Chapter 1

1. History of computer security involving to info-sec
   1. CS-sec:
      1. Begin: right after the first mainframe dev.
      2. Focus: physical security
      3. MULTICS: 1st OS with sec-integrated →UNIX
   2. Info-sec
      1. Begin: RAND R.609, first recognized policy document
      2. Focus: data, access, personnel of multiple levels
      3. DEFCON:1993
      4. Social networks
      5. Art and science
         1. Art: no hard rules, not uni-accepted, no manual
         2. Science: tech, fault from ware, time can eliminate
         3. Social science
2. Definition and concepts of info-sec
   1. Security: state of secure and freee from danger; action to secure
   2. Info security:
      1. Software
      2. Hardware(computer)
      3. Data(info),
      4. Network
      5. People
      6. Procedures
   3. Layers of sec: operation, physical, personal, network, communication, info
   4. C.I.A Triad: confidentiality, integrity, availability
   5. Info char: authenticity
   6. Key info sec concepts:
      1. Access, asset, attack, control&safeguard&conuntermeasure, exploit, exploit, exposure, loss, protection, risk, threat, bulnerability
      2. Computer can be subject/ object of attacks
      3. McCumber Cube:
         1. X-axis: storage, processing, transmission
         2. Y-axis: C.I.A
         3. Z-axis: policy, edu, tech
      4. Balance protection and availability
3. Security in SysDev life cycle(SDLC): design, implement Infosys:
   1. Consist:
      1. Investigation: problem, obj, pre-cost-benefit analysis
      2. Analysis: assessment of organization, cursys, support capability, end with doc
      3. Logic design: spec-tech, cost-benefit analysis
      4. Physical design: solution
      5. Implementation: software, components, training
      6. Maintenance and Change: longest and most expensive, until begin again
   2. Approach:
      1. SwA CBK: DOD and DHS, secure software assurance, common body of knowledge
      2. NIST: initiation, Dev/Acq, Implement/Assess, Op&maintenance, disposal
4. Info-sec professions role in organization
   1. Key: senior management
      1. CIO: plan
      2. CISO: masses, manage, implementation→CIO
   2. Data: owners, custodians, users

Quiz:

1. Difference between a threat agent and a threat?

Threat is the category event adversely affect C.I.A of info, while agent is specific instance.

1. Difference between vulnerability and exposure?

Vulnerability is the weakness, exposure is when the former is known to the attacker.

1. How is infrastructure protection (assuring the security of utility services) related to information security?

The C.I.A all depends on infrastructure, reliable

1. What type of security was dominant in the early years of computing?

Predominantly physical security and simple document classification, from theft espionage and sabotage.

1. Three components of the C.I.A. triad? What are they used for?

Confidentiality(access control), integrity(complete), availability(access maintain).

Model of infosec, a standard for CS-sec in industry and gov.

1. If the C.I.A. triad is incomplete, why is it so commonly used in security?

The sec of C.I.A is as important today as always, although not adequate.

1. Describe the critical characteristics of information. How are they used in the study of computer security?

C.I.A + accuracy, authenticity, possession, utility.

1. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?

Software, hardware, data, people, procedure, network.

Data?

All associated as integrated whole.

1. What system is the predecessor of almost all modern multiuser systems?

Mainframe CSys?

MULTICS?

1. Which paper is the foundation of all subsequent studies of computer security?

RAND Report R-609 for DOD

1. Why is the top-down approach to information security superior to the bottom-up approach?

Top down has strong upper mngt support, dedicated funding, clear plan and the influence org culture, while bottom up lacks participant support and org staying power.

1. Why is a methodology important in the implementation of information security? How does a methodology improve the process?

Ensures complete process without missing steps, raise success probiblites.

Follow SDLC waterfall model steps: investigation, analysis, logical design, physical design, implementation and maintennance

1. Which members of an organization are involved in the security systems development life cycle? Who leads the process?

Upper MNGT

Senior executive

1. How can the practice of information security be described as both an art and a science? How does the view of security as a social science influence its practice?

Art: no hard rules with users and policy, no uni-accepted complete sols, no manual

Sci: tech, fault from ware, time can eliminate

Socl: examine behaviours, start/end with peole, interact

1. Who is ultimately responsible for the security of information in the organization?

CISO

1. What is the relationship between the MULTICS project and the early development of computer security?

Early CS-sec focus on this sys, the 1st OS integrated sec into core func.

1. How has computer security evolved into modern information security?

Before ARPANET, physically secured, after it was just one component, raise need to secure info and transmit hardware

1. What was important about RAND Report R-609?

First widely recognized CS-sec management and policy document

1. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these decisions are carried out?

CIO/VP-IT?

Owner/User?

1. Who should lead a security team? Should the approach to security be more managerial or technical?

Champion or senior officer

top-down, managerial

Chapter 2

1. Infosec implementation more of management than technology

Quiz

1. Why is information security a management problem? What can management do that technology cannot?

More managerial than technical, upper mngt support, dedicated funding, clear plan and the influence org culture, while bottom up lacks participant support and org staying power

1. Why is data the most important asset an organization possesses? What other assets in the organization require protection?

Data is ability to deliver value to its customer and transactions.

Hardware, software, goods and network also require protection, ability of the organization to function, the safe operation of applications, and technology assets

1. Which management groups are responsible for implementing information security to protect the organization’s ability to function?

Both general mgnt and IT mgnt, IS mgnt

1. Has the implementation of networking technology created more or less risk for businesses that use information technology? Why?

More, coz connected make it easier for unauthorized access

1. What is information extortion? Describe how such an attack can cause losses, using an example not found in the text.

Steal info ask for money or disclose

1. Why are employees one of the greatest threats to information security?

Access to reveal, add, delete, and modify data. Store in unprotect areas or fail following procedures.

1. How can you protect against shoulder surfing?

Mind people, mind place

1. How has the perception of the hacker changed over recent years? What is the profile of a hacker today?

Small-scale to large.

Elite hacker with good skills and novice hacker with scripts written by the fromer

1. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?

Skilled dev unskilled use

Protect against former is more difficult or even impossible; stay up to date patches and against public hacking tool

1. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?

viruses, worms, Trojan horses, logic bombs, and back doors.

Yes, unleash

1. Why does polymorphism cause greater concern than traditional malware? How does it affect detection?

Malicious code change over time, hard to detect

1. What is the most common violation of intellectual property? How does an organization protect against it? What agencies fight it?

Unlawful use or duplication of software, software piracy

Digital watermarks, embedded code, copyright codes, bad sectors, online registration.

Software and Info Industry Assoc (SIIA) and the Business Software Alliance (BSA).

1. What are the various forces of nature? Which type might be of greatest concern to an organization in Las Vegas? Jakarta? Oklahoma City? Amsterdam? Miami? Tokyo?

Fire, flood, earthquakes, lightning, mudslides, tornados, hurricanes, typhoons, tsunamis, electrostatic discharge (ESD), and dust contamination

1. How is technological obsolescence a threat to information security? How can an organization protect against it?

Outdated, unreliable untrustworthy, caused by lack of planning and fail anticipating.

Proper planning by mgnt, discover\_>upgrade or replace

1. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?

Yes, asse

Reduce/remove from owner, duplicate sell copies

1. What are the types of password attacks? What can a systems administrator do to protect against them?

Crack(reverse), brute force, dict attack

Strong encryption, limit attempt, strong password

1. What is the difference between a denial-of-service attack and a distributed denial of service attack? Which is more dangerous? Why?

Connection/request, locations samutanously

DDoS, zombie first, no control can apply

1. For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?

Network access

Social engineering to unwitting employee

1. What methods does a social engineering hacker use to gain information about a user’s login ID and password? How would this method differ if it targeted an administrator’s assistant versus a data-entry clerk?

Pretend authority requesting information, bogus software on user machines, using deception to act on the conscience of users.

Data-entry clerk swayed easily, assistant require more convincing proof

1. What is a buffer overflow, and how is it used against a Web server?

Data sent to buffer more than it can handle.

Mismatch of processing rates between two communicating entities.