COMPUTER AND COMMUNICATION TECHNOLOGY

ETHICS, PRIVACY AND SECURITY

COMPUTER AND PRIVACY

Introduction

- Computer users all over the world have consistently indicated that privacy is one of the key elements in their willingness or reluctance to using information technology.
- Collecting information about users has become a lucrative business, with some companies funding their activities primarily through the sale of marketing data or lists of potential customers with details that allow targeted contacts.
- Unsolicited commercial e-mail, or spam, has become a daily annoyance for millions of e-mail users.
- On the interpersonal level, some people use Web-based services to look into the personal background of individuals on the Internet;
    - employers use search engines and archives to read public postings by potential employees;
    - and criminals sift through personal details to construct forged identities in the furtherance of identity theft.
- All these activities are possible without the use of computers, but they are greatly facilitated by the availability of large-scale databases online and of efficient search engines for collating data from different sources.
- Research that might have taken months of legwork, perhaps requiring personal visits to government offices to copy data laboriously by hand, can now be completed in minutes.
- As a result, finding out about people's lives has changed from one-by-one investigation into massive collation of data about millions of people at a time.

- Personal computers have provided fertile ground for data collection about individuals.

- Many Web sites store information about individual users' browsing patterns in files called cookies, which reside on the user's hard disk.
- Cookies allow personalized views of a Web site; for example, an online bookstore can keep track of all the books that a user has searched for or requested additional information on.
- This information then allows the bookstore software to suggest additional titles that might interest that specific user.
- On a less friendly note, some users of particular software programs have been surprised to discover that their programs are placing unauthorized calls to data collection sites on the Internet to upload information about their systems or system usage.
- All of these phenomena raise issues of privacy in the age of cyberspace.

Concepts of Privacy

- Privacy can be thought of as the power to hide parts of the truth about oneself, or sometimes the power to control the use of truths about one that other people know.
- For example, many people would consider that the books they read or what they say in private to each other ought to remain private.
- In addition, the concept of informational privacy covers truths they may have revealed to others for specific purposes but that ought nonetheless to be controlled.
- Medical records, for instance, would seem to be semi-private under this view; a patient could reasonably approve having her gynecological data shared with doctors and nurses without wanting the details to be published in a newspaper or on the Web.
-
- In daily life, many people also have concerns about their privacy at work.
- In general, in the USA, the reasonable expectation of privacy governs to what extent employers may monitor electronic communications except personal phone calls.
- Because organizations own or control their e-mail, voice-mail and Internet-access systems, managers do have the right to monitor or intercept communications made via those media.

- However, it is generally accepted that employees be allowed to make personal phone calls from work; indeed, according to the Electronic Communications Privacy Act (ECPA) , any manager monitoring a live phone call is supposed to stop listening as soon as it is clear that the call is a personal one.
- All of this monitoring supposes that employees are aware of the likelihood of monitoring and that monitoring is carried out in a fair, unbiased way that cannot be construed as harassment or persecution of individual employees.
- Normally, employees must sign waivers (in many places every year) stating that they understand that the communications channels provided by their employer are the property of and under the control of the employer and may be monitored or intercepted at any time.
- A good rule of thumb is that no one should be doing anything on employer-supplied equipment that they would be embarrassed to discuss with their manager.
- Certainly writing extensive personal e-mail messages at work or spending hours on the Web in searches that are unrelated to one′s job will result in questions about an employee′s level of productivity.

Technological Threats

Office software

- Modern computer technology offers many avenues for violating users′ privacy.
- For example, few users realize that if they allow Microsoft Office products to use "fast saves," they silently keep a full record of all the changes that they have made in a document.
- The same principle applies to changes made with "track changes" enabled. When such documents are sent to others, much more information may be revealed than expected; examples include comments from editors, reconsidered phrases, and even factual information that was supposed to be suppressed.
- Even the seemingly inoffensive Properties sheet may carry more freight than a user wants; many documents show the names of previous employers, details of managers' names and positions, and even comments that should not be made public.
- Before sending any MS-Office products to anyone else, all users should check to see that

- The properties sheet has no more information that they wish to reveal;
- They have unchecked "fast save" in the TOOLS | OPTIONS | SAVE menu;
- They have turned off TRACK CHANGES by using the TOOLS | TRACK CHANGES | ACCEPT OR REJECT CHANGES menu and converting all changes into decisions on the final copy to be released.

Malware and spyware

- Malicious software such as viruses (programs that reproduce by inserting themselves into other programs) and worms (self-reproducing programs that propagate through networks) sometimes carry victims′ documents with them.
- Recent examples of such privacy-busting malware include the Sircam worm and the Nimda virus-worm .
- Spyware is software that covertly transfers information about an unsuspecting user to a corporate site where the information can be collated and used for marketing or as material to be sold for a profit.
- Spyware often enters a system through freeware or shareware, especially those that are ad-supported .
- Some browser plug-ins that offer new functions may contain spyware.
- Even HTML-enabled e-mail sometimes contains tiny one-pixel graphics images (Web bugs) that reside on undocumented Web sites; reading such e-mail causes a hit on the data collection site, thus confirming that the message has been opened and allowing an advertiser to be charged for the potential exposure to another victim of covert monitoring.

- Many spyware products allow uncontrolled downloading of arbitrary code, thus threatening the integrity of the operating system; for example, the update-dll.exe file has already been found in three different versions in the wild, some of which may be transformed to download unauthorized code.
- This file is installed by the Aureate / Radiate toolkit, which is used in programs that currently reside on over 30 million computers today.

- Spyware programs have also been demonstrated to cause browser and operating system crashes.
- For example, one of the files associated with the Aureate/Radiate toolkit is advert.dll, which is routinely removed by technical support personnel to stop repeated system crashes.
- One way of discovering that a computer is infested with spyware is to set a personal firewall to alert the user whenever a new request for an outbound connection is made.
- Tools such as BlackIce , Norton Personal Firewall , and ZoneAlarm provide such functions.
- In addition, a spyware-blocking tool called Silencer can block all messages from being returned to spyware "mother ships." blocked.

- Many spyware programs resist uninstallation; even after going through the uninstall routines, functional programs may persist and continue to communicate with their host systems (this is known as "phoning home" in a reference to the movie "E.T.").
- It can be frustrating and time-consuming to remove all vestiges of unwanted spyware, and most users lack the technical ability to ferret through the system registry and file system looking for unauthorized entries.

- Another category of threats to privacy is the remote-administration trojan, sometimes called RAT.
- These tools masquerade as legitimate programs for administrators to use when providing technical support; however, products such as BackOrifice ,NetBus , and SubSeven are trojan horses which include undocumented functions that allow unauthorized individuals to gain complete control over the compromised systems.
- Infested systems can show bizarre behavior, such as repeated opening and closing of the CD-ROM tray, disabled keyboards, and pop-up messages.
- Worse still, the remote attackers can extract all kinds of information, including screen snapshots, lists of files, copies of private files, and even keyboard logs showing the keys pressed while entering passwords.

- Any online activity, including instant messaging, is vulnerable to invasion by these stealthy invaders.

- A number of products are available to address the removal of some or all of these types of malware.
- Aureate/Radiate DLL Remover and AdAware from Lavasoft specifically address certain types of spyware; PestPatrol , from the company that commissioned this paper, addresses the removal of trojans, hacker tools and denial-of-service attack agents in addition to spyware and adware.