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 : Interference & Interception

Interference

➢ Interference is **an event in which an organization tries to attack and exploit an organization's computers or information networks**.

➢ Hackers use interference operations to **spread misinformation**

➢ The goal of these attacks is to create, discord and increase unrest.

➢ To do this, attackers need to find ways to **amplify their voices**, often **turning to social media to spread misinformation through fake accounts**.

➢ Because there's **no process for validating information sources** on social media, it provides the ideal space to present extreme arguments as legitimate news.

Cyber security experts find ways to safe guard the attacks:

➢ **Ensure robust security protocols are in place**.

➢ **Recruit a team of cyber security experts**.

➢ **Demonstrate cyber resilience**.

Ensure robust security protocols are in place

➤ To prevent cyber attacks, organizations need to **invest in proper equipment and implement effective protocols.**

➤ When implementing changes, cyber security teams should evaluate their organizations' unique needs and identify potential vulnerabilities that foreign entities can exploit.

Recruit a team of cyber security experts.

➢ Cyber security strategies require **constant attention, revision and improvement.**

➢ It's vital for businesses to build highly qualified teams of cyber security experts who can identify and address threats effectively, especially during highly sensitive times like the 2020 presidential race.

Demonstrate cyber resilience.

➢ Cyber resilience refers to an organization's ability to **respond to and recover from a cyber attack.**

➢ To build cyber resilience, **security teams should be well trained and adaptable.**

➢ Running through potential security scenarios to refine the response strategy is just as important as developing a breadth of knowledge that allows for on-the-spot problem-solving.

➢ To effectively prevent cyber interference, security teams need to be current on the latest foreign intelligence and be ready to react as quickly as possible.
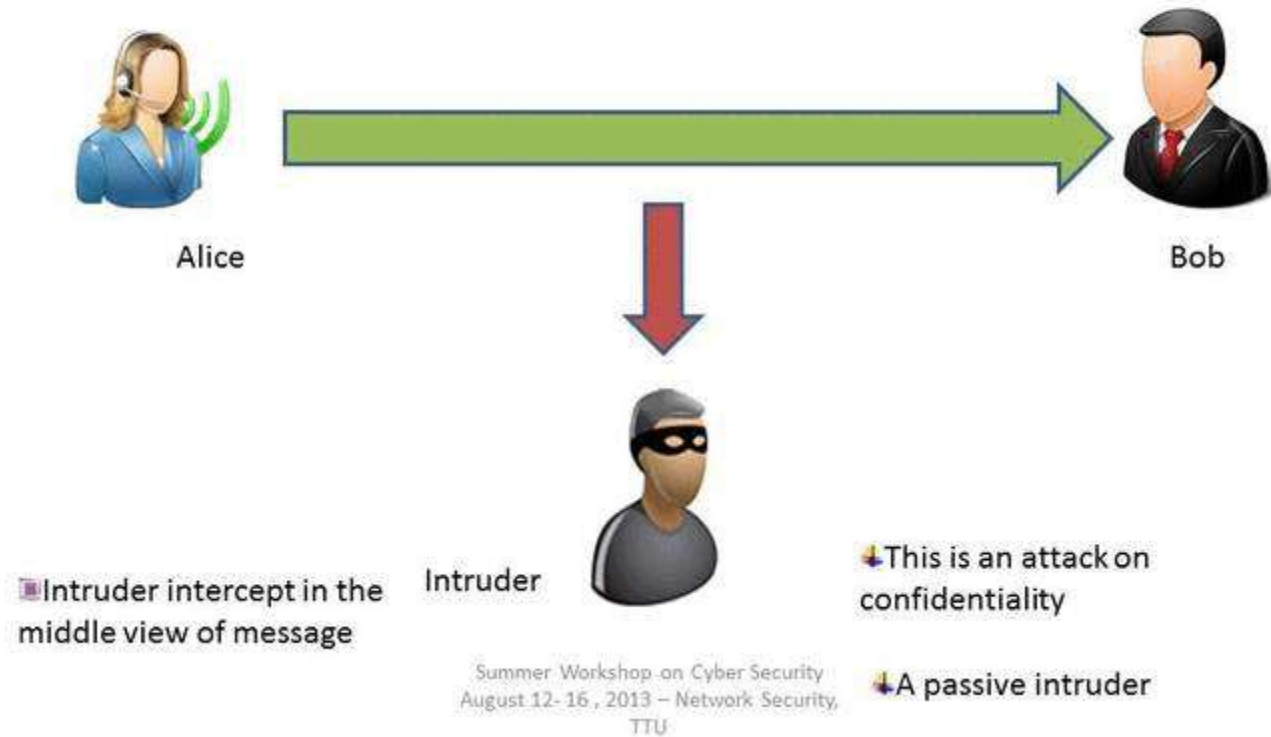
Interception

- ➢ Interception might take the form of **unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail**, and can be conducted against data at rest or in motion.

- ➢ Properly executed, interception attacks can be very difficult to detect.

- ➢ An interception is where an unauthorized individual gains access to confidential or private information.

- ➢ **Interception attacks** are attacks against network **confidentiality**

Security Attacks...

Interception

Alice → Bob

Intruder

■Intruder intercept in the middle view of message

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

This is an attack on confidentiality

A passive intruder

Examples of Interception attacks:

➢ Eavesdropping on communication.

➢ Wire tapping telecommunications networks.

➢ Illegal copying of files or programs.

➢ Obtaining copies of messages for later replay.

➢ **Packet sniffing** and key logging to capture data from a computer system or network.

Reduce the attack :

•**Using Encryption** - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.

•**Traffic Padding** - It is a function that produces cipher text output continuously, even in the absence of plain text.

➤ A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted.

➤ When input plaintext is not present, the random data are encrypted and transmitted.

➤ This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Any Query????

Thank you……

Interference & Interception / 19SB402/NETWORKING AND CYBERSECURITY/Mr.R.Kamalakkannan/CSE-IOT/SNSCE