# SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

**An Autonomous Institution**

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : covert channels –Backdoors – Bots

# covert channel

- A covert channel is a path for the **illegal flow of information between subjects within a system, utilizing system resources** that were not designed to be used for inter-subject communication.
- Note several **features** of this definition….
- Information flows in **violation of the security metapolicy** though not necessarily in violation of the policy.
- The flow is between subjects within the system; two human users talking over coffee is not a covert channel.
- The **flow occurs via system resources** (file attributes, flags, clocks, etc.) that were not intended as communication channels.

- Attempted access by SL(security level) to a high level resource returns one of two error messages: Resource not found or Access denied.
- By modulating the status of the resource, SH(shell) can send a bit of information on each access attempt by SL.
- This is called a covert storage channel because SH is recording information within the system state.

# Types of Covert Channels

- It is possible to distinguish many types of covert channels, depending on the attribute manipulated:
- **Timing**: how much time did a computation take?
- **Implicit**: what control path does the program take?
- **Termination:** does a computation terminate?
- **Probability**: what is the distribution of system events?
- **Resource exhaustion**: is some resource depleted?
- **Power:** how much energy is consumed?
- In practice, many researchers distinguish only storage and timing channels.

- A covert channel is any path for information between subjects, utilizing system resources that were not designed to be used for inter-subject communication.

- A useful distinction is between storage and timing channels, though the breakdown is not always clear for specific channels

# Backdoors(Remote Access)

- The backdoor is any **sort of method** which allows any **organization, hacker, or even government to access your system without your permission.**
- A **Backdoor can be installed on your system by hackers** in the form of some **malware application** or using your device's software vulnerabilities.
- Backdoors are **used mainly by hackers** for using your data, invading your privacy, crypto-jacking, surveillance, etc.
- In recent days, **hackers have discovered so many new ways to get access to user's devices and install all the malware applications to get their private data.**

- Hackers can generally install backdoors in two places in your phone or systems

- **Hardware** – It allows **remote access to the user's system**

- **Software – It is even more dangerous as malware files/apps are disguised in the name of other legitimate applications.** Hence, your device's OS finds it challenging to recognize that someone else is accessing your phone.

- This **backdoor concept was invented for legal purposes like tech support, but now they are used mainly by cyber attackers for their profit.**

- ***Note: All the malware like rootkits, trojans, spyware, cryptojackers, keyloggers, worms and even ransomware are considered to be backdoors if installed in user's devices without their permission or knowledge.***

# Prevent a Device from Backdoors

- Backdoors are very challenging to detect, and hence it is better to take precautions and be aware that no one else is accessing your system through a backdoor. These are the ways that may come in handy

- **Using anti-virus and anti-malware apps on your device** is always a good idea as it detects a lot of unusual activity before the user even recognizes it. As soon as it catches, it tries to eliminate those viruses before they start infecting your device.

- **Now backdoors can't be installed** in your device without you giving access to the hacker to install those malicious apps or software in your devices, so if you stay a **bit alert while downloading files, you can stop hackers to even gain access to your device**, without which backdoors can't be installed so never download any files from suspicious and pirated sites.

- **Always use good and enhanced security in your device like updated password managers,** which encrypts all your information using 256-bit AES encryption and also use biometrics or OTP's for transferring data in place of simple patterned locks because this generates random complex passwords, which makes it difficult for cyber attackers to guess. Hence, they can't gain access to your device.

- With each day passing, hackers are developing a new way to install backdoors. Still, even software developers are not leaving behind to publish new features in their updates to fix their vulnerabilities and fill all the loopholes existing.

# Bots

- A botnet is a collection of **internet-connected devices,** which may include personal computers (PCs), servers, mobile devices and internet of things (IoT) devices, that are infected and controlled by a common type of malware.

## How do botnets work

- The term *botnet* is derived from the words ***robot* and *network***. A *bot*, in this case, is a device infected by malicious code, which then becomes part of a network, or *net*, of **infected machines all controlled by a single attacker or attack group.**

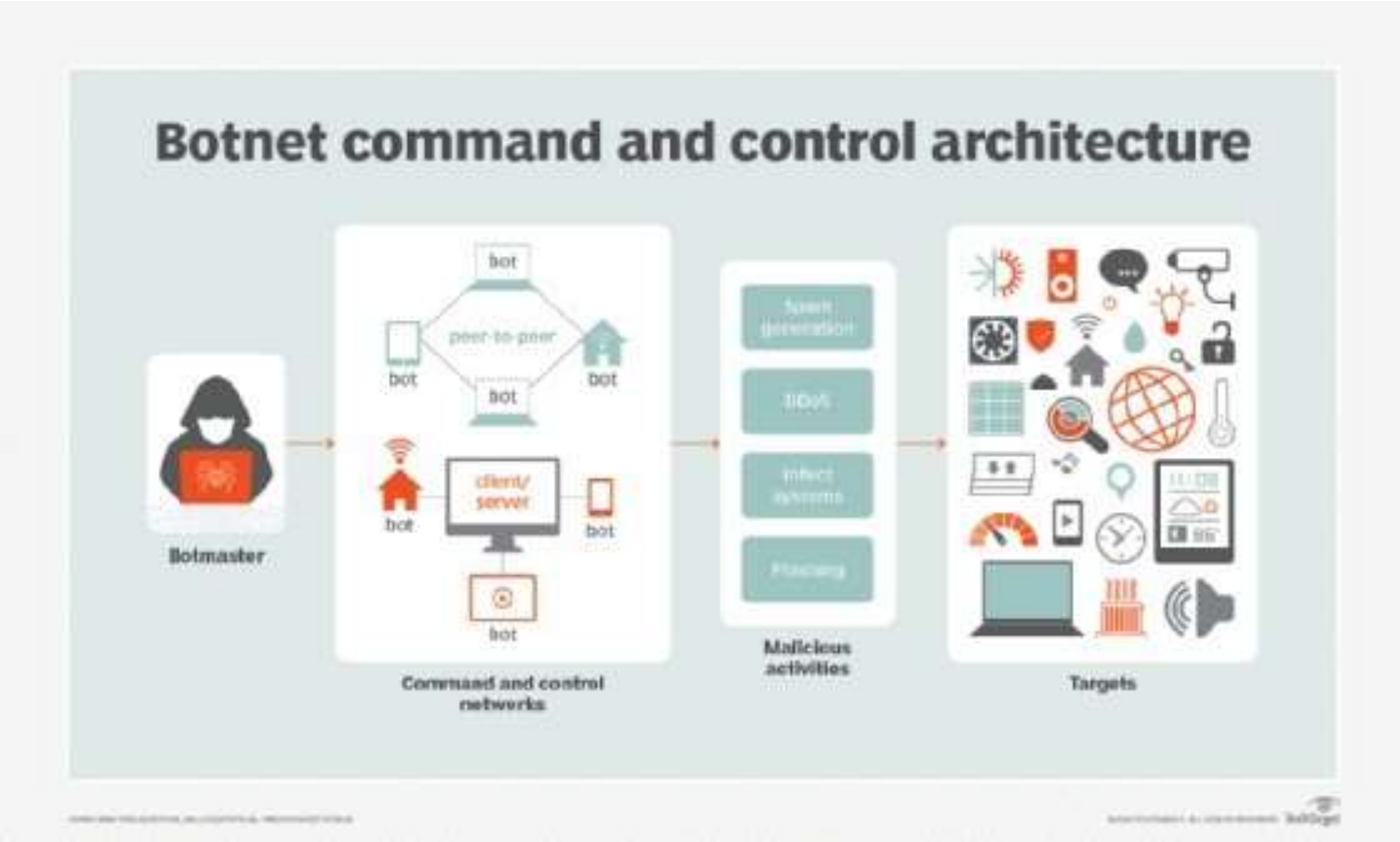
- The botnet malware typically looks for **devices with vulnerable endpoints across the internet, rather than targeting specific individuals, companies or industries.**

- The objective for creating a botnet is to **infect as many connected devices as possible and to use the large-scale computing power** and functionality of those devices for automated tasks that generally remain hidden to the users of the devices.

# The architecture of a botnet

- Botnet infections are usually **spread through malware or spyware.** Botnet malware is typically designed to **automatically scan systems and devices for common vulnerabilities** that haven't been patched in hopes of infecting as many devices as possible.

- Once the **desired number of devices is infected, attackers can control the bots using two different approaches**.


Botnet command and control architecture
bot
peer-to-peer
bot
bot
bot
client/
server
bot
bot
bot
Botmaster
Command and control
network
Malicious
activities
Targets

## The client-server botnet

- The traditional client-server model involves setting up a command and control (C&C) server and sending automated commands to infected botnet clients through a communications protocol, such as Internet Relay Chat (IRC).

## The P2P botnet

- The other approach to controlling infected bots involves a peer-to-peer (P2P) network. Instead of using C&C servers, a P2P botnet relies on a decentralized approach.

- Infected devices may be programmed to scan for malicious websites or even for other devices that are part of a botnet. The bots can then share updated commands or the latest versions of the malware.

# Preventing botnets with cybersecurity controls

- strong user authentication methods;
- secure remote firmware updates, permitting only firmware from the original manufacturer;
- secure boot to ensure devices only execute code produced by trusted parties;
- Advanced behavioral analysis to detect unusual IoT traffic behavior; and
- Methods using automation, machine learning and artificial intelligence (AI) to automate protective measures in IoT networks before botnets can cause serious harm.

Any Query????

Thank you……