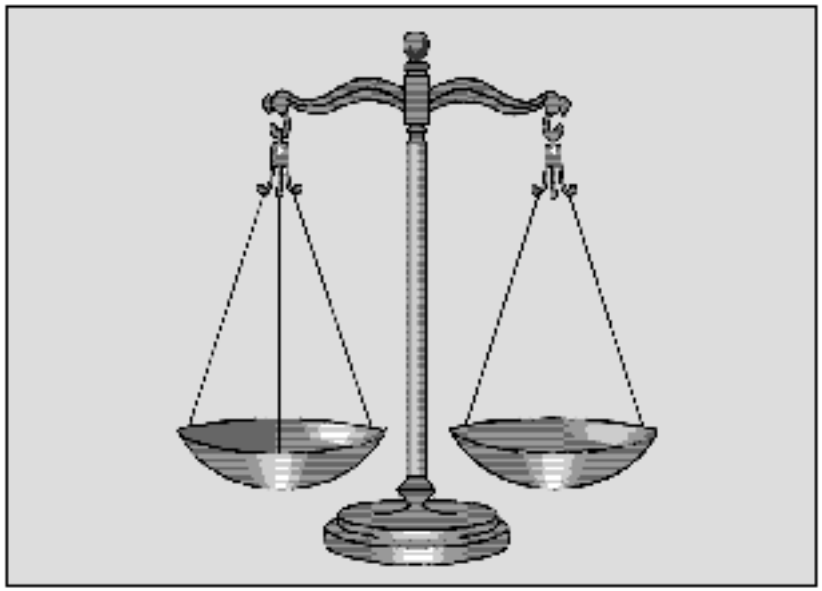

Computers, Ethics, and Public Policy

Information Security

Computing Ethics in the news

- Chinese cybersecurity laws
- http://blogs.wsj.com/chinarealtime/2016/06/03/untangling-chinas-cybersecurity-laws/

- "Many of these measures involve the concept of 'secure and controllable' technology, a loosely defined term that involves government security checks and data storage within the country."

Chinese Cyber laws (2)

- Generally a requirement for vendors to share source code
- Ask companies for help in decryption
- Legislation
  - National Security Law (7/2015)
  - Counterterrorism Law (12/2015)
  - Banking Sector IT guidelines (1/2015, but suspended)
  - Insurance Sector IT Guidelines (currently draft)

An interesting article from Wired

- Top information security threats "we" will face in 2015
- http://www.wired.com/2015/01/security-predictions-2015/
  - Nation-State attacks
  - Extortion
  - Data Destruction
  - Bank Card Breaches
  - Third-Party Breaches
  - Critical Infrastructure

China and industrial robots

- http://money.cnn.com/2016/06/23/technology/china-industrial-robots/index.html
- China now buying more than 25% of all industrial robots
  - China's workforce is shrinking (it’s hard to change public opinion concerning the 1-child policy)
  - Decreased interest in low-level jobs
  - Result is increased labor costs

What is information security?

Why is information security important/a concern?

- Value of information
- Impact on an organization due to damages/ misuses of information
- Ease of information access due to the growth of the Internet and networking capabilities of machines and people's awareness

What's the difference between:

- Information Assurance
- Information Security
- Computer Security
- Cybersecurity

From the US Code, Title 44, Sec. 3542

The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

From: http://www.law.cornell.edu/uscode/44/3542.html

IA is set of technical and managerial controls designed to ensure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems. IA includes measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Cooper et. al. 2010. An exploration of the current state of information assurance education. SIGCSE Bull. 41, 4, 109-125.

Other aspects of information security (beyond CIA)

- Authentication – of the information/data, of the sender and of the receiver
- Non-repudiation – that the sender cannot deny having sent the data, nor the receiver having received the data

Some examples of violating:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation

How might confidentiality, integrity, availability, authentication, and non-repudiation be part of:

- Hacking
- Privacy
- IP
- Democratic access to computing

Some additional information security terms

- Cryptography
- Vulnerability
- Threat*
  - Disclosure
  - Deception
  - Disruption
  - Usurpation
- Risk

* Shirey, Robert W. *Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards*. Internet Draft: draft-irtf-psrg-secarch-sect1-00, November 1994.

Aims of security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Levels of Information Security

- The application
- The operating system
- The network
- The data management system
- Physical protection is also important

Ideas from Elisa Bertino, Purdue

How is Information Security realized?

- Confidentiality is enforced by the access control mechanism
- Integrity is enforced by the access control mechanism and by the semantic integrity constraints
- Availability is enforced by the recovery mechanism and by detection techniques for denial of service attacks
- Non-repudiation is accomplished through audit (commonly using logs)

Ideas from Elisa Bertino, Purdue

How is Information Security realized?

- User authentication verifies the identity of subjects wishing to access the information
- Information authentication ensures information authenticity - it is supported by signature mechanisms
- Encryption protects information when being transmitted across systems and when being stored on secondary storage
- Intrusion detection protects against impersonation of legitimate users and also against insider and external threats

Ideas from Elisa Bertino, Purdue

Implementing Information Security

- It consists of:
  - Defining a *security policy*
  - Choosing some *mechanism* to enforce the policy
  - Providing *assurance* that both the mechanism and the policy are sound

Ideas from Elisa Bertino, Purdue

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the information
  - Challenge: If policies conflict, discrepancies may create security vulnerabilities
- Mechanisms enforce policies

Ideas from Elisa Bertino

Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

Ideas from Elisa Bertino, Purdue

Management and Legal Issues

- Cost-Benefit Analysis
  - Is it more cost-effective to prevent or recover?
- Risk Analysis
  - Should we protect some information?
  - How much should we protect this information?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people adopt them?

Ideas from Elisa Bertino, Purdue

Human Factor Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Ideas from Elisa Bertino, Purdue

Thought Questions for Today

1. To what extent can information security be viewed as a subset of computing, given that it seems to focus on the data?
2. To what extent may computing be viewed as a subset of information security, as information security also involves information systems, law, public policy, criminal justice, and other fields?
3. Should information security ethics need to be viewed as a separate field than computing ethics?