**Module 18**

**Hacking IoT**

Internet of thing is discovered in 1999 by kelvin Ashton.

Iot stand for internet of thing and it is also known as the internet of everything.

IoT is the most emerging topic for nowadays. Emerging means this days we can see that technology is shifted toward automation, and every automation work is connected to the Iot.

Later the years we can see differe nt of iot devices are developed like smart watch, fitbit, driverless car, smart phone.

**Work of IOT**

**Sensing Technology:-** sensor is first part of iot which sense or collect the data. Sensor can sense many thing from the environment like temperature either it is hot or cold, location, moisture, humidity. Today’s iot devices like fit bit it can sense our hear bit, body temperature and gives variety of information about Human biological.

**Iot gateway** :- Gateway is used in iot to communicate the device with user. Basically it connect the internal network to the external network. Iot senser collect the data and through gateway it communicate with user or cloud,

**Cloud Server and Data Storage**:- After gateway information travel to the cloud where data are analyzed and transmit to the user, where user can perform task on the basis of data.

**Remote control using mobile app** :- what ever data user got on that basis, he can collect the iot device like from mobile apps lights, fan, refrigerator are gadget can be controlled.

**IOT technology**

**Short range wireless communication**:

Bluetooth , wifi , QR code and bar code.

**Medium range wireless communication**:

LTE- advanced

**Wired communication**:

Ethernet

**Long range wireless communication:**

IOT roaming , cellular

**Advantages of IOT**

Easy to use.

Easy control the iot device.

Cost efficient.

Improved work safety

Sped up the work

**Disadvantages of IOT**

Lack of security and privacy

Vulnerable web interface



Coding error(buffer overflow)

Storage issue.



Physical theft and tempering

**IOT attack surfaces**

**Attack surface area & Vulnerability**

Ecosystem general:

* System wide failure
* Lost access procedure

Device memory:

* Clear text username
* Clear text password

Device physical interface:

* use CLI
* admin CLI
* Removal storage media

Device web interface:

* Username enumeration
* Weak password
* Account lockout

Device firmware:

* Vulnerability services
* Sensitive data exposure

Device network services:

* Injection
* DDoS
* Poorly implement encryption

Administrative interface:

* Two factor authentication
* Capable to wipe the device

Local storage:

* Unencrypted data
* Lack of data integrity check

Cloud web interface:

* Owasp webtop 10
* Credential management vulnerability.
* Insecure password recovery mechanism.

Third party backend APIs:

* Location leaked
* Device information leaked

Update mechanism:

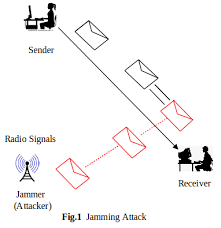
* No manual update mechanism
* Lack of update
* Update sent without encryption

Mobile application:

* Insecure data storage
* Weak password

**Jamming Attack**

In this attacker, attack network between wireless and IOT device for compromising the device. Attacker perform DDoS attack, in which attacker send malicious traffic with high volume, this impact to the iot device because legitimate traffic get stuck in malicious traffic and failed to communication.



**How to Defend Against IOT hacking**

* Disable the guest and demo login.
* Use blocking or lock out mechanism for excessive log in attempts
* Use strong authentication.
* Implement IPS and IDS
* Implement end-to-end encryption.
* Disable telnet port(23)
* Use vpn architecture.