Lecture 8
Jargon
Security

adware Software (typically installed without a user's knowledge or consent) that displays advertisements (such as browser popups).

cookie A small file given to a web browser by a webserver used to store information like a user ID or preferences for customized web pages.

cracking Breaking into or circumventing a computer system (such as copy protection).

form Just like a company would use a paper form to collect information voluntarily, a webpage uses a form for a user to enter information to submit to the company over the Internet.

hacking Forcefully entering into a computer system to access (or modify) its data without consent. Originally, this term actually had a positive connotation for programmers with the ability to modify an existing program to achieve a new goal.

log A file that keeps track of application or system events, often used to track usage or troubleshoot problems.

malware A general category of **mal**icious soft**ware** that can attack your computer in various ways. Virus, spyware, and worms are all considered malware.

packet sniffing The act of intercepting others' network packets and reading them, allowing a person to read another's email, view the same websites, read conversations, among other things.

phishing Obtaining an innocent user's account information by falsely acting as a legitimate company or website. (Consider fishing in a sea of users by giving bait as a legitimate-looking email to obtain information.)

piracy Illegally reproducing copyrighted work. Music, photographs, movies, and software are all potentially copyrighted and can be pirated.

privacy A reasonable expectation that sensitive or personal information is kept safe and only pre-determined people are allowed to access, view, or edit it.

processor serial number A unique identifier imprinted in the hardware of a processor, potentially accessible by software.

registration code A unique code provided to every legitimately purchased copy of software. It can be used to ensure legality and prevent piracy.

security Protecting a computer so that only authorized users are allowed to view and edit its information.

serial number A unique identifier that, if registered with the manufacturer, can identify the purchaser, often used by hardware and software manufacturers for warranty eligibility.

spyware Malware that stealthily obtains information on a user's identity or activities without consent, often submitting thereafter to a database. Originally intended to be harmless, to help target users for advertising.

virus Malware with the ability to self-replicate, but it generally cannot self-propagate to other computers. Usually a user must assist it by sharing infected files or media.

warez An application that normally has tight copy protection to prevent piracy becomes warez when it is cracked and made freely (and illegally) available online.

worm Malware with the ability to self-replicate and self-propagate through a network and attack other computers (*e.g.*, by sending a copy of itself to everyone in a user's address book).

zombie An infected computer that floods another computer with packets in an attempt to infect or crash it without the consent or knowledge of the infected computer's owner.