Home/Network Computing

How to avoid becoming road kill on the Internet (Information Superhighway)

Home Computing

- not as simple as it used to be
- almost all computers need to have sys-admin
- disk drives will fail, just a matter of when
- Internet connection brings with it all kinds of new problems
  - must stay current on virus deterrents
  - staying current on OS patches now a necessity

- software installs not always as simple as intended, may have undesired side-effects
- computer may be shared
- computer may need to interact with other computers at home

Responsible Computing

- many scenarios you come across in “Cyberspace” have “Realspace” analogies, and vice-versa
  - Many people think there is nothing wrong with “port-scanning”, but could you convince a Police Officer it was OK for you to be walking around someone else's house checking all the doors and windows to see if they were locked?
  - “Everyone else was doing it.” doesn't make it right and won't get you out of a speeding ticket.

- legal system still catching up
- “File Sharing” services current example of Cyberspace abuse
  - Would you leave your front door open so that anyone could wander into your house, turn on your stereo, and make copies of all your CD's?
- analogy of your computer being your house and the Internet being the roadway system goes a long way

- above all else apply “Common Sense”
  - “All I really need to know I learned in Kindergarten” - Robert Fulghum
  - Do unto others as you would have done unto yourself
- Mom and Dad were right: Never Talk To Strangers
  - Do you really know anything about the people you are trusting with the operation of your computer?
  - Any idiot can put up a Web Site

- many of the nasty aspects of Realspace have moved into Cyberspace
  - Theft
  - Cyberstalking
  - Harassment
  - Inappropriate use of shared (community) resources
  - Forgery/Theft-of-Identity

- Some aspects made worse because “perpetrators” have (possibly justified but most often not) belief they're acting anonymously

Software Licensing

- “Agreements” are a two-way street
  - This download includes additional applications that are bundled within the software's installer file, some of which may be provided by parties other than the developer of this download. These applications may deliver advertisements, collect information, overlay content or graphics on the Web site you are viewing, or modify your system settings.

- You could be legally giving “them” permission to do anything they want to your computer
- Providers usually get something in return
  - very rarely pure charity
  - most often monetary
  - sometimes based on future returns
  - could be clandestine

- Best to think of everything in terms of risk/benefit
  - benefit from being able to do task software does
  - risk software being able to do anything to your computer, balance with source of software

- Stealing software benefits nobody in the long run
  - providers of anything receive something in return, most often monetary (if not they won't provide it)
  - company's ability to produce quality software depends on how much money they have to work with
  - quality of software becomes more important in competitive environment

Life on the Internet

- Internet has lots of people with nothing better to do than be anti-social
  - attempt hacking in to other computers
  - virus writers
  - Denial of Service (DoS) attacks
  - Cyberstalking
  - Various forms of harrassment

- can result in dammage to your computer
  - loss of files
  - theft of information
  - loss of productivity
  - embarassment (e.g. worms who send email as you)
- can also cause Realspace losses depending on what gets compromised

- how you use Internet can leave you open to abuses
- how you use Internet may be abusive, or at least anti-social, without you realizing it
- will break things down a bit based on specific activities
- helps a bit if you know how Internet works

Networking

- information flows through Internet inside “packets”
- “packet header” used to route packet from source computer to destination computer
- each computer on net has unique numeric address
  - This address may be shared among several computers (NAT)

- information inside packet depends on application programs on source/destination computers
- depending on physical network packets may be viewable (maybe just admins, maybe anybody)

- watching packets fly by known as “packet sniffing”
- if information inside packets not encrypted by sender before transmitting packet sniffers can see information
- some transactions more risky than others, e.g. initialization of telnet connection
- unless applications say network transmissions encrypted assume they're not

- most forms of encryption used on Internet based on “Public Key Encryption” technologies
- Web browsers/servers use “SSL” which is a form of Public Key Encryption

Email

- wide variety of risks with email...
  - SPAM
  - Viruses/Worms
  - transport layer not encrypted
  - authentication (to read) may not be encrypted
  - email can be forged
  - mis-configurations leading to further abuses (“open relays”)
  - mis-use, either malicious or ignorance

- SPAM typically number one annoyance
- server-side filtering risky to admins
  - need to assume there will be false-positives
  - can cause load problems on servers
- typically client-side filtering best
  - procmail on UNIX one approach
  - depending on signal-to-noise ratio may be better off with filtering based on “allow acceptable mail” instead of “reject unacceptable mail” (e.g. TMDA)

- DO NOT reply to SPAM requesting removal from list
  - proves you read your email, can charge other SPAM-ers more when they sell your address
- huge variety of places to harvest addresses from
  - companies may sell them
  - USENET articles
  - “mailto” in Web pages
  - packet snooping

- viruses/worms run close second to SPAM (overtaking it when a “big one” gets let loose...)
- currently Windows-based systems most vulnerable for variety of reasons
  - most popular (biggest bang-for-buck)
  - little or no system-level protection from user-level software damaging machine
  - often suffers from “new cool features” having higher priority than “vulnerability management” (changes promised)

- OTHER SYSTEMS ARE NOT IMMUNE, JUST LESS PROBABLE NOW
  - used to be MacOS was number one target...
  - UNIX-based systems do have virus problems, but attacks need to be more advanced (more later) and typically not email-based
  - Attacks on Linux expected to rise as its popularity rises

- anti-virus software (and keeping virus definitions file up to date) is not optional at this point
- email clients with fewer whiz-bang features offer fewer vulnerabilities viruses/worms can exploit

- most common worms arrive as file attachment email client will execute for you
- will use your “Address book” and “Mail Folders” to locate other email addresses and propagate themselves to all your friends... :-)
  - Current Klez virus includes email transport agent, doesn't need to rely on SMTP server, can forge email
- use “disposable email addresses” when doing relatively high-risk things

- almost nothing can be done to prevent “attempted forgeries”
  - email headers include enough information to track forgeries but users typically don't see extra headers
  - “Digital Signatures” of various forms can be used to help authenticate email if forgery is an issue
  - systems available from commercial vendors as well as freely available (PGP)
  - some can be used to encrypt message as well (PGP at least)

- most vendors' current systems don't leave mail transport mechanisms in a state they can be abused but as time goes on things change
- only run SMTP server if you HAVE to
- UNIX-based systems be careful about “sendmail” configuration
- Windows systems be VERY careful with what “services” get started
- SPAM-ers will find/use “Open Relays”

- individuals may be anti-social via email, maliciously or through ignorance
- mail-bombing most common malicious form
- sending email in difficult-to-read formats also quite anti-social
  - attachments in vendor-specific format “forces” recipient to go buy vendor's software to have the “privilege” of corresponding with you

- think about whether what you're sending needs to be anything other than ASCII text
- closest things to universal standard for sending “enhanced text” are HTML or, if absolutely necessary, PDF (still a tiny bit too vendor-specific but at least format is open and currently most systems have free PDF readers)

Web Browsing

- you can be tracked in various ways
  - web servers get (at least) your computer's numeric address
  - web sites may send “cookies” to your browser, browser sends cookies back on future visits
  - with cooperation from other sites one can potentially track your movements amongst those other sites

- Be careful about using public systems
  - Nothing stopping person who provided a publically available computer from logging all transactions that happen on that machine
  - OK for general web browsing, but think hard before connecting to a site you need to authenticate to in order to read your email or do banking transactions, etc.