CSE 265: System and Network Administration

- Ethics
  - The principles of conduct that govern a group of people

- Morals
  - Proclamation of what is right and good
  - Probably too late to help much here

- We are discussing Ethics
  - Policies concerning computer use are generally either for users or admins
Informed Consent (1/2)

- Take cues from the medical community
- “Informed” + “Consent”

- “Informed”
  - Know of options
  - Possible benefits and drawbacks of the options
  - Various probabilities of success
  - Explained so that the person is able to understand
- “Consent”
  - Must have option to permit/refuse action, without coercion
  - Not always possible (legally incompetent, or unable to give consent)
    - Must have high likelihood of success
    - Must be in best interest of patient
    - Likely that the patient will be thankful if successful
    - Violating informed consent must be last resort

- Principles applied to SA tasks
  - People should understand rules under which they are operating
    - E.g., SLA specifies maintenance windows
Professional Code of Conduct

- Example code from SAGE: System Administrators' Guild
  - Not
  - a set of enforceable laws
  - an enumeration of procedures
  - all-encompassing
  - an enumeration of sanctions and punishments
- Reinforces need for SAs to maintain a high standard of professionalism
SAGE Code of Ethics (1/3)

- **The integrity of a system administrator must be beyond reproach.**
  - SAs come in contact with privileged information regularly
  - Need to protect integrity and privacy of data
  - Must uphold law and policies as established for their systems

- **A system administrator shall not unnecessarily infringe upon the rights of users.**
  - No tolerance for discrimination except when required for job
  - Must not exercise special powers to access information except when necessary
Communications of system administrators with all whom they may come in contact shall be kept to the highest standards of professional behavior.

- Must keep users informed of computing matters that might affect them
- Must give impartial advice, and disclose any potential conflicts of interest

The continuance of professional education is critical to maintaining currency as a system administrator.

- Reading, study, training, and sharing knowledge and experiences are requirements
SAGE Code of Ethics (3/3)

- A system administrator must maintain an exemplary work ethic.
  - A sysadmin can have a significant impact on an organization – a high level of trust is maintained by exemplary behavior

- At all times system administrators must display professionalism in the performance of their duties.
  - Need to be professional, even when dealing with management, vendors, users, or other sysadmins
Network/Computer User Code of Conduct

- Need an Acceptable Use Policy
  - When is personal use of equipment permitted?
  - What types of personal use are forbidden?
    - Can you start a business?
    - Can you surf adult sites?
  - What if the equipment is at your home?
- Might combine with a monitoring/privacy policy
  - Explain that monitoring might happen as part of running the network/server
- There are many archived policies that are useful as starting points to develop new ones
Privileged Access Code of Conduct

- Many users need privileged access
  - Sysadmins, programmers of device drivers, software installers, etc.
- Such people need a special code of conduct
  - Since privileges can be abused
- Such users should **sign** a statement of having read the policy, and be given a copy
- Sysadmins should track those who have privileges on which systems
- Such access should expire unless renewed by signing again

**sudo's reminders**
1) respect the privacy of others
2) think before you type
Privileged access code points

- Privileged access comes with responsibility to use it properly
- Access to be used only when necessary (and management will describe such uses)
- Acknowledge that mistakes happen, and encourage procedures (such as backups) to minimize damage
- Procedures to deal with situation in which SA gets information that would not otherwise be public
  - E.g., learn about illegal or prohibited activities, or privileged info (pending sale of business)
- Warning about possible penalties for violations, including termination
- Legal requirements may also apply (e.g., SEC, FCC rules)
Copyrights

- AUP should require members to abide by current copyright laws
  - “Borrowing” non-freely redistributable software or content is usually illegal
  - Companies caught using pirated software have significant legal and financial liabilities
  - Pirated software can also be a source of viruses
  - Sysadmins are often blamed for copyright violations found on their networks (permitted or installed)
- Best approach is to make it easy for users – use open source, or get broad site licenses for other packages
Working with Law Enforcement

- Sysadmins are often contacted to help with investigations into computer-related crime
  - Also harassment issues, or need for records
- Need a procedure (prevent panic, significant mistakes)
  - Often work with a manager or legal department
  - Keep records of all communication and work performed (e.g., commands typed)
  - Must verify identity of investigator before anything else
    - Social engineering is often a successful attack method!
- Working with law enforcement can take a lot of time
  - Might need to make policies to reduce likelihood of need
Being Told to Do Something Illegal/Unethical

• What do you do when
  - You overhear (or read) about
    • A co-worker dealing drugs from the office?
    • Plans for sabotaging the company?
    • Stealing equipment and reselling via online auction?
    • Having an affair with the boss?
  - You are asked to read someone else's email?
    • By a non-SA colleague
    • By your manager
Protecting Yourself

- Have organizational policies that you can point to, and get guidance from
- Verify the (unreasonable) request
  - Perhaps you mis-heard it?
  - Get request in writing
- Verify with your manager (get permission)
- Make logs of all requests and communication
- Have a witness
  - Someone to watch what you are doing and agrees with your actions
- Contact organizational ombudsman, security, police if appropriate