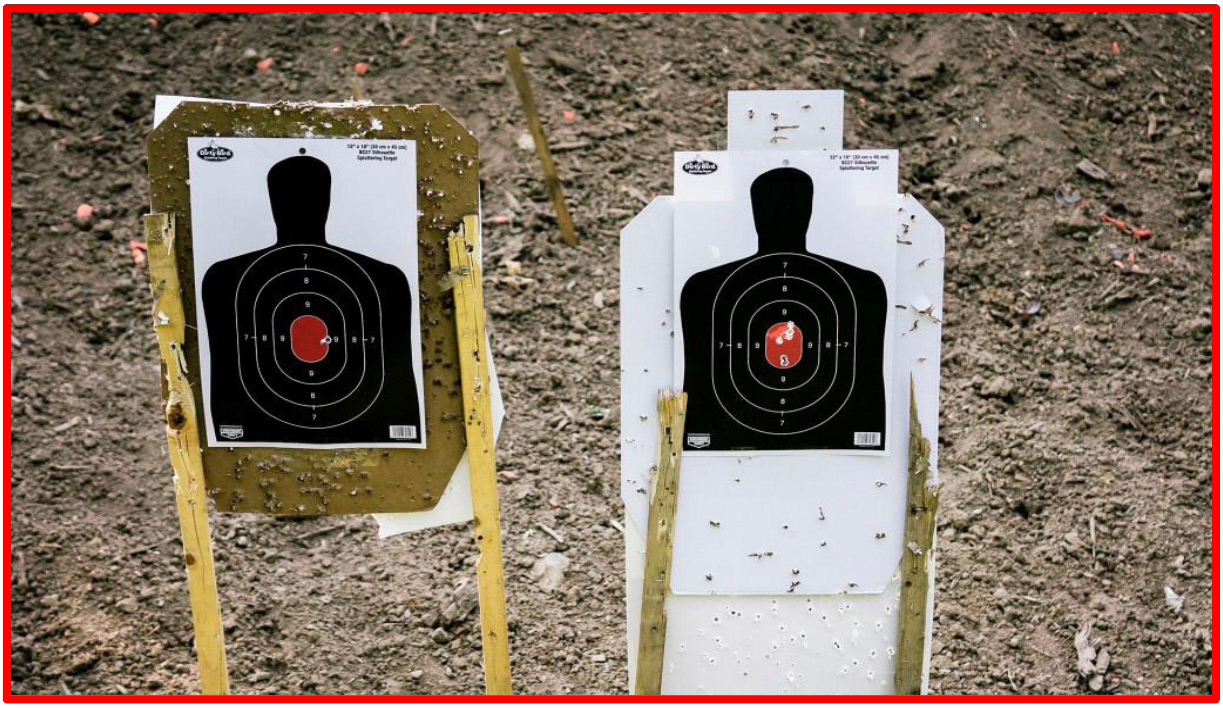


Figure 6 - Rifle seemed to be pointed at the target on the right; the researchers were able to make it hit the bull's-eye on the left instead.

These are a few examples, and all these can be done just by sitting and controlling IoT from somewhere in the world.

Attackers can hack into smart homes, nuclear plant, thermal power plant, food productions, manufacturing, telecom; the list goes which makes the world not a safe place to live in.

# THE 5 WORST EXAMPLES OF IOT HACKING AND VULNERABILITIES IN RECORDED HISTORY

**IoT hacking can be extremely effective, producing D-DoS attacks that can cripple our infrastructure, systems, and way of life.**

We've all heard of cyber security concerns when it comes to IoT devices and there's an inherent risk that comes with connecting more and more devices to the internet and to each other. Malicious hackers can launch attacks and infiltrate thousands or millions of unsecured devices, crippling infrastructure, downing networks, or gaining access to private information. And as we rely more and more on IoT in our daily lives, those attacks can become more disruptive or even dangerous. In this article, we'll focus on some of the biggest hacks and vulnerabilities we've seen before. Hopefully, this article can inspire you when it comes to putting security first in your IoT development journey.

**Here are the 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History:**

## 1. The Mirai Botnet (aka Dyn Attack)

Back in October of 2016, the largest D-DoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were things like digital cameras and DVR players.

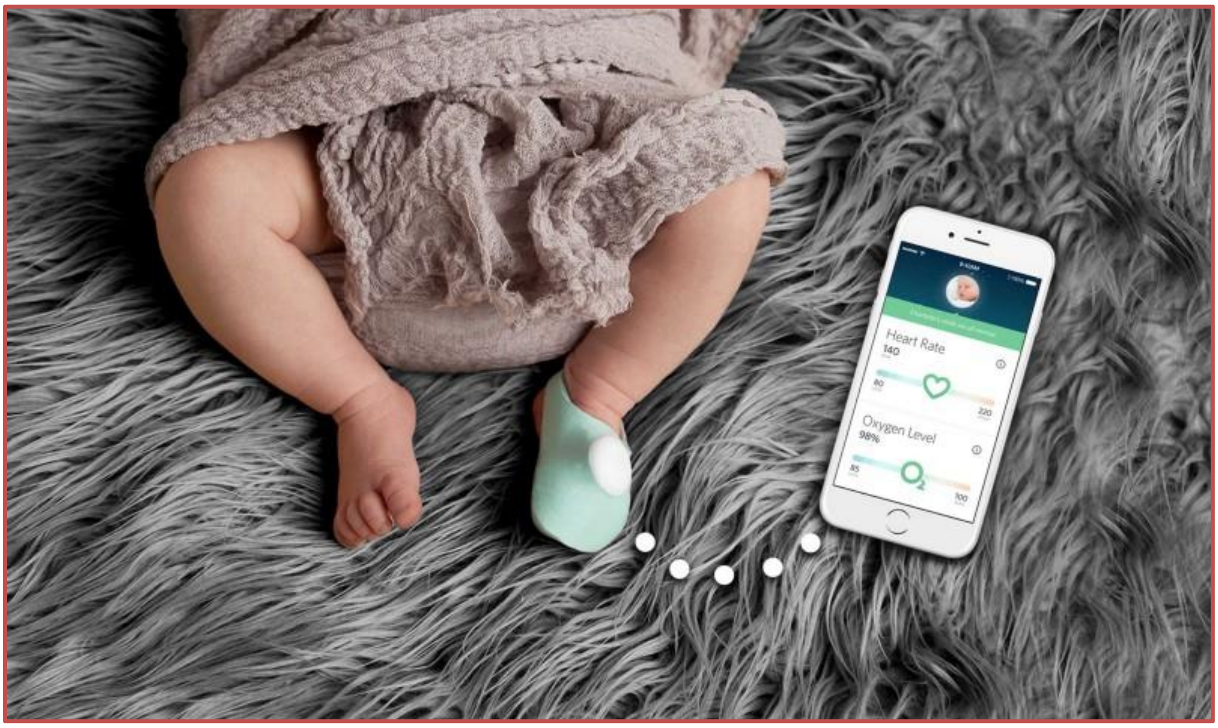
## 2. The Hackable Cardiac Devices from St. Jude

Early last year, CNN wrote, “The FDA confirmed that St. Jude Medical’s implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks, the FDA said.

The devices, like pacemakers and defibrillators, are used to monitor and control patients’ heart functions and prevent heart attacks.”

The article continued to say, “The vulnerability occurred in the transmitter that reads the device’s data and remotely shares it with physicians. The FDA said hackers could control a device by accessing its transmitter.”

# 3. The Owlet Wi-Fi Baby Heart Monitor Vulnerabilities



Right behind the St. Jude cardiac devices is the Owlet Wi-Fi baby heart monitor. According to Cesare Garlati, Chief Security Strategist at the prpl Foundation:

“This latest case is another example of how devices with the best of intentions, such as alerting parents when their babies experience heart troubles, can turn dangerous if taken advantage of by a sinister party.

Sadly, this is more often than not in the case of embedded computing within so-called smart devices. The connectivity element makes them exploitable and if manufacturers and developers don’t consider this and take extra steps to secure devices at the hardware layer, these are stories that we will, unfortunately, keep hearing.”

## 4. The TREND net Webcam Hack

“TRENDnet marketed its Secure View cameras for various uses ranging from home security to baby monitoring and claimed they were secure, the FTC said. However, they had faulty software that let anyone who obtained a camera’s IP address look through it — and sometimes listen as well.

Further, from at least April 2010 [until about January 2012], TRENDnet transmitted user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers’ login information in clear, readable text on their mobile devices, the FTC said.

It is basic security practice to secure IP addresses against hacking and to encrypt login credentials or at least password-protect them, and TRENDnet’s failure to do so was surprising.”

# Conclusion:

The Internet of Things (IoT) industry is still evolving and growing rapidly and exposing IoT devices to zero-day attacks, new attack methods/vulnerabilities. Securing the IoT devices is challenging due to size, memory, processing power etc. Securing IoT devices is a responsibility of vendors, developers, and users. All of them need to be educated about security and impact if ignored. Vendors should design and implement IoT devices with device security in mind and provide ways to apply security updates in a simple way. Users have to make sure that they do what is required. Even if the vendor provides for security the user can ignore things and cause issues.