

Computer and Network Security

Tom Kelliher, CS 200

Oct. 6, 2009

1 Administrivia

Announcements

Assignment

Read: Chapter 7.

Turn in answers to these questions: 6, 9, 18.

From Last Time

Privacy.

Coming Up

Computer reliability.

2 Chapter Summary

1. “The most secure computer is one that’s kept completely unplugged, locked away in a closet.” It is, however, not very useful.”

2. billg e-mail forgery.
3. University of Calgary CS courses:

- (a) Virus writing (2003).
- (b) Spam, spyware writing (2005).

Labs will be run on a “closed” network. Ethics?

4. Viruses, worms, and trojans.

- (a) What is a buffer overflow attack?
- (b) The Nov. 2, 1988 Internet worm.
- (c) Trojan horses: nefarious code hidden within a useful program. Example: spyware distributed with Kazaa clients?

Add-ons distributed with main program. “Phone home” software.

“More” ethical if disclosed in EULA?

- (d) Zombie armies used to launch DOS attacks.

What is a DOS attack?

- (e) Defense: authorization and authentication systems. (?)

Weaknesses of password systems.

5. The hacker ethic:

- (a) Unlimited and total access to computers.

- (b) All information should be free.

- (c) Mistrust authority.

- (d) Hackers should be judged by their skill in hacking, not earned degrees, etc.

(e) Art and beauty can be created on a computer.

(f) Computers can change your life for the better.

The will of the hacker is to improve the situation; there is no malicious intent.

6. System security “tools:” Crack, John the Ripper, Satan, TripWire, Wireshark.

7. Online and electronic voting:

(a) Pentagon plan for online voting for 2004 election was canceled in Feb. 2004.

(b) Benefits, risks?

3 Discussion Questions

1. 21—