Information Security in Systems and Networks

November 30, 2006

Damira Pon

University at Albany, SUNY

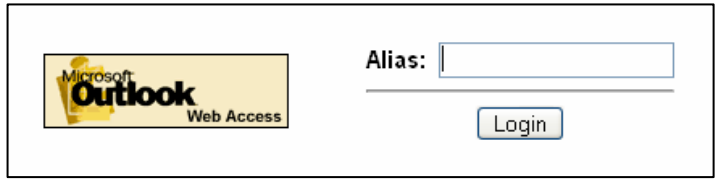
Password Protection

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Everywhere the Eye can See



Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Basic Problem

- How do you prove to someone that you are who you claim to be?
  - Any system with access control must solve this problem

- What you know
  - Passwords
  - Secret key
- Where you are
  - IP address
- What you are
  - Biometrics
- What you have
  - Secure tokens

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords
Authentication

- User has a secret password.
- System checks it to authenticate the user.
  - Vulnerable to eavesdropping when password is communicated from user to system

- How is the password stored?
- How does the system check the password?
- How easy is it to guess the password?
  - Easy-to-remember passwords tend to be easy to guess
  - Password file is difficult to keep secret

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Windows Passwords

- Set or change password → Windows generates a LM hash and a NT hash.
- Two hashing functions used to encrypt passwords
  - LAN Manager hash (LM hash)
    - Password is padded with zeros until there are 14 characters.
    - It is then converted to uppercase and split into two 7-character pieces
    - Each half is encrypted using an 8-byte DES (data encryption standard) key
    - Result is combined into a 16-byte, one way hash value
  - NT hash (NT hash)
    - Converts password to Unicode and uses MD4 hash algorithm to obtain a 16-byte value
- Hashes are stored in the Security Accounts Manager database
  - Commonly known as " SAM" or "the SAM file"
- SAM is locked by system kernel when system is running.
  - File location: C:\WINNT\SYSTEM32\CONFIG
- SYSKEY

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Unix Passwords

- Unix Passwords
  - Use modified DES as if it were a hash function
  - Encrypt NULL string using password as the key (truncates passwords to 8 characters!)
  - Artificial slowdown: run DES 25 times
  - Can instruct modern UNIXes to use MD5 hash function
- Shadow Password
  - Utilized in UNIX systems
  - Store hashed passwords in /etc/shadow file which is only readable by system administrator (root)
  - Add expiration dates for passwords
  - Early Shadow implementations on Linux called the login program which had a buffer overflow!

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Problems

- Problem: passwords are not truly random
  - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are 948 ≈ 6 quadrillion possible 8-character passwords
  - People like dictionary words, human and pet names ≈ 1 million common passwords
  - On average each person has 8-12 passwords:
  - Different systems impose different requirements on passwords.
  - Passwords need to be changed often.
  - Some passwords are used occasionally (once a year).

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Password

Impact on Security

What we found on Al Qaeda computers were two things:

1) Simple hacking tools are available to anyone who looks for them on the Internet.

2) **Tools such as LOphtCrack allow admittance into almost anyone's account if a simple eight-digit password is used**. People are frightened when they learn that using only an eight-digit password with standard numbers and letters will allow anyone to figure out their passwords in less than two minutes when one downloads a publicly available tool like LOphtCrack from the Internet. This was the kind of tool which we found, nothing terribly sophisticated.

-- **Richard Clark**, Presidents Advisor on Cyber Security (2001-2003)

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Methods of Attack

- Dictionary Attack
  - Quick technique that tries every word in a specific dictionary
- Hybrid Attack
  - Adds numbers or symbols to the end of a word
- Brute Force Attack
  - Tries all combinations of letters, numbers & symbols
- Popular programs for Windows password cracking
  - LC4
  - Sam Inside
  - Crack
  - John the Ripper (JTR)

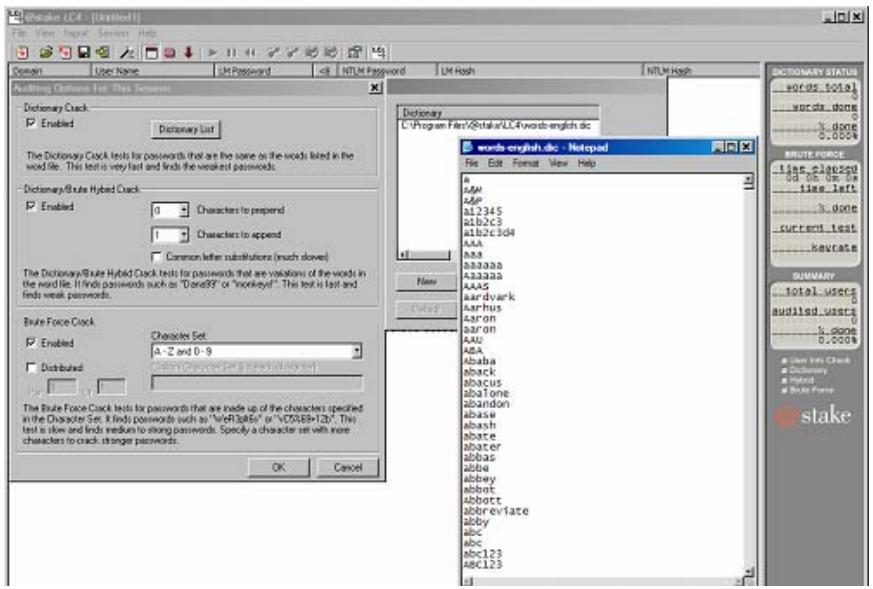
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Dictionary Attack

- Password file /etc/passwd is world-readable
  - Contains user IDs and group IDs which are used by many system programs



- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can compute H(word) for every word in the dictionary and see if the result is in the password file
  - With 1,000,000-word dictionary and assuming 10 guesses per second, brute-force online attack takes 50,000 seconds (14 hours) on average
    - This is very conservative. Offline attack is much faster!

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Security Levels

- Filing System
  - Clear text
- Dedicated Authentication Server
  - Clear text
- Encrypted
  - Password + Encryption = bf4ee8HjaQkbw
- Hashed
  - Password + Hash function = aad3b435b51404eeaad3b435b51404ee
- Salted Hash
  - (Username + Salt + Password) + Hash function = e3ed2cb1f5e0162199be16b12419c012

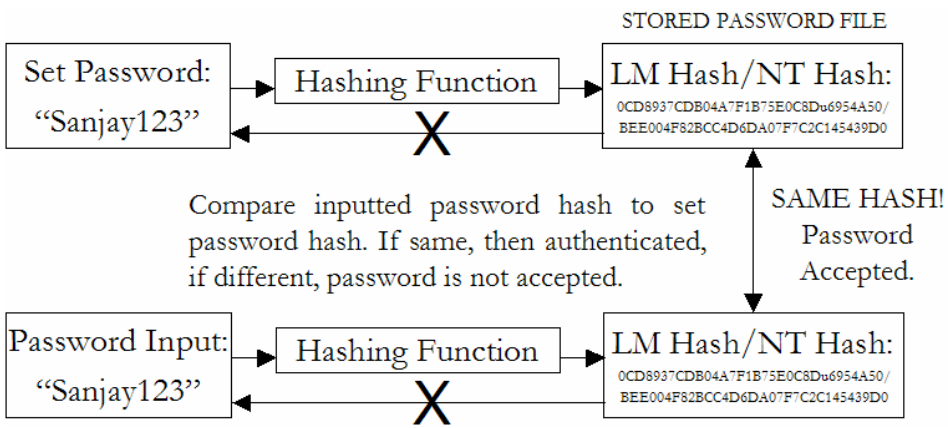
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Hashing

- Instead of user password, store hash of password
- When user enters password, compute its hash and compare with entry in password file
  - System does not store actual passwords!



- Hash function H must have some properties
  - One-way: given H(password), hard to find password
    - No known algorithm better than trial and error
  - Collision-resistant: given H(password1), hard to find password2 such that H(password1)=H(password2)
    - It should even be hard to find any pair p1,p2 s.t. H(p1)=H(p2)

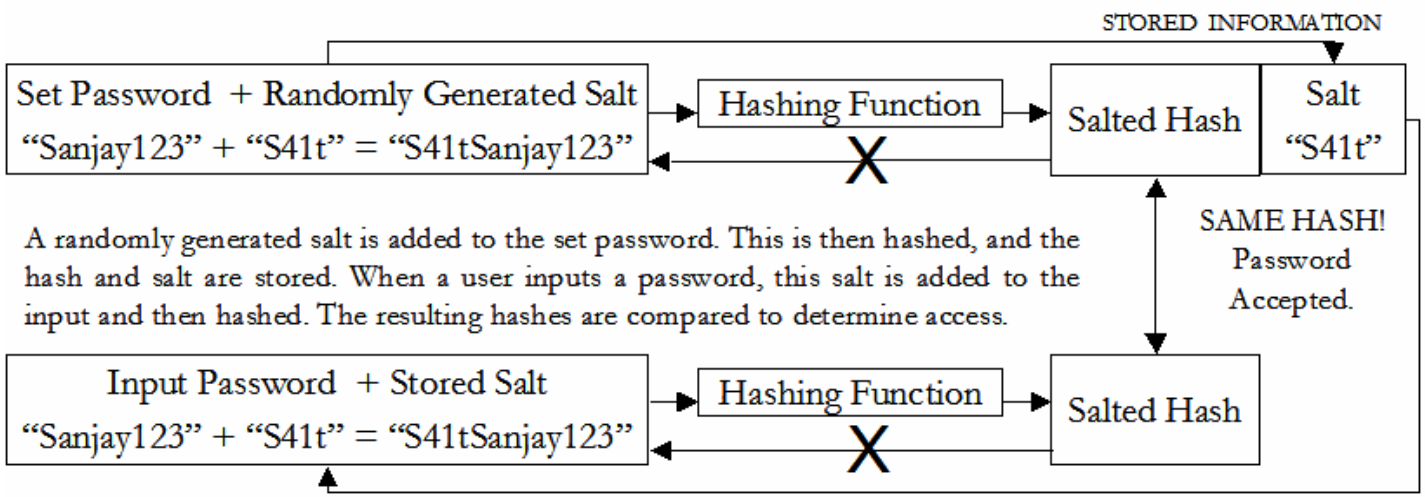
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Salting

- Salting requires adding a random piece of data and to the password before hashing it.
  - This means that the same string will hash to different values at different times
  - Users with the same password have different entries in the password file
  - Salt is stored with the data that is encrypted
- Hacker has to get the salt add it to each possible word and then rehash the data prior to comparing with the stored password.



Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Salting Advantages

- Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
  - Same hash function on all UNIX machines
  - Identical passwords hash to identical values; one table of hash values can be used for all password files
- With salt, attacker must compute hashes of all dictionary words once for each password entry
  - With 12-bit random salt, same password can hash to 212 different hash values
  - Attacker must try all dictionary words for each salt value in the password file

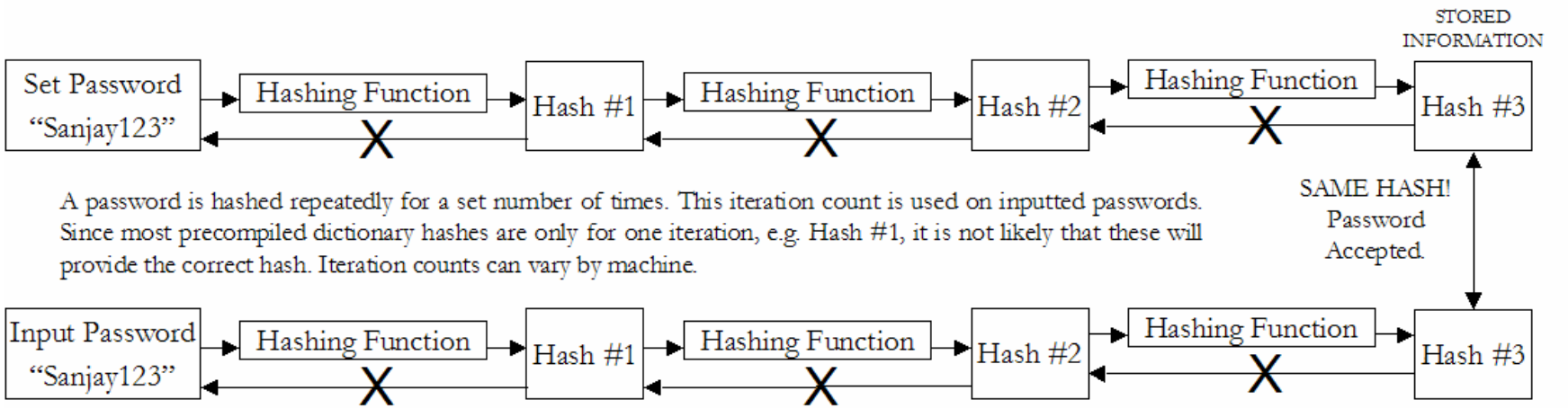
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Iteration Count

- The same password can be rehashed many times over to make it more difficult for the hacker to crack the password.
- This means that the precompiled dictionary hashes are not useful since the iteration count is different for different systems
  - Dictionary attack is still possible!



Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Authentication Protocols

- Set of rules that governs the communication of data related to authentication between the server and the user
- TRANSFORMED PASSWORD
  - Password transformed using one way function before transmission
  - Prevents eavesdropping but not replay
- CHALLENGE-RESPONSE
  - Server sends a random value (challenge) to the client along with the authentication request. This must be included in the response
  - Protects against replay
- TIME STAMP
  - The authentication from the client to server must have time-stamp embedded
  - Server checks if the time is reasonable
  - Protects against replay
  - Depends on synchronization of clocks on computers
- ONE-TIME PASSWORD
  - New password obtained by passing user-password through one-way function n times which keeps incrementing
  - Protects against replay as well as eavesdropping

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Challenge Response

- User and system share a secret key
- Challenge: system presents user with some string
- Response: user computes response based on secret key and challenge
  - Secrecy: difficult to recover key from response
    - One-way hashing or symmetric encryption work well
  - Freshness: if challenge is fresh and unpredictable, attacker on the network cannot replay an old response
    - For example, use a fresh random number for each challenge
- Good for systems with pre-installed secret keys
  - Car keys; military friend-or-foe identification

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Improving Security

- Add biometrics
  - For example, keystroke dynamics or voiceprint
  - Revocation is often a problem with biometrics
- Graphical passwords
  - Goal: increase the size of memorable password space

- Rely on the difficulty of computer vision
  - Face recognition is easy for humans, hard for machines
  - Present user with a sequence of faces, he must pick the right face several times in a row to log in
- Other examples
  - Click on a series of pictures in order
  - Drawing a picture
  - Clicking four correct points on a picture

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Personal Token Authentication

- Personal Tokens are hardware devices that generate unique strings that are usually used in conjunction with passwords for authentication
- A variety of different physical forms of tokens exist
  - e.g. hand-held devices, Smart Cards, PCMCIA cards, USB tokens
- Different types of tokens exist:

  - **Storage Token:** A secret value that is stored on a token and is available after the token has been unlocked using a PIN
  - **Synchronous One-time Password Generator:** Generate a new password periodically (e.g. each minute) based on time and a secret code stored in the token
  - **Challenge-response:** Token computes a number based on a challenge value sent by the server
  - **Digital Signature Token:** Contains the digital signature private key and computes a computes a digital signature on a supplied data value

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Biometric Authentication

- Uses certain biological characteristics for authentication
  - Biometric reader measures physiological indicia and compares them to specified values
  - It is not capable of securing information over the network
- Different techniques exist
  - Fingerprint Recognition
  - Voice Recognition
  - Handwriting Recognition
  - Face Recognition
  - Retinal Scan
  - Hand Geometry Recognition

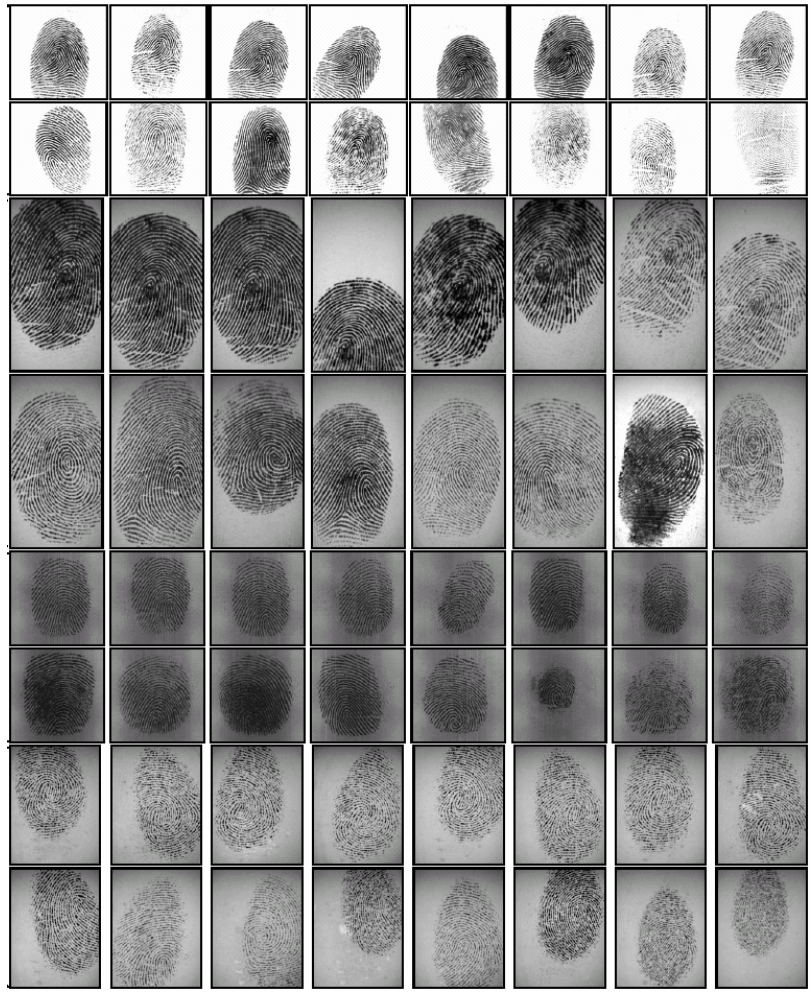
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Fingerprint Authentication

- Unique patterns in peoples fingerprints are used for unique identification
- Most tested of all biometric systems
- Commonly used in crime labs for forensic investigations



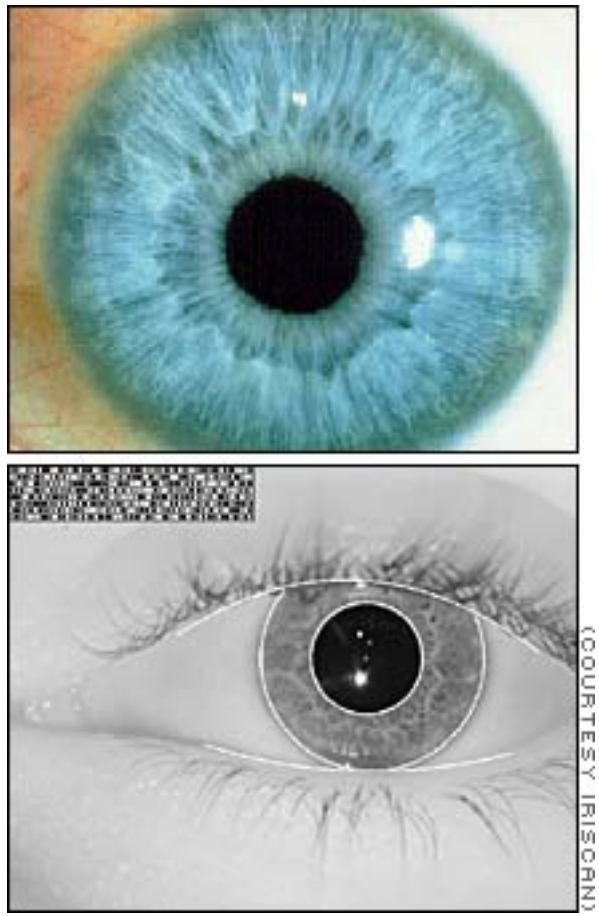
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Iris Authentication

- The scanning process takes advantage of the natural patterns in people's irises, digitizing them for identification purposes.
  - Probability of two irises producing exactly the same code: 1 in 10 to the 78th power
  - Independent variables (degrees of freedom) extracted: 266
  - IrisCode record size: 512 bytes
  - Operating systems compatibility: DOS and Windows (NT/95)
  - Average identification speed (database of 100,000 IrisCode records): one to two seconds



Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Ten Common Mistakes

1. Leaving passwords blank or unchanged from default value.
2. Using the letters p-a-s-s-w-o-r-d as the password.
3. Using a favorite movie star name as the password.
4. Using a spouse's name as the password.
5. Using the same password for everything.
6. Writing passwords on post-it notes.
7. Pasting a list of passwords under the keyboard.
8. Storing all passwords in an Excel spreadsheet on a PDA or inserting passwords into a rolodex.
9. Writing all passwords in a personal diary.
10. Giving the password to someone who claims to be the system administrator.

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Passwords

Protection/Detection

- Protection (Windows):
  - Disable storage of LAN Manager hashes.
  - Configure both Local and Domain Account Policies (Password & Account Lockout Policies).
  - Audit access to important files.
  - Implement SYSKEY security on all systems.
  - Set BIOS to boot first from the hard drive.
  - Password-protect the BIOS.
- Protection (All)
  - Enforce strong passwords (long, different types of characters)!
  - Change your passwords frequently.
  - Use two or three factor authentication.
  - Use one time passwords

http://www.microsoft.com/athome/security/privacy/password_checker.mspx

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

“Relativity applies to physics, not ethics” - Albert Einstein

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

Definition

- Work Ethics
  - Define the principles of an organization
  - Tries to promote integrity and transactional transparency
- Need for Cyber Ethics
  - Cyber Ethics can be defined as the field of inquiry dealing with ethical problems aggravated, transformed or created by computer and network technology.

Definition from Maner, W. (1978). *Starter Kit in Computer Ethics.*

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

Need

- Why is cyber ethics needed?
  - New technology
  - Understanding of policy
  - Compliance with policy
  - Work environment
  - Increases security!

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

THE SYSTEM ADMINISTRATORS' CODE OF ETHICS

We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct, and agree to be guided by this code of ethics, and encourage every System Administrator to do the same.

Professionalism I will maintain professional conduct in the workplace and will not allow personal feelings or beliefs to cause me to treat people unfairly or unprofessionally.

Personal Integrity I will be honest in my professional dealings and forthcoming about my competence and the impact of my mistakes. I will seek assistance from others when required.

I will avoid conflicts of interest and biases whenever possible. When my advice is sought, if I have a conflict of interest or bias, I will declare it if appropriate, and recuse myself if necessary.

Privacy I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it.

Laws and Policies I will educate myself and others on relevant laws, regulations, and policies regarding the performance of my duties.

Communication I will communicate with management, users, and colleagues about computer matters of mutual interest. I will strive to listen to and understand the needs of all parties.

System Integrity I will strive to ensure the necessary integrity, reliability, and availability of the systems for which I am responsible.

I will design and maintain each system in a manner to support the purpose of the system to the organization.

Education I will continue to update and enhance my technical knowledge and other work-related skills. I will share my knowledge and experience with others.

Responsibility to Computing Community I will cooperate with the larger computing community to maintain the integrity of network and computing resources.

Social Responsibility As an informed professional, I will encourage the writing and adoption of relevant policies and laws consistent with these ethical principles.

Ethical Responsibility I will strive to build and maintain a safe, healthy, and productive workplace.

I will do my best to make decisions consistent with the safety, privacy, and well-being of my community and the public, and to disclose promptly factors that might pose unexamined risks or dangers.

I will accept and offer honest criticism of technical work as appropriate and will credit properly the contributions of others.

I will lead by example, maintaining a high ethical standard and degree of professionalism in the performance of all my duties. I will support colleagues and co-workers in following this code of ethics.

LOPSA USENIX [sage]

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

Ten Commandments

1. Thou shalt not use a computer to harm others.
2. Thou shalt not interfere with others' computer work.
3. Thou shalt not snoop around in others' computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software you have not paid for.
7. Thou shalt not use other's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual property.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt use a computer in ways that ensure consideration and respect for your fellow humans.

Adapted from: Barquin, R.C. (1992). In Pursuit of a 'Ten Commandments' for Computer Ethics. *Computer Ethics Institute.*

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

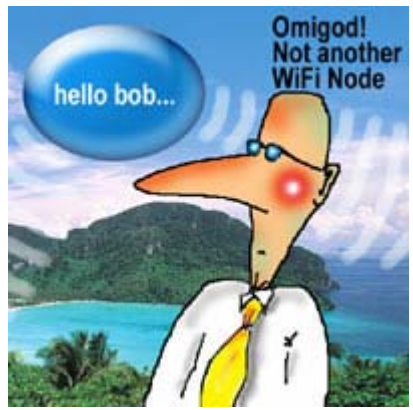
Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #1

- You have just realized that your next-door neighbor has an insecure wireless access point and your computer connects automatically to it. Should you use this wireless access point?



Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Question

- Just because you CAN does it mean that you SHOULD?

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #2

- You have just gotten robbed and your entire CD collection has been stolen. You know that there are programs that you can download music for free. Should you be able to download the music from your original CD's?

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Notes

- Something that is ILLEGAL may be different than something that is UNETHICAL.

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #3

- You have a 9-5 job and your company provides you with a blackberry and cell phone so that you will be accessible 24 hours a day with no overtime pay. Considering this, you are very busy with a spouse and three kids. Should you be able to use company time for personal activities?

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #3, cont'd.

- What about
  - Paying bills?
  - Online gambling?
  - Setting up day care arrangements?
  - Music file-sharing?
  - Pornography?
  - Looking at the summary for the last episode of "Lost", "Desperate Housewives", or "CSI"?

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #4

- You will be split into two groups to come up with a conclusion based on the upcoming scenario.
- After about 5 minutes you will be asked to reconvene and discuss what you would choose.

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #4, cont'd.

- You receive an anonymous email which includes all technical and business details of a key competitor's project. Your company is behind and if you use the information, you will likely beat your competitor- and be a hero. If you don't use the information, your company will lose a great deal of money and you will likely be the scapegoat. If you use the information, no one – except you – will ever know. What do you do?

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

CyberEthic Surfivor Scenario #4 in Defcon

- Situation
  - Two separate groups
  - Unanimous decisions in both groups
  - "Business is War"
  - "Immoral" and even "Illegal"
  - Split judging among peers
- Results
  - Leadership is important

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

“Ethics is not definable, is not implementable, because it is not conscious; it involves not only our thinking, but also our feeling.”

-Valdemar W. Setzer

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics

Six Steps Towards Making Ethical Decisions

1. Identify the ethical issue or problem.
2. List the facts that have the most bearing on the decision.
3. Identify anyone who might be affected by your decision and how.
4. Explain what each affected person would want you to do about the issue.
5. List three alternative actions and identify the best and worst case scenario for each alternative, anyone who would be harmed by this choice (and how), any values that would be compromised by selecting this alternative, and any automatic reasons why this alternative should not be selected (legal issues, rules, etc.).
6. Determine a course of action.

Source: http://lessonplans.btskinner.com/ethics1.html

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance

Cyber Ethics
Final Thoughts

- How do you know what the right thing to do is?
  - Enron and your mom

Sanjay Goel & Damira Pon

University at Albany, State University of New York / NYS Center for Information Forensics and Assurance