गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

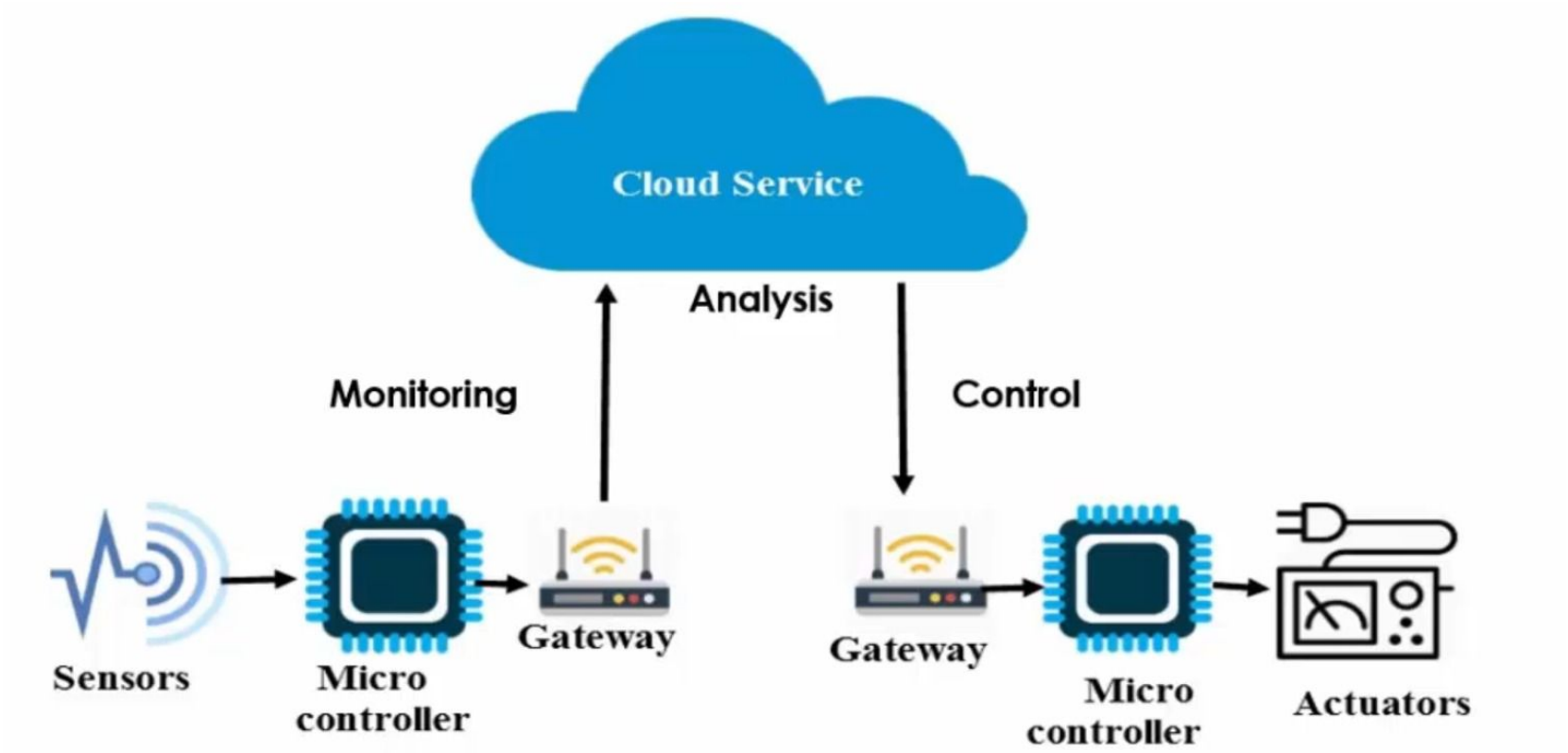
विद्यया ऽमृतमश्नुते
एन सी ई आर टी
NCERT

Indian
Cyber
Crime
Coordination
Centre

Internet of Things (IoT) and Mobile Security

Securing IoT Devices

Internet of Things

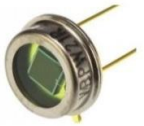


Internet of Things - Components

Temperature Sensor

Humidity Sensor

Proximity Sensor

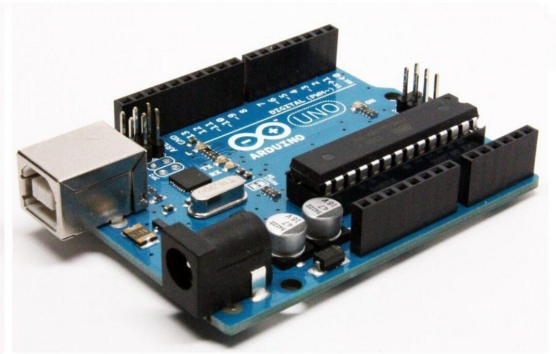


Light Sensor

Metal Sensor

Color Sensor

Sensors



Microcontroller

DC Motor

DC Gear Motor

RC Servo motor

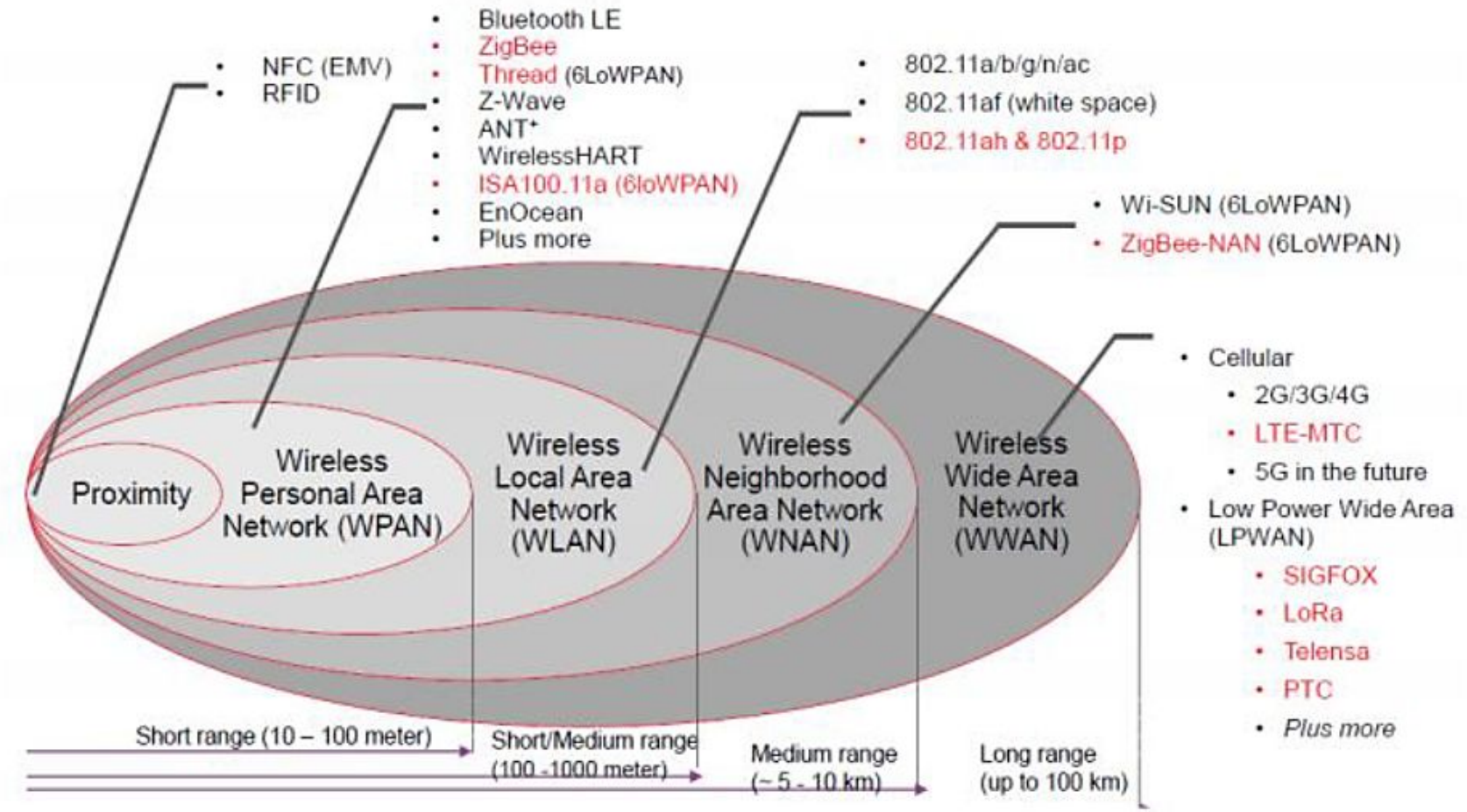
BLDC Motor

Smart Servo motors

Harmonic drives

Actuators

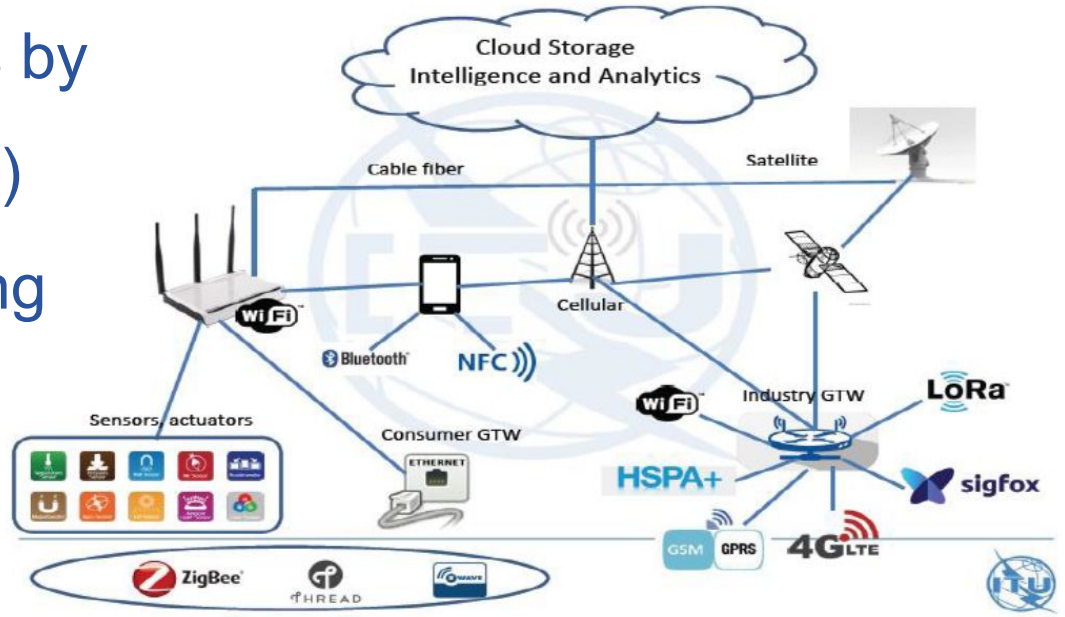
Communication technologies in IoT domain



5G, Wi-Fi 6, WiFi 6E, WiFi HaLow, Bluetooth Mesh

Definition of IoT

A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies



Concerned Organisations & Initiatives

TEC - Telecommunication Engineering Centre

ITU - International Telecommunication Union

- **SG20** - IoT and Smart Cities & Communities - NWG 20 by TEC

oneM2M - one Machine to Machine

TSDSI - Telecommunications Standards Development Society of India

IoT Applications

1

Smart Cities

Intelligent transport System, Waste management, Water distribution, Smart Parking, Safety & Security

2

Health Care

Remote patient monitoring / diagnostics, Tele-medicine, wearable health devices

3

Smart Home

Security & alarm, Connected appliances, Smart lighting system

4

Utilities / Energy

Smart metering, smart grid, Electric line monitoring, gas / oil / water pipeline monitoring

5

Transport System

Vehicle tracking, V2V and V2I applications, traffic control, Navigation, Infotainment

6

Public safety system

Commercial & home security monitoring, alerts, Fire alarm, Police / medical alert

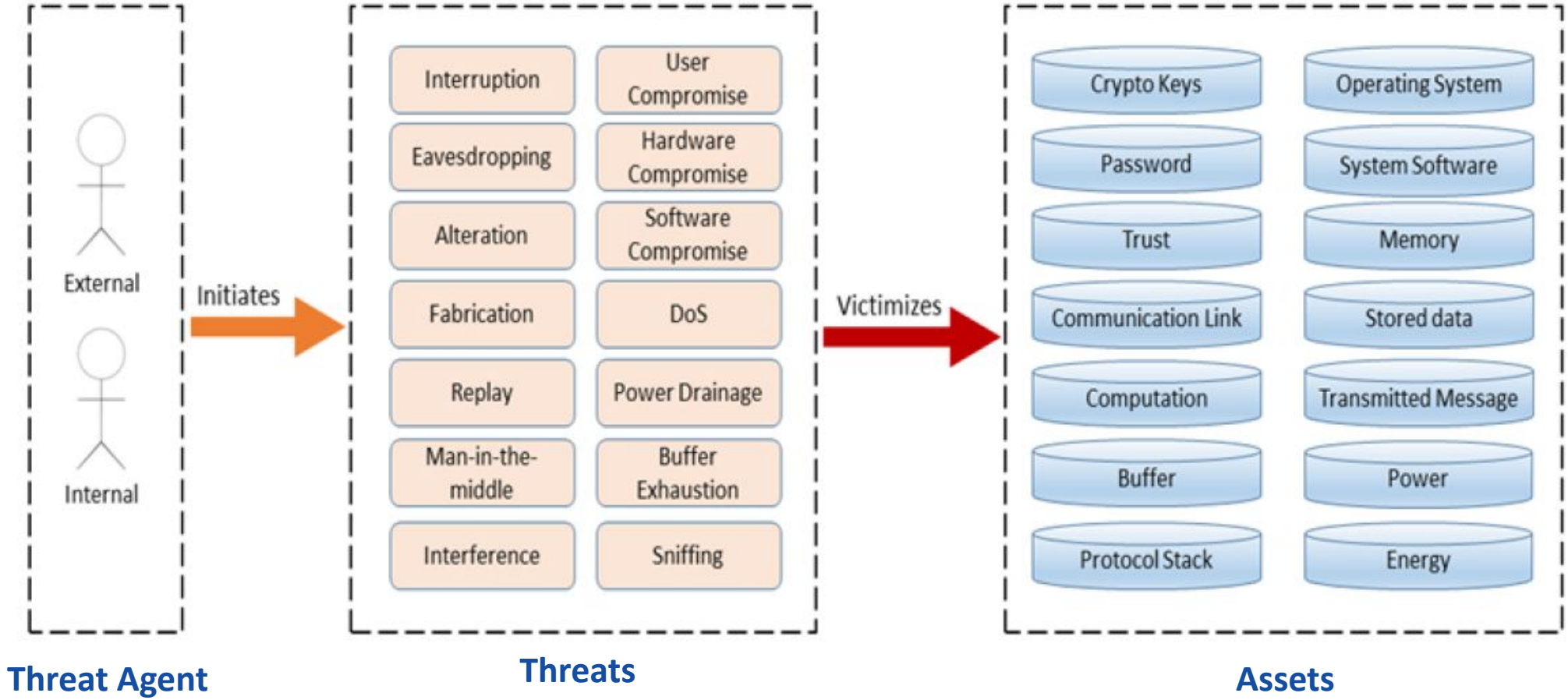
Security challenges for IoT devices

1. IoT products are generally deployed in insecure / exposed environments
2. Limited security planning and weak OS & application architecture
3. Limited capabilities such as processing, memory and power
4. Due to the fragmentation of standards & regulations
5. Difficult security integration of entire network
6. lack of secure Over-the-Air (OTA) Updates for IoT software & firmware

Privacy Issues

1. Collection, use and disclosure of IoT data
2. De-identification of IoT data
3. Consent (capacity, voluntary, current, specific and informed)
4. Dependency on vendors
5. Interoperability
6. Managing IoT devices
7. Accountability and Transparency

Threats in IoT environment



Mirai Botnet

The Mirai botnet attack targeted the DNS service provider Dyn in October 2016. As a result of the attack, numerous major websites and online services, including Twitter, Reddit, Spotify, GitHub, and many others, experienced disruptions or outages due to the compromised IoT devices overwhelming Dyn's servers with a massive distributed denial-of-service (DDoS) attack.

Distributed Denial of Service Attack (DDoS)

A DDoS attack is a malicious attempt to disrupt the regular functioning of a network, service, or website by overwhelming it with a flood of internet traffic.

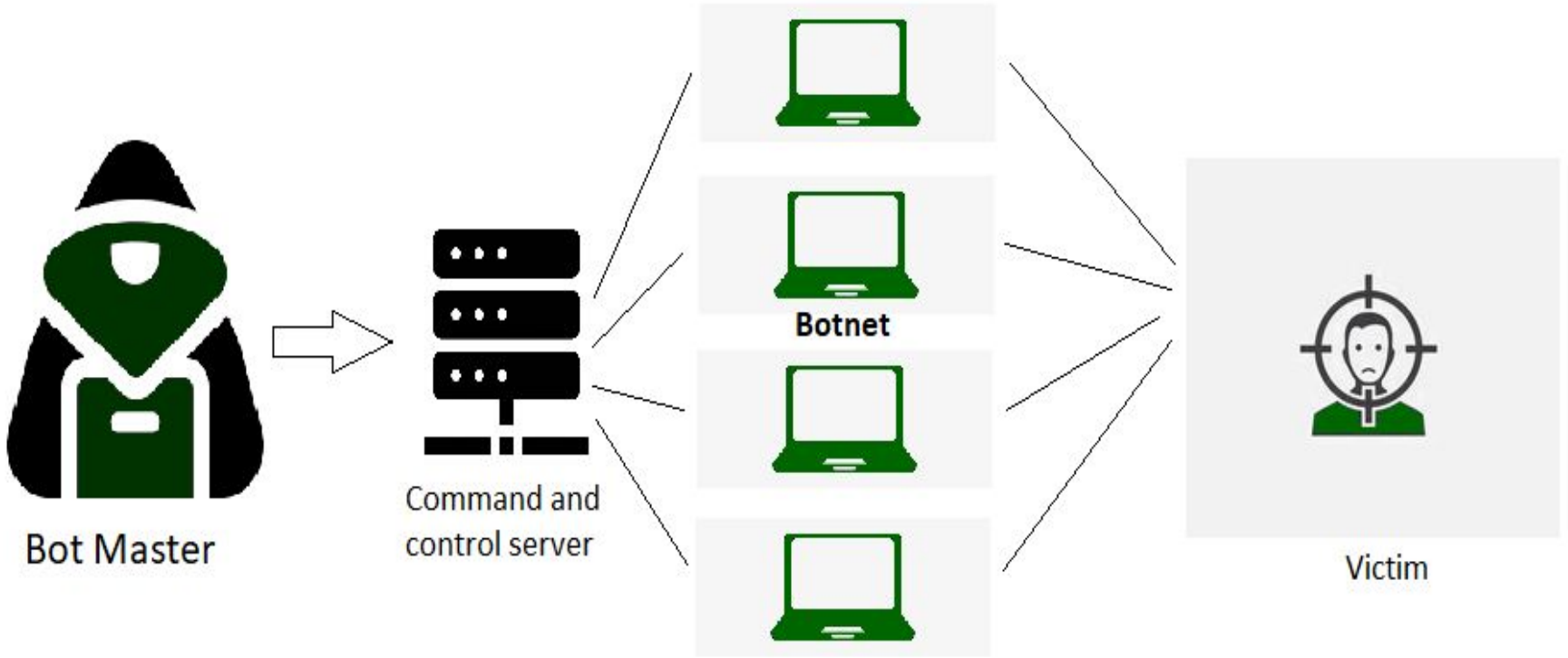
Key characteristics:

- Distributed nature
- Multiple sources
- High volume of traffic

How Does a DDoS Attack Work?

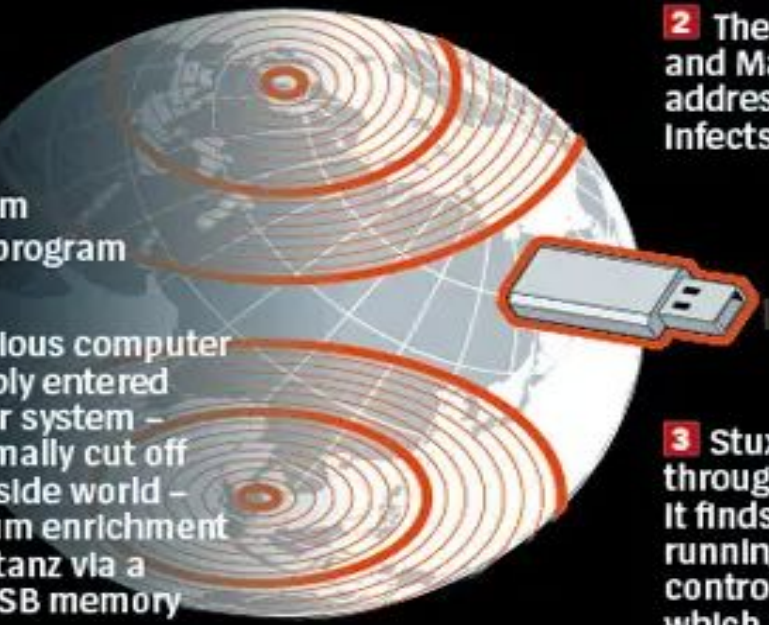
- Step 1: Botnet creation
- Step 2: C&C communication
- Step 3: Attack launch
- Step 4: Victim overwhelmed
- Step 5: Service disruption

Distributed Denial of Service Attack (DDoS)



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program



1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

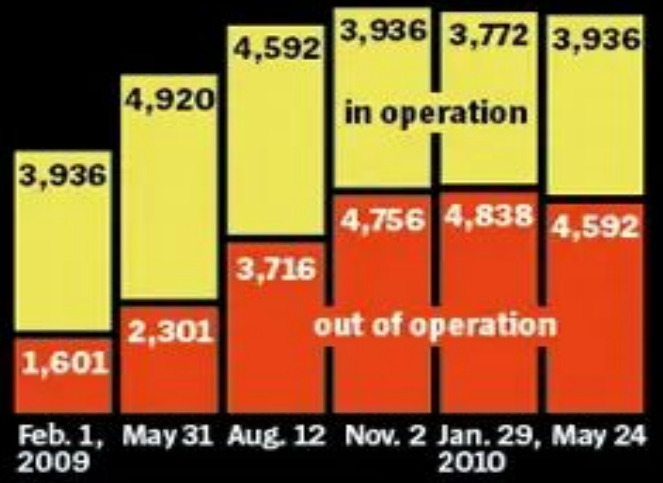
2 The virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

Iranian centrifuges for uranium enrichment

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Attack on IoTs

- DDoS attack
- Message Interception attack (MIM)
- Timing attack (side channel attack)
- Injection attack
- Crypto Jacking
- SPAM attack
- Replay attack
- Node capture attack
- Vulnerable 3PP library

WiFi Router Vulnerabilities

WiFi Attacks

- Evil Twin Attack
- Jamming Signals
- Misconfiguration Attack
- Honey Spot Attack
- Unauthorized/Ad hoc Connection Attack

Precautions

- Avoid public WiFi networks
- Use VPN connection if you have to use public WiFi network.
- Always change the default credentials of your router.

Bluetooth Vulnerabilities

- Always keep Bluetooth in off state when not in use.
- Hackers can exploit open bluetooth for-
  - Bluesnarfing
  - Eavesdropping
  - Denial of Service
  - Viruses and Worms
  - Bluetooth headsets vulnerabilities
- Avoid pairing Bluetooth devices in crowded spaces.

Vulnerabilities of IoT Devices

- Security Vulnerabilities
- Data Privacy Concerns
- Regulatory and Compliance Risks
- Network Vulnerabilities
- Legacy Systems
- Lack of Security Updates
- Insecure Communication
- Device Manipulation
- Supply Chain Attacks

Securing IoT Devices

- Choose Reputable Manufacturers
- Change Default Credentials
- Implement Strong Authentication
- Strong Encryption
- Secure Communication
- Disable Unnecessary Features
- Regularly Update Firmware
- Network Segmentation
- Disable Unused Ports and Services

Securing IoT Devices

- Physical Security
- Security by Design
- User Education
- IoT Security Standards
- Regulatory Compliance
- Disable Unused Ports and Services
- Privacy Considerations
- Regular Audits
- Vulnerability Monitoring

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Thanks