Watermarking
Computer Forensics
Risk Management
Legal and Ethical Issues

Lecture 12

November 20, 2003

Courtesy of Professors
Chris Clifton & Matt Bishop

Digital Watermarking

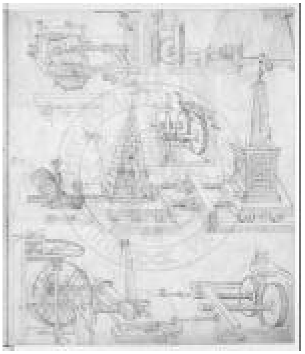
- A digital pattern or signal is inserted into an image
  - Can serve as a digital signature
  - Can identify the intended recipient (unique to each copy)
  - Can identify document source (common to multiple copies)

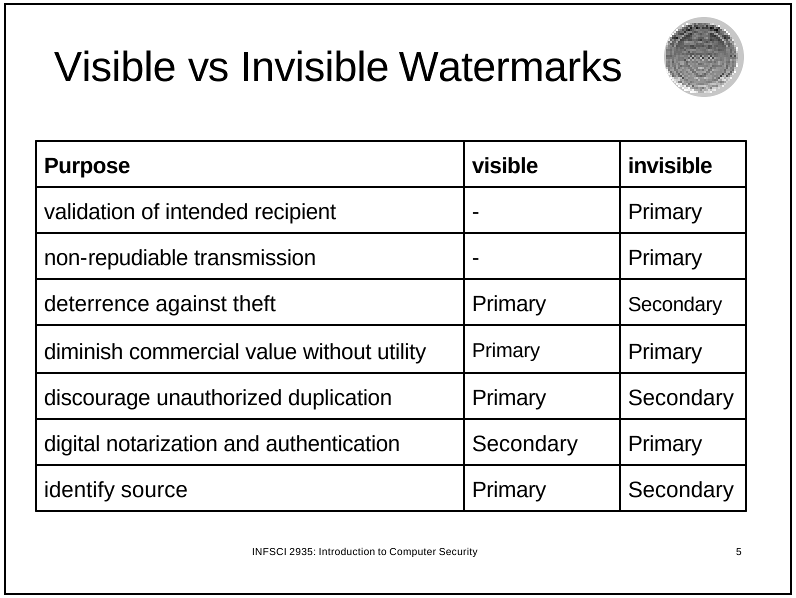
Watermarking

- Watermarked image is transformed image
  - Original image remains intact, recognizable
  - Persistent in viewing, printing and re-transmission and dissemination
- Contrast to *fingerprinting* and *encryption*
  - In digital fingerprinting, original file remains but a new file is created that describes the original file (e.g., checksum in Tripwire)
  - Encryption transforms an image to an unrecognizable image

Watermarking

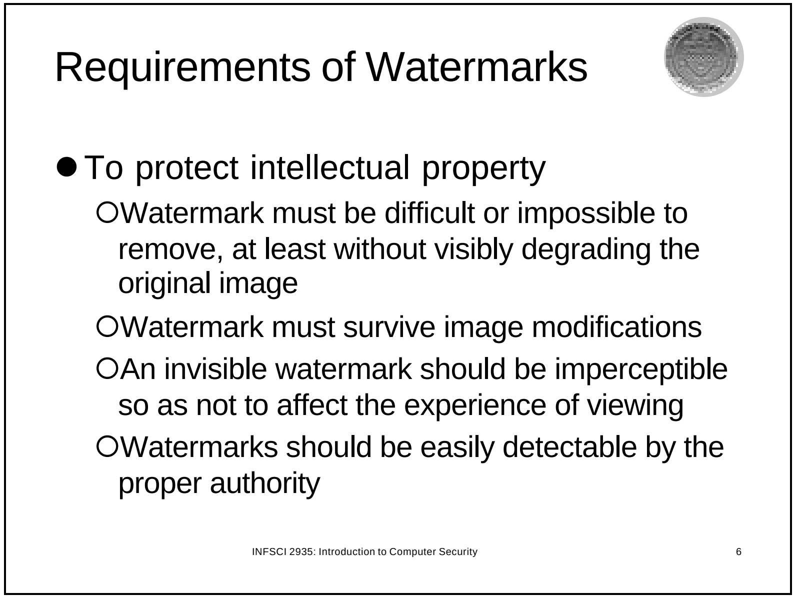
- Visible watermarks
  - Similar to physical counterpart (digitally stamped!)
- Invisible watermarks
  - Useful as for identifying the source, author, owner, distributor or authorized consumer
  - Permanently, unalterably mark the image
- Also used for tracing images in the event of their illicit distribution
  - Unique watermark for each buyer





Visible vs Invisible Watermarks

Purpose	visible	invisible
validation of intended recipient	-	Primary
non-repudiable transmission	-	Primary
deterrence against theft	Primary	Secondary
diminish commercial value without utility	Primary	Primary
discourage unauthorized duplication	Primary	Secondary
digital notarization and authentication	Secondary	Primary
identify source	Primary	Secondary



Requirements of Watermarks

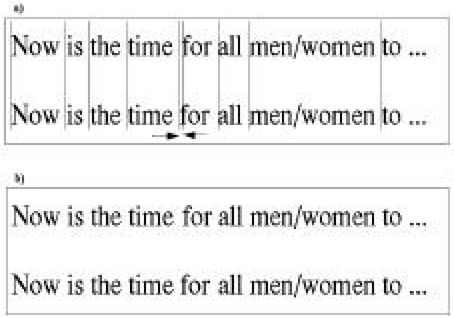
- To protect intellectual property
  - Watermark must be difficult or impossible to remove, at least without visibly degrading the original image
  - Watermark must survive image modifications
  - An invisible watermark should be imperceptible so as not to affect the experience of viewing
  - Watermarks should be easily detectable by the proper authority

Watermarking techniques For image

- Spatial domain watermarking
  - Simplest: flip the lowest order bit of chosen pixels
  - Superimpose a watermark
  - Color separation – watermark in only one color band
  - Picture cropping can be used to eliminate some spatial watermark
- Frequency domain watermarking
  - Use Fast Fourier Transform – alter the values of chose frequencies
  - Watermarks will be dispersed spatially (cropping or spatial technique will not defeat it)

Watermarking for Text

- Text-line coding
  - Text lines of a document page are shifted imperceptibly up or down
- Word-shift coding
  - Spacing between words in a line text is altered
- Character coding
  - E.g., endline at the top of a letter, say “t” is extended



Now is the time for all men/women to ...

Now is the time for all men/women to ...

Now is the time for all men/women to ...

Now is the time for all men/women to ...

Steganography

- Art of hiding information in the midst of irrelevant data
- This is NOT cryptography
- Useful to hide the existence of secret communication

Example of Steganography (Text – page 48)

Dear George,
Greetings to all at Oxford. Many thanks for **your**
letter and for the summer examination **package**.
All entry forms and fees forms should be **ready**
for final dispatch to the syndicate by **Friday**
20th or at the latest I am told by the **21st**.
Admin has improved here though there is **room**
for improvement still; just give us all two or **three**
more years and we will really show you! **Please**
don't let these wretched 16+ proposals **destroy**
your basic O and A pattern. Certainly **this**
sort of change, if implemented **immediately**,
would bring chaos.
Sincerely yours,

Computer Forensic

Courtesy of Professors
Chris Clifton & Matt Bishop

What is Computer Forensics?

- Forensics:
  - The use of science and technology to investigate and establish facts in criminal or civil courts of law.
- Computer Forensics:
  - Commonly defined as the collection, preservation, analysis and court presentation of computer-related evidence.
  - Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a computer system.

What is Computer Forensics?

- Understand what happened
  - Proper acquisition and preservation of computer evidence.
  - Authentication of collected Data for court Presentation
  - Recovery of all available data, including delete files
  - Prevention of future incidents
- Often similar problems to Audit

  But audit trail may be inadequate!
  - Audit information incomplete/insufficient
  - Audit trail damaged
  - We don’t own the computer

What is the Challenge?

- Audit information incomplete/erased
  - Reconstruct deleted information
- “Acceptable” state of system unknown
  - Need to identify violation in spite of this
- Goal not obvious
  - Transformations may have been applied to data
- Strong burden of proof
  - Not enough to know what happened
  - Must be able to prove it

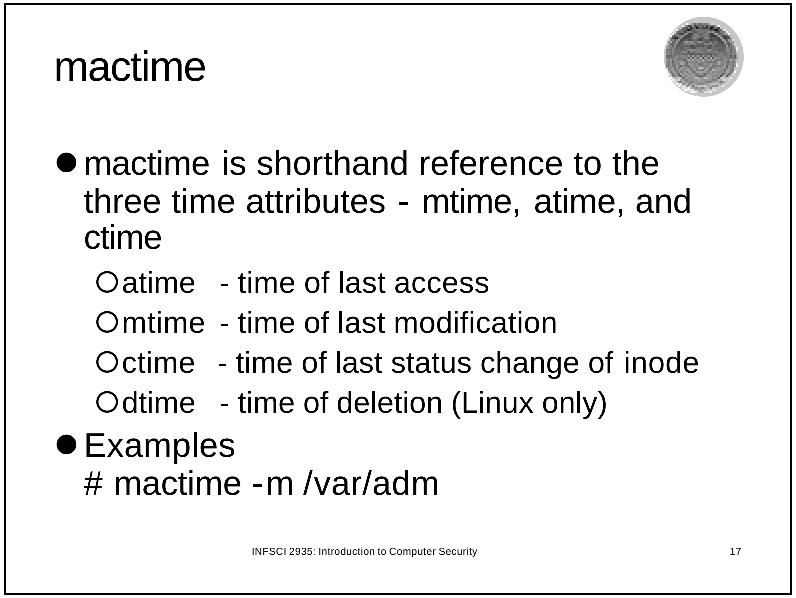
FBI List of Computer Forensic Services

- Content (what type of data)
- Comparison (against known data)
- Transaction (sequence)
- Extraction (of data)
- Deleted Data Files (recovery)
- Format Conversion
- Keyword Searching
- Password (decryption)
- Limited Source Code (analysis or compare)
- Storage Media (many types)

The Coroner's Toolkit (TCT) Overview

- Collections of tools to assist in a forensic examination of a computer (primarily designed for Unix systems)

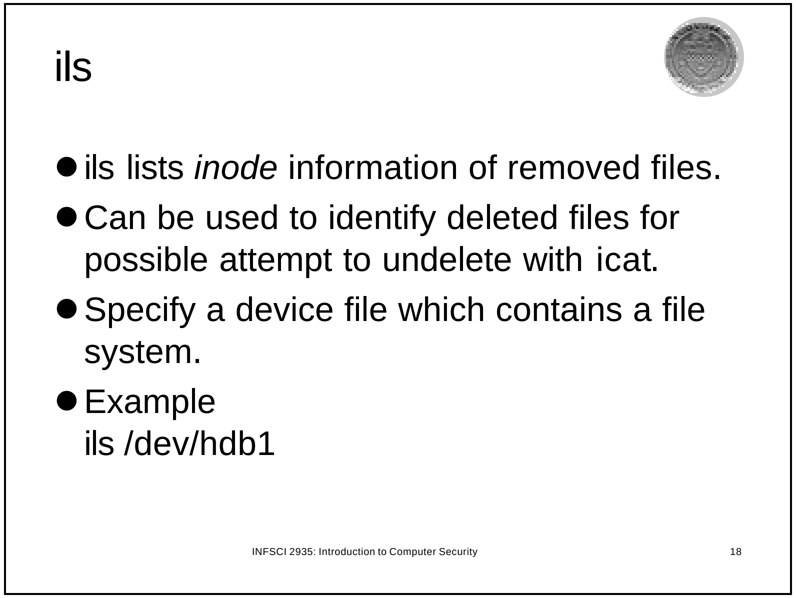
- mactimes - report on times of files
- ils - list inode info (usually removed files)
- icat - copies files by inode number
- unrm - copies unallocated data blocks
- lazarus - create structure from unstructured data
- file - determine file type
- pcat - copy process memory
- grave-robber - captures forensic data



mactime

- mactime is shorthand reference to the three time attributes - mtime, atime, and ctime
  - atime - time of last access
  - mtime - time of last modification
  - ctime - time of last status change of inode
  - dtime - time of deletion (Linux only)
- Examples

```
# mactime -m /var/adm
```

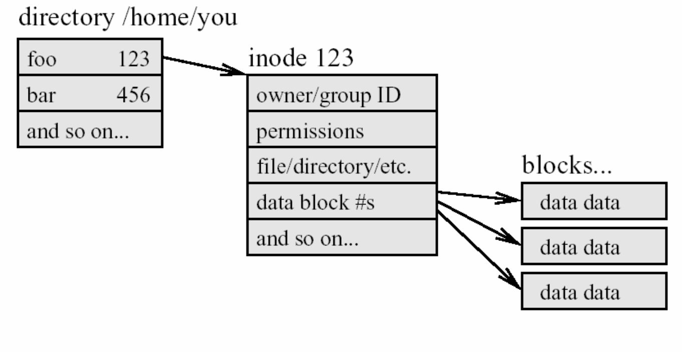


ils

- ils lists *inode* information of removed files.
- Can be used to identify deleted files for possible attempt to undelete with icat.
- Specify a device file which contains a file system.
- Example

```
ils /dev/hdb1
```

Unix file



directory /home/you

foo	123
bar	456
and so on...	

inode 123

- owner/group ID
- permissions
- file/directory/etc.
- data block #s
- and so on...

blocks...

- data data
- data data
- data data

Icat, file

- icat copies files by *inode* number from a device which contains a file system
- Can be used to recover a deleted file

  Example
  icat /dev/hdb1 17
- file – determine file type
- Similar to UNIX System V file command, but may generate better indication of file type

## unrm

- unrm – copies unallocated data blocks
  - ○Used to copy unallocated blocks to an output file in order to be processed by lazarus. Example

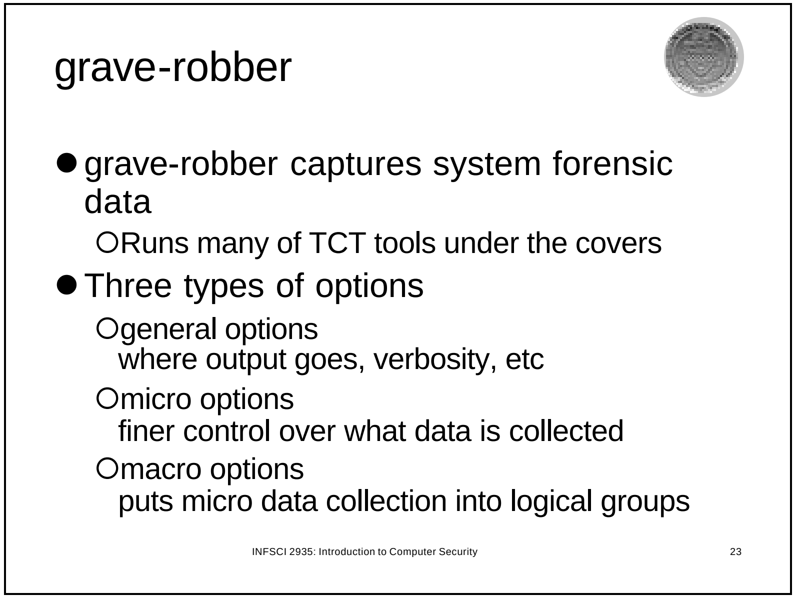
    # unrm /dev/hdb1 > /tmp/unrm.of.hdb1
- lazarus – attempts to make sense out of raw data blocks

  Example

  # lazarus /tmp/unrm.of.hdb1

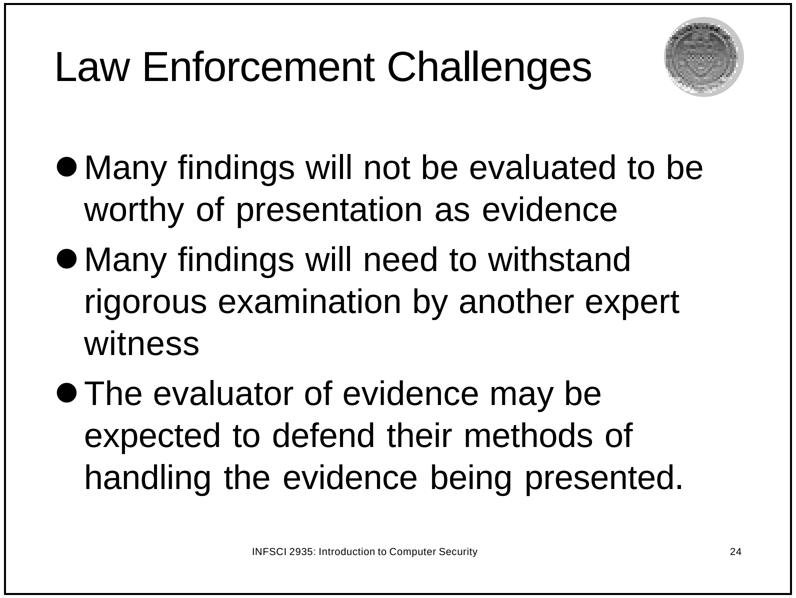
pcat

- pcat – copies process memory
  - ○This is used to try to understand what a program is (doing), especially when the executable file has been deleted.
- Modern UNIX systems have a /proc file system that makes process information available in a convenient manner, including the executable file, current directory, and process memory.



grave-robber

- grave-robber captures system forensic data
  - Runs many of TCT tools under the covers
- Three types of options
  - general options
    where output goes, verbosity, etc
  - micro options
    finer control over what data is collected
  - macro options
    puts micro data collection into logical groups



Law Enforcement Challenges

- Many findings will not be evaluated to be worthy of presentation as evidence
- Many findings will need to withstand rigorous examination by another expert witness
- The evaluator of evidence may be expected to defend their methods of handling the evidence being presented.

Broader Picture: What to Do

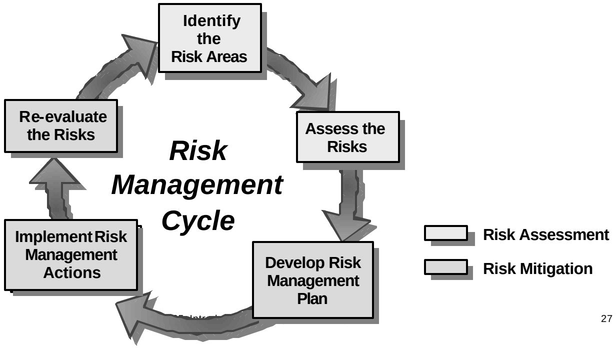
- do not start looking through files
- start a journal with the date and time, keep detailed notes
- unplug the system from the network if possible
- do not back the system up with dump or other backup utilities
- if possible without rebooting, make byte by byte copies of the physical disk
- capture network info
- capture process listings and open files
- capture configuration information to disk and notes
- collate mail, DNS and other network service logs to support host data
- capture exhaustive external TCP and UDP port scans of the host
- contact security department or CERT/management/police or FBI
- if possible freeze the system such that the current memory, swap files, and even CPU registers are saved or documented
- short-term storage
- packaging/labeling
- shipping

Risk management

Courtesy of Professors

Risk Management

- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)



Risk

- The *likelihood* that a particular *threat* using a specific *attack*, will exploit a particular *vulnerability* of a system that results in an undesirable *consequence* (NIST)
  - ○*likelihood* of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event

Risk Assessment/Analysis

- A process of analyzing *threats* to and *vulnerabilities* of an information system and the *potential impact* the loss of information or capabilities of a system would have
  - List the threats and vulnerabilities
  - List possible control and their cost
  - Do cost-benefit analysis
    - Is cost of control more than the expected cost of loss?
- The resulting analysis is used as a basis for identifying appropriate and cost-effective counter-measures
  - Leads to proper security plan

Benefits of Risk Assessment

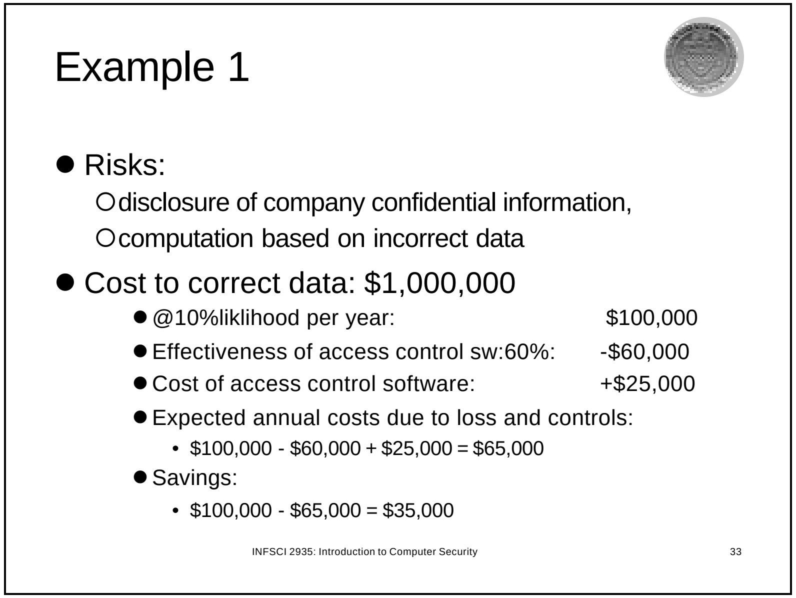
- Improve awareness of security issues among employees
- Identify assets, vulnerabilities, and controls
  - A systematic analysis produces a comprehensive list of assets and risks
- Improve basis for decisions
  - Controls may reduce productivity
  - Controls need to be justified
  - Some risks are serious enough
- Justify expenditures for security
  - Some controls may be too expensive without any obvious benefit

Risk Assessment steps

- Identify assets
  - Hardware, software, data, people, supplies
- Determine vulnerabilities
  - Intentional errors, malicious attacks, natural disasters
- Estimate likelihood of exploitation
  - Considerations include
    - Presence of threats
    - Tenacity/strength of threats
    - Effectiveness of safeguards
  - Delphi approach
    - Raters provide estimates that are distributed and re-estimated

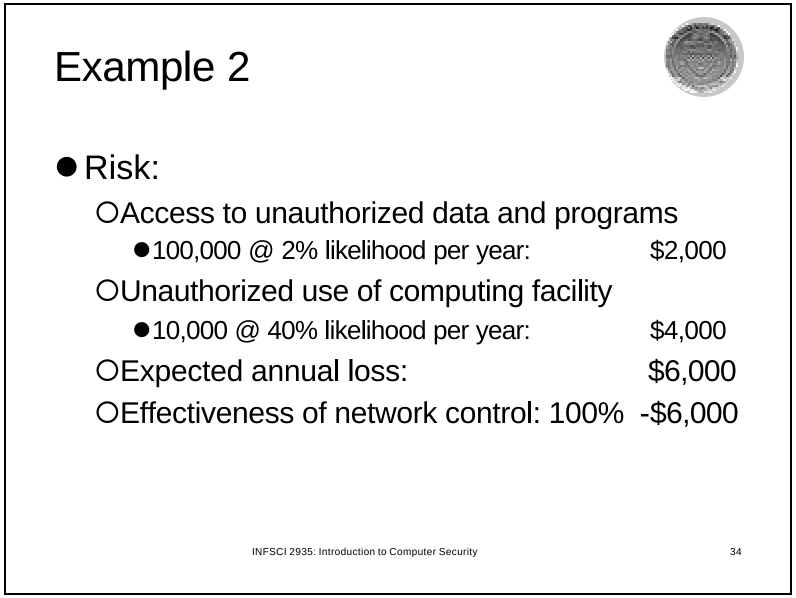
Risk Assessment steps (2)

- Compute expected annual loss
  - Physical assets can be estimated
  - Data protection for legal reasons
- Survey applicable (new) controls
  - If the risks of unauthorized access is too high, access control hardware, software and procedures need to be re-evaluated
- Project annual savings of control



Example 1

- Risks:
  - ○ disclosure of company confidential information,
  - ○ computation based on incorrect data
- Cost to correct data: $1,000,000
  - @10%liklihood per year: $100,000
  - Effectiveness of access control sw:60%: -$60,000
  - Cost of access control software: +$25,000
  - Expected annual costs due to loss and controls:
    - $100,000 - $60,000 + $25,000 = $65,000
  - Savings:
    - $100,000 - $65,000 = $35,000



Example 2

- Risk:
  - ○ Access to unauthorized data and programs
    - 100,000 @ 2% likelihood per year: $2,000
  - ○ Unauthorized use of computing facility
    - 10,000 @ 40% likelihood per year: $4,000
  - ○ Expected annual loss: $6,000
  - ○ Effectiveness of network control: 100% -$6,000

Example 2 (2)

- Control cost

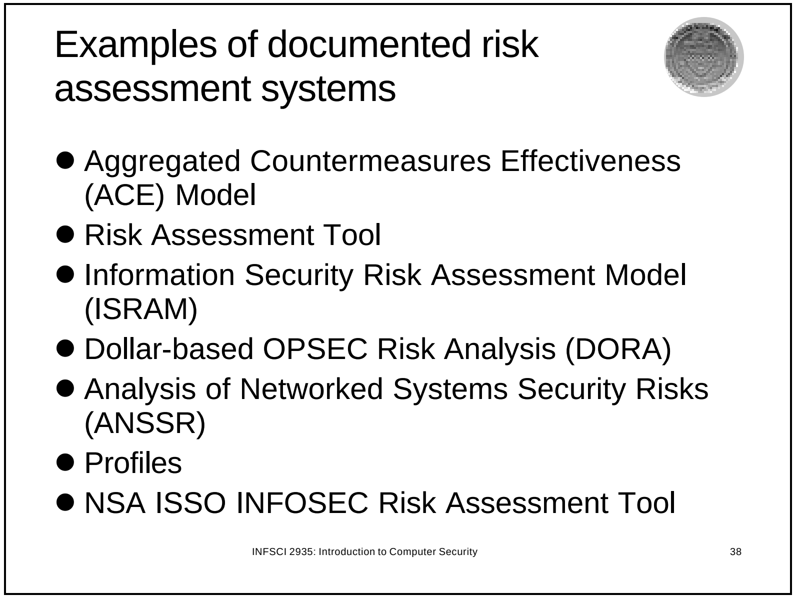
○Hardware	+$10,000
○Software	+$4,000
○Support personnel	+$40,000
○Annual cost	$54,000
○Expected annual cost (6000-6000+54000)	$54,000
○Savings (6000 – 54,000)	-$48,000

Some Arguments against Risk Analysis

- Not precise
  - Likelihood of occurrence
  - Cost per occurrence
- False sense of precision
  - Quantification of cost provides false sense of security
- Immutability
  - Filed and forgotten!
  - Needs annual updates
- No scientific foundation (not true)
  - Probability and statistics

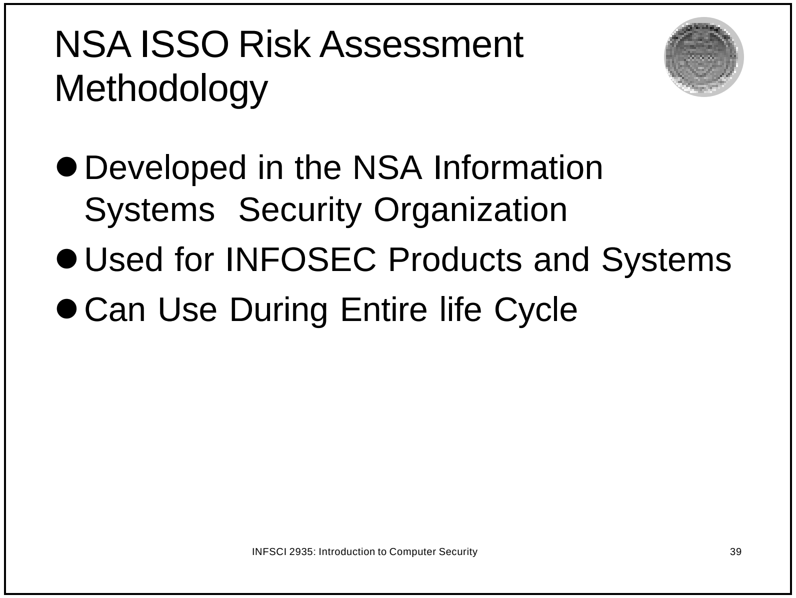
Risk Mitigation

- Risk Mitigation is any step taken to reduce risk
- Residual Risk (RR)
  - Portion of risk remaining after security measures have been applied (NIST)
- Safeguards for RR
  - Difficult to completely eliminate RR
  - Keep RR minimum, at acceptable level



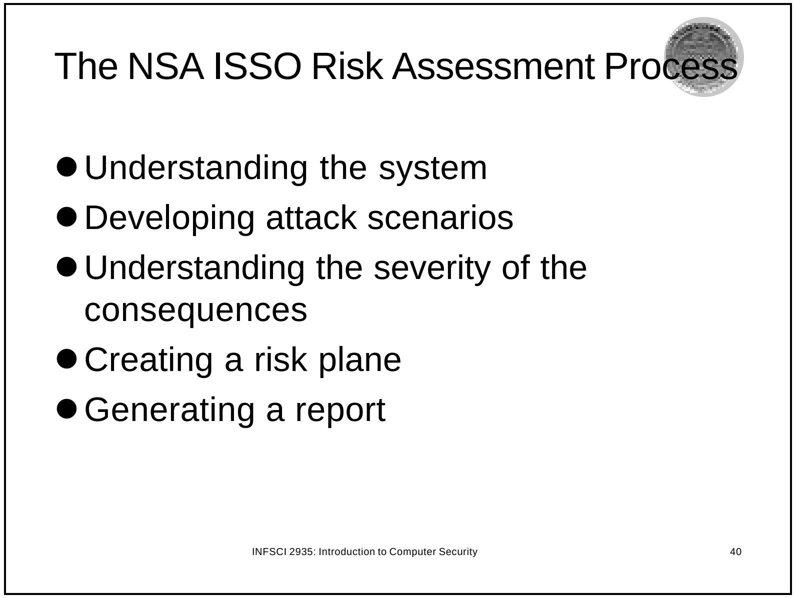
Examples of documented risk assessment systems

- Aggregated Countermeasures Effectiveness (ACE) Model
- Risk Assessment Tool
- Information Security Risk Assessment Model (ISRAM)
- Dollar-based OPSEC Risk Analysis (DORA)
- Analysis of Networked Systems Security Risks (ANSSR)
- Profiles
- NSA ISSO INFOSEC Risk Assessment Tool



NSA ISSO Risk Assessment Methodology

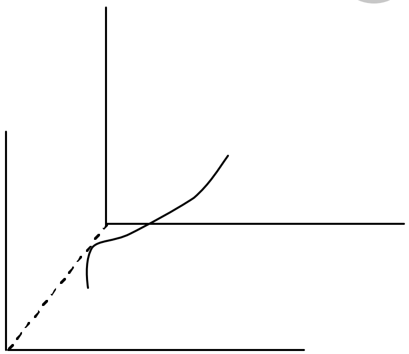
- Developed in the NSA Information Systems Security Organization
- Used for INFOSEC Products and Systems
- Can Use During Entire life Cycle



The NSA ISSO Risk Assessment Process

- Understanding the system
- Developing attack scenarios
- Understanding the severity of the consequences
- Creating a risk plane
- Generating a report

The Risk Plane



Y -axis

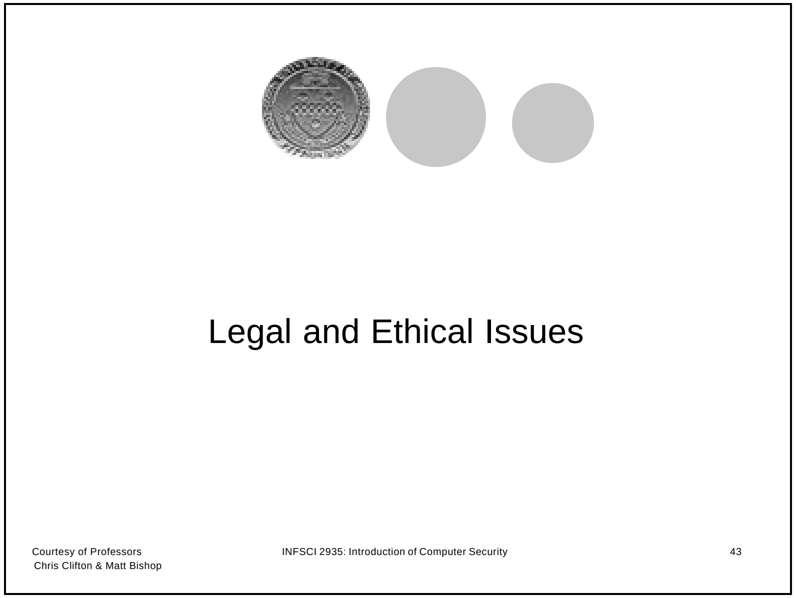
The severity of the Consequences of that successful attack.

X -axis

The likelihood of a successful attack

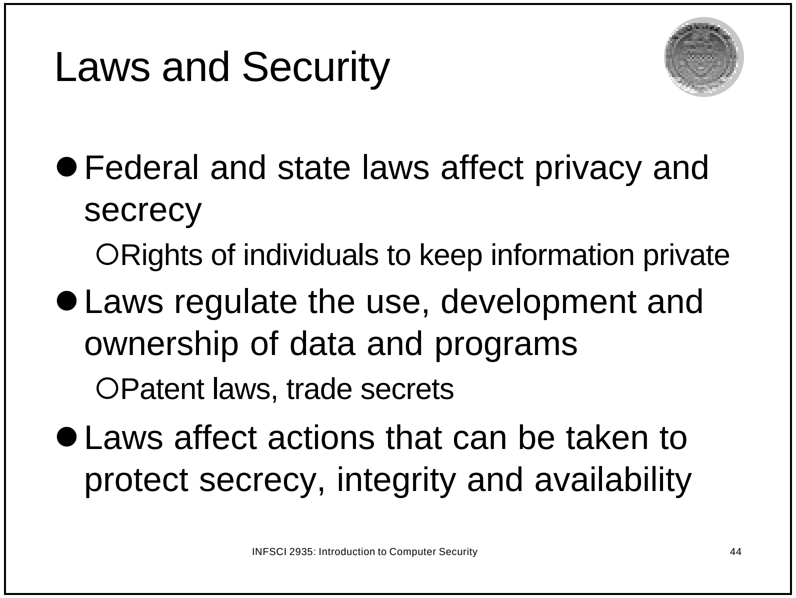
Risk Index

- Risk Index, as defined by the “Yellow Book”, is the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system
  - ○Minimum User Clearance=Rmin
  - ○Maximum Data Sensitivity=Rmax
  - ○Risk Index=Rmax – Rmin
    - ●Risk index is between O and 7



Legal and Ethical Issues

Courtesy of Professors
Chris Clifton & Matt Bishop



Laws and Security

- Federal and state laws affect privacy and secrecy
  - Rights of individuals to keep information private
- Laws regulate the use, development and ownership of data and programs
  - Patent laws, trade secrets
- Laws affect actions that can be taken to protect secrecy, integrity and availability

Copyrights

  - ○ Designed to protect *expression* of ideas
  - ○ Gives an author exclusive rights to make copies of the *expression* and sell them to public
- Intellectual property (copyright law of 1978)
  - ○ Copyright must apply to an original work
  - ○ It must be done in a tangible medium of expression
- Originality of work
  - ○ Ideas may be public domain
- Copyrighted object is subjected to fair use

Copyright infringement

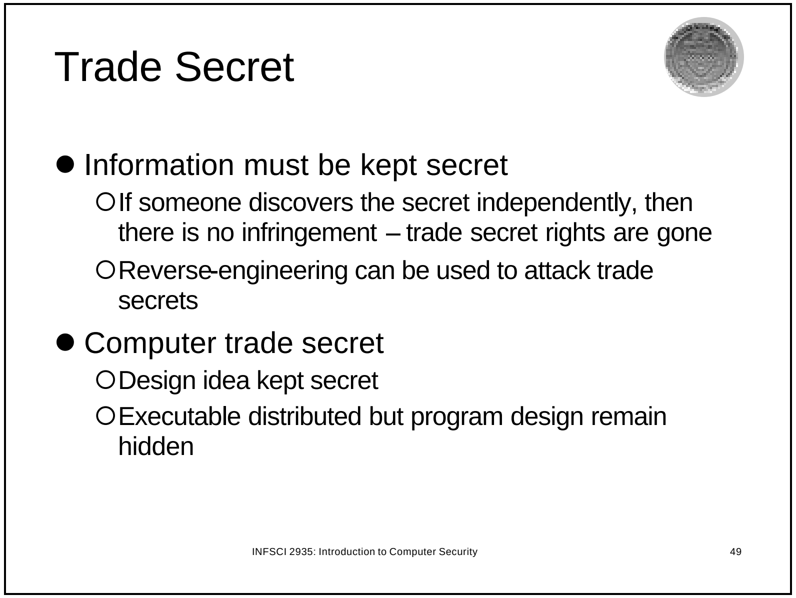
  - ○ Involves copying
  - ○ Not independent work
    - Two people can have copyright for identically the same thing
- Copyrights for computer programs
  - ○ Copyright law was amended in 1980 to include explicit definition of software
  - ○ Program code is protected not the algorithm
  - ○ Controls rights to copy and distribute

Patent

- Protects innovations
  - Applies to results of science, technology and engineering
  - Protects new innovations
    - Device or process to carry out an idea, not idea itself
  - Excludes newly discovered laws of nature
    - 2+2 = 4

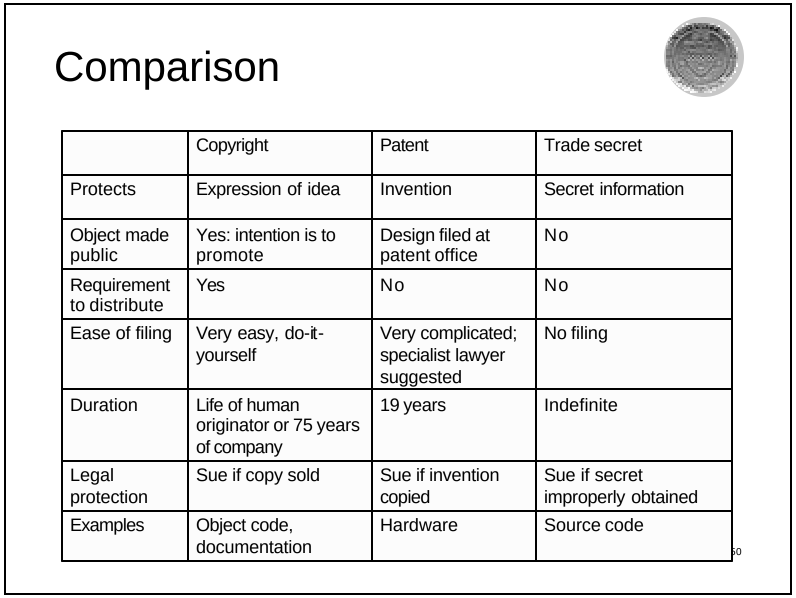
Patent

- Requirements of novelty
  - If two build the same innovations, patent is granted to the first inventor, regardless of who filed first
  - Invention should be truly novel and unique
  - Object patented must be non-obvious
- Patent Office registers patents
  - Even if someone independently invents the same thing, without knowledge of the existing patent
- Patent on computer objects
  - PO has not encouraged patents for software – as they are seen as representation of an algorithm



Trade Secret

- Information must be kept secret
  - If someone discovers the secret independently, then there is no infringement – trade secret rights are gone
  - Reverse-engineering can be used to attack trade secrets
- Computer trade secret
  - Design idea kept secret
  - Executable distributed but program design remain hidden



Comparison

	Copyright	Patent	Trade secret
Protects	Expression of idea	Invention	Secret information
Object made public	Yes: intention is to promote	Design filed at patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years of company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue if secret improperly obtained
Examples	Object code, documentation	Hardware	Source code

Employee and Employer Rights

- Employees generate idea and products
- Ownership is an issue in computer security
  - Rights of employer to protect the works of employees
- Ownership of products
  - Eve writes programs at night and sells it herself
  - If Eve is a programmer in a company and the program remotely corresponds to her job,
    - Employer may claim it!
  - If Eve is self-employed but an earlier version was developed for a company
    - Company may show that it had paid for the program and then claim ownership

Employee and Employer Rights

- Ownership of patents
  - If employee lets employer file the patent employer is deemed to own the patent and therefore the rights to the innovation
  - Employer has right to patent if the employee's job function includes inventing the product
- Similar issues for ownership of copyright
  - A special issue is work-for-hire
    - Employer is the author of the work

Employee and Employer Rights

- Work-for-hire situations
  - The employer has a supervisory relationship overseeing the manner in which the creative work is done
  - The employer has right to fire the employee
  - The employer arranges work to be done before the work was created
  - A written statement that states the employer has hired the employee to do certain work
- Alternate to work-for-hire is License
  - Programmer owns the product- sells license to company
  - Beneficial for the programmer

Computer crime

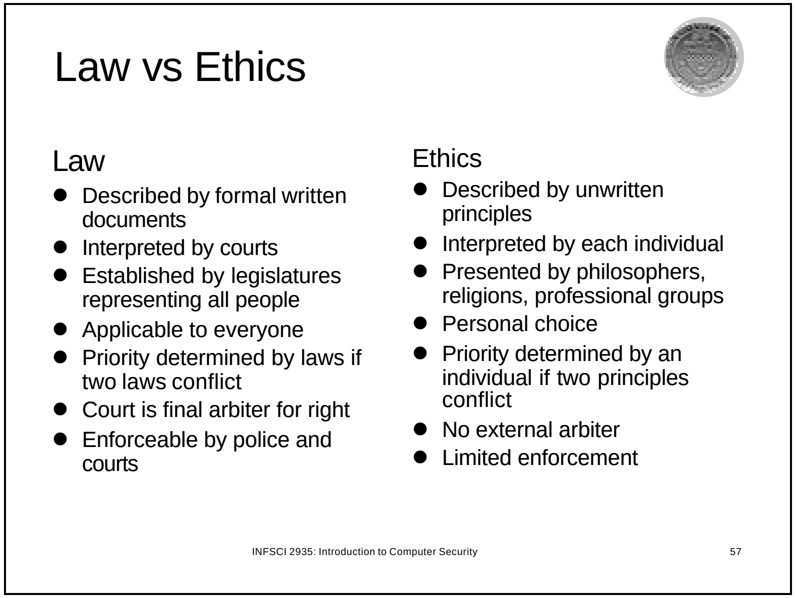
- Hard to predict for the following reason
  - Low computer literacy among lawyers, police agents, jurors, etc.
  - Tangible evidence like fingerprints and physical clues may not exist
  - Forms of asset different
    - Is computer time an asset?
  - Juveniles
    - Many involve juveniles

Computer Crime related laws

- Freedom of information act
  - Provides public access to information collected by the executive branch of the federal government
- Privacy act of 1974
  - Personal data collected by government is protected
- Fair credit reporting act
  - Applies to private industries – e.g., credit bureaus
- Cryptography and law
  - France: no encryption allowed (to control terrorism)
  - US, UK, Canada, Germany:
    - Control on export of cryptography; but they are published!

Ethics

- An objectively defined standard of right and wrong
- Often idealistic principles
- In a given situation several ethical issues may be present
- Different from law



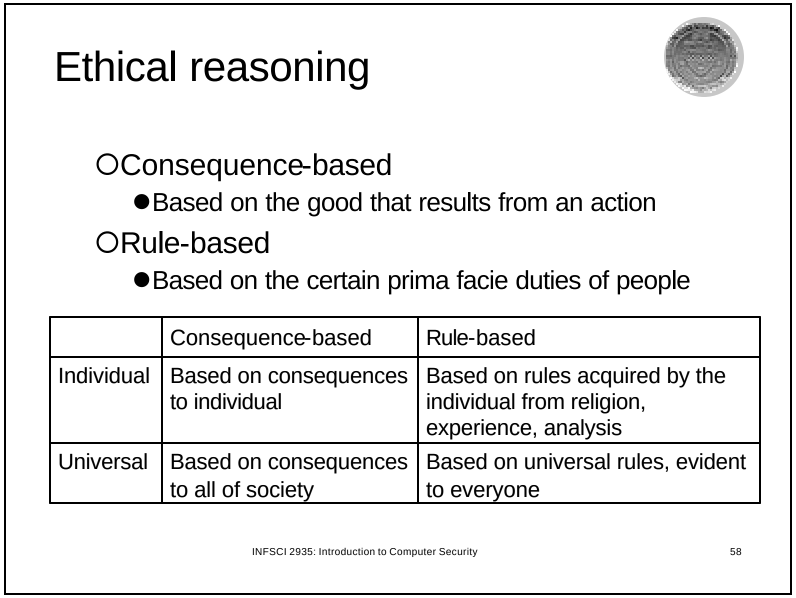
Law vs Ethics

Law

- Described by formal written documents
- Interpreted by courts
- Established by legislatures representing all people
- Applicable to everyone
- Priority determined by laws if two laws conflict
- Court is final arbiter for right
- Enforceable by police and courts

Ethics

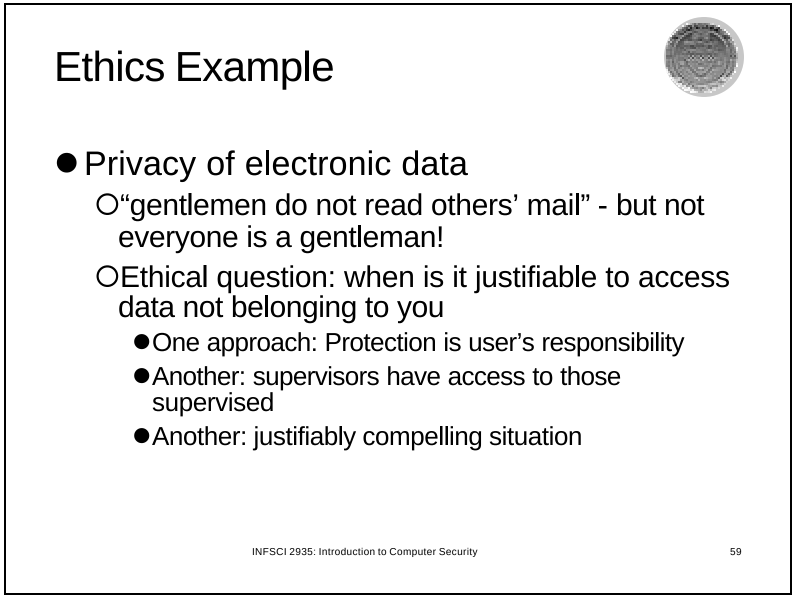
- Described by unwritten principles
- Interpreted by each individual
- Presented by philosophers, religions, professional groups
- Personal choice
- Priority determined by an individual if two principles conflict
- No external arbiter
- Limited enforcement



Ethical reasoning

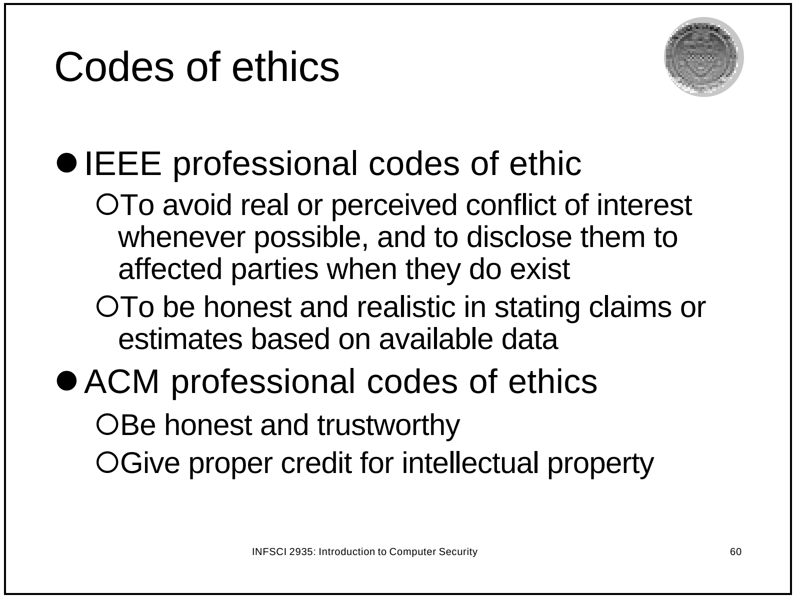
- ○Consequence-based
  - ●Based on the good that results from an action
- ○Rule-based
  - ●Based on the certain prima facie duties of people

	Consequence-based	Rule-based
Individual	Based on consequences to individual	Based on rules acquired by the individual from religion, experience, analysis
Universal	Based on consequences to all of society	Based on universal rules, evident to everyone



Ethics Example

- Privacy of electronic data
  - “gentlemen do not read others’ mail” - but not everyone is a gentleman!
  - Ethical question: when is it justifiable to access data not belonging to you
    - One approach: Protection is user’s responsibility
    - Another: supervisors have access to those supervised
    - Another: justifiably compelling situation



Codes of ethics

- IEEE professional codes of ethic
  - To avoid real or perceived conflict of interest whenever possible, and to disclose them to affected parties when they do exist
  - To be honest and realistic in stating claims or estimates based on available data
- ACM professional codes of ethics
  - Be honest and trustworthy
  - Give proper credit for intellectual property