Homework1

潘亦晟

515021910384

1 Problem One

1. 可控性(Control lability) 对信息的传播及内容具有控制能力。
2. 不可抵赖性 (Non -repudiation),信息的发送者无法否认已经出或部 信息的发送者无法否认已经出或部 信息的发送者无法否认已经出或部 分内容，信息的接收者无法否认已经或 分内容，信息的接收者无法否认已经或 分内容，信息的接收者无法否认已经或 信, 实现方式：数字签名和可信第三方认证
3. 可存活性 (Survivability)
4. 可认证性 (Authenticity) 保证信息使用者和服务都是真实声称，防止冒充和重演的攻击。实现方式：账号密码验证。
5. 可审查性 (Auditability) 在可认证性之上，还包含对传输、消息源的真实进行核实。

2 Problem Two

safety是防止事故（可能或不涉及人类代理人的事故，但在任何情况下都不是故意的）。

security 是人的恶意活动的预防（抢劫、入室盗窃、抢劫、恐怖活动等）。

在计算机安全研究中，我们面对的威胁主要是欺诈和偷窃，恶意黑客，外国间谍，工业间谍等人为恶意破坏计算机系统安全的行为，符合security中恶意的特征；如果在计算机安全研究中讨论safety，更多的可能是应对诸如由自然灾害造成的网络中断，硬件损坏等意外

3 Problem Three

The first section of the handbook contains background and overview material, briefly discusses of threats, and explains the roles and responsibilities of individuals and organizations involved in computer security. It explains the executive principles of computer security that are used throughout the handbook.

computer security is based on eight major elements:

- Computer security should support the mission of the organization.
- Computer security is an integral element of sound management.
- Computer security should be cost-effective.
- Computer security responsibilities and accountability should be made explicit.
- System owners have computer security responsibilities outside their own organizations.
- Computer security requires a comprehensive and integrated approach.
- Computer security should be periodically reassessed.

- Computer security is constrained by societal factors.

We also clear that the responsibilities are from (1)senior management (2)program/functional managers/application owners (3)computer security management (4)technology providers (5)supporting organizations (6)users

We also discuss nine common threats: (1)Errors and Omissions (2)Fraud and Theft (3)Employee Sabotage (4)Loss of Physical and Infrastructure Support(5)Malicious Hackers (6)Industrial Espionage (7)Malicious Code (8)Foreign Government Espionage (9)Threats to Personal Privacy

The next three major sections deal with security controls: Management Controls(II), Operational Controls (III), and Technical Controls (IV). Most controls cross the boundaries between management, operational, and technical. Each chapter in the three sections provides a basic explanation of the control; approaches to implementing the control, some cost considerations in selecting, implementing, and using the control; and selected interdependencies that may exist with other controls. Each chapter in this portion of the handbook also provides references that may be used in actual implementation.

- The Management Controls section addresses security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

  This part first introduces Computer Security Program Management and Computer Security Risk Management. Then explains the relationship among security and planning and how they fit together. Finally it discuss computer security assurance.

- The Operational Controls section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise - and often rely upon management activities as well as technical controls

  The important security considerations within some of the major categories of support and operations are: (1)user support,(2)software support, (3)configuration management, (4)backups, (5)media controls, (6)documentation, and (7)maintenance.

  We also discusses seven major areas of physical and environmental security controls: (1）physical access controls, (2)fire safety, (3)supporting utilities, (4)structural collapse, (5)plumbing leaks, (6)interception of data, and (7)mobile and portable systems.

- The Technical Controls section focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations - and should be consistent with the management of security within the organization.

  We mainly discuss four aspects of technical controls : (1) identification and authentication (I&A), which prevents unauthorized people (or unauthorized processes) from entering a computer system. (2) logical access controls, which prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. (3) audit, which maintain a record of system activity both by system and application processes and by user activity of systems and applications. (4) cryptography ,which provides an important tool for protecting information and is used in many aspects of computer security.

Finally, an example is presented to aid the reader in correlating some of the major topics discussed in the handbook. It describes a hypothetical system and discusses some of the controls that have been implemented to protect it. This section helps the reader better understand the decisions that must be made in securing a system, and illustrates the interrelationships among controls.