Safe Computing

Tom Kelliher, CS 102

Sept. 17, 2003

1 Administrivia

Announcements

PowerPoint assignment due Friday. E-mail attachment *before* class.

Assignment

Read 2.6–2.10. Questions on pp. 93–94: 13, 14, 17, and 18.

From Last Time

PowerPoint lab.

Outline

1. Introduction to safe computing.

Coming Up

Lab.

2 Introduction to Safe Computing

1. Important to control our cyber-selves and secure our PCs.

   (a) Identity theft.

   (b) SPAM.

   (c) Loss of data through hacking.

   (d) Responsibility to secure PCs. Incrimination?

2. History of hacking. In the beginning, hacking was a good thing. Mentality of hackers.

3. Acceptable Use Policies/Terms of Service

   (a) No spam.

   (b) No commercial use.

   (c) No illegal activity.

   (d) No excessive use of resources.

   (e) No damage.

   (f) Right to cut you off.

   (g) No re-selling of service.

   (h) Limit on number of nodes in a home network.

   Goucher AUP.

4. Passwords

(a) **Never** reveal.

(b) Choose good passwords. How to choose?

(c) How many to use? How often to change? Why?

5. Anonymizers and throw-away e-mail addresses as tools.

6. Social engineering as a hacker's tool.

7. Safe computing:

(a) Viruses, trojans, worms; what are they?

(Come as disguised executables in e-mail, DOS attacks via "drones," SQL Slammer: three minutes after release was scanning 55 million hosts per sec. Worldwide damage within 10 minutes.)

Macro viruses, script viruses.

(b) Prevention: virus scanning software:

   i. Config to check everything.

   ii. Auto-download updates.

   iii. Be paranoid.

(c) More prevention: firewall:

   i. Types of protection: inbound blocking, outbound monitoring.

   ii. Basics of networks: workstations, routers, DNS/IP, ports.

   iii. How they work.

   iv. Spyware. In KaZaA.

   v. Is ICF enough?

   vi. Free firewall: Zone Alarm.

   Symantec has Norton Personal Firewall.