Cryptographic Methods of Information Security

Lecture-1

Dr. Abdul Razaque, PhD & Post Doctorate (Professor)

Learning Objectives

- Upon completion of this material, you should be able to:
  - Define information security
  - Recount the history of computer security and how it evolved into information security
  - Define key terms and critical concepts of information security
  - List the phases of the security systems development life cycle
  - Describe the information security roles of professionals within an organization

Introduction

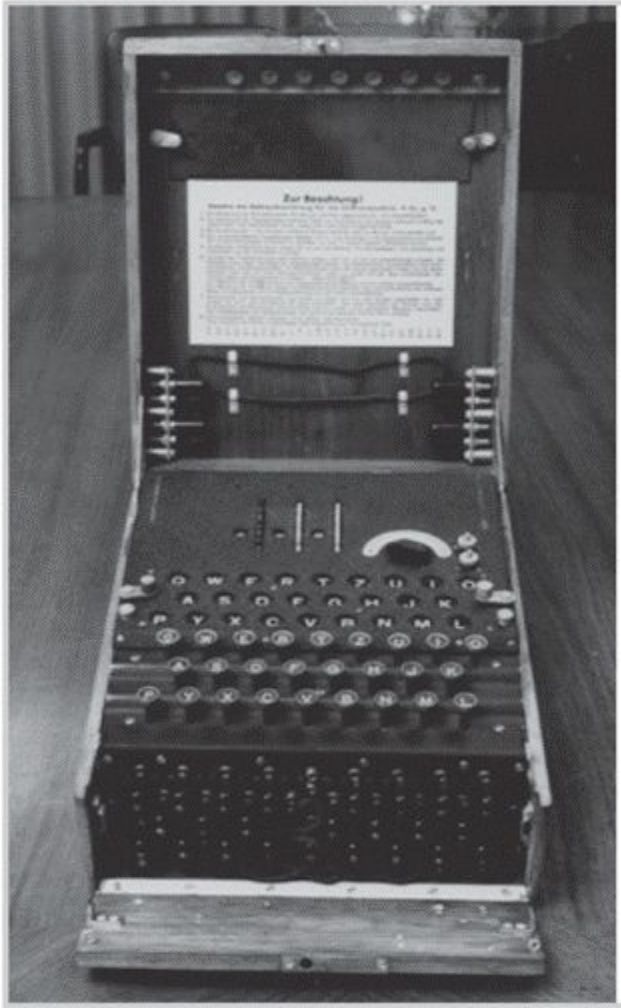
- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.”—Jim Anderson, Emagined Security, Inc.
- Security professionals must review the origins of this field to understand its impact on our understanding of information security today.

The History of Information Security

- Computer security began immediately after the first mainframes were developed.
  - Groups developed the code-breaking computations during World War II created the first modern computers.
  - Multiple levels of security were implemented.
- Physical controls limiting access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and sabotage

Date	Document
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems.*
1970	Willis H. Ware authors the report *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security—RAND Report R-609, which was not declassified until 1979. It became known as the seminal work identifying the need for computer security.*
1973	Schell, Downey, and Popek examine the need for additional security in military systems in *Preliminary Notes on the Design of Secure Military Computer Systems.*
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the *Federal Register.*
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[7]
1979	Morris and Thompson author "Password Security: A Case History," published in the *Communications of the Association for Computing Machinery* (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1984	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report, the authors examined four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[8]
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the system administrator or other privileged users...the naive user has no chance."[9]
1992	Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

Table 1-1 Key Dates in Information Security



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Figure 1-1 The Enigma[1]

Source: National Security Agency. Used with permission.[2]

The 1960s

- Advanced Research Project Agency (ARPA) began to examine the feasibility of redundant networked communications.
- Larry Roberts developed the ARPANET from its inception.

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Figure 1-2 Development of the ARPANET

Source: Courtesy of Dr. Lawrence Roberts. Used with permission.[4]

The 1970s and 80s

- ARPANET grew in popularity, as did its potential for misuse.
- Fundamental problems with ARPANET security were identified.
  - No safety procedures for dial-up connections to ARPANET
  - Nonexistent user identification and authorization to system

The 1970s and 80s (cont'd)

- Information security began with Rand Report R-609 (paper that started the study of computer security and identified the role of management and policy issues in it).
- The scope of computer security grew from physical security to include:
  - Securing the data
  - Limiting random and unauthorized access to data
  - Involving personnel from multiple levels of the organization in information security

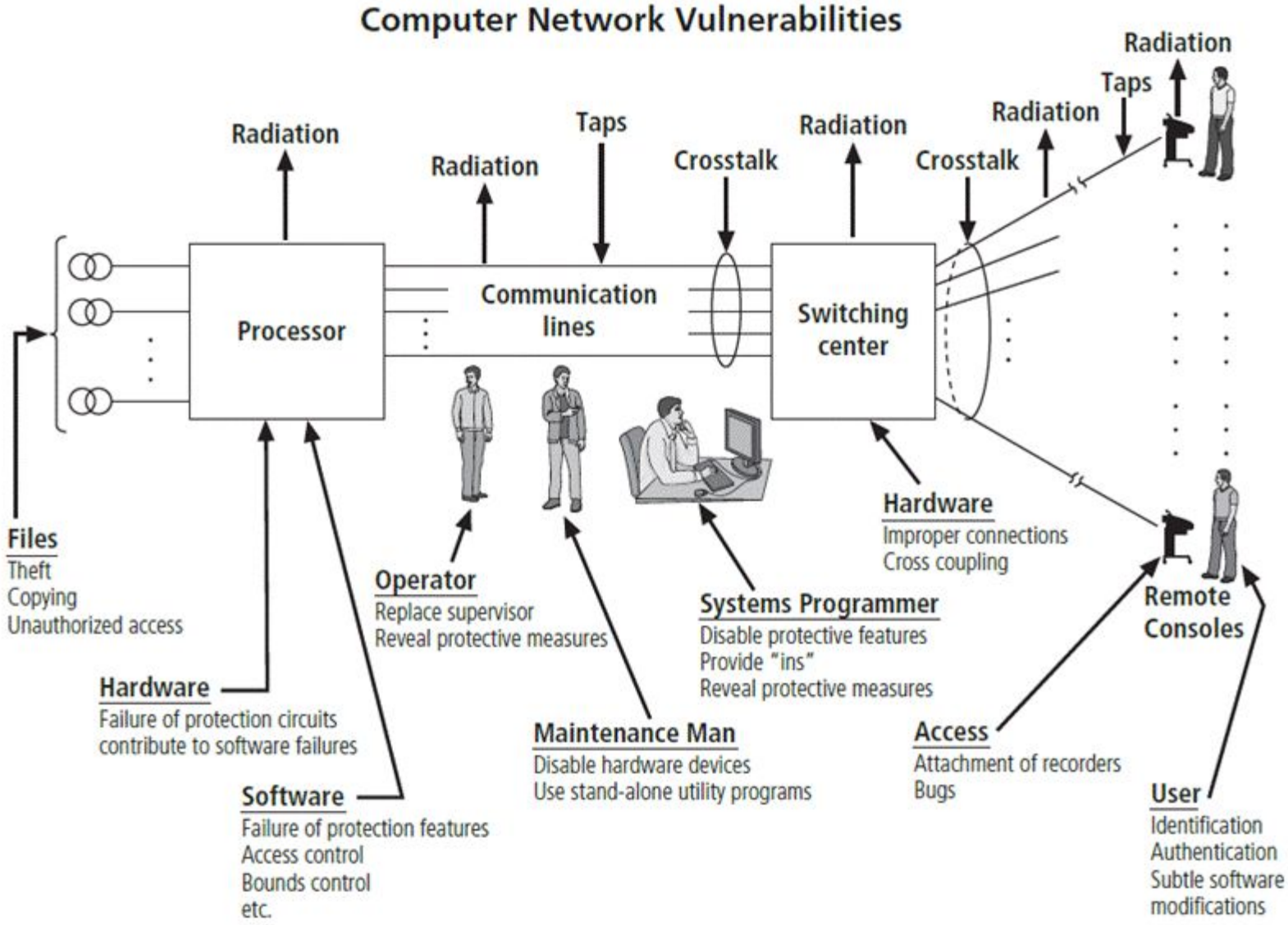


Figure 1-4 Illustration of computer network vulnerabilities from Rand Report R-609

Source: Rand Report R-609. Used with permission.[10]

MULTICS

- Early focus of computer security research centered on a system called Multiplexed Information and Computing Service (MULTICS).
- First operating system was created with security integrated into core functions.
- Mainframe, time-sharing OS was developed in the mid-1960s by General Electric (GE), Bell Labs, and Massachusetts Institute of Technology (MIT).
- Several MULTICS key players created UNIX.
  - Primary purpose of UNIX was text processing.
- Late 1970s: The microprocessor expanded computing capabilities and security threats.

The 1990s

- Networks of computers became more common, as did the need to connect them to each other.
- Internet became the first global network of networks.
- Initially, network connections were based on de facto standards.
- In early Internet deployments, security was treated as a low priority.
- In 1993, DEFCON conference was established for those interested in information security.

2000 to Present

- The Internet brings millions of unsecured computer networks into continuous communication with each other.
- The ability to secure a computer's data was influenced by the security of every computer to which it is connected.
- Growing threat of cyber attacks has increased the awareness of need for improved security.
  - Nation-states engaging in information warfare

What Is Security?

- “A state of being secure and free from danger or harm; the actions taken to make someone or something secure.”
- A successful organization should have multiple layers of security in place to protect:
  - Operations
  - Physical infrastructure
  - People
  - Functions
  - Communications
  - Information

What is Security? (cont'd)

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Includes information security management, data security, and network security
- C.I.A. triangle
  - Is a standard based on confidentiality, integrity, and availability, now viewed as inadequate.
  - Expanded model consists of a list of critical characteristics of information.

nformation security

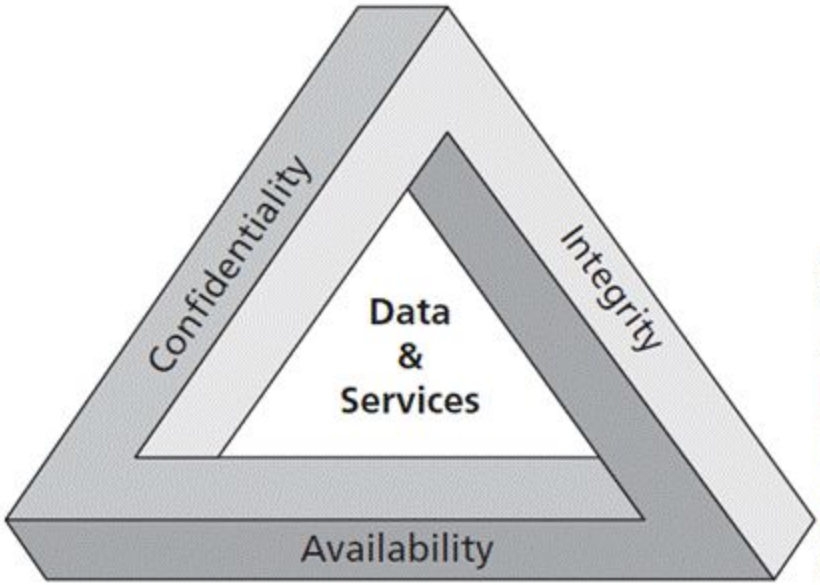


Figure 1-6 The C.I.A. triangle

Key Information Security Concepts

- A computer can be the subject of an attack and/or the object of an attack.
  - When the subject of an attack, the computer is used as an active tool to conduct attack.
  - When the object of an attack, the computer is the entity being attacked.

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

Components of an Information System

- Information system (IS) is the entire set of people, procedures, and technology that enable business to use information.
  - Software
  - Hardware
  - Data
  - People
  - Procedures
  - Networks

Balancing Information Security and Access

- Impossible to obtain perfect information security—it is a process, not a goal.
- Security should be considered a balance between protection and availability.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort: Systems administrators attempt to improve security of their systems.
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful type of top-down approach also involves a formal development strategy referred to as systems development life cycle.

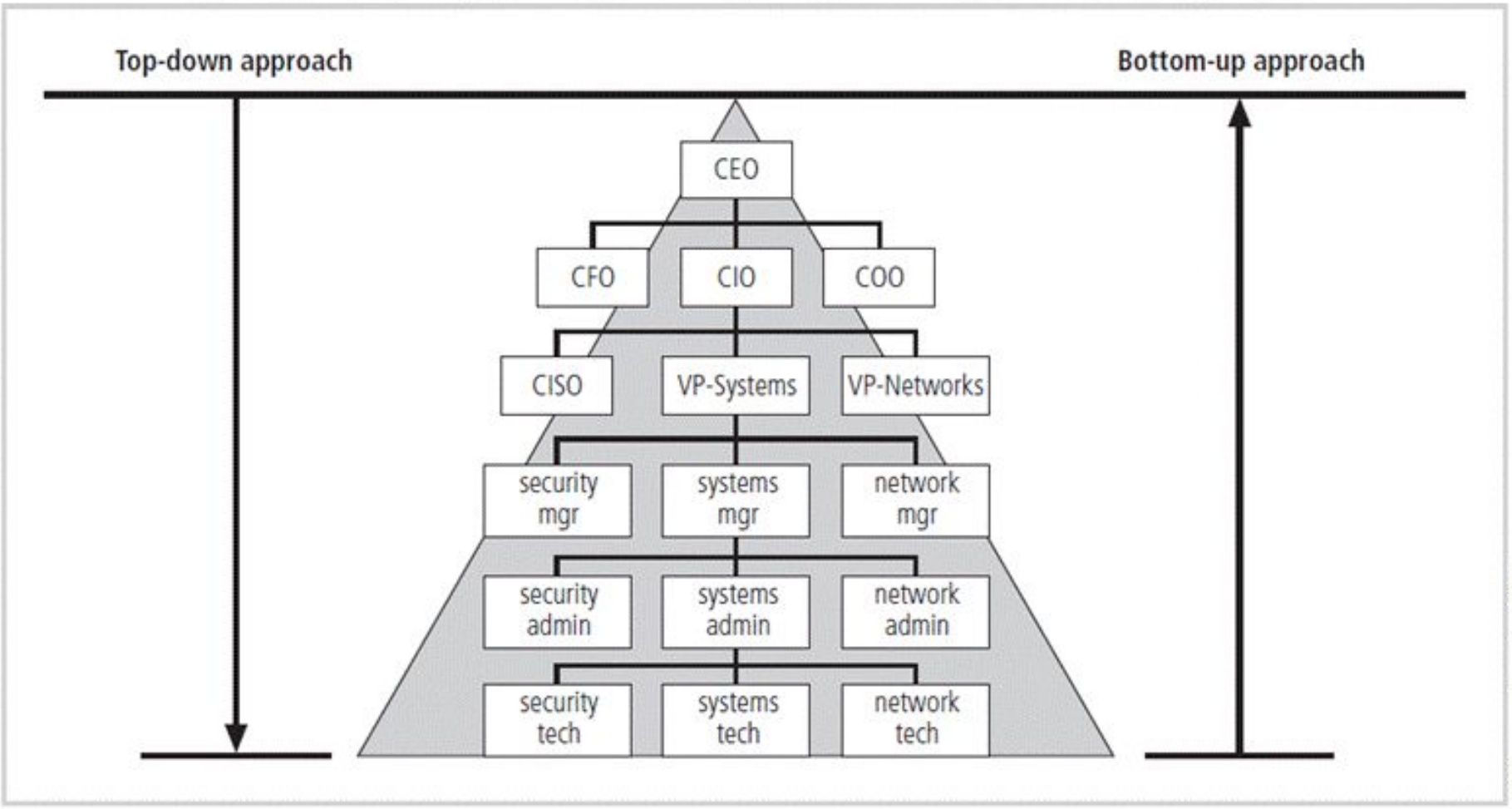


Figure 1-12 Approaches to information security implementation

Security Professionals and the Organization

- Wide range of professionals are required to support a diverse information security program.
- Senior management is the key component.
- Additional administrative support and technical expertise are required to implement details of IS program.

Senior Management

- Chief information officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising the senior executives on strategic planning
- Chief information security officer (CISO)
  - Has primary responsibility for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

Information Security Project Team

- A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodian: responsible for information and systems that process, transmit, and store it
- Data users: individuals with an information security role

Communities of Interest

- Group of individuals united by similar interests/values within an organization
  - Information security management and professionals
  - Information technology management and professionals
  - Organizational management and professionals

Information Security: Is It an Art or a Science?

- Implementation of information security is often described as a combination of art and science.
- “Security artisan” idea: based on the way individuals perceive system technologists and their abilities

Security as Art

- No hard and fast rules nor many universally accepted complete solutions
- No manual for implementing security through entire system

Security as Science

- Dealing with technology designed for rigorous performance levels
- Specific conditions cause virtually all actions in computer systems.
- Almost every fault, security hole, and systems malfunction is a result of interaction of specific hardware and software.
- If developers had sufficient time, they could resolve and eliminate faults.

Security as a Social Science

- Social science examines the behavior of individuals interacting with systems.
- Security begins and ends with the people that interact with the system, intentionally or otherwise.
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles.

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Computer security began immediately after the first mainframes were developed.
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.

Summary (cont'd)

- Security should be considered a balance between protection and availability.
- Information security must be managed similar to any major system implemented in an organization. Implementation of information security is often described as a combination of art and science.

Thanks

- Question Please