Attack Types

Le-2

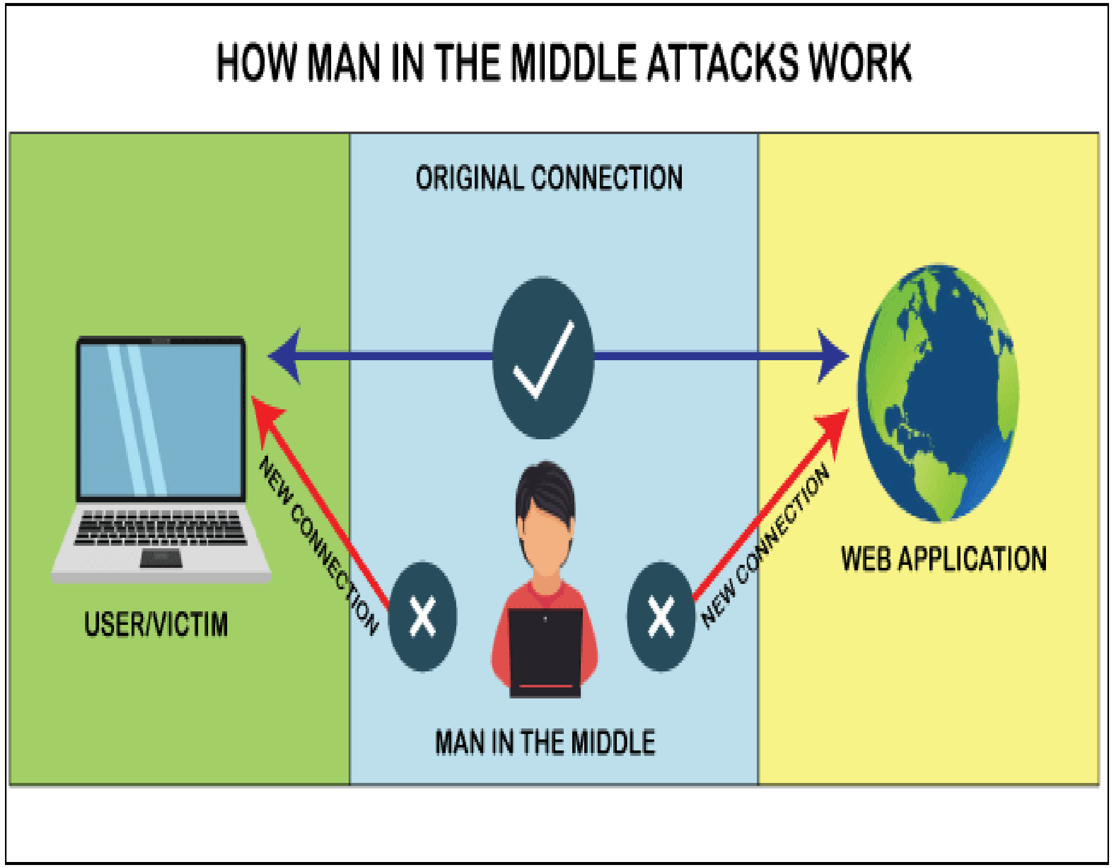
Attack Types

Some of the major IoT attack types are:

- Man-in-the- Middle Attack
- Routing Attack
- DoS(Denial of service)/DDoS(Distributed DDoS) Attack
- Physical Attack
- False Data Injection Attack
- Elevation of Privilege Attack
- Some other types of attacks

Man-in-the-Middle (MitM) Attack

- An attacker puts himself between the two communicating parties so that he can observe, control, and gain access to the information being shared between them and also interfere with that communication.



Types of MitM Attacks

- MitM can be done in the following ways:
- a) ARP Spoofing: Due to the inadequate authentication process of ARP (Address Resolution Protocol) it can be spoofed easily. Here, an attacker associates its MAC address to the IP address of any authentic user by sending falsified ARP messages.
- Another type of attack on ARP protocol is ARP cache poisoning where the attacker sends forged ARP requests and reply messages as a result of which his MAC address is linked with some authentic IP address in the ARP cache table.

Types of MitM Attacks

b) IP Spoofing: The attacker forges the source IP address in the packet. He can conceal his original identity and location by impersonating someone else in the network. Source-based packet filtering becomes less effective as a result of IP spoofing.

c) DNS Spoofing: It is an attack in which an attacker alters the records of the DNS server so that a particular domain name is associated with the fake IP address of the malicious actor.

Types of MitM Attacks

- ii) ICMP Redirecting: Network traffic is maliciously redirected to unauthorized locations through the use of ICMP Redirect attacks. Also known as ICMP Redirect spoofing or ICMP Redirect hijacking.
  - The attacker can compel a router to redirect packets meant for the victim through the attacker's machine.
  - They could be employed to aid man-in-the-middle attacks, snoop on private data, or impair network availability.
- iii) Port Stealing: The attacker uses a switch's forwarding mechanism to launch a MitM attack. The switch is manipulated to fool the attacker into relaying the packets for the victim system without really changing their content.

Routing Attack

- It alters the routing information of the routing protocol causing the packets to be delivered to the malicious node or dropped. There are various ways to alter the routing information, the most prevalent of them are:
- i) Sinkhole: The compromised node advertises a fake routing path through itself attracting a huge traffic.
- ii) Blackhole: When the malicious node discards every packet that it receives from other neighboring nodes, it is called a blackhole attack. A blackhole and sinkhole attack together can stop all the communication around the blackhole node.

Routing Attack

iii) Selective Forwarding/Grayhole: This attack adds somewhat more intelligence to the blackhole attack. Unlike a blackhole attack, it drops or forwards packets selectively.

iv) Wormhole: A tunnel is created between multiple malicious nodes allowing interception and diversion of a lot of data packets.

- A tunnel is an out-of-band fast transmission channel. A packet passing through the tunnel reaches its destination before the packet following a genuine path.
- As the packet following the normal route uses multi-hops and reaches its

destination later, it is dropped.

Routing Attack

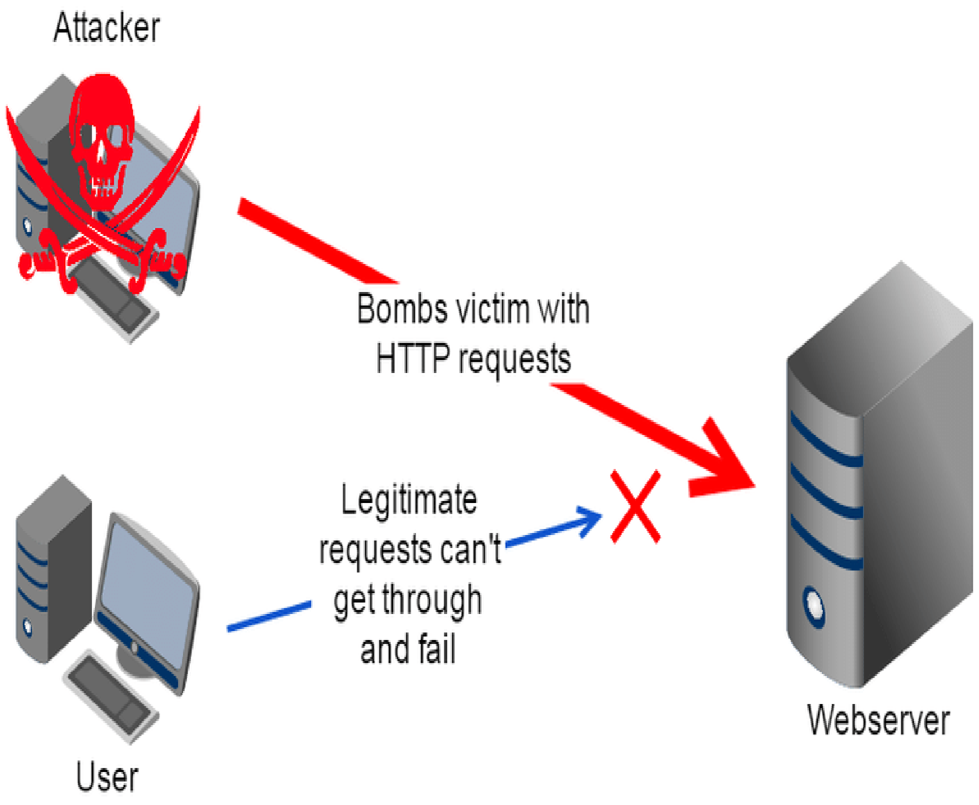
v) Replay: An attacker replays the previously received control packets like routing information and threatens the freshness of the message.

vi) HELLO Flooding: Malicious node convinces other nodes that it is present in their vicinity although it is sitting somewhere else in the network topology. It does so by sending a broadcast message with high transmission power.

vii) Sybil: An attacker can launch the Sybil attack by fabricating multiple false identities of a node to form contradictory routing paths in the network.

DoS (Denial of Service)

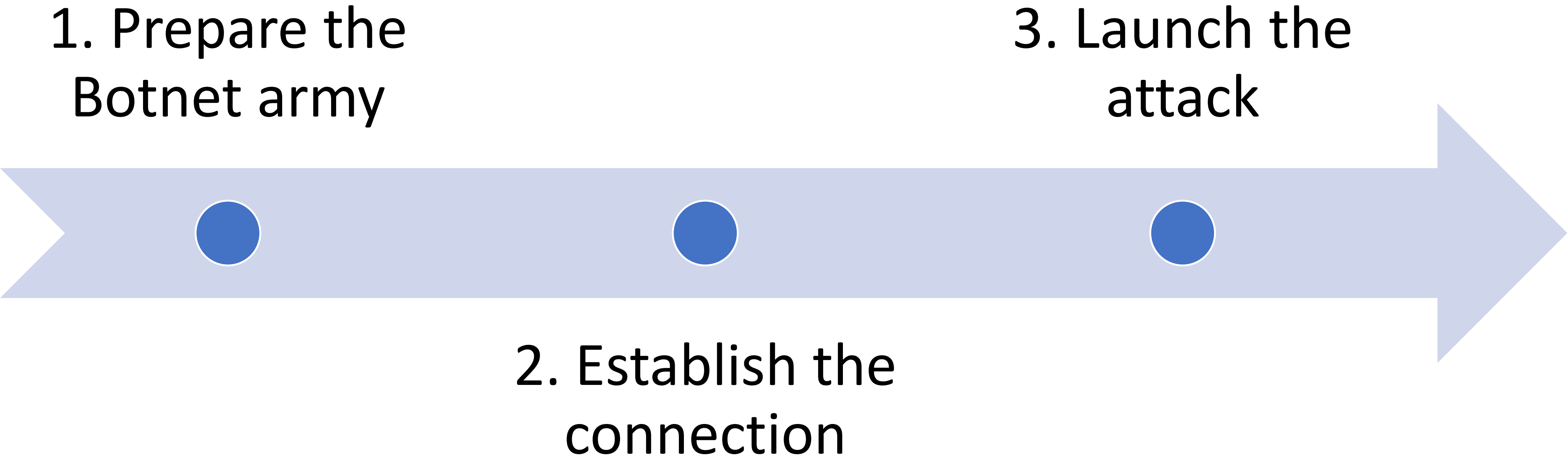
- DoS attack is an attack strategy in which an attacker overwhelms the resources of the victim's system to such an extent that the attacked system is not able to provide any service or resources to the legitimate users.
- It affects the availability of the system.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Distributed Denial of Service (DDoS) Attack

- Numerous compromised machines called botnets present at different geographic locations send traffic toward the victim node at the same time making it unavailable for legitimate users.
- DDoS attacks have been there in different forms and are still evolving rendering them difficult to detect.

DDoS Attack Scenario

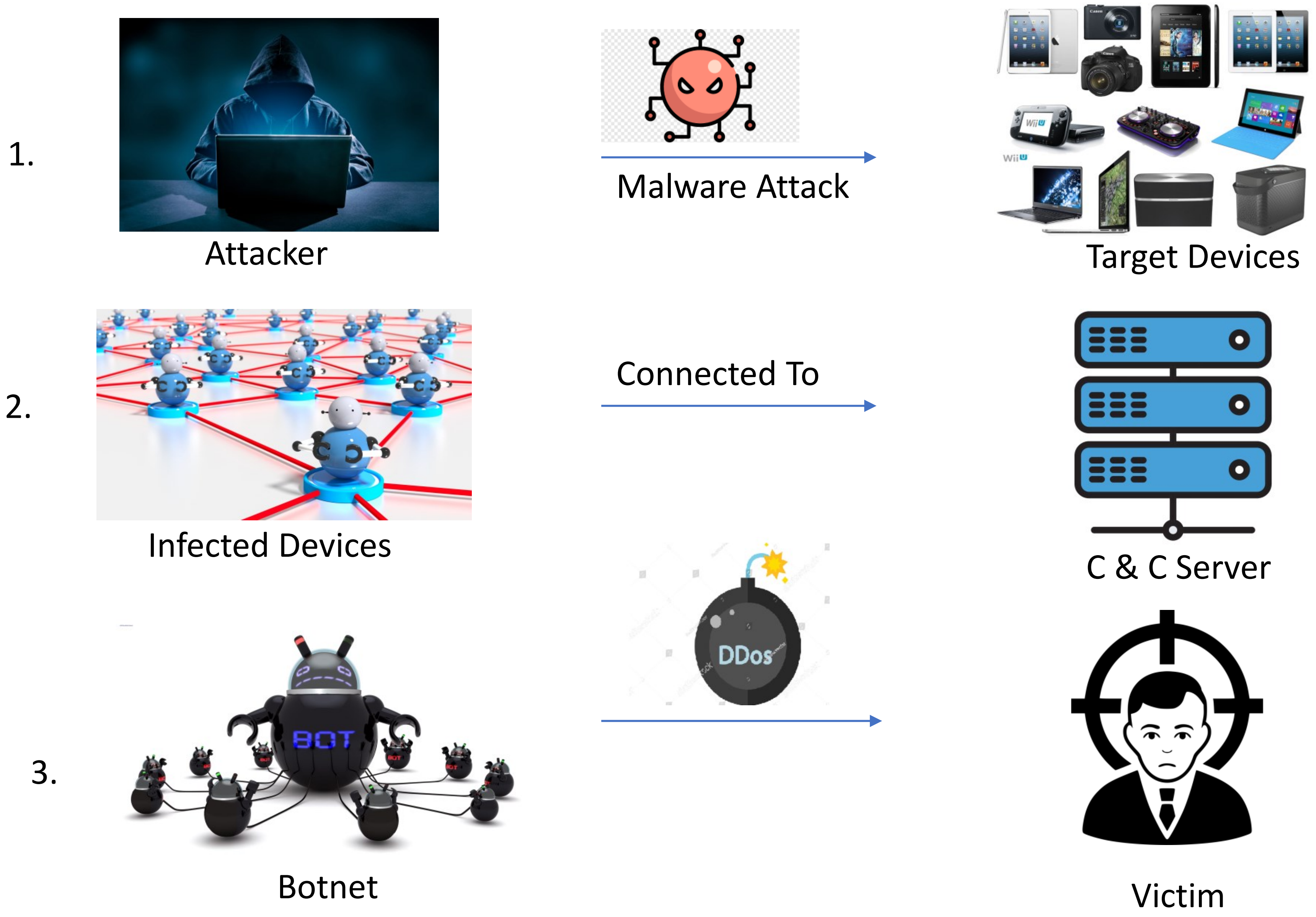


1. Prepare the Botnet army

2. Establish the connection

3. Launch the attack

Steps to perform DDoS Attack

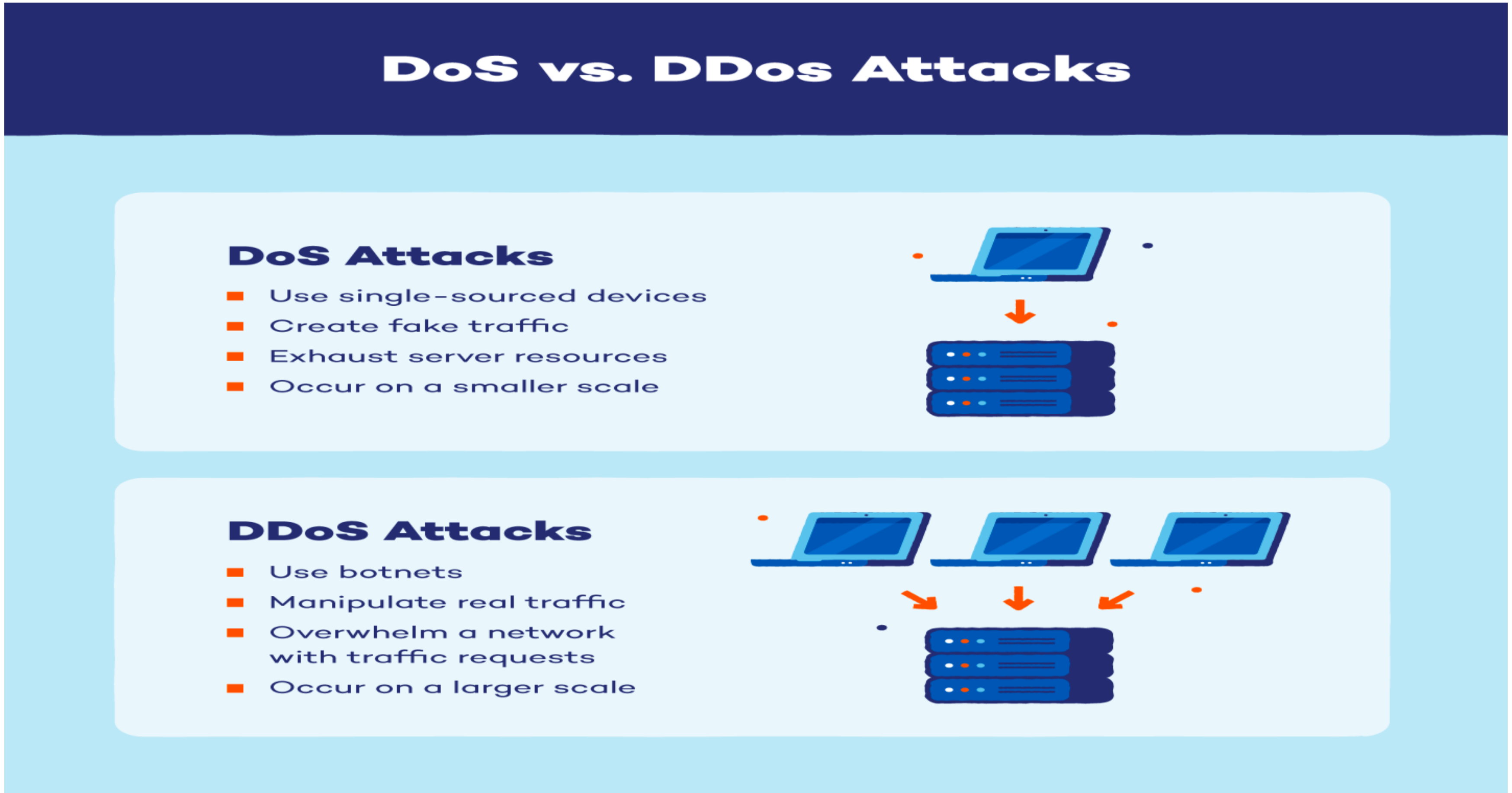


1. Attacker — Malware Attack → Target Devices

2. Infected Devices — Connected To → C & C Server

3. Botnet → Victim

DoS vs DDoS Attack



DoS vs. DDos Attacks

DoS Attacks

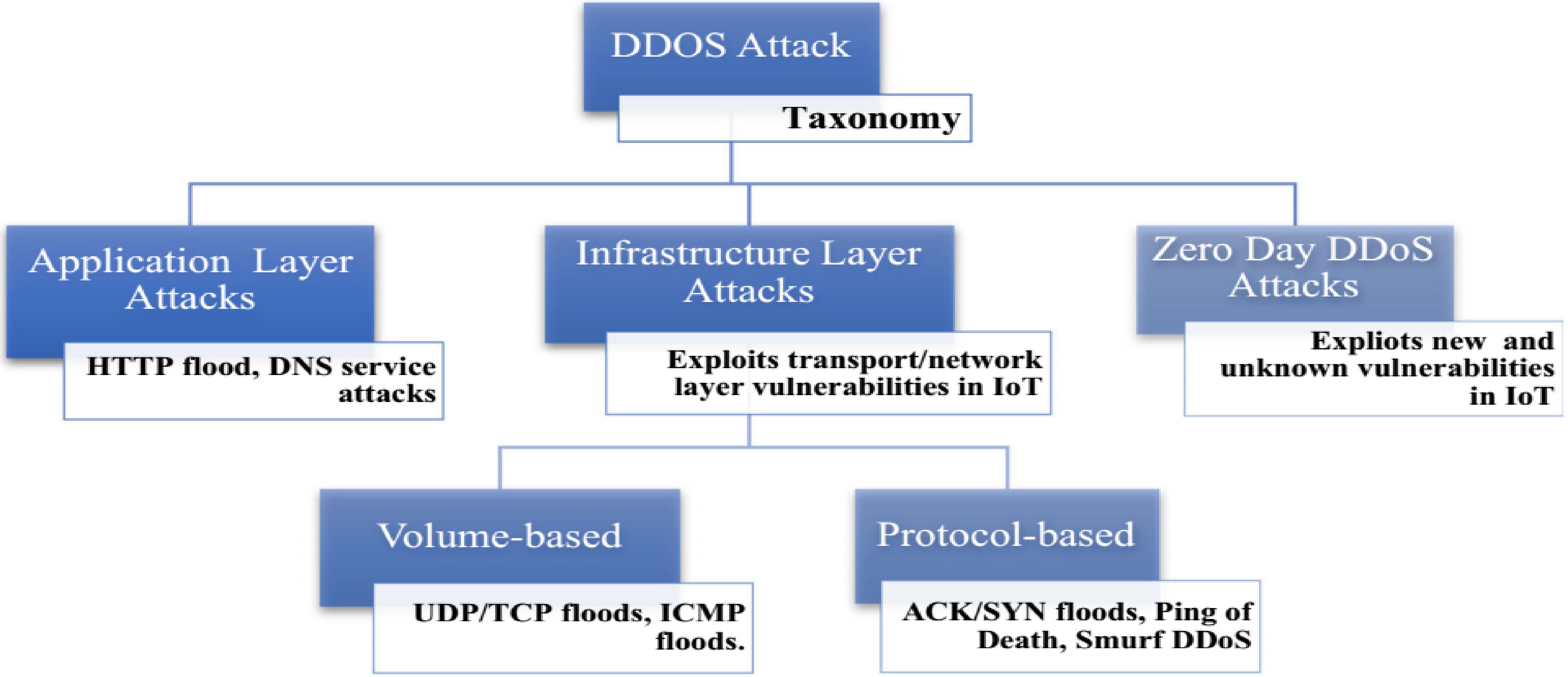
- Use single-sourced devices
- Create fake traffic
- Exhaust server resources
- Occur on a smaller scale

DDoS Attacks

- Use botnets
- Manipulate real traffic
- Overwhelm a network with traffic requests
- Occur on a larger scale

Types of DoS/DDoS attacks

- DoS/DDoS attacks can be of different types depending on the type of packets used by the attacker to flood the victim



DDOS Attack

Taxonomy

Application Layer Attacks

HTTP flood, DNS service attacks

Infrastructure Layer Attacks

Exploits transport/network layer vulnerabilities in IoT

Zero Day DDoS Attacks

Expliots new and unknown vulnerabilities in IoT

Volume-based

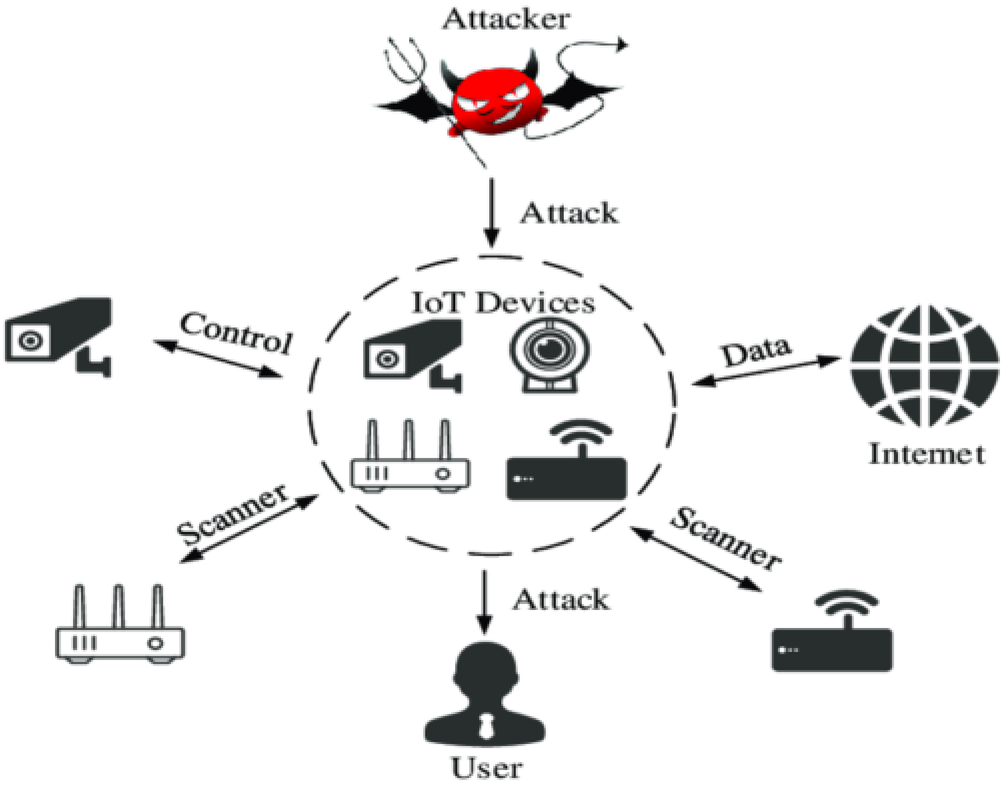
UDP/TCP floods, ICMP floods.

Protocol-based

ACK/SYN floods, Ping of Death, Smurf DDoS

Physical Attacks

- IoT devices are typically set up in hostile, dynamic, and heterogeneous environments, in contrast to standard Internet Technology (IT) infrastructure.
- At any point, sensitive information could leak or be altered in such scenarios.



Types of Physical Attacks

i) Node destruction: The act of destroying a node physically using any means rendering it useless is known as node destruction.

ii) Tampering: An intruder alters, adds, or destroys information from the end device. An end node is forcibly taken over and compromised by the attacker. Therefore, the attacker has the power to get all data.

iii) Tag Cloning: The technique of reproducing or duplicating the data recorded on an RFID (Radio Frequency Identification) tag is termed ”tag cloning,” also known as” RFID cloning.” RFID tags can be duplicated using specialized tools and procedures.

Types of Physical Attacks

iv) Sleep Deprivation: Also known as Exhaustion attack, tries to deplete IoT devices’ resources to the point where they are unable to function correctly or communicate with other devices or the network. These resources could be bandwidth, power, or memory.

v) RF (Radio Frequency) Jamming: The devices’ capability to share wireless bandwidth is rendered ineffective by Radio Frequency (RF) jamming.

vi) Node Injection: The attacker alters the network topology by introducing or putting a new node in between two or more existing nodes. It is a variant of MitM attack.

Elevation of Privilege

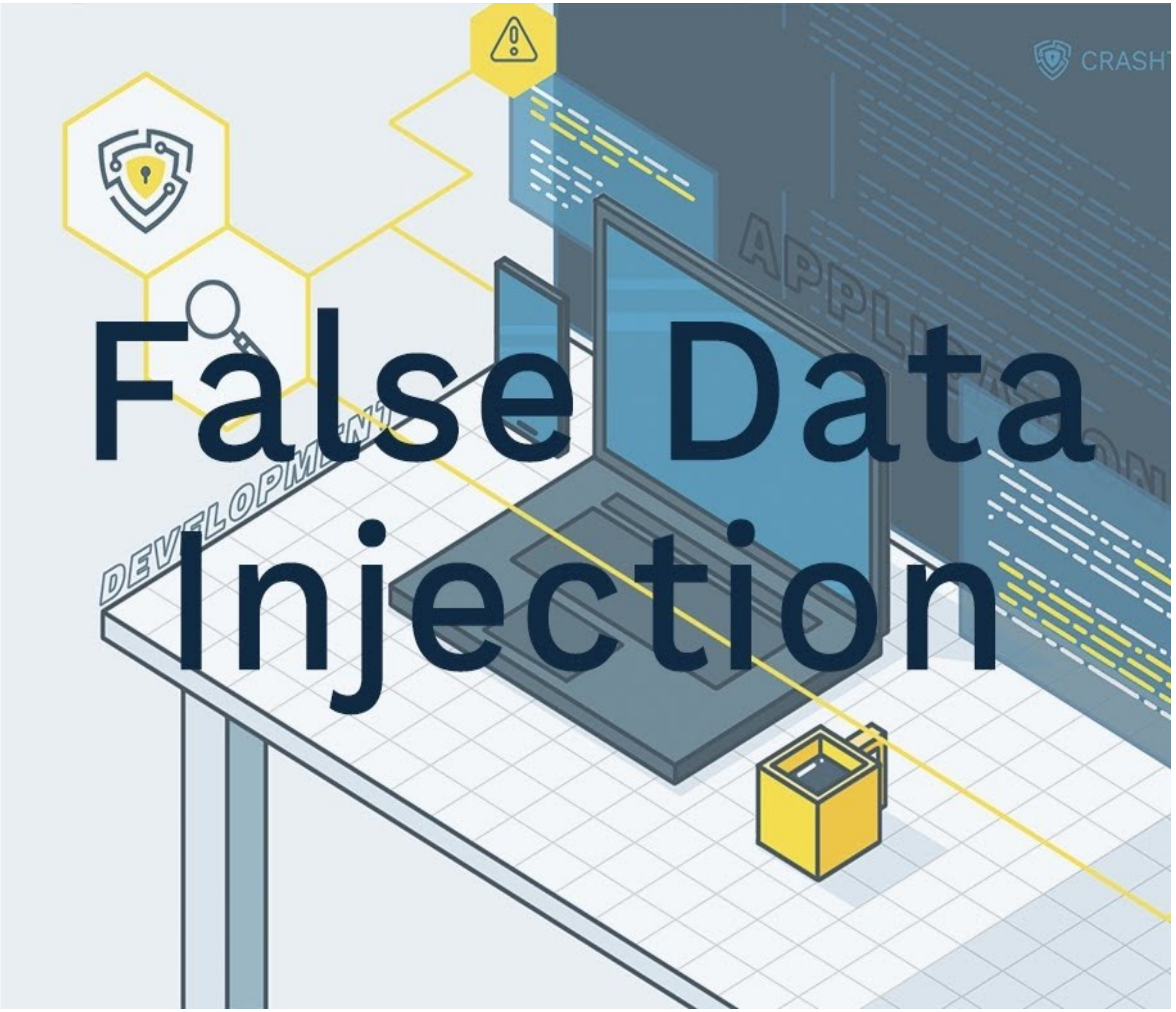
The attacker wants to heighten his privilege once he has already gained access to the lower level after exploiting some vulnerabilities in the system. Following are the well-known attacks in this category:

i) User to Root (U2R): The attacker first accesses the system/device as a normal user and later upgrades his role to a root user. Now, being a root user, he can exploit various other system vulnerabilities.

ii) Remote to Local (R2L): The malicious actor without having an account in the remote system transmits packets to the distant system over a network.

False Data Injection (FDI)

- In FDI, an attacker injects some malicious data into the IoT sensor due to which various integrity violations may occur.
- For example, injecting false data may lead to the wrong estimation of the state of the device employed in some critical environment.



Types of False Data Injection (FDI)

- i) Cross-Site Scripting (XSS): JavaScript code that is embedded in web pages is frequently used by web applications to allow dynamic client-side behavior. The user's web browser is used to execute this script code.
- A sandboxing system is used to restrict a program to only access the resources connected to its origin site to safeguard the user's environment from harmful JavaScript code.
- Unfortunately, if a user is tricked into downloading malignant JavaScript code via an intermediate, legitimate website, these protection methods fail.
- In such a case, all resources that belong to the trusted site are completely accessible to the malicious script.

Types of False Data Injection (FDI)

ii) SQL Injection: In this type of attack, user data is coupled into SQL query, now that a part of the user’s input is treated as a normal SQL code.

An attacker can send SQL commands to the database directly by using these loopholes. Web applications that combine user input into SQL queries to the database are at considerable risk from these attacks.

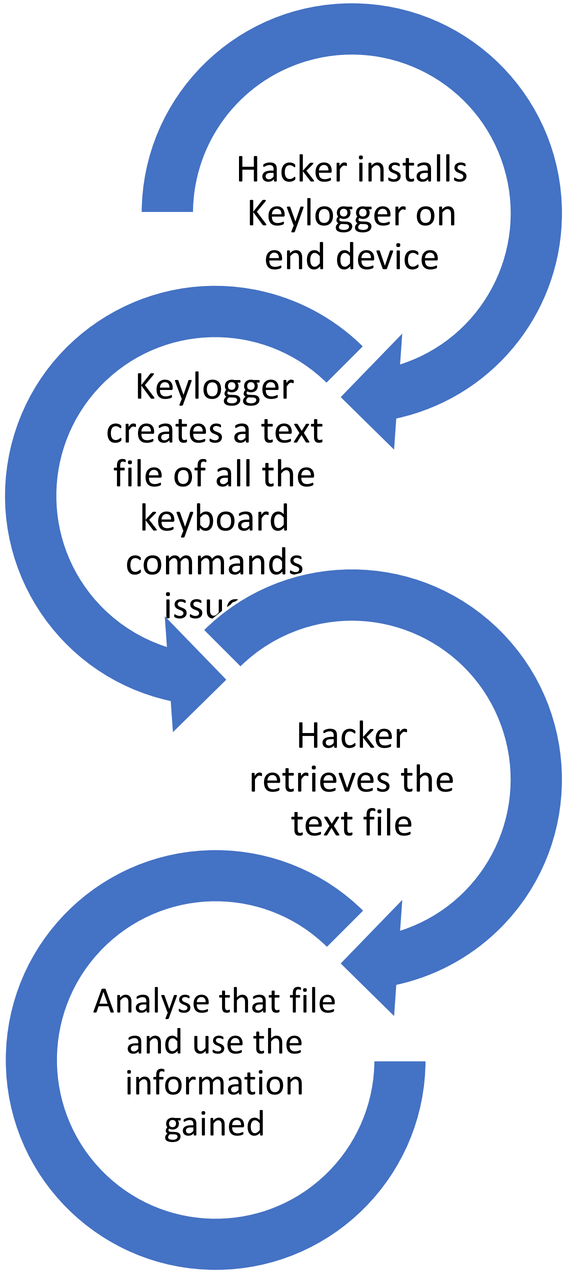
This is the way most of the web applications used on the internet operate, leaving them susceptible to SQL injection

Some other types of attacks

ii) Snooping/Eavesdropping: Snooping or Eavesdropping means unauthorized access to or inception of data. It may include activities from just watching the emails that appear on the victim's computer screen to examining his keystrokes.

More sophisticated snooping attacks may include the use of software tools for examining the user's activities remotely or examining the data when the data is in motion.

An example of such a tool is Keylogger, which is a software used to observe keystrokes including personal information like login credentials and password of the victim. It is a passive attack and hence difficult to detect.



Hacker installs Keylogger on end device

Keylogger creates a text file of all the keyboard commands issu

Hacker retrieves the text file

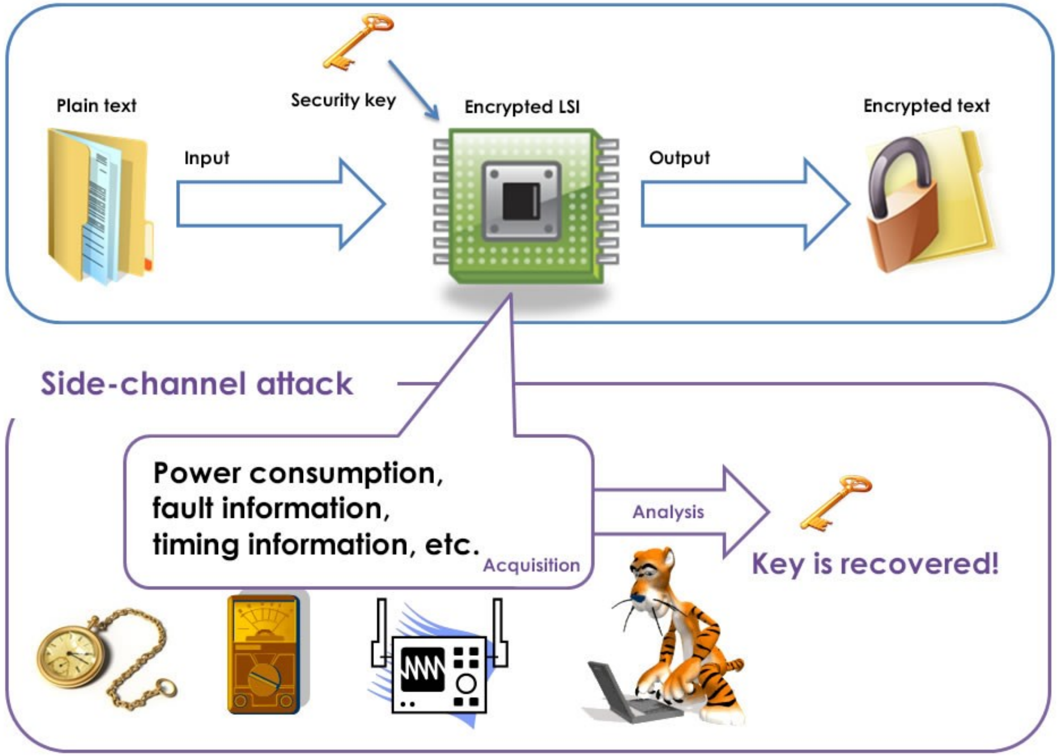
Analyse that file and use the information gained

Some other types of attacks

Side Channel Attack

It is an attack strategy where the attacker exploits the extra information related to the way a particular protocol or algorithm is implemented.

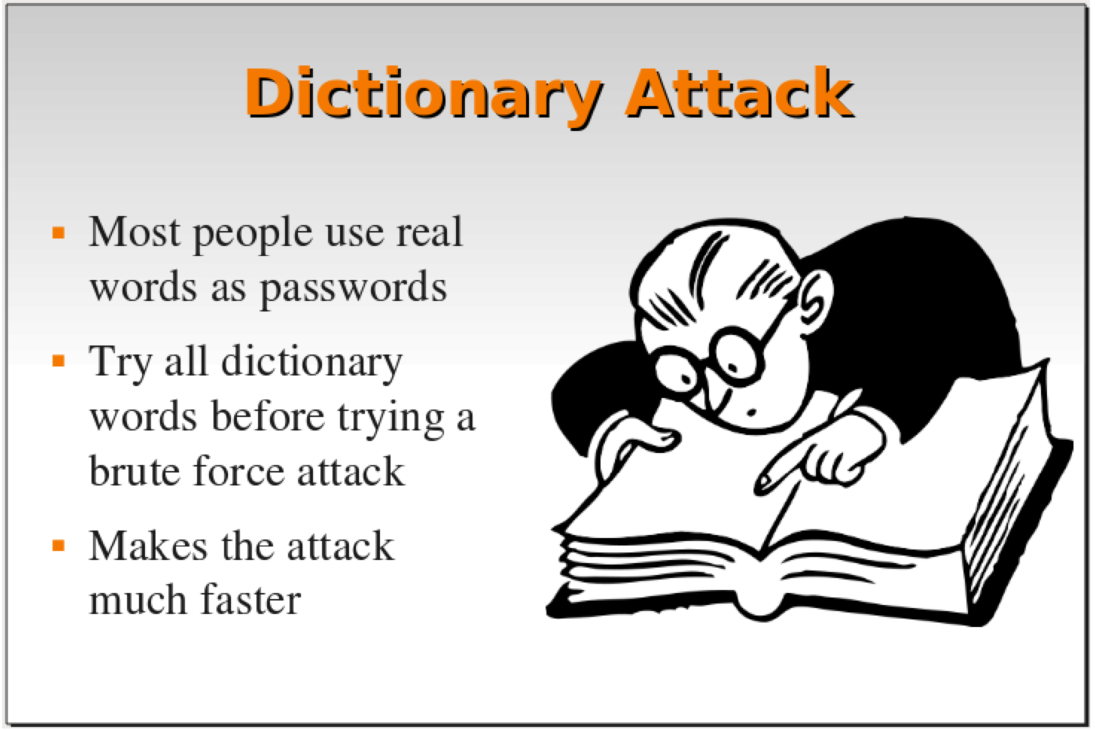
This extra information could be power consumption, timing information, sound, electromagnetic leaks, etc.



Some other types of attacks

Dictionary Attack

- ➢ Dictionary Attack aims to gain illicit access IoT devices by using restricted subset of keyspace.
- ➢ It may involve trying millions of possibilities which may be obtained from past security breaches.



Dictionary Attack

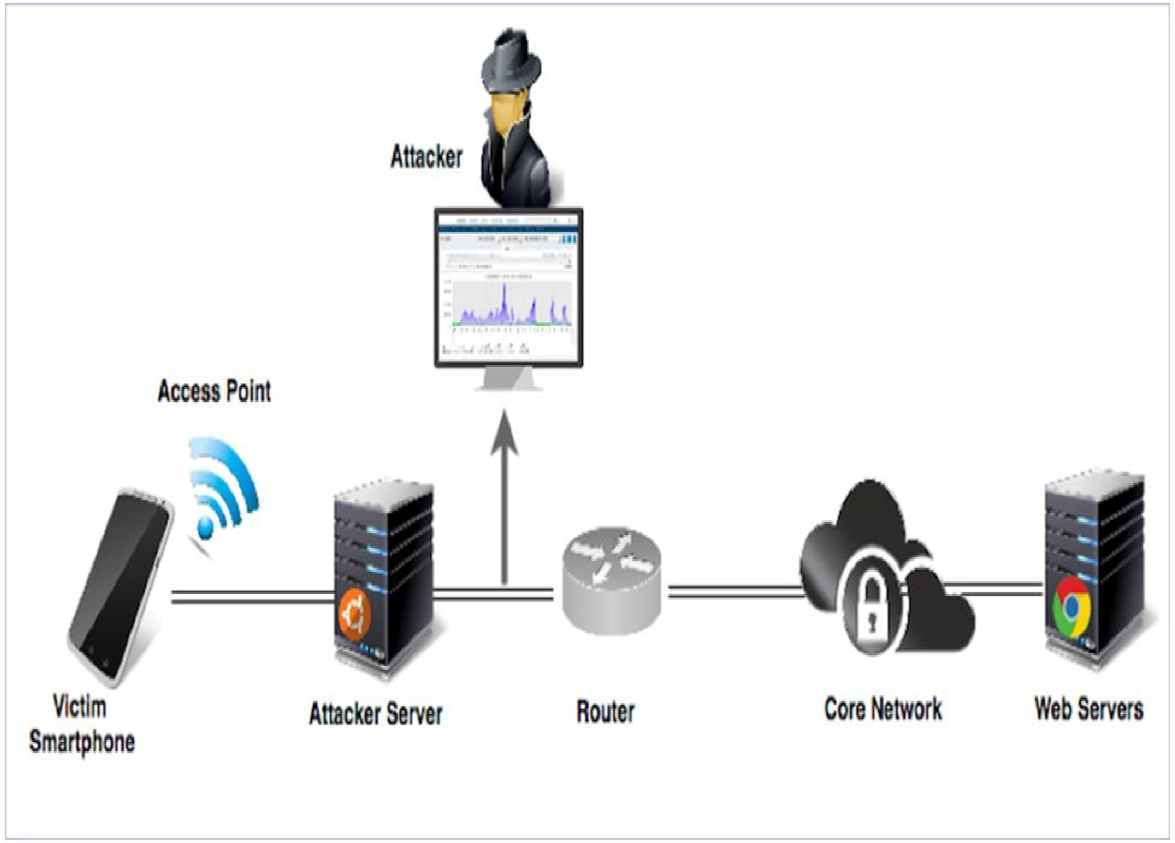
- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

Some other types of attacks

Traffic Analysis

In traffic analysis, the adversary has no access to the data(if it is encrypted) but he can obtain some other kind of information by monitoring online traffic.

This information can be electronic addresses like e-mail addresses or some request-response pairs with the help of which adversary can guess the nature of the transaction. It is also a passive attack that cannot be detected easily.



Some other types of attacks

Malware

- Malware or malicious software is developed by an attacker to obtain unauthorized entry into the victim's system. Various kinds of malware include Ransomware, Spyware, Trojan horse, and virus.

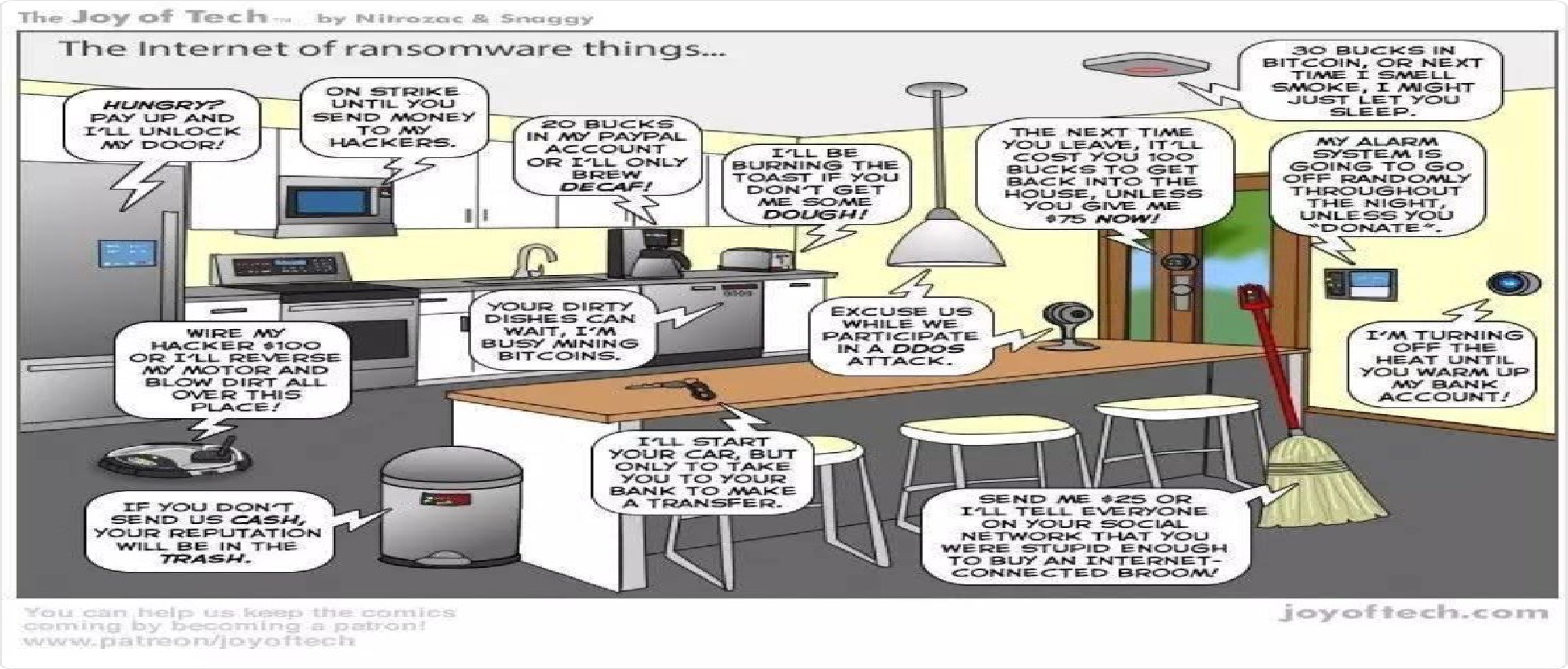
Ransomware Attack

- It is a kind of malware attack, where the attacker takes hold of some file, folder, or an entire device forcibly and does not release it until the ransom amount is paid.
- It is one of the most common cyberattacks.

Social Engineering Attack

- It involves using psychological manipulation to trick users into revealing sensitive information or performing actions that could compromise the security of IoT systems.
- Examples include pretexting, baiting, and tailgating.
- Baiting: a false promise or reward to trap victims and steal their sensitive information by infecting their systems with malware.
  - Congratulations! You are the lucky winner of…”
  - “Yay! We have a free gift for you; download it now.”

Ransomware Attack


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Attack Against Confidentiality

- Snooping/Eavesdropping:
- Traffic Analysis
- Dictionary Attack
- Side Channel Attack
- Sybil Attack

Attack Against Data Integrity

1. Modification
2. Masquerading/spoofing
3. Replaying
4. Repudiation
5. False Data Injection (FDI)
6. Firmware Modification Attack

Attack Against Availability

- Device/node Capture
- Routing Attack
- Denial of Service(DoS)
- Distributed Denial of Service(DDoS)
- Battery Draining Attack

Traditional Defence Mechanisms

- Filter Packets
- Adopt Encryption
- Employ Robust password Authentication Scheme
- Audit and log Activities
- Use Intrusion Detection System (IDS)
- Prevent Intrusion Using Intrusion prevention System