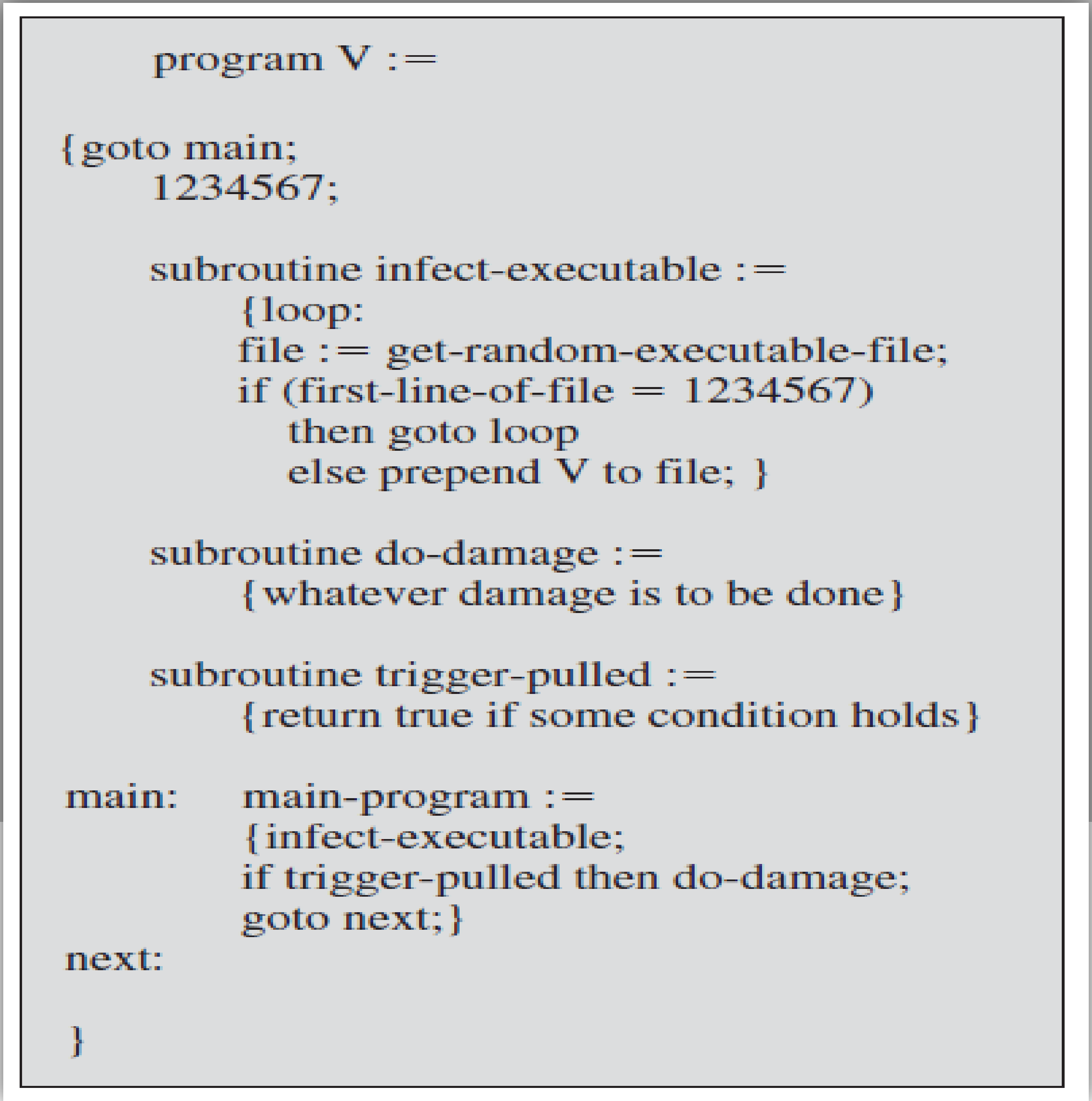
Simple Virus (1)

- A virus can be prepended or post-pended to an executable program, or it can be embedded in some other fashion.
- The key to its operation is that the infected program, when invoked, will first execute the virus code and then execute the original code of the program.
- A very general depiction of virus structure is shown in the next Figure. In this case, the virus code , **V**, is prepended to infected programs, and it is assumed that the entry point to the program, when invoked, is the first line of the program.
- The infected program begins with the virus code and works as follows:



```
          program V :=

{goto main;
          1234567;

          subroutine infect-executable :=
                    {loop:
                    file := get-random-executable-file;
                    if (first-line-of-file = 1234567)
                         then goto loop
                         else prepend V to file; }

          subroutine do-damage :=
                    {whatever damage is to be done}

          subroutine trigger-pulled :=
                    {return true if some condition holds}

main:          main-program :=
                    {infect-executable;
                    if trigger-pulled then do-damage;
                    goto next;}
next:

}
```

Simple Virus (2)

1. The first line of code is a jump to the main virus program.
2. The second line is a special marker that is used by the virus to determine whether or not a potential victim program has already been infected with this virus.
3. When the program is invoked, control is immediately transferred to the main virus program. The virus program may first seek out uninfected executable files and infect them.
4. Next, the virus may perform some action, usually detrimental to the system.
5. Finally, the virus transfers control to the original program.

Worms (1)

- The main difference between a virus and a worm is that a worm does not need a host document. In other words, a worm does not need to attach itself to another program.
- In that sense, a worm is self-contained program.
- On its own, a worm is able to send copies of itself to other machines over a network.
- Therefore, whereas a worm can harm a network and consume network bandwidth, the damage caused by a virus is mostly local to a machine.

Worms (2)

- But note that a lot of people use the terms 'virus' and 'worm' synonymously.
- That is particularly the case with the vendors of anti-virus software. A commercial anti-virus program is supposed to catch both viruses and worms.
- Since, by definition, a worm is supposed to hop from machine to machine on its own, it needs to come equipped with considerable networking support.

Worm Hopping (1)

A program may hop from one machine to another by a ***three*** basic means:

1. By using the remote shell facilities, as provided by *rsh* and *rexec* in Unix, to execute a command on the remote machine. If the target machine can be compromised in this manner, the intruder could install a small bootstrap program on the target machine that could bring in the rest of the malicious software.
2. By cracking the passwords and logging in as a regular user on a remote machine. Password crackers can take advantage of the people's tendency to keep their passwords as simple as possible.

Worm Hopping (2)

3. By using a network program. In networking with sockets, typically the communication is started with a client socket sending a request for a link to a server socket that is constantly listening for such requests. What that means is that when a machine sends out its first- contact message to another machine, it is to a port that is being monitored by some server program.

- ❖ [Obviously, after an intrusion into a machine hosting a server has taken place, the malicious software can create its own server sockets].

Harm Caused by Worms (1)

- In all cases, the extent of harm that a worm can carry out would depend on the privileges accorded to the guise under which the worm programs are executing.
- So if a worm manages to guess someone's password on a remote machine (and that someone does not have super-user privileges), the extent of harm done might be minimal.
- Nevertheless, even when no local "harm" is done, a propagating worm can bog down a network and, if the propagation is fast enough, can cause a shutdown of the machines on the network.

Harm Caused by Worms (2)

- This can happen particularly when the worm is not smart enough to keep a machine from getting re-infected repeatedly and simultaneously. Machines can only support a certain maximum number of processes running simultaneously.
- Thus, even "harmless" worms can cause a lot of harm by bringing a network down to its knees.

How afraid should we be of viruses and worms? (1)

- The short answer is: very afraid. Viruses and worms can certainly clog up your machine, steal your information, and cause your machine to serve as a zombie in a network of such machines controlled by bad guys to provide illegal services, spew out spam, spyware, and such.
- For a long answer, it depends on your ***computing habits***. Good computing habits and wed surfing practices are more effective than the best available anti-virus programs.

How afraid should we be of viruses and worms? (2)

- You must also bear in mind ***the false sense of security*** that can be engendered by the anti-virus software. Those who build viruses unleash their malware only if it cannot be detected by the latest signatures.
- They could be able to cause a lot of damage out there before the software companies start sending out their patches and the anti-virus companies start including the new signature in their tools.

Finally . . .

- ❑ **Acknowledgment:** These lecture notes are based on the textbook by William Stallings and notes prepared by Avinash Kak, Purdue University. My sincere thanks are devoted to them and to all other people who offered the material on the web.

- ❑ Students are advised to study and solve the problems and answer the questions in **Assignment-11**.