BMS-214: Ethics and the Responsible Conduct of Research

Computers, Data Management, and Security

Tom Ferrin, Ph.D.

Depts. of Pharmaceutical Chemistry and Biopharmaceutical Sciences
Resource for Biocomputing, Visualization, and Informatics
University of California at San Francisco
Copyright Statement

This material is copyrighted 2007 by Thomas Ferrin. All rights reserved. These slides, or parts thereof, may not be reproduced in any form, except for use within the UCSF BMS-214 course, without written permission from the author.
Some Data Issues Related to Computers

- Insecurity of many computer systems
  - Who really has access to a computer, especially when it’s connected to a network?
- General lack of audit trails
  - Who accessed what data and when?
- Susceptibility of computers to malware
  - Huge ongoing problem with only partial technical solution
- Difficulties of long-term data retention
  - How long are backup tapes good for?
  - As the technology changes, is old backup media still compatible with new backup devices?
- Software complexity
  - As new versions of software are released, will it still read data files created with older versions?
What Can Be Done?

Technology exists to address many of these issues, but it can be expensive and often must be applied diligently and on an ongoing basis.

E.g. Audit trail systems for databases
Data Security Involves Tradeoffs

Confidentiality
- Ensuring that information doesn’t fall into the wrong hands

Integrity
- Ensuring that information is not damaged, corrupted or destroyed

Availability
- Ensuring that information can be made continuously available to the right people, at the right time

Each organization or application must find the proper balance among these competing principles
Today’s Digital World can be mean, tough, and unforgiving!

- Internet phishing scams
- Trojan Horse malware
- Destructive viruses
- Deceptive Web sites that collect personal data or install malicious software
- Insecure computer systems containing personal data
- Open computer networks that are easily snooped
- Identity fraud
- Spyware
- And on and on...
How Are Institutions Responding?

Organizational Practices:
- Creation of security and confidentiality policies
- Creation of security and confidentiality committees
- Hiring information security officer
- Conducting education and training programs
- Imposing sanctions for violations
- Improving authorization forms

Technical Practices and Procedures:
- Individual authentication of all users
- Per-user access controls
- Audit trails (user accountability)
- Physical security and disaster recovery
- Protection of external electronic communication (encryption)
- Protection of remote access points (network firewalls)
- Protection from malicious software (malware)
- Authentication of data records
- Single sign-on
- Ongoing system vulnerability assessment
How Are Individuals Responding?

Outside of the institutional setting, most individuals are pretty much doing…. Nothing!
What can individuals do?

- Raise your awareness level and educate yourself about information security
- Take advantage of existing technology to improve your secure digital environment
- Get into the habit of always practicing safe information security
“Trojan Horse” Software Example

Password authentication program

- Normally prompts a user to provide their username and password, then verifies that the password is correct and, if so, gives user access to the system

- Malware version: Do the same, except also send a copy of the username and password to the bad guys

As a user of this system, you have no idea that anything is amiss!

Therefore, your only protection is to do your best to ensure malware never gets installed on your computer.
The term **malware** (short for *malicious software*) refers to software explicitly designed to cause damage to a computer workstation, server or network.

Malware is typically classified based upon it’s intent and the symptoms/effects it causes, as well as how it’s executed and propagates:

- Classifications can often overlap, though, and the distinction between one type of malware and another is not always obvious
- Common classifications include: viruses, trojans, worms, adware, spyware, browser helper objects, keyloggers, browser hijackers,...
The Malware Explosion

Malware originally was most often propagated via floppy disks. In 1999 that changed, and e-mail became the propagation mechanism of choice. The ubiquity of networked computers and e-mail means that malware can infect 10 million or more computers in just a few hours (e.g. ILOVEYOU worm).

Anti-virus software (AVS) is only a partial answer, since new malware can always propagate faster than the anti-virus signature updates and not all types of malware are detected by AVS.† But it’s sure a lot better than doing nothing!

† AVS does a pretty good job handling viruses, trojans, and worms.
Protection from Malware

Organizations **AND INDIVIDUALS** must exercise and enforce strict discipline in their installation and use of software:

- Regularly check for and install any security-related operating system updates
- Install virus-checking programs and keep them updated on all computers (Sophos Anti-Virus available at no cost for use on all UCSF computers. Symantec Antivirus v9 is another good choice.)
- Install network firewalls that limit exposure from outside attackers

Protection from malware is currently the **most technically challenging** area of computer security.
New Malware Challenges

So, you’ve installed all the latest OS updates and AV software. Your computer should be pretty safe now, right?

Wrong!

- Adware
- Spyware
- Hijackers
- Dialers
- Toolbars
- Network redirectors
- KeyLoggers
- Browser helper objects

(At least for the time being this new type of malware is primarily targeted PCs and not Macs.)
How does it get on my system?

Bundlers
- Freeware (Weatherbug, WebSearch toolbar, etc)
- Peer-to-Peer applications (Kazaa, eDonkey, Grokster)
- Misleading EULA (end user license agreement)

Drive-By Downloads
- Browsing to a website that “tricks” the user into installing
  “If a user gets tricked into pressing "Yes" once, the user often receives extra web browser toolbars and extra popups, along with programs that transmit information about what web sites the user visits.”
  (source: www.benedelman.org)
- Using security vulnerabilities (e.g., HTML exploit)

Distribution by other malware

E-mail attachments
Drive-By Downloads – a common vector

A common technique of malware installation is a browser pop-up that’s disguised as a *Windows* error dialog, advising the user that there’s an “infection” already on the computer, and trick him/her into visiting a website that ... you guessed it, installs a malicious application...

In this case, since the “warning” is a web pop-up, clicking anywhere on the windows except for the red X in the upper right-hand corner - including the NO button! - will cause the user to visit the intended website.
Drive-By Downloads – a common vector

This is not the helpful Web site it pretends to be and will actually install spyware on your computer if you let it.
Malware is a Business!

What do Malware creators have to gain?

Adware & spyware creators find it to be a profitable business
- Financial backing from advertisers and VCs
- Personal information extracted can lead to:
  - compromise of financial information
  - compromise of contact information
  - Identity theft

“Investors Supporting Spyware” report
- http://www.benedelman.org/spyware/investors/

McAfee projects that in 2005 these new forms of malware will surpass viruses in both rate of growth and number of examples; malware growth will continue unabated, while viruses level off.
“Potentially Unwanted Programs” by McAfee, Feb 2005

Malware vendors are actively working to create legislation favorable to their “business” methods
What Can You Do?

Malware programs are becoming progressively more complex and intelligent, and as a result are proving to be increasingly difficult to detect and remove!

So prevention is the single best method to avoid malware.

It’s pretty much taken for granted these days that a single anti-malware program is not sufficient to remove an infestation.

- Spybot Search & Destroy may find a handful of apps/reg settings/cookies, AdAware will find more,... So standard protocol in malware removal these days is to run multiple (sometimes as many as 3-4!) anti-malware programs.

If you can’t/won’t do this, at least try out Webroot’s highly rated Spy Sweeper (http://www.webroot.com/consumer)
Conclusions

Maintaining the confidentiality, integrity, and availability of computer data involves tradeoffs. Organizations and individuals must strike the proper balance among these competing principles and you need to be knowledgeable about the issues in order to do this.

Current technology only does a good job of addressing some of the challenges associated with computer usage and data. It’s important to know what you can do to provide and maintain a safe computing environment.
Additional Information:

“Malware: what it is and how to prevent it” by Adam Baratz & Charles McLaughlin. (Available free from http://arstechnica.com/articles/paedia/malware.ars)


Good Web sites:
http://en.wikipedia.org/wiki/Malware
http://www.microsoft.com/technet/security/alerts/info/malware.mspx