COMPUTER SECURITY
PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

Chapter 19

Legal and Ethical Aspects

Computer Crime/Cybercrime

"Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity."

Types of Computer Crime

- **the U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:**

computers as targets

involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

computers as storage devices

using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

computers as communications tools

crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Article 2 Illegal access

The access to the whole or any part of a computer system without right.

Article 3 Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices

a   The production, sale, procurement for use, import, distribution or otherwise making available of:

  i   A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

  ii   A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and

b   The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

a   Any input, alteration, deletion or suppression of computer data;

b   Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 9 Offenses related to child pornography
  a   Producing child pornography for the purpose of its distribution through a computer system;
  b   Offering or making available child pornography through a computer system;
  c   Distributing or transmitting child pornography through a computer system;
  d   Procuring child pornography through a computer system for oneself or for another person;
  e   Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting
  Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

	Committed (net %)	Insider (%)	Outsider (%)	Source Unknown (%)
Virus, worms or other malicious code	74	18	46	26
Unauthorized access to/use of information, systems or networks	55	25	30	10
Illegal generation of spam e-mail	53	6	38	17
Spyware (not including adware)	52	13	33	18
Denial of service attacks	49	9	32	14
Fraud (credit card fraud, etc.)	46	19	28	5
Phishing (someone posing as your company online in an attempt to gain personal data from your subscribers or employees)	46	5	35	12
Theft of other (proprietary) info including customer records, financial records, etc.	40	23	16	6
Theft of intellectual property	35	24	12	6
Intentional exposure of private or sensitive information	35	17	12	9
Identity theft of customer	33	13	19	6
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks	30	14	14	6
Zombie machines on organization's network/bots/use of network by BotNets	30	6	19	10
Web site defacement	24	4	14	7
Extortion	16	5	9	4
Other	17	6	8	7

Table 19.2

CERT 2007 E-Crime Watch Survey Results

Law Enforcement Challenges

Characteristics of law enforcement agencies

- Failure to catch up with cybercrime technologies
- Inexperience with cybercrimes
- Inability to solve cybercrimes
- Lack of collaboration with industry

Lack of collaborations/global cooperation

Characteristics of cybercrime victims

Lack of confidence with law enforcement agencies

Weak defense mechanisms

Low reporting rates

Compliance with cybercriminal's demands

Characteristics of cybercriminals

Globalization of cybercrime

Increased success/confidence

- Sophisticated technology
- Links with organized crime

- Expertise/experience
- Unique profiles

Figure 19.1 The Vicious Cycle of Cybercrime [KSHE06]

Patents

Unauthorized making, using or selling
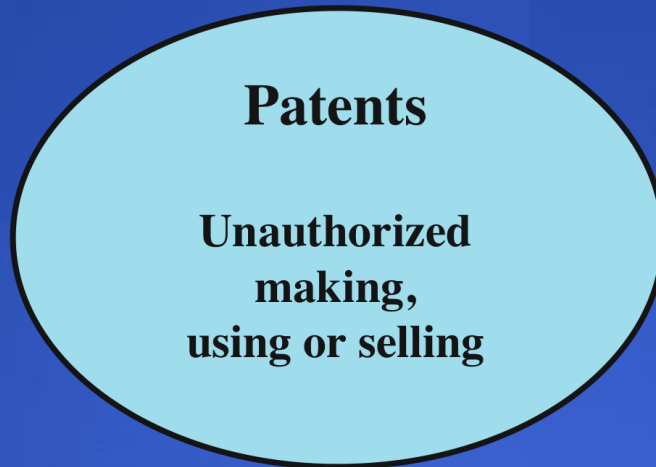
intellectual property is defined as "any intangible asset that consists of human knowledge and ideas".

Intellectual Property

Trademarks
Unauthorized use or colorable imitation

Copyrights

Unauthorized use

infringement is "the invasion of the rights secured by copyrights, trademarks, and patents".

Figure 18.2 Intellectual Property Infringement

Copyright

- **protects tangible or fixed expression of an idea but not the idea itself**

- **creator can claim and file copyright at a national government copyright office if:**

    - **proposed work is original**

    - **creator has put original idea in concrete form**

Copyright Rights

- copyright owner has these exclusive rights, protected against infringement:
  - reproduction right
  - modification right
  - distribution right
  - public-performance right
  - public-display right
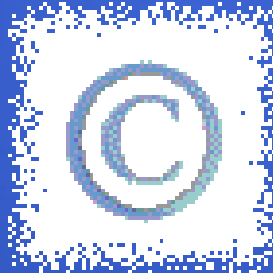
- examples of items that can be copyrighted include:
  - literary works
  - musical works
  - dramatic works
  - pantomimes and choreographic works
  - pictorial, graphic, and sculptural works
  - motion pictures and other audiovisual works
  - sound recordings
  - architectural works
  - software-related works

Patent

- grant a property right to the inventor

- "the right to exclude others from making, using, offering for sale, or selling" the invention in the United States or "importing" the invention into the United States

- types:

utility	design	plant
• any new and useful process, machine, article of manufacture, or composition of matter	• new, original, and ornamental design for an article of manufacture	• discovers and asexually reproduces any distinct and new variety of plant

Trademark

- a word, name, symbol, or device
  - used in trade with goods
  - indicates source of goods
  - distinguishes them from goods of others
- trademark rights may be used to:
  - prevent others from using a confusingly similar mark
  - but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark

U.S. Digital Millennium Copyright ACT (DMCA)

- signed into law in 1998

- implements WIPO treaties to strengthen protections of digital copyrighted materials

- encourages copyright owners to use technological measures to protect their copyrighted works
  - measures that prevent access to the work
  - measures that prevent copying of the work

- prohibits attempts to bypass the measures
  - both criminal and civil penalties apply to attempts to circumvent

DMCA Exemptions

- **certain actions are exempted from the provisions of the DMCA and other copyright laws including:**

| fair use | reverse engineering | encryption research | security testing | personal privacy |
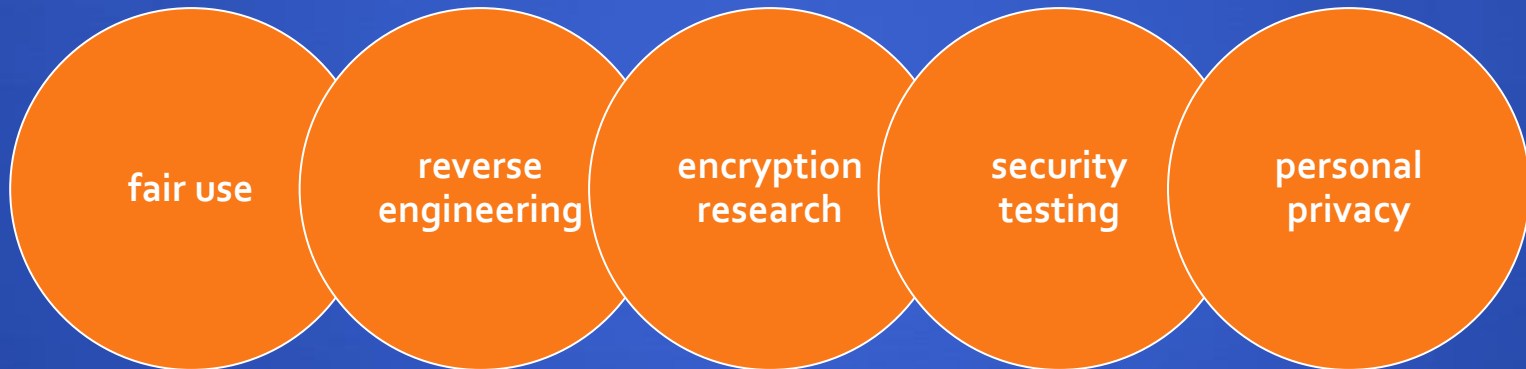
- **considerable concern exists that DMCA inhibits legitimate security and encryption research**
  - **feel that innovation and academic freedom is stifled and open source software development is threatened**

Digital Rights Management (DRM)

- **systems and procedures that ensure that holders of digital rights are clearly identified and receive stipulated payment for their works**
  - may impose further restrictions such as inhibiting printing or prohibiting further distribution

- **no single DRM standard or architecture**

- **objective is to provide mechanisms for the complete content management life cycle**

- **provide persistent content protection for a variety of digital content types / platforms / media**
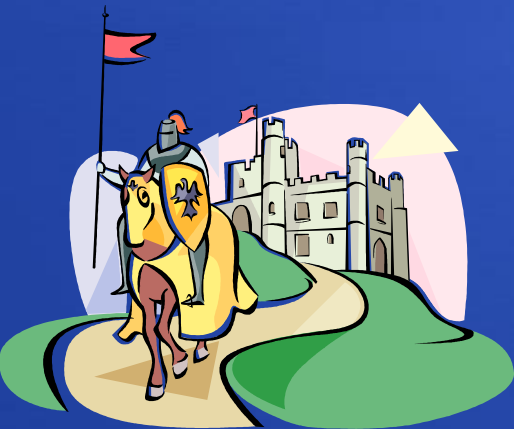
DRM

Components
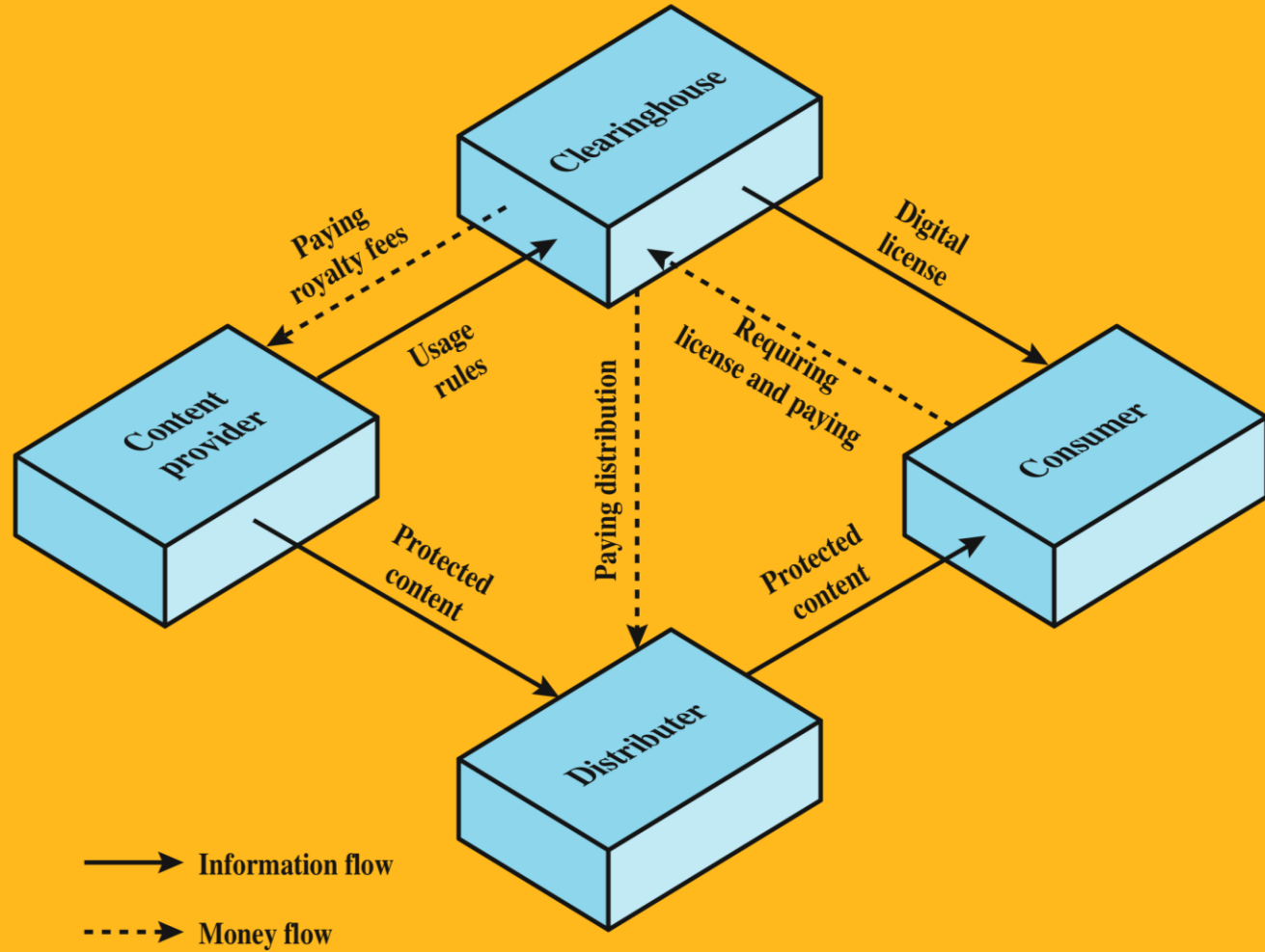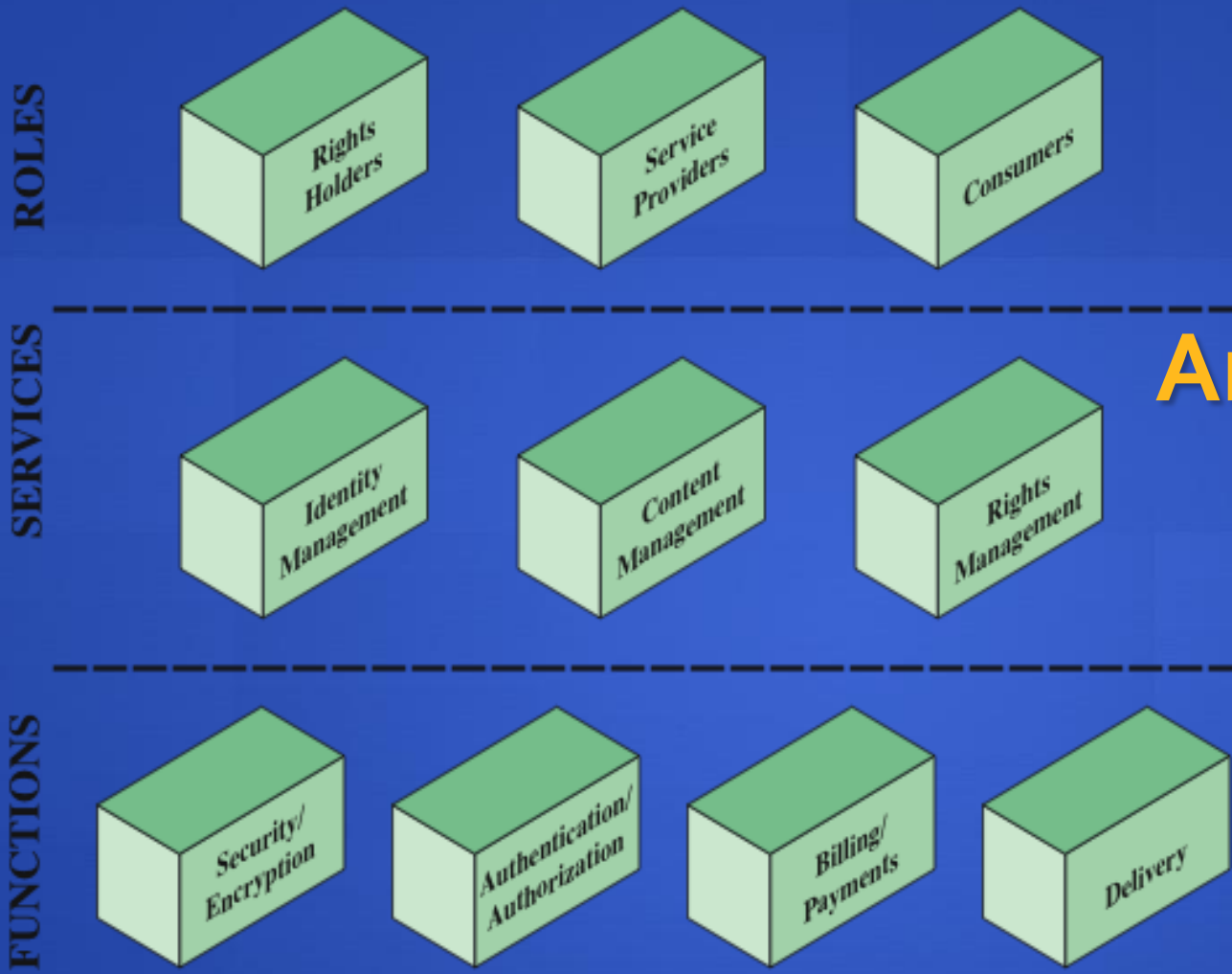

Figure 19.3 DRM Components

Figure 19.4   DRM System Architecture

Privacy

- **overlaps with computer security**

- **dramatic increase in scale of information collected and stored**
  - **motivated by law enforcement, national security, economic incentives**

- **individuals have become increasingly aware of access and use of personal information and private details about their lives**

- **concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights**

European Union (EU) Data Protection Directive

- **adopted in 1998 to:**
  - **ensure member states protect fundamental privacy rights when processing personal information**
  - **prevent member states from restricting the free flow of personal information within EU**

- **organized around principles of:**

notice	consent	consistency	access

security	onward transfer	enforcement

# United States Privacy Initiatives

Privacy Act of 1974

- dealt with personal information collected and used by federal agencies
- permits individuals to determine records kept
- permits individuals to forbid records being used for other purposes
- permits individuals to obtain access to records and to correct and amend records as appropriate
- ensures agencies properly collect, maintain, and use personal information
- creates a private right of action for individuals

Also have a range of other privacy laws

ISO 27002 states . . .

"An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information should be implemented."
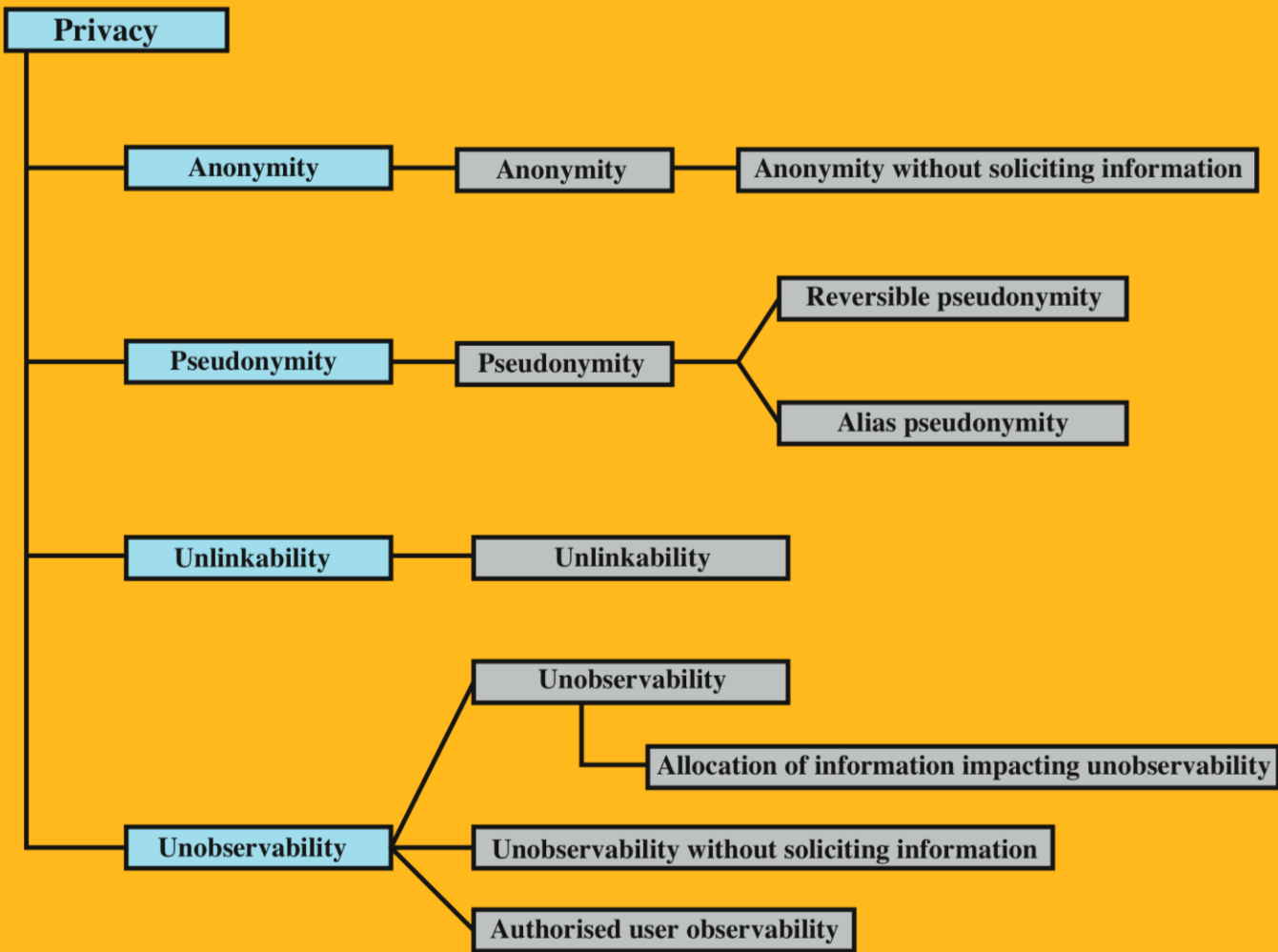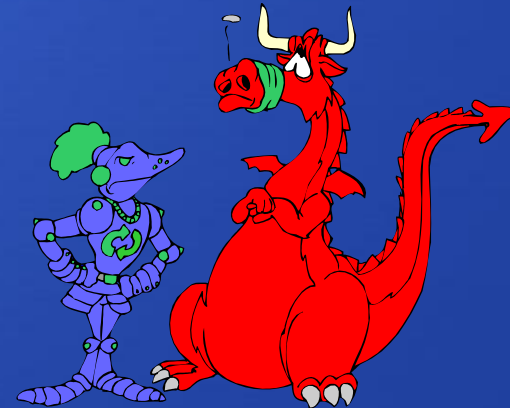
Figure 19.5 Common Criteria Privacy Class Decomposition
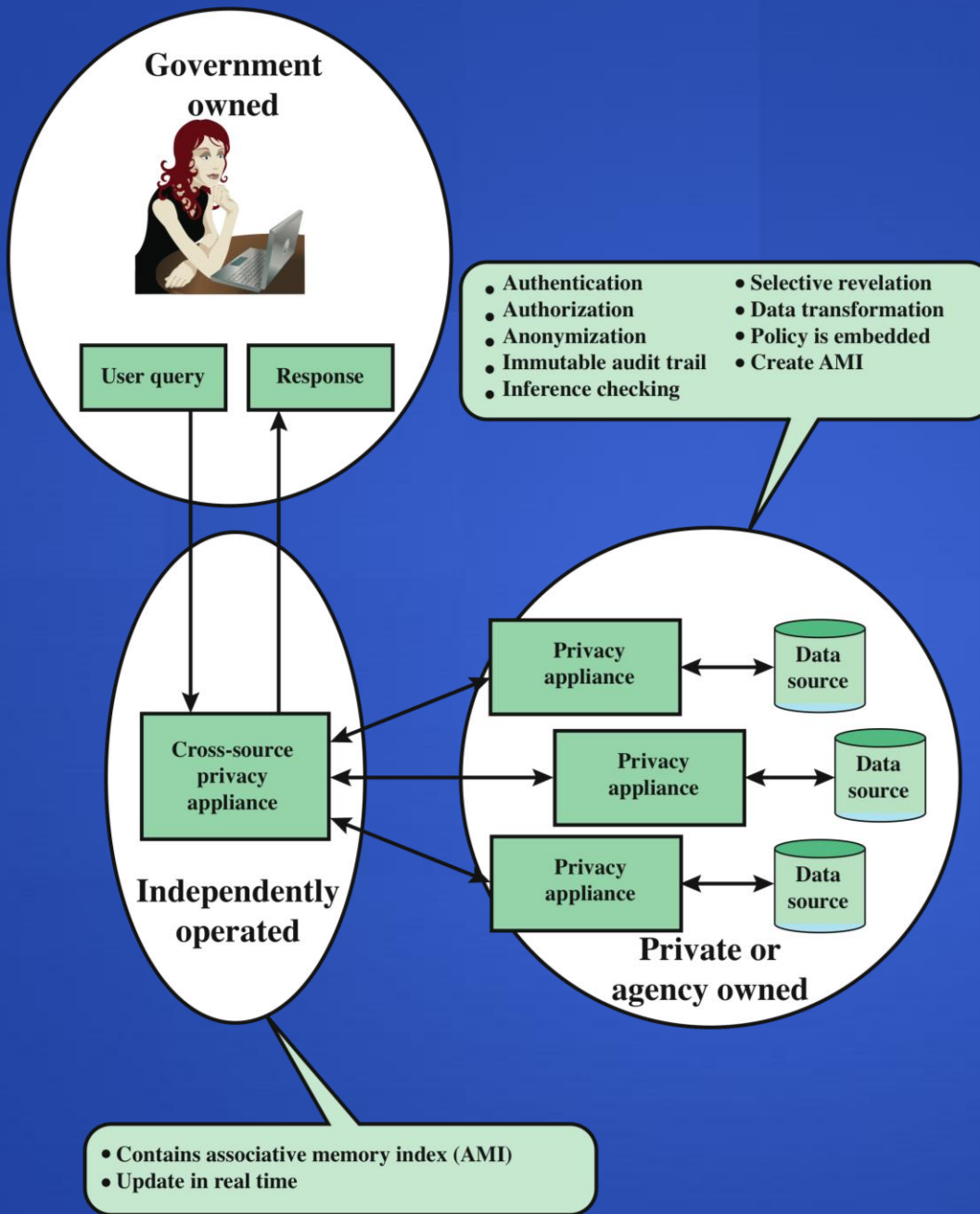
Privacy and Data Surveillance

Figure 19.6 Privacy Appliance Concept

Ethical Issues

- ethics:

  "a system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions."

- many potential misuses and abuses of information and electronic communication that create privacy and security problems

- basic ethical principles developed by civilizations apply

  - unique considerations surrounding computers and information systems
  - scale of activities not possible before
  - creation of new types of entities for which no agreed ethical rules have previously been formed
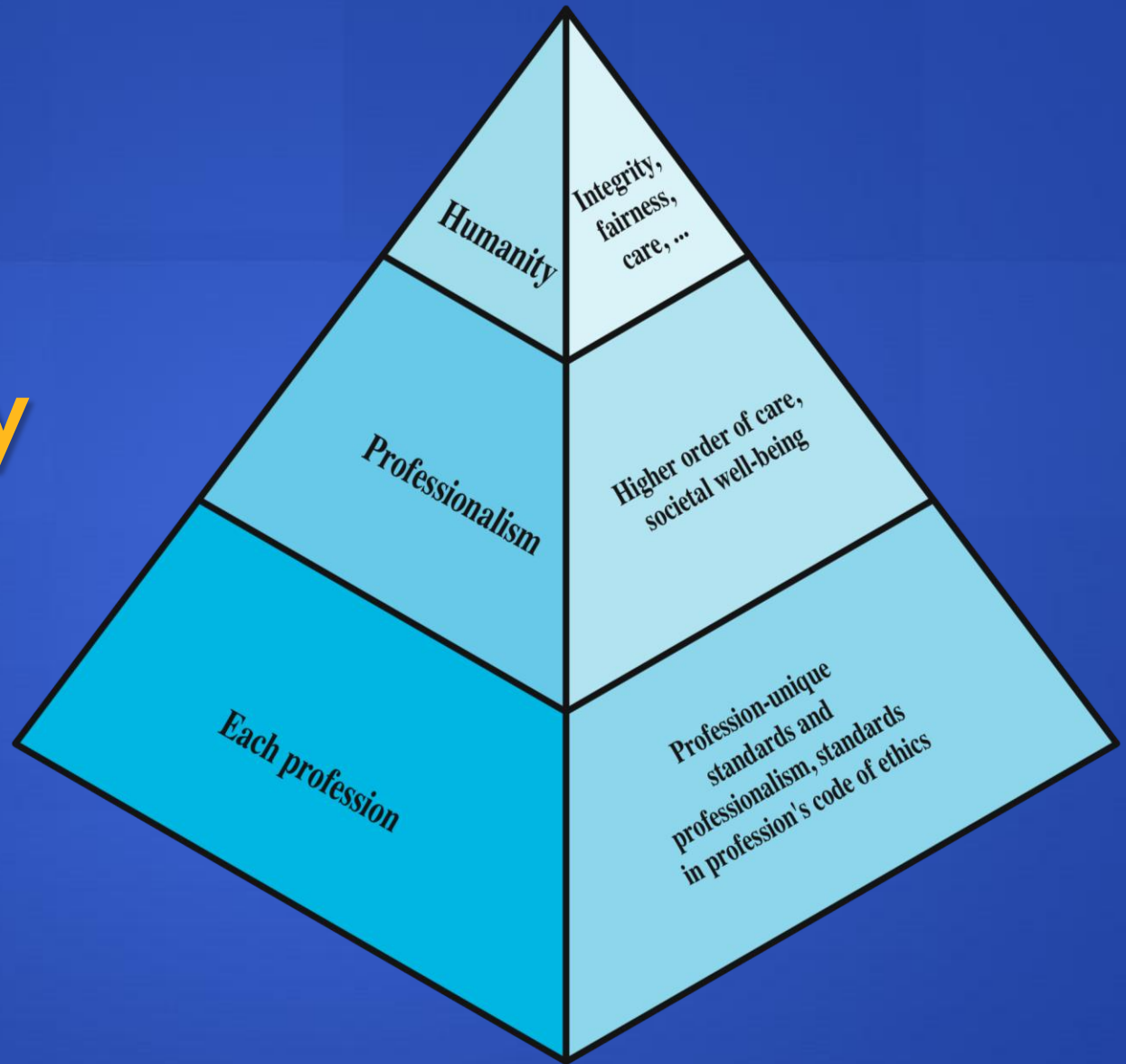
Ethical Hierarchy

Figure 19.7 The Ethical Hierarchy

Ethical Issues Related to Computers and Information Systems

- **some ethical issues from computer use:**
  - **repositories and processors of information**
  - **producers of new forms and types of assets**
  - **instruments of acts**
  - **symbols of intimidation and deception**

- **those who understand, exploit technology, and have access permission, have power over these**

Table 19.3
Potential Ethical Dilemmas

Technology Intrusion	Privacy internal to the firm Privacy external to the firm Computer surveillance Employee monitoring Hacking
Ownership Issues	Moonlighting Proprietary rights Conflicts of interest Software copyrights Use of company assets for personal benefit Theft of data, software, or hardware
Legal Issues and Social Responsibilities	Embezzlement, fraud and abuse, such as through EFTs or ATMs Accuracy and timeliness of data Over-rated system capabilities and "smart" computers Monopoly of data
Personnel issues	Employee sabotage Ergonomics and human factors Training to avoid job obsolescence

Ethical Question Examples

- **whistle-blower**
  - when professional ethical duty conflicts with loyalty to employer
  - e.g. inadequately tested software product
  - organizations and professional societies should provide alternative mechanisms

- **potential conflict of interest**
  - e.g. consultant has financial interest in vendor which should be revealed to client

Codes of Conduct

- ethics are not precise laws or sets of facts

- many areas may present ethical ambiguity

- many professional societies have adopted ethical codes of conduct which can:

  1. • be a positive stimulus and instill confidence
  2. • be educational
  3. • provide a measure of support
  4. • be a means of deterrence and discipline
  5. • enhance the profession's public image

ACM Code of Ethics and Professional Conduct

1. GENERAL MORAL IMPERATIVES.

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE.

4.1 Uphold and promote the principles of this Code.
4.2 Treat violations of this code as inconsistent with membership in the ACM.

Figure 19.8 ACM Code of Ethics and Professional Conduct
(Copyright ©1997, Association for Computing Machinery, Inc.)

IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.9 IEEE Code of Ethics
(Copyright ©2006, Institute of Electrical and Electronics Engineers)

AITP Standard of Conduct

In recognition of my obligation to management I shall:
- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:
- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:
- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:
- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Figure 19.10 AITP Standard of Conduct
(Copyright ©2006, Association of Information Technology Professionals)

Comparison of Codes of Conduct

- all three codes place their emphasis on the responsibility of professionals to other people

- do not fully reflect the unique ethical problems related to the development and use of computer and IS technology

- common themes:
  - dignity and worth of other people
  - personal integrity and honesty
  - responsibility for work
  - confidentiality of information
  - public safety, health, and welfare
  - participation in professional societies to improve standards of the profession
  - the notion that public knowledge and access to technology is equivalent to social power

The Rules

- **collaborative effort to develop a short list of guidelines on the ethics of computer systems**

- **Ad Hoc Committee on Responsible Computing**
  - **anyone can join this committee and suggest changes to the guidelines**

- *Moral Responsibility for Computing Artifacts*
  - **generally referred to as *The Rules***
  - ***The Rules* apply to software that is commercial, free, open source, recreational, an academic exercise or a research tool**

- **computing artifact**
  - **any artifact that includes an executing computer program**
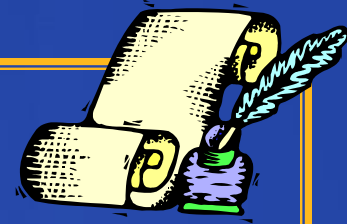
As of this writing, the rules are as follows:

1) The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.

2) The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying, or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.

3) People who knowingly use a particular computing artifact are morally responsible for that use.

4) People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.

5) People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.

Summary

- **cybercrime and computer crime**
  - types of computer crime
  - law enforcement challenges
  - working with law enforcement
- **intellectual property**
  - types of intellectual property
  - intellectual property relevant to network and computer security
  - digital millennium copyright act
  - digital rights management

- **privacy**
  - privacy law and regulation
  - organizational response
  - computer usage privacy
  - privacy and data surveillance
- **ethical issues**
  - ethics and the IS professions
  - ethical issues related to computers and information systems
  - codes of conduct
  - The Rules