Systems Security

Santosh Arya (2003EE10343)

Outline

- The Security Problem
- Program Threats
- System and Network Threats

The Security problem

- A system is **secure** if its resources are used and accessed as intended under all circumstances.

- Security must consider external environment of the system, and protect it from:
  - -Unauthorized access
  - -Malicious modification or destruction
  - -Accidental introduction of inconsistency
  - -legitimate use of the system (denial of service)

- ***Definition***:

  Intruder/Crackers: attempts to breach security

  Attack: attempt to break security

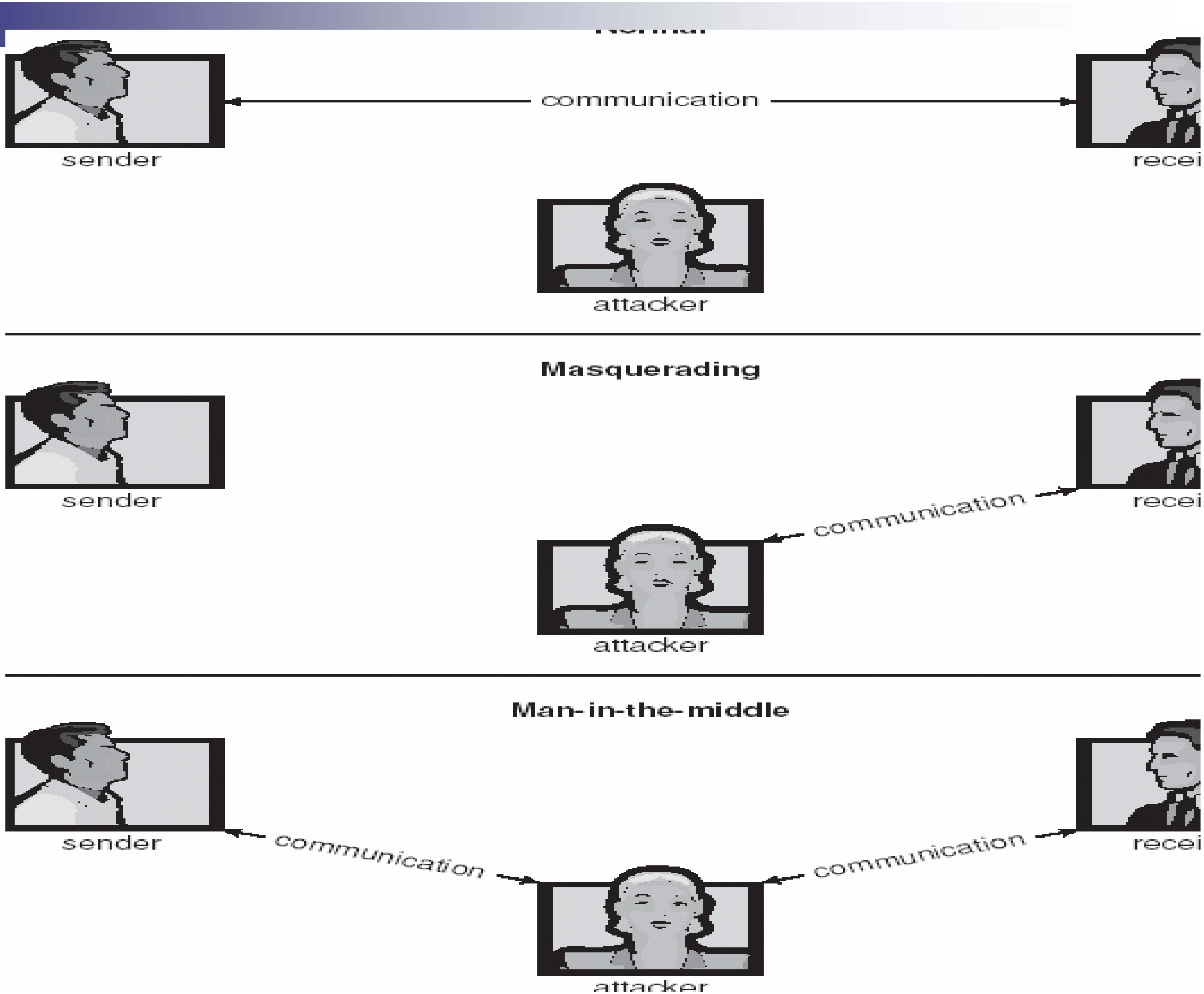
  Threat: potential for security violation (vulnerability)

- ***Categories***:

- **Breach of confidentiality-** involves unauthorized reading of data
- **Breach of integrity-** involves unauthorized modification of data
- **Breach of availability-** involves unauthorized destruction of data
- **Theft of service-** involves unauthorized use of resources
- **Denial of service-** involves preventing legitimate use of the system

- ***Method***:
  - Masquerading (breach authentication)
  - Replay attack
    - message modification
  - Man-in-the-middle attack
  - Session hijacking
- ***Security measures levels***:

1) Physical
2) Human
3) Operating System
4) Network


Normal
communication
sender
recei
attacker
Masquerading
sender
communication
recei
attacker
Man-in-the-middle
sender
communication
communication
recei
attacker

Program threats

- ➢ Back-door daemon- provides information or allows easy access even if the original exploit is blocked.
- ➢ **Trojan Horse:**
- ▪ Many systems have mechanisms for allowing programs written by users to be executed by other users → other users may misuse these rights.

  example- text-editor program
- ▪ A code segment that misuses its environment is called a **Trojan horse**.

➢ ***Variation of Trojan horse***:

- ❑ A program that emulates a login program.

  - User's authentication key and password are stolen by the login emulator, which was left running on the terminal by the thief

  - printed out a login error message and exited.

- ❑ **Spyware**–accompanies a program the user has chosen to install

  - goal is to download ads to display on the user's system

  - create **pop-up browser** windows

  - capture information (**covert channels**)

- ▪ Spyware is a micro example of "violation of the principle of least privilege."

Program Threats

- **Trap Door**:
- The designer of a program might leave a hole in the software that only he/she is capable of using.
- Specific user id/password that circumvents normal security procedures.
- Could be included in a compiler.
- **Logic Bomb**:
- Program that initiates a security incident only under certain circumstances.

Program Threats

- **Stack and Buffer Overflow**:
- The attack exploits a bug in a program.
- Attacker determines the vulnerability and writes a program to –

  1. Overflow an input field, command-line argument, or input buffer

  2. Overwrite the current return address on the stack with the address of the exploit code loaded in step 3.

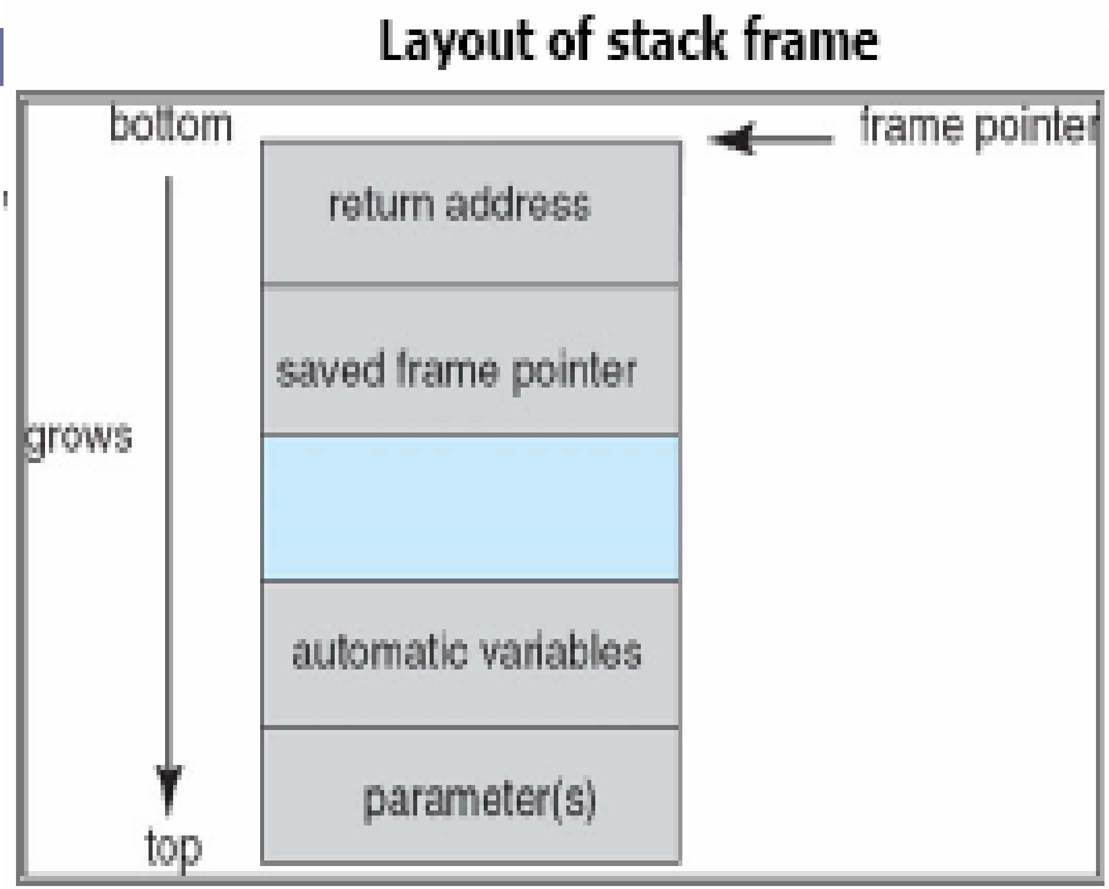
  3. Write a simple set of code for the next space in the stack that includes the commands that the attacker wishes to execute.

C program with Buffer overflow condition

```
    #include <stdio.h >
    #define BUFFER SIZE 256
    int main(int argc, char*argv[ ])
    {
          char buffer[BUFFER SIZE];
          if (argc < 2)
                    return -1;
          else {
                    strcpy(buffer,argv[1]);
                    return 0;
    }
}
```

- Bound checking- replace the line “strcpy(buffer, argv[1]);” with “strncpy(buffer,argv[1], sizeof(buffer)-1);”

- Stack frame



- A cracker could execute a buffer-overflow attack to replace the return address in the stack frame so that it now points to the code segment containing the attacking program.

Program Threats

- **Viruses**:-
- Self-replicating and are designed to “infect” other programs.
- A virus is a fragment of code embedded in a legitimate program.
- Virus are usually borne via email or as a macros (Microsoft Word documents).
- **Virus dropper** inserts the virus, usually a Trojan horse
- **Categories**- file, boot, macro, source code, polymorphic ,encrypted, stealth, tunneling, multipartite, armored and more….

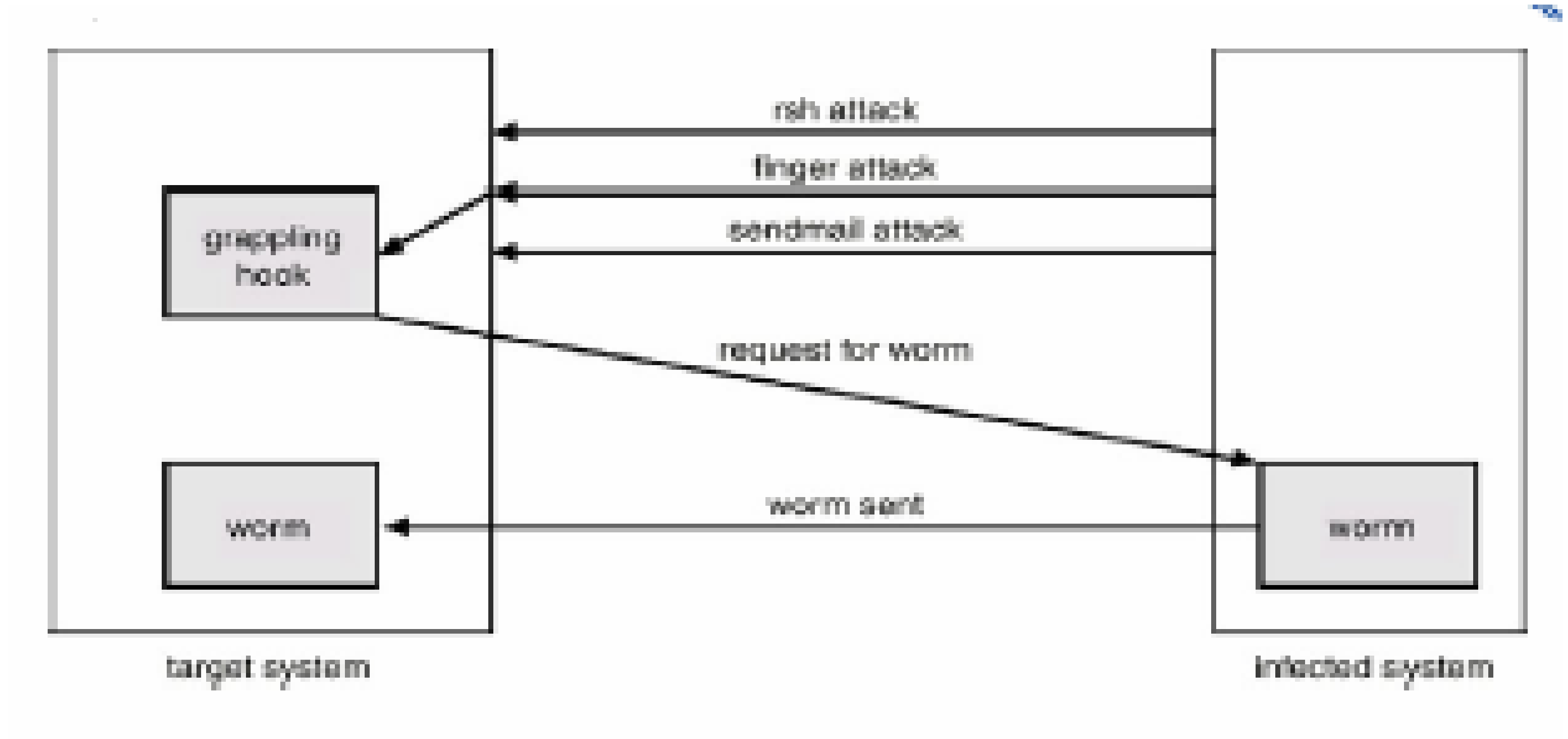
System and Network Threats

- A system and network attack is used to launch a program attack, and vice-versa.
- **Worms**:
  - A worm is a process that uses the spawn mechanism to ravage system performance.
  - Spawns copies of itself, using up systems resources and perhaps locking out all other processes.
  - made up of two programs, a grappling hook (bootstrap or vector) program and the main program.
  - The grappling hook connected to the machine where it originated and uploaded a copy of the main worm onto the hooked system.

Morris internet worm

- Exploited the UNIX networking utility rsh for easy remote login without password control
- Exploited buffer-overflow vulnerability in finger daemon with a 536 byte parameter
- Exploited nondisabled debug option (for showing status of the mail system) vulnerability in sendmail

Morris internet worm



Systems and Network Threats

- **Port Scanning**:
- Port scanning is means to detect a system’s vulnerabilities to attack.
- Automated involving a tool that attempts to create a TCP/IP connection to a specific port or a range of ports
- Since port scans are detectable , the are launched from zombie systems (independent system for nefarious purposes).

System and Network Threats

- **Denial of Service**:
- DOS are aimed at disrupting legitimate use of a system or facility
- It is network based and fall into two categories-
  1. an attack that uses so may facility resources that useful work can be done. ex- download a Java applet
  2. disrupting the network of the facility
- Distributed denial-of-service attacks (DDOS)- comes from multiple site at once, towards a common target.

THANK YOU